SPACE-TIME CODE DESIGNS WITH NON-VANISHING DETERMINANTS FOR THREE, FOUR AND SIX TRANSMITTER ANTENNAS

Genyuan Wang† *Jian-Kang Zhang*‡ *Yimin Zhang*† *and Kon Max Wong*‡

†Center for Advanced Communications,
Villanova University, Villanova, PA 19085, USA
‡Department of Electrical and Computer Engineering,
McMaster University, Hamilton, Ontario Canada L8S 4K1

ABSTRACT

The design of a linear space-time code with full rate, large diversity product, and non-vanishing minimum determinant of codewords continues to attract great attention. However, in most available no-vanishing determinant space-time codes for three, four, and six transmitter antennas, the average power at each layer is different, which results in a high peak to average power ratio. In this paper, a new cyclic algebraic space-time design scheme is proposed and the optimal codes in this class are provided by using some specific cyclic field extensions. Our proposed codes not only include the available non-vanishing determinant cyclotomic space-time codes for three, four, and six transmitter antennas, but also have the desirable property that the optimal codes can be achieved with the same average power at each layer.

1. INTRODUCTION

Linear space-time block code designs based on algebraic field extensions have recently attracted great attention, see for example [1]- [9], due to the possibility of systematic constructions of full diversity and high data rate codes. Diagonal algebraic space-time block codes were first proposed in [3], where an n-dimensional diagonal space-time code $\mathrm{diag}([y_1, y_2, \cdots, y_n])$ was generated by $[y_1, \cdots, y_n]^T = G[x_1, \cdots, x_n]^T$, with matrix G and transmitted symbols $x_1, x_2, \cdots, x_n$ being properly chosen based on algebraic extension theory to achieve full diversity. The idea behind the diagonal algebraic space-time code can be tracked back to [1, 2], where the full diversity multi-dimensional signal constellation designs in both Rayleigh fading and additive Gaussian noise channel were considered. However, the symbol rate for the above diagonal space-time code design is one per channel use. In [6], a full diversity space-time code for two transmitter antennas was proposed, where the symbol rate reached two per channel use. By employing algebraic number theory and threaded/multi-layer codes [7], more general full diversity and high symbol rate space-time code designs were proposed in [4, 6–8]. Meanwhile, another type of full diversity and high rate space-time code was also presented [5] based on cyclic field extensions and division algebras. In the early studies of this topic, the structure of code designs with high (full) rate and full diversity received more attention than the high diversity product. In most existing codes, the minimum determinant of non-zero codewords, which is the minimum determinant of any two different codewords, vanishes as the symbol constellation size increases. Other space-time codes with a full symbol rate and high diversity product have been recently generated in [11–14]. These codes not only have high diversity products, but also have the non-vanishing determinant property; i.e., the minimum determinant does not decrease as the symbol constellation size increases. Although the codes in [11, 13] for two transmitter antennas have the same average powers at different layers, the cyclotomic space-time codes in [14] and [12] for three, four and six transmitter antennas have different average powers at different layers; i.e., a higher peak to average power ratio.

In this paper, we propose a more general full diversity and full rate linear space-time code design with the non-vanishing determinant based on some specific cyclic field extensions, which is called a cyclic algebraic space-time code design. This class of cyclic algebraic space-time codes includes all the cyclotomic space-time codes developed in [12] and [14] for three, four, and six transmitter antennas. In addition, the optimal cyclic algebraic space-time codes with the largest diversity products were constructed with the same average power at each layer. [1]

The following notations are used throughout this paper: capital English letters, such as X and G: space-time codeword or matrix; L_t: number of transmitter antennas; $\mathbb{N}$: natural numbers; $\mathbb{Z}$: ring of integers; $\mathbb{Q}$: field of rational numbers; $\mathbb{C}$: field of complex numbers; $\phi(n)$: Euler function of positive integer n; $\zeta_m = \exp\left(j\frac{2\pi}{m}\right)$; $\mathbb{K}, \mathbb{F}$: general fields; $\mathbb{F}(\beta)$: field generated by β based on field $\mathbb{F}$; $(\mathbb{K}/\mathbb{F}, \beta, \sigma)$: cyclic field extension $\mathbb{K}/\mathbb{F}$ with $\mathbb{K} = \mathbb{F}(\beta)$, and σ of the generator of cyclic Galois group $Gal(\mathbb{K}/\mathbb{L})$; $X(\mathbb{K}/\mathbb{F}, \beta, \sigma, \rho)$: space-time code generated with cyclic field extension $(\mathbb{K}/\mathbb{F}, \beta, \sigma)$, $1, \rho, \cdots, \rho^{n-1}$ are the numbers used for adjusting at different layers of the code.

