Space-Time Block Code Designs Based on Quadratic Field Extension for Two-Transmitter Antennas

Genyuan Wang, Jian-Kang Zhang, *Senior Member, IEEE*, and Moeness Amin, *Fellow, IEEE*

***Abstract*—Space-time block code designs based on algebraic field extension for full rate, large diversity product, and nonvanishing minimum determinant of codewords have received great attention. There are many different types of codes available for two-transmitter antennas, such as cyclotomic space-time block codes, the golden space-time block code, and rotation-based space-time block codes. In this paper, a more general space-time block code design scheme, which is called quadratic space-time block coding, is proposed for the two-transmitter antennas using quadratic field extension. The optimal design of the quadratic space-time block codes in terms of a diversity product criterion is also presented. It is shown that the optimal quadratic space-time block codes designed in this paper do not belong to the existing space-time block code family such as the cyclotomic, golden, and rotation-based space-time block codes. The simulation results demonstrate that the average codeword error rate of the optimal quadratic space-time block code attains about 0.5 dB signal to noise ratio gain over those of the optimal cyclotomic and golden space-time block codes.**

***Index Terms*—Algebraic number theory, diversity product, full-rate, lattices, multilayer space-time block codes, quadratic field extensions.**

I. Introduction

LINEAR space-time block code designs based on algebraic field extensions have recently attracted great attention, see for example [1]–[12], due to the possibility of systematic constructions of full diversity and high data rate codes. In [6], a full diversity space-time block code for two transmitters was proposed, where the symbol rate reaches two per channel use. By employing algebraic number theory and the threaded/multilayer code structure [14], more general full diversity, high symbol rate space-time block code designs were proposed in [4], [6], [7], [10], and [11]. Within the same time frame, another type of full diversity, high rate space-time block code was developed in [9] based on cyclic field extension and division algebras. In the early studies of this topic, the structures of code designs with high (full) rate and full diversity received more attention than the high diversity product. In most of the codes provided in these studies, the minimal determinant of nonzero codewords, which is the minimal determinant of the difference between any two distinct codewords, vanishes as the symbol constellation size increases. Therefore, other space-time block codes with full symbol rate and high diversity product have been recently developed [17]–[20]. These codes not only have high diversity products, but also have nonvanishing determinant property, i.e., the minimum determinant does not decrease with the symbol constellation size increasing. In this paper, a new systematic space-time block code design, which is called a quadratic space-time block code design, with full diversity, full rate, and nonvanishing determinant for the two-transmitter antennas is proposed. The optimal codewords of the quadratic space-time block code are also obtained. The quadratic space-time block code design scheme is a generalization of those in [17]–[20]. It is shown that the optimal codewords with the improved diversity product are not included in the class of codes proposed in [17]–[20].

This paper is organized as follows. In Section II, the space-time block code design scheme based on quadratic field extension is proposed. In Section III, the optimal single-layer quadratic space-time block codes are presented. The optimal full-rate quadratic space-time block codes are discussed in Section IV. Simulation results are provided in Section V.

The following notations are used throughout this paper: capital English letters, such as X and G, represent space-time codeword or matrix. $\mathbb{N}$ denotes natural numbers; $\mathbb{Z}$ denotes a ring of integers; $\mathbb{Q}$ denotes a field of rational numbers; $\mathbb{C}$ denotes a field of complex numbers; $\zeta_m = \exp\left(i\frac{2\pi}{m}\right)$; $\mathbb{K}$ and $\mathbb{F}$ denote general fields; $\mathbb{F}(\beta)$ denotes a field generated by β and field $\mathbb{F}$. Notation $X(\mathbb{K}/\mathbb{F}, \beta_1, \beta_2, \rho)$ denotes a space-time block code generated with quadratic field extension $(\mathbb{K}/\mathbb{F}, \beta_1)$, where β_1 is one of the roots of some minimal quadratic polynomial over $\mathbb{F}$ and $\rho \in (\mathbb{K}/\mathbb{F}, \beta_1)$ with ρ^2 being an integer of field $\mathbb{F}$.

II. Quadratic Space-Time Block Code Designs

First, we give a scheme for the systematic design of a space-time block code using quadratic field extensions. Let $\mathbb{F}$ be a field. $x^2 + px + q$ is an irreducible polynomial over $\mathbb{F}$ with algebraic integers p and q. Polynomial $x^2 + px + q$ has two roots:

$$\alpha_1 = \frac{-p + \sqrt{p^2 - 4q}}{2} \notin \mathbb{F},\ \alpha_2 = \frac{-p - \sqrt{p^2 - 4q}}{2} \notin \mathbb{F}. \tag{1}$$

Let $\mathbb{K} = \mathbb{F}(\alpha_1)$ be the field generated by $\mathbb{F}$ and α_1. Then, the dimension of $\mathbb{K}$ over $\mathbb{F}$ is 2, i.e., $[\mathbb{K} : \mathbb{F}] = 2$. $\{1, \alpha_1\}$ is a basis of $\mathbb{K}$ over $\mathbb{F}$. $\mathbb{K}$ is called a quadratic extension of $\mathbb{F}$. Let

Manuscript received September 06, 2004; revised November 17, 2011; accepted November 22, 2011. Date of publication January 31, 2012; date of current version May 15, 2012. The work of J.-K. Zhang was supported in part by the Natural Sciences and Engineering Research Council of Canada Award.

G. Wang and M. Amin are with the Center for Advanced Communications, Villanova University, Villanova, PA 19085 USA (e-mail: genyuan.wang@villanova.edu; moeness.amin@villanova.edu).

J.-K. Zhang is with the Department of Electrical and Computer Engineering, McMaster University, Hamilton, ON L8S 4L8 Canada (e-mail: jkzhang@mail.ece.mcmaster.ca).

Communicated by E. Viterbo, Associate Editor for Coding Techniques.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2012.2184633

$\sigma_k, k = 1, 2$ be the two embeddings of $\mathbb{K}$ to $\mathbb{C}$ such that they are fixed on $\mathbb{F}$, i.e., $\sigma_k(y) = y$, for any $y \in \mathbb{F}$ and $\sigma_1(\alpha_1) = \alpha_1,\ \sigma_2(\alpha_1) = \alpha_2$. Now, we are ready to define a quadratic space-time block code.

Definition 1: A quadratic space-time block code $X(\mathbb{F}, \alpha_1, \alpha_2, \rho)$ based on an irreducible quadratic polynomial $x^2 + px + q$ over field $\mathbb{F}$ is a set of matrices X having the form of

$$X = \begin{bmatrix} y_1(1) & \rho y_2(1) \\ \rho y_2(2) & y_1(2) \end{bmatrix} \tag{2}$$

where

$$\begin{bmatrix} y_k(1) \\ y_k(2) \end{bmatrix} = \begin{bmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{bmatrix} \begin{bmatrix} x_k(1) \\ x_k(2) \end{bmatrix} \tag{3}$$

with $\rho^2,\ x_k(1),\ x_k(2),\ k = 1, 2$, being integers of $\mathbb{F}$ and α_1, α_2 being the two roots of polynomial $x^2 + px + q$ given in (1). Particularly, when $\rho = 0$, it is called a single-layer code, otherwise, it is called a two-layer or full-rate code. ■