2. MOTIVATION AND PROBLEM DESCRIPTION

Before providing the cyclic algebraic space-time code design, we first review cyclotomic space-time designs, based on which most of full rate non-vanishing determinant linear space-time codes are developed.

†The work of G. Wang, Y. Zhang is supported in part by the ONR under Grant No. N00014-04-1-0617 and NSF under Grant No. EEC-0203459.

[1]At the time of the submission of this paper, the authors learned that G. Rekaya, J. C. Belfiore and E. Viterbo recently also developed a non-vanishing determinant space-time code design for three, four and six transmitter antennas with the same average power at different layers [15].

2.1. Full Rate Cyclotomic Space-Time Codes Designs

In this subsection, we recall cyclotomic lattices, cyclotomic space-time codes and some of their fundamental properties in [1, 2, 9]. For two positive integers m and n, let $N = mn$ and $L_t = \frac{\phi(N)}{\phi(m)}$. The variable L_t corresponds to the number of transmitter antennas in a space-time code. There are totally 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 co-prime for any $1 \leq i \leq L_t$, (see for example p. 75 of [18]). With these L_t integers and $N = mn$, we define an $L_t \times L_t$ matrix $G_{m,n} = (\zeta_N^{(1+l_i m)\ell})_{0\leq i \leq t, 1 \leq \ell \leq L_t}$. It can be verified that $G_{m,n}$ is unitary when $n = L_t$. We now define cyclotomic lattices.

Definition 1 *An L_t dimensional cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$ is a set of L_t dimensional points $[y_1, \cdots, y_{L_t}]^T$ such that*

$$[y_1, \cdots, y_{L_t}]^T = G_{m,n}[x_1, \cdots, x_{L_t}]^T, \; x_l \in \mathbb{Z}[\zeta_m]. \tag{1}$$

Following the structure of threaded space-time codes [7], a general multi-layer cyclotomic space-time code is defined as follows.

Definition 2 *Let L_t be the number of transmitter antennas and $\Gamma_{L_t}(G_{m_l,n_l})$ be an L_t-dimensional cyclotomic lattice given in Definition 1. Let $\rho_1, \cdots, \rho_{L_t}$ be L_t fixed complex numbers. Then, a multi-layer cyclotomic space-time code is defined as*

$$\begin{bmatrix} \rho_1 y_1(1) & \rho_2 y_2(1) & \cdots & \rho_{L_t-1} y_{L_t-1}(1) & \rho_{L_t} y_{L_t}(1) \\ \rho_{L_t} y_{L_t}(2) & \rho_1 y_1(2) & \cdots & \rho_{L_t-2} y_{L_t-2}(2) & \rho_{L_t-1} y_{L_t-1}(2) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \rho_2 y_2(L_t) & \rho_3 y_3(L_t) & \cdots & \rho_{L_t} y_{L_t}(L_t) & \rho_1 y_1(L_t) \end{bmatrix} \tag{2}$$

where $[y_l(1), \cdots, y_l(L_t)]^T$ is a point in cyclotomic lattice $\Gamma_{L_t}(G_{m_l,n_l})$ with $y_{l_1}(l_2) = \sigma_{l_2}(x_{l_1}), l \leq l_1, l_2 \leq L_t$ and σ_l are the L_t embeddings of $\mathbb{Q}(\zeta_{mn})$ to $\mathbb{C}$ that is fixed on $\mathbb{Q}(\zeta_m)$ for $l = 1, \cdots, L_t$. This multi-layer cyclotomic space-time code is denoted by $X(\rho_1 G_{m_1,n_1}, \cdots, \rho_{L_t} G_{m_{L_t},n_{L_t}})$. An L-layer ($1 \leq L \leq L_t$) cyclotomic space-time code is defined as a multi-layer cyclotomic space-time code $X(\rho_1 G_{m_1,n_1}, \cdots, \rho_{L_t} G_{m_{L_t},n_{L_t}})$ when $\rho_l = 0$ for $l > L$ and is denoted by $X(\rho_1 G_{m_1,n_1}, \cdots, \rho_L G_{m_L,n_L})$.