From the definition of quadratic space-time block codes, it can be cast as a generalization of the 2×2 cyclotomic space-time block codes [10], [12], [18], [20], the golden space-time block code [19], and the rotation-based space-time block code [17]. In order to design a space-time block code with a large diversity product and nonvanishing determinant, we focus on a quadratic space-time block code design that either $\mathbb{F} = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$ or $\mathbb{F} = \mathbb{Q}(\zeta_4)$, and $\rho^2,\ x_k(1),\ x_k(2),\ k = 1, 2$ in (3) belong to either $\mathbb{Z}[\zeta_3] = \mathbb{Z}[\zeta_6]$ or $\mathbb{Z}[\zeta_4]$. Usually, $\mathbb{Z}[\zeta_4]$ is called a Gaussian integer ring, whereas $\mathbb{Z}[\zeta_3] = \mathbb{Z}[\zeta_6]$ is called an Eisenstein integer ring. Correspondingly, the quadratic space-time block code with $\mathbb{F} = \mathbb{Q}(\zeta_4)$ is called a Gaussian quadratic space-time block code, which is denoted by $X(\mathbb{Q}(\zeta_4), \alpha_1, \alpha_2, \rho)$, whereas the quadratic space-time block code with $\mathbb{F} = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$ is called an Eisenstein quadratic space-time block code, denoted by $X(\mathbb{Q}(\zeta_3), \alpha_1, \alpha_2, \rho)(X(\mathbb{Q}(\zeta_6), \alpha_1, \alpha_2, \rho))$. Definition 1 shows that a single-layer quadratic space-time block code is a lattice code over $\mathbb{Z}[\zeta_3]$ or $\mathbb{Z}[\zeta_4]$, with the generating matrix of the complex lattice being

$$G = \begin{bmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{bmatrix} \tag{4}$$

whereas a two-layer quadratic space-time block code is a lattice code over either $\mathbb{Z}[\zeta_3] \times \mathbb{Z}[\zeta_3]$ or $\mathbb{Z}[\zeta_4] \times \mathbb{Z}[\zeta_4]$, with the generating matrix of the complex lattice given by

$$G = \begin{bmatrix} 1 & \alpha_1 & 0 & 0 \\ 1 & \alpha_2 & 0 & 0 \\ 0 & 0 & \rho & \rho\alpha_1 \\ 0 & 0 & \rho & \rho\alpha_2 \end{bmatrix}. \tag{5}$$

Therefore, the absolute value $|\det(G)|$ of the generating matrix G is $|\det(G)| = |\rho|^{2(L-1)}|\alpha_1 - \alpha_2|^L = |\rho|^{2(L-1)}|\sqrt{p^2 - 4q}|^L$ for the $L (L = 1, 2)$ layer quadratic space-time block code. The following lemma [20] gives a diversity product criterion to compare two quadratic space-time block codes.

Lemma 1: Let $X(\mathbb{Q}(\zeta_{m_1}), \beta_1, \beta_2, \rho_1)$ and $X(\mathbb{Q}(\zeta_{m_2}), \gamma_1, \gamma_2, \rho_2)$ be two L ($L = 1$, or $L = 2$) layer quadratic space-time block codes over $\mathbb{Z}[\zeta_{m_1}]$ and $\mathbb{Z}[\zeta_{m_2}]$, respectively. Then, $X(\mathbb{Q}(\zeta_{m_1}), \beta_1, \beta_2, \rho_1)$ is better than $X(\mathbb{Q}(\zeta_{m_2}), \gamma_1, \gamma_2, \rho_2)$ if $d_{\min}(X(\mathbb{Q}(\zeta_{m_1}), \beta_1, \beta_2, \rho_1)) = d_{\min}(X(\mathbb{Q}(\zeta_{m_2}), \gamma_1, \gamma_2, \rho_2))$ and

$$\begin{aligned} &\rho_1^{2(L-1)}|\beta_1 - \beta_2|^L |\det(\Lambda_{\zeta_{m_1}})|^L \\ &\le \rho_2^{2(L-1)}|\gamma_1 - \gamma_2|^L |\det(\Lambda_{\zeta_{m_2}})|^L \end{aligned}$$

where $d_{\min}(X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, \rho)) \min_{X \in X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, \rho), X \neq 0} |\det(X)|$, $\det(\Lambda_{\zeta_3}) = \det(\Lambda_{\zeta_6}) = \frac{\sqrt{3}}{2}$ and $\det(\Lambda_{\zeta_4}) = 1$ and we make a convention that $0^0 = 1$. ■

The following two consequences can be obtained immediately from Lemma 1.