2.2. Problem in the Cyclotomic Space-Time Code Designs

The key to designing a full rate cyclotomic space-time code is to find a proper cyclotomic field extension $\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_m)$ in (2) for given L_t and $\rho_l, l = 1, \cdots, L_t$, such that the resulting code achieves full diversity and a large diversity product. From the early studies, we know that there are infinite ways of determining the values of m, n, and ρ_l to generate full diversity full rate space-time codes. However, most of these codes do not have a large diversity product and the minimum determinant of codewords decreases to zero very rapidly as the constellation size of the codewords increases. Recently, the generation of large diversity product space-time codes with a non-vanishing determinant has received much attention. The vital point to design this type of codes is to find a proper field extension $\mathbb{K}/\mathbb{F}$ and $\rho_l, l = 1, \cdots, L_t$, such that the determinant of each codeword belongs to the same lattice. The codewords provided in [11–14] have the property that $\mathbb{F} = \mathbb{Q}(\zeta_4)$ or $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$, $\rho_l \in \mathbb{Z}[\zeta_4]$ or $\mathbb{Z}[\zeta_3] = \mathbb{Z}[\zeta_6]$, and the determinant of each codeword belongs to $\mathbb{Z}[\zeta_m]$. However, in the code design of [12] and [14], $\rho_l = \rho^l, l = 1, \cdots, L_t$, with $|\rho| > 1$. Therefore, $|\rho_l|$ takes different values for different l; i.e., the average powers of the codewords at different layers are different. This results in a high peak to average power ratio. A close examination of the code design in [12, 14] reveals that the field extension $\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_m)$ based on minimal polynomial $x^n - \zeta_m$, $m = 3, 4$, or 6, and ρ_l may not be a good choice. In this paper, we develop a code design using a more general field extension $\mathbb{K}/\mathbb{Q}(\zeta_m)$ with the minimal polynomial $x^n - \alpha$ for $\alpha \in \mathbb{Z}[\zeta_m]$ and ρ_l. The resulting new space-time codes have non-vanishing determinants with the same average power at each layer; i.e., $|\rho_l| = 1$, for 3, 4 and 6 transmitter antennas.

3. FULL RATE CYCLIC ALGEBRAIC SPACE-TIME CODES FOR 3, 4, AND 6 TRANSMITTER ANTENNAS

The existing cyclotomic code designs are obtained based on the cyclic field extension $(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n), \zeta_{mn})$ with the minimal polynomial $x^n - \zeta_m$, $m = 6$ or $m = 3$. In this section, we generalize the cyclic field extension to $(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n), \beta)$ with a minimal polynomial $x^n - \alpha$, and $\beta^n = \alpha \in \mathbb{Z}[\zeta_m]$. We find optimal full rate space-time codes for three, four, and six transmitter antennas in this class. The results show that optimal full rate space-time codes can be achieved with $|\rho| = 1$, which means that the average powers at different layers of the codewords are identical; i.e., a lower peak to average power ratio than that achieved by the cyclotomic space-time codes. Before providing the optimal codes, we introduce some concepts and results.

Definition 3 *[18] A Galois extension $\mathbb{K}/\mathbb{F}$ is called cyclic if the Galois group $Gal(\mathbb{K}/\mathbb{F})$ is a cyclic group.*

By the cyclic extension theory we have the following proposition.