1) If $X(\mathbb{Q}(\zeta_4), \beta_1, \beta_2, \rho)$ is a quadratic space-time block code, then $X(\mathbb{Q}(\zeta_4), \beta_1\zeta_4^k, \beta_2\zeta_4^k, \rho)$ for $k = 1, \ldots, 4$ is also a quadratic space-time block code with the same diversity product as that of $X(\mathbb{Q}(\zeta_4), \beta_1, \beta_2, \rho_1)$.
2) If $X(\mathbb{Q}(\zeta_3), \beta_1, \beta_2, \rho)$ is a quadratic space-time block code, then $X(\mathbb{Q}(\zeta_3), \beta_1\zeta_6^k, \beta_2\zeta_6^k, \rho)$ for $k = 1, \ldots, 6$ is also a quadratic space-time block code with the same diversity product as that of $X(\mathbb{Q}(\zeta_3), \beta_1, \beta_2, \rho)$.

Therefore, in this paper, we only consider one of the aforementioned code structures for the design of optimal quadratic space-time block codes.

Lemma 2: For any L ($L = 1$ or $L = 2$) layer quadratic space-time block code $X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, \rho)$ with $m = 3$ or $m = 4$, the following two statements are true.

1) $d_{\min}(X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, 0) = 1$ if $L = 1$.
2) $d_{\min}(X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, \rho) = 1$ if $\rho^2 \in \mathbb{Z}[\zeta_m]$ and $L = 2$.

■

Proof: By Definition 1, we know that for any quadratic space-time block code $X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, \rho)$, there is an irreducible polynomial $x^2 + px + q$ over $\mathbb{Q}(\zeta_m)$ with roots α_1 and α_2. Therefore, $\mathbb{Q}(\zeta_m, \alpha_1)$ is a 2-D field extension of $\mathbb{Q}(\zeta_m)$, i.e., $[\mathbb{Q}(\zeta_m, \alpha_1) : \mathbb{Q}(\zeta_m)] = 2$, $\{1, \alpha_1\}$ is a basis of $\mathbb{Q}(\zeta_m, \alpha_1)$ over $\mathbb{Q}(\zeta_m)$. There are two embeddings σ_1 and σ_2 of $\mathbb{Q}(\zeta_m, \alpha_1)$ to $\mathbb{C}$ such that σ_1 and σ_2 are fixed in $\mathbb{Q}(\zeta_m)$, i.e., $\sigma_k(x) = x, k = 1, 2$, for $x \in \mathbb{Q}(\zeta_m)$, and $\sigma_1(\alpha_1) = \alpha_1,\ \sigma_2(\alpha_1) = \alpha_2$.

Let us first consider the case when $L = 1$. Notice that the codeword matrix X in the single-layer quadratic space-time block code $X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, 0)$ has the form of $X = \begin{bmatrix} y_1(1) & 0 \\ 0 & y_1(2) \end{bmatrix}$, where $\begin{bmatrix} y_1(1) \\ y_1(2) \end{bmatrix} = \begin{bmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{bmatrix} \begin{bmatrix} x_1(1) \\ x_1(2) \end{bmatrix}$ with $x_1(1),\ x_1(2) \in \mathbb{Z}[\zeta_m]$. Therefore, we have

$$\begin{aligned} \det(X) &= y_1(1)y_1(2) = \sigma_1(x_1)\sigma_2(x_1) \\ &= \mathbb{N}_{\mathbb{Q}(\zeta_m, \alpha_1)/\mathbb{Q}(\zeta_m)}(x_1) \end{aligned} \tag{6}$$

where $x_1 = x_1(1) + x_1(2)\alpha_1 \in \mathbb{Z}[\zeta_m, \alpha_1]$ and $\mathbb{N}_{\mathbb{Q}(\zeta_m, \alpha_1)/\mathbb{Q}(\zeta_m)}(x_1)$ is the relative algebraic norm of x_1 in the field $\mathbb{Q}(\zeta_m, \alpha_1)$ over field $\mathbb{Q}(\zeta_m)$. From [1], [12], and [26], we know that $\det(X) \in \mathbb{Z}[\zeta_m]$ for $m = 3$ or $m = 4$ and $\det(X) \neq 0$ if $X \neq 0$, i.e., $d_{\min}(X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, 0) = 1$. This completes the proof of Statement 1 in Lemma 2.

Now, let us consider the case when $L = 2$. In this case, the codeword of $X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, \rho)$

has the form of $X = \begin{bmatrix} y_1(1) & \rho y_2(1) \\ \rho y_2(2) & y_1(2) \end{bmatrix}$, where $\begin{bmatrix} y_2(1) \\ y_2(2) \end{bmatrix} = \begin{bmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{bmatrix} \begin{bmatrix} x_2(1) \\ x_2(2) \end{bmatrix}$ with $x_2(1), x_2(2) \in \mathbb{Z}[\zeta_m]$. Then, we obtain $\det(X) = y_1(1)y_1(2) - \rho^2 y_2(1)y_2(2)$. Since $\rho^2 \in \mathbb{Z}[\zeta_m]$, $y_1(1)y_1(2) = \mathbb{N}_{\mathbb{Q}(\zeta_m,\alpha_1)/\mathbb{Q}(\zeta_m)}(x_1) \in \mathbb{Z}[\zeta_m]$, $y_2(1)y_2(2) = \mathbb{N}_{\mathbb{Q}(\zeta_m,\alpha_1)/\mathbb{Q}(\zeta_m)}(x_2) \in \mathbb{Z}[\zeta_m]$ with $x_1 = x_1(1) + x_1(2)\alpha_1 \in \mathbb{Z}[\zeta_m, \alpha_1]$ and $x_2 = x_2(1) + x_2(2)\alpha_1 \in \mathbb{Z}[\zeta_m, \alpha_1]$, we have

$$\det(X) \in \mathbb{Z}[\zeta_m]. \tag{7}$$

Since ρ^2 is not an algebraic norm of $\mathbb{Q}(\zeta_m, \alpha_1)$ over $\mathbb{Q}(\zeta_m)$ if either $x_1 \neq 0$ or $x_2 \neq 0$, we arrive at the fact that $\mathbb{N}_{\mathbb{Q}(\zeta_m,\alpha_1)/\mathbb{Q}(\zeta_m)}(x_1) \neq \rho^2 \mathbb{N}_{\mathbb{Q}(\zeta_m,\alpha_1)/\mathbb{Q}(\zeta_m)}(x_2)$, i.e.,

$$\det(X) \neq 0, \quad \text{if } X \neq 0. \tag{8}$$

Combining (8) and (7), then for either $m = 3$ or $m = 4$, and $X \neq 0$, we attain $|\det(X)| \geq 1$, i.e., $d_{\min}(X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, \rho) = 1$. This completes the proof of Statement 2, and, thus, of Lemma 2. □

Notice: If $X(\mathbb{F}, \alpha_1, \alpha_2, \rho)$ is a quadratic space-time block code based on an irreducible polynomial $x^2 + px + q$ over field $\mathbb{F}$, then we have another space-time block code $\tilde{X}(\mathbb{F}, \alpha_1, \alpha_2, \rho)$ in which the codeword has the form of $\tilde{X} = \begin{bmatrix} z_1(1) & \rho z_2(1) \\ \rho z_2(2) & z_1(2) \end{bmatrix}$, where $\begin{bmatrix} z_k(1) \\ z_k(2) \end{bmatrix} = \begin{bmatrix} \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_1 \end{bmatrix} \begin{bmatrix} x_k(1) \\ x_k(2) \end{bmatrix}$, with $x_k(1), x_k(2)$ $k = 1, 2$ are integers of $\mathbb{F}$. When $\mathbb{F} = \mathbb{Q}(\zeta_m), m = 3$ or $m = 4$, following the discussion similar to the proof for the quadratic space-time block code $X(\mathbb{F}, \alpha_1, \alpha_2, \rho)$, we can prove that $\det(\tilde{X}) \in \mathbb{Z}[\zeta_m]$. In addition, when ρ^2 is not a relative algebraic norm of $\mathbb{F}(\alpha_1)$ over $\mathbb{F}$, we have $\det(\tilde{X}) \neq 0$. If we let $x_1(1) = x_1(2) = 1, x_2(1) = x_2(2) = 0$, then we obtain $\det(\tilde{X}) = (\alpha_1 - \alpha_2)^2 = p^2$. Therefore, $d_{\min}(\tilde{X}(\mathbb{F}, \alpha_1, \alpha_2, \rho) \leq |p|^2$. Since the generating matrix of the two-layer code $\tilde{X}(\mathbb{F}, \alpha_1, \alpha_2, \rho)$ is