Proposition 1 *[18] Let $\mathbb{F}$ be a field containing a primitive nth root of unity, and let $\mathbb{K} = \mathbb{F}(\sqrt[n]{\alpha})$ for some $\alpha \in \mathbb{F}$. Then $\mathbb{K}/\mathbb{F}$ is a cyclic Galois extension. Moreover, $m = [\mathbb{K} : \mathbb{F}]$ is equal to the order of the coset $\alpha\mathbb{F}^{*n}$ in the group $\mathbb{F}^*/\mathbb{F}^{*n}$, and $\min(\mathbb{F}, \sqrt[n]{\alpha}) = x^m - d$ for some $d \in \mathbb{F}$.*

From Proposition 1, we know that for a field $\mathbb{F}$ containing a primitive nth root of unity and its extension $\mathbb{F}[\sqrt[n]{\alpha}]$ with a minimal polynomial $x^n - \alpha$ over $\mathbb{F}$, $\mathbb{K}/\mathbb{F}$ is a cyclic Galois extension of dimension n. Therefore, there are a number of n embeddings $\sigma_l = \sigma^l$ of $\mathbb{K}$ to $\mathbb{C}$ such that $\sigma(x) = x$ for $x \in \mathbb{F}$ and $\sigma(\sqrt[n]{\alpha}) = \omega \sqrt[n]{\alpha} = \zeta_n \sqrt[n]{\alpha}$.

Definition 4 *An n-dimensional cyclic algebraic space-time code $X(\mathbb{K}/\mathbb{F}, \beta, \sigma, \rho)$ based on a cyclic field extension $\mathbb{K}/\mathbb{F}$ with $\beta = \sqrt[n]{\alpha}$ is a set of $n \times n$ matrices with the form of*

$$X = \begin{bmatrix} x_1 & \rho x_2 & \cdots & \rho^{n-2} x_{n-1} & \rho^{n-1} x_n \\ \rho^{n-1}\sigma(x_n) & \sigma(x_1) & \cdots & \rho^{n-3}\sigma(x_{n-2}) & \rho^{n-2}\sigma(x_{n-1}) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \rho\sigma^{n-1}(x_2) & \rho^2\sigma^{n-1}(x_3) & \cdots & \rho^{n-1}\sigma^{n-1}(x_n) & \sigma^{n-1}(x_1) \end{bmatrix} \tag{3}$$

where $x_l, l = 1, \cdots, n$, are determined by $x_l = \sum_{k=1}^{n} x_{k,l}\beta^{k-1}$ with $x_{k,l}$ being algebraic integers in $\mathbb{F}$. While ρ in (3) can be any complex number, in this paper, it is chosen from algebraic integers in field $\mathbb{F}$.

Similar to (2), the cyclic algebraic space-time code defined in (3) can be rewritten as points of a complex lattice $[y_l(1), \cdots, y_l(n)]^T$

with $y_l(k) = \sigma^{l-1}(x_k)$ is a point in complex lattice $\Gamma_n(G_{n,\beta})$ with a generating matrix $G_{n,\beta}$ over $\mathbb{Z}[\zeta_n]$ for $l = 1, \cdots, n$,

$$G_{n,\beta} \triangleq (\zeta_n^{i\ell})_{0\le i\le(n-1),1\le\ell\le n}\mathrm{diag}(1, \beta, \cdots, \beta^{n-1}) \qquad (4)$$

Therefore, $[y_1(1), y_1(2), \cdots, y_1(n), \rho y_2(1), \rho y_2(2), \cdots, \rho y_2(n), \cdots, \rho^{n-1}y_n(1), \rho^{n-1}y_n(2), \cdots, \rho^{n-1}y_n(n)]$ can be considered as a point of larger complex lattice $\Gamma_{nn}(G_{n,\beta}, \rho G_{n,\beta}, \cdots, \rho^{n-1}G_{n,\beta})$, with a generating matrix $\mathcal{G}(G_{n,\beta}, \rho G_{n,\beta}, \cdots, \rho^{n-1}G_{n,\beta})$ over $\underbrace{\mathbb{Z}[\zeta_n] \times \mathbb{Z}[\zeta_n] \times \cdots \mathbb{Z}[\zeta_n]}_{n}$,

$$\mathcal{G}(G_{n,\beta}, \rho G_{n,\beta}, \cdots, \rho^{n-1}G_{n,\beta}) = \mathrm{diag}(G_{n,\beta}, \rho G_{n,\beta}, \rho^{n-1}G_{n,\beta})$$

The absolute value of the determinant $|\det(\mathcal{G}(G_{n,\beta}, \rho G_{n,\beta}, \cdots, \rho^{n-1}G_{n,\beta}))|$ of the generating matrix $\mathcal{G}(G_{n,\beta}, \rho G_{n,\beta}, \cdots, \rho^{n-1}G_{n,\beta})$ is

$$|\det(\mathcal{G}(G_{n,\beta}, \rho G_{n,\beta}, \cdots, \rho^{n-1}G_{n,\beta}))| = |\det(G_n)|^n (\rho\beta)^{n^2(n-1)/2}.$$

As a result, for a given integer n, we can compare two n-dimensional cyclic algebraic space-time codes $X(\mathbb{K}_1/\mathbb{F}_1, \beta_1, \sigma_1, \rho_1)$ and $X(\mathbb{K}_2/\mathbb{F}_2, \beta_2, \sigma_2, \rho_2)$ with the following criterion by using the results developed in [14].

Lemma 1 *For any two n-dimensional cyclic algebraic space-time codes $X(\mathbb{K}_1/\mathbb{F}_1, \beta_1, \sigma_1, \rho_1)$ and $X(\mathbb{K}_2/\mathbb{F}_2, \beta_2, \sigma_2, \rho_2)$, the former is better than the latter if $d_{min}(\mathbb{K}_2/\mathbb{F}_2, \beta_2, \sigma_2, \rho_2) = d_{min}(\mathbb{K}_1/\mathbb{F}_1, \beta_1, \sigma_1, \rho_1)$ and $|\beta_1\rho_1| \le |\beta_2\rho_2|$, where*

$$d_{min}(\mathbb{K}/\mathbb{F}, \beta, \sigma, \rho) = \min_{X\neq 0, X\in X(\mathbb{K}/\mathbb{F},\beta,\sigma,\rho)} |\det(X)| \qquad (5)$$

is called the minimal determinant of code $X(\mathbb{K}/\mathbb{F}, \beta, \sigma, \rho)$.

In a special case where $\mathbb{F} = \mathbb{Q}(\zeta_n)$ and $\alpha = \zeta_n$, the cyclotomic space-time code is a cyclic algebraic space-time code. For all the cyclotomic space-time codes with non-vanishing determinants, $\mathbb{F} = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$, or $\mathbb{F} = \mathbb{Q}(\zeta_4)$. In this paper, we only consider the special case where $\mathbb{F} = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$, or $\mathbb{F} = \mathbb{Q}(\zeta_4)$. In the following, we will design optimal cyclic algebraic space-time codes for three, four, and six transmitter antennas over $\mathbb{F} = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$ or $\mathbb{F} = \mathbb{Q}(\zeta_4)$ under the diversity product criterion.

Definition 5 *[12] Let $\mathbb{K}$ be a field and $\mathbb{F}$ a cyclic extension of degree d of $\mathbb{F}$, σ be the generator of Galois cyclic Galois group $Gal(\mathbb{K}/\mathbb{F})$. Take $\gamma \in \mathbb{F}^*$. The algebra $A = (\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ generated by $\mathbb{K}$ and an element e is called a cyclic algebra, where $e^d = \gamma$, and $e{\centerdot}\bar{x} = \bar{x}{\centerdot}\sigma(e)$, for any $\bar{x} \in K$. This algebra $A = (\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ can be written as $A = (\mathbb{K}/\mathbb{F}, \sigma, \gamma) \doteq \mathbb{K} \oplus e{\centerdot}\mathbb{K} \oplus \cdots \oplus e^{d-1}{\centerdot}\mathbb{K}$. This algebra can be constructed as a subalgebra of $M_d(\mathbb{K})$, the d-dimensional matrix algebra over $\mathbb{K}$ for $l = 0, \cdots, d-1$ by setting*

$$e = \begin{pmatrix} 0_{(d-1)\times 1} & I \\ \gamma & 0_{1\times(d-1)} \end{pmatrix} \quad \bar{x} = diag(\sigma^l(x)) \qquad (6)$$

From the definitions of cyclic algebra and cyclic algebraic space-time codes, we know that an n-dimensional cyclic algebraic space-time code $X(\mathbb{K}/\mathbb{F}, \beta, \sigma, \rho)$ is a degree n cyclic algebra $(\mathbb{K}/\mathbb{F}, \sigma, \rho^n)$. In the design and proof of the optimality of a cyclic algebraic space-time code, we need the following lemma.