$$\tilde{G} = \begin{bmatrix} \alpha_1 & \alpha_2 & 0 & 0 \\ \alpha_2 & \alpha_1 & 0 & 0 \\ 0 & 0 & \rho\alpha_1 & \rho\alpha_2 \\ 0 & 0 & \rho\alpha_2 & \rho\alpha_1 \end{bmatrix} \tag{9}$$

we attain $\det(\tilde{G}) = \rho^2(\alpha_1^2 - \alpha_2^2)^2 = \rho^2(\alpha_1 - \alpha_2)^2(\alpha_1 + \alpha_2)^2 = \rho^2(\alpha_1 - \alpha_2)^2 p^2$ and as a result, $\frac{d_{\min}(\tilde{X}(\mathbb{Q}(\zeta_m),\alpha_1,\alpha_2,\rho))}{\det(\tilde{G})\det(\Lambda_m)^2} \leq \frac{p^2}{\rho^2(\alpha_1-\alpha_2)^2 p^2 \det(\Lambda_m)^2} = \frac{1}{\rho^2(\alpha_1-\alpha_2)^2 \det(\Lambda_m)^2} = \frac{d_{\min}(X(\mathbb{Q}(\zeta_m),\alpha_1,\alpha_2,\rho))}{\det(G)\det(\Lambda_m)^2}$. From Lemma 1 and [20], we know that the code $\tilde{X}(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, \rho))$ is not superior to the quadratic space-time block code $X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, \rho))$. Therefore, in this paper, we focus on the quadratic space-time block code design $X(\mathbb{Q}(\zeta_m), \alpha_1, \alpha_2, \rho))$.

Theorem 1: Let $\mathbb{F} = \mathbb{Q}(\zeta_3)$ or $\mathbb{F} = \mathbb{Q}(\zeta_4)$ and ρ^2 be an algebraic integer of $\mathbb{F}$. If we let $X(\mathbb{F}, \alpha_1, \alpha_2, \rho)$ be a quadratic space-time block code based on an irreducible polynomial $x^2 + px + q$ over $\mathbb{F}$, then for any algebraic integer p_0 of $\mathbb{F}$, quadratic space-time block code $X(\mathbb{F}, \alpha_1 + p_0, \alpha_2 + p_0, \rho)$ has the same diversity product as that of $X(\mathbb{F}, \alpha_1, \alpha_2, \rho)$. ■