Lemma 2 *[12], [17] A cyclic algebra in Definition 5 is a division algebra if and only if $\gamma, \gamma^2, \cdots, \gamma^{d-1}$ are not algebraic norms of elements in $\mathbb{K}(\gamma, \gamma^2, \cdots, \gamma^{d-1})$.*

3.1. Optimal Cyclic Algebraic Space-time Code for Three Transmitter Antennas

In this subsection, we assume that $\mathbb{F} = \mathbb{Q}(\zeta_3)$ and $\mathbb{K} = \mathbb{F}(\beta)$ is a cyclic field extension of degree 3 for some β with $\beta^3 = \alpha \in \mathbb{Z}[\zeta_3]$. Now let us consider field extension towers $\mathbb{Q} \subset \mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\zeta_3, \beta)$. Then, any $z \in \mathbb{Z}[\zeta_3, \beta]$ can be written as $z = z_1 + z_2\beta + z_3\beta^2 \in \mathbb{Q}(\zeta_3, \beta) = \mathbb{F}(\beta)$, where $z_k \in \mathbb{Z}[\zeta_3], k = 1, 2, 3$. Notice that $\mathbb{N}_{\mathbb{Q}(\zeta_3,\beta)/\mathbb{Q}(\zeta_3)}(z) = \prod_{k=1}^3 \sigma_k(z)$, where $\sigma_k, k = 1, 2, 3$, are the three embeddings of $\mathbb{Q}(\zeta_3, \beta)$ to $\mathbb{C}$ that is fixed over $\mathbb{Q}(\zeta_3)$ with $\sigma_k(\beta) = \zeta_3^{k-1}\beta$. Hence, from the definition of the relative algebraic norm we have

$$\mathbb{N}_{\mathbb{Q}(\zeta_{\zeta_3},\beta)/\mathbb{Q}(\zeta_3)}(z) = z_1^3 + \beta^3 z_2^3 + \beta^6 z_3^3 - 3\beta^3 z_1 z_2 z_3. \qquad (7)$$

If we let $\beta = 2^{1/3}$, then we know from the algebraic number theory that $\mathbb{Q}(\zeta_3, 2^{1/3})/\mathbb{Q}(\zeta_3)$ is a cyclic field extension of degree 3. In the following we prove that ζ_3 and ζ_6 are not the algebraic norm of some integer of $\mathbb{Q}(\zeta_3, 2^{1/3})$ over $\mathbb{Q}(\zeta_3)$.

Theorem 1 *[16] For any $x, y \in \mathbb{Z}[\zeta_3, 2^{1/3}]$, if $\mathbb{N}_{\mathbb{Q}(\zeta_3,2^{1/3})/\mathbb{Q}(\zeta_3)}(x) = \zeta_6\mathbb{N}_{\mathbb{Q}(\zeta_3,2^{1/3})/\mathbb{Q}(\zeta_3)}(y)$, $\mathbb{N}_{\mathbb{Q}(\zeta_3,2^{1/3})/\mathbb{Q}(\zeta_3)}(x) = \zeta_3\mathbb{N}_{\mathbb{Q}(\zeta_3,2^{1/3})/\mathbb{Q}(\zeta_3)}(y)$, or $\mathbb{N}_{\mathbb{Q}(\zeta_3,2^{1/3})/\mathbb{Q}(\zeta_3)}(x) = \zeta_3^2\mathbb{N}_{\mathbb{Q}(\zeta_3,2^{1/3})/\mathbb{Q}(\zeta_3)}(y)$ then, $x = y = 0$.*

The proofs of all theorems in this paper are provided in [16]. Similarly, we can prove that number 2 is not the algebraic norm of some integer of $\mathbb{Q}(\zeta_3, \zeta_6) = \mathbb{Q}(\zeta_{18})$ over $\mathbb{Q}(\zeta_3)$.

Theorem 2 *[16] For any $x, y \in \mathbb{Z}[\zeta_{18}], (x, y \in \mathbb{Z}[\zeta_9])$, if $\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(x) = 2\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(y)$ $(\mathbb{N}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3)}(x) = 2\mathbb{N}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3)}(y))$, then, $x = y = 0$.*

For any cyclic algebraic space-time codeword $X \in X(\mathbb{Q}(\zeta_3, \beta)/\mathbb{Q}(\zeta_3), \beta, \sigma, \rho)$ with the following form

$$X = \begin{bmatrix} x & \rho y & \rho^2 z \\ \rho^2\sigma(z) & \sigma(x) & \rho\sigma(y) \\ \rho\sigma^2(y) & \rho^2\sigma^2(z) & \sigma^2(x) \end{bmatrix}, \qquad (8)$$

where $x = \sum_{l=1}^3 x_l\beta^{l-1}$, $y = \sum_{l=1}^3 y_l\beta^{l-1}$, $z = \sum_{l=1}^3 z_l\beta^{l-1}$, with $x_l, y_l, z_l \in \mathbb{Z}[\zeta_3], \beta^3 \in \mathbb{Z}[\zeta_3], \rho^3 \in \mathbb{Z}[\zeta_3]$, we can prove that its determinant belongs to $\mathbb{Z}[\zeta_3]$; i.e.,

Theorem 3 *[16] The determinant $\det(X)$ of matrix X with the form of (8) belongs to $\mathbb{Z}[\zeta_3]$, i.e., $\det(X) \in \mathbb{Z}[\zeta_3]$.*

Furthermore, we can prove the following result.

Theorem 4 *[16] Under the diversity product criterion, space-time codes $X(\mathbb{Q}(\zeta_3, 2^{1/3})/\mathbb{Q}(\zeta_3), 2^{1/3}, \sigma, \zeta_9)$, $X(\mathbb{Q}(\zeta_3, 2^{1/3})/\mathbb{Q}(\zeta_3), 2^{1/3}, \sigma, \zeta_{18})$, $X(\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3), \zeta_9, \sigma, 2^{1/3})$, $X(\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6), \zeta_{18}, \sigma, 2^{1/3})$ are the optimal full rate cyclic space-time codes for three transmitter antennas with the minimal determinant 1.*

Remarks: The cyclic algebraic code $X(\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3), \zeta_9, \sigma, 2^{1/3})$ is a cyclotomic space-time code, but $X(\mathbb{Q}(\zeta_3, 2^{1/3})/\mathbb{Q}(\zeta_3), 2^{1/3}, \sigma, \zeta_9)$ is not. Although they have the same diversity product, i.e., the same performance under the diversity product criterion, the former with $\rho = 2^{1/3} > 1$ has different average power at each layer and the latter with $|\rho| = |\zeta_9| = 1$ has the same average power at each layer. Therefore, the latter has a lower peak to average power ratio.

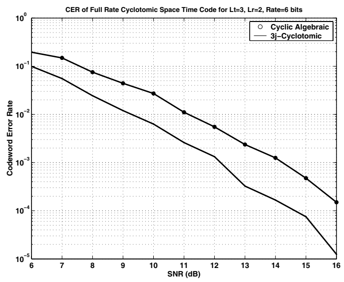

Fig. 1. Codeword error probability of cyclic algebraic space-time code and cyclotomic space-time with three transmitter and two receiver antennas

3.2. Cyclic Algebraic Space-Time Code for 4 and 6 Transmitter Antennas

Similar to Theorem 4 for the three transmit antenna case, we have the following non-vanishing determinant theorems for four and six transmitter antennas.