Proof: Let α_1 and α_2 be the two roots of minimal polynomial $x^2 + px + q$ of field $\mathbb{F}$. Then, $\alpha_1 + p_0$ and $\alpha_2 + p_0$ are the two roots of polynomial $(x - \alpha_1 - p_0)(x - \alpha_2 - p_0)$. Since $(x - x_1 - p_0)(x - x_2 - p_0) = x^2 + (p - 2p_0)x + (q - p_0 p + p_0^2)$ with $p - 2p_0$ and $q - p_0 p + p_0^2$ being integers of $\mathbb{F}$, and $x_1 + p_0 \notin \mathbb{F}$ and $x_2 + p_0 \notin \mathbb{F}$, the polynomial $(x - x_1 - p_0)(x - x_2 - p_0)$ is a minimal polynomial of $\mathbb{F}$. Therefore, $\{1, \alpha_1 + p_0\}$ is a base of field $\mathbb{F}(\alpha_1 + p_0)$ over $\mathbb{F}$. Since $\alpha_1 \in \mathbb{F}(\alpha_1 + p_0)$ and $\alpha_1 + p_0 \in \mathbb{F}(\alpha_1)$, we have $\mathbb{F}(\alpha_1) = \mathbb{F}(\alpha_1 + p_0)$. Therefore, ρ^2 is an algebraic norm of $\mathbb{F}(\alpha_1)$ over $\mathbb{F}$ if and only if it is an algebraic norm of $\mathbb{F}(\alpha_1 + p_0)$ over $\mathbb{F}$. From Lemma 2 and [18], we know that $d_{\min}(X(\mathbb{F}(\alpha_1), \alpha_1, \alpha_2, \rho) = d_{\min}(X(\mathbb{F}(\alpha_1 + p_0), \alpha_1 + p_0, \alpha_2 + p_0, \rho) = 1$ if ρ^2 is not an algebraic norm of $\mathbb{F}(\alpha_1)$ over $\mathbb{F}$ and that $d_{\min}(X(\mathbb{F}(\alpha_1), \alpha_1, \alpha_2, \rho) = d_{\min}(X(\mathbb{F}(\alpha_1 + p_0), \alpha_1 + p_0, \alpha_2 + p_0, \rho) = 0$ if ρ^2 is an algebraic norm of $\mathbb{F}(\alpha_1)$ over $\mathbb{F}$. In addition, the generating matrices of $X(\mathbb{F}, \alpha_1, \alpha_2, \rho)$ and $X(\mathbb{F}, \alpha_1 + p_0, \alpha_2 + p_0, \rho)$ are $\mathrm{diag}(G_1, \rho G_1)$ and $\mathrm{diag}(G_2, \rho G_2)$, respectively, with $G_1 = \begin{bmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{bmatrix}$ and $G_2 = \begin{bmatrix} 1 & \alpha_1 + p_0 \\ 1 & \alpha_2 + p_0 \end{bmatrix}$. Therefore, we have $\det(G_1) = \det(G_2)$. Using Lemma 1, we know that the quadratic space-time block code $X(\mathbb{F}, \alpha_1 + p_0, \alpha_2 + p_0, \rho)$ has the same diversity product as that of $X(\mathbb{F}, \alpha_1, \alpha_2, \rho)$. This completes the proof of Theorem 1. □

III. Optimal Single-Layer Quadratic Space-Time Block Codes

In this section, we consider the design of the optimal single-layer space-time block codes over Gaussian and Eisenstein rings.

Theorem 2: $X\left(\mathbb{Q}(\zeta_4), \frac{-i+\sqrt{3}}{2}, \frac{-i-\sqrt{3}}{2}, 0\right)$ is the optimal single-layer Gaussian quadratic space-time block code with minimal determinant 1. ■

Proof: We first note that $\alpha_1 = \frac{-i+\sqrt{3}}{2}$ and $\alpha_2 = \frac{-i-\sqrt{3}}{2}$ are the two roots of quadratic polynomial $x^2 + ix - 1$ over $\mathbb{Q}(\zeta_4)$. Since $\alpha_1, \alpha_2 \notin \mathbb{Q}(\zeta_4)$, $x^2 + ix - 1$ is irreducible over $\mathbb{Q}(\zeta_4)$. Therefore, $\mathbb{Q}(\zeta_4, \alpha_1)$ is a 2-D field extension over $\mathbb{Q}(\zeta_4)$, $x^2 + ix - 1$ is the minimal polynomial of α_1, and $\{1, \alpha_1\}$ is a basis of $\mathbb{Q}(\zeta_4, \alpha_1)$ over $\mathbb{Q}(\zeta_4)$. Let σ_1 and σ_2 are the two embeddings of $\mathbb{Q}(\zeta_4, \alpha_1)$ that is fixed on $\mathbb{Q}(\zeta_4)$ and $\sigma_1(\alpha_1) = \alpha_1$, $\sigma_2(\alpha_1) = \alpha_2$. The codeword of the single-layer quadratic space-time block code $X(\mathbb{Q}(\zeta_4), \frac{-i+\sqrt{3}}{2}, \frac{-i-\sqrt{3}}{2}, 0)$ has the form of $X = \mathrm{diag}(y_1, y_2)$, where $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ with $x_1, x_2 \in \mathbb{Z}[\zeta_4]$. Then, $\det(X) = y_1 y_2 = \mathbb{N}_{\mathbb{Q}(\zeta_4,\alpha_1)/\mathbb{Q}(\zeta_4)}(x_1 + x_2\alpha_1) \in \mathbb{Q}[\zeta_4]$. From Lemma 2, $X\left(\mathbb{Q}(\zeta_4), \frac{-i+\sqrt{3}}{2}, \frac{-i-\sqrt{3}}{2}, 0\right)$ is a single-layer quadratic space-time block code with minimal determinant 1.