Theorem 5 *[16] $X(\mathbb{Q}(\zeta_4, \beta)/\mathbb{Q}(\zeta_4), (2+j)^{1/4}, \sigma, \zeta_{16})$ is an optimal cyclic algebraic space-time code for four transmitter antennas with full rate, full diversity non-vanishing determinant 1 and its average power at each layer is identical.*

Theorem 6 *[16] $X(\mathbb{Q}(\zeta_6, \beta)/\mathbb{Q}(\zeta_6), (2+\zeta_6)^{1/6}, \sigma, \zeta_{36})$ is an optimal cyclic algebraic space-time code for six transmitter antennas with full rate, full diversity, determinant non-vanishing and identical average power at each layer.*

4. SIMULATION RESULTS

In this section we consider a MIMO system with three transmitter antennas and two receive antennas. We compare the error performance of the space-time code $X(\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3), \zeta_9, \sigma, (3+\exp(j\pi/3))^{1/3})$ proposed in [12] with our proposed code $X(\mathbb{Q}(\zeta_3, 2^{1/3})/\mathbb{Q}(\zeta_3), 2^{1/3}, \sigma, \zeta_9)$. While both have non-vanishing determinants, the latter has a lower peak to average power ratio than the former, since $|\rho| = |(3+\exp(j\pi/3))^{1/3}| > 1$ in the former code. Whereas $|\rho| = |\zeta_9| = 1$ in the latter. Moreover, according to the diversity product criterion, the proposed code also has better codeword error performance. Our simulation results depicted in Fig.1 show that our new code achieves about 2dB gains over the one proposed in [12].

5. CONCLUSION

A systematic non-vanishing determinant space-time code design has been proposed using some cyclic field extensions. Based on the diversity product criterion, the optimal space-time codes for three, four and six transmitter antennas have been obtained. We have proved that these optimal codes have the same average power at each layer and, subsequently a low peak to average power ratio.

6. REFERENCES

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

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

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

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

[5] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high rate space-time block codes from division algebras," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2596-2616, Oct. 2003.

[6] M. O. Damen and N. C. Beaulieu, "On two high-rate algebraic space-time codes," *IEEE Trans. Inform. Theory,* vol. 49, pp. 1059-1063, April 2003.

[7] H. El Gamal and M. O. Damen, "Universal space-time coding," *IEEE Trans. Inform. Theory,* vol. 49, pp. 1097-1119, May 2003.

[8] X. Ma and G. B. Giannakis, "Full-diversity full rate complex-field space-time coding," *IEEE Trans. Signal Processing,* vol. 51, pp. 2917-2930, Nov. 2003.

[9] G. Wang, H. Liao, H. Wang, and X.-G. Xia, "Systematic and optimal cyclotomic space-time code designs based on high dimensional lattices," *Proc. Globecom'03*, San Francisco, Dec. 2003. Also, submitted to *IEEE Trans. Inform. Theory*, Feb. 2003.

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

[11] H. Yao and G. W. Wornell, "Achieveing the full MIMO diversity-multiplexing frontier with rotatio-based space-time codes," in *Proceedings Allerton Conf. Commun., Cont., and Computing,*(Illinois), Oct. 2003.

[12] J. C. Belfiore and G. Rekaya, "Quaternionic Lattices for space-time coding," in *Proceedings of ITW2003,* Paris, France, March 2003.

[13] J. C. Belfiore, G. Pekaya, and E. Viterbo, "The Golden Coden: A 2×2 full rate space-time code with non vanishing determinants," in *Proceedings of ISIT2004*, June 2004.

[14] G. Wang, and X-G. Xia, "On optimal multi-layer cyclotomic space-time code designs," in *Proceedings of ISIT2004*, June 2004.

[15] G. Rekaya, J. C. Belfiore and E. Viterbo " Algebraic 3×3, 4×4 and 6×6 Space-Time Codes with non-vanishing Determinants," *ISITA2004,* Parma, Italy, Oct. 2004

[16] G. Wang, J.-K. Zhang, Y. Zhang, M. Amin, and K. M. Wong, "Space-time code designes with non-vanishing determinants based on cyclic field extension families," *IEEE Trans. Inform. Theory*, submitted, 2004.

[17] A. A. Albert, *Structure of Algebras,* AMS Colloqium Pub. XXIV, 1961.

[18] P. Morandi, *Field and Galois Theory*, Springer-Verlag, New York, 1996.