In the following, we prove that $X\left(\mathbb{Q}(\zeta_4), \frac{-i+\sqrt{3}}{2}, \frac{-i-\sqrt{3}}{2}, 0\right)$ is the optimal single-layer Gaussian quadratic space-time block code. We know from Lemma 2 that the minimal determinant of any single-layer Gaussian quadratic space-time code is 1. Combining this with Lemma 1, we only need to prove that for any quadratic space-time block code

$X(\mathbb{Q}(\zeta_4),\beta_1,\beta_2,0)$ based on quadratic polynomial x^2+px+q, $|\beta_1-\beta_2|\geq|\alpha_1-\alpha_2|=|\frac{-i+\sqrt{3}}{2}-\frac{-i-\sqrt{3}}{2}|=\sqrt{3}$. To this end, by Theorem 1 we can always assume that $p\in\mathbb{Z}[\zeta_4]$ and $|p|<2$ without loss of generality. Since β_1 and β_2 are two roots of the irreducible quadratic polynomial x^2+px+q over $\mathbb{Q}(\zeta_4)$ with $p,q\in\mathbb{Z}[\zeta_4]$ and $|p|<2$, we have $\beta_1-\beta_2=\sqrt{p^2-4q}$ with $p\in\mathbb{Z}[\zeta_4]$ and $|p|<2$. Notice that constraints $p\in\mathbb{Z}[\zeta_4]$ and $|p|<2$ can be simplified into $p\in\{0,\pm1,\pm i,\pm1\pm i\}$. Therefore, we consider the following two cases.

Case 1. $p\in\{0,\pm1,\pm i\}$. In this case, if $q\neq0$, then we have $|\beta_1-\beta_2|^2=|p^2-4q|\geq4|q|-|p|^2\geq3$. If $q=0$, then $x^2+px+q=x^2+px$ is reducible in $\mathbb{Q}(\zeta_4)$, which is impossible.

Case 2. $p\in\{\pm1\pm i\}$. This case is equivalent to $p^2=\pm2i$. In addition, since $p,\ q\in\mathbb{Z}[\zeta_4,]$, we obtain $p^2-4q\in\mathbb{Z}[\zeta_4]$. Suppose that $|p^2-4q|<3$. Then, $|p^2-4q|=|\pm2i-4q|\leq2$ for $q\in\mathbb{Z}[i]$, which is equivalent to the fact that $q=0$ or $p^2=2i$ and $q=i$ or $p^2=-2i$ and $q=-i$. This leads us to consider the following three subsituations.

1) $q=0$. Then, $x^2+px+q=x^2+px$ is reducible in $\mathbb{Q}(\zeta_4)$, which is impossible.
2) $p^2=2i$ and $q=i$. Then, $p=\pm(1+i)$ and $p^2-4q=-2i=(1-i)^2$. Therefore, $\beta_1=\frac{-p+\sqrt{p^2-4q}}{2}=\frac{\pm(1+i)+\sqrt{1-i}}{2}\in\mathbb{Q}(\zeta_4)$ and $\beta_2=\frac{-p-\sqrt{p^2-4q}}{2}=\frac{\pm(1+i)-\sqrt{1-i}}{2}\in\mathbb{Q}(\zeta_4)$. This means that $x^2+px+q=(x-\beta_1)(x-\beta_2)$ is reducible in $\mathbb{Q}(\zeta_4)$, which is impossible either.
3) $p^2=-2i$ and $q=-i$. In this case, we have $p^2-4q=2i=(1+i)^2$ and as a result, $\beta_1=\frac{-p+\sqrt{p^2-4q}}{2}\in\mathbb{Q}(\zeta_4)$ and $\beta_2=\frac{-p-\sqrt{p^2-4q}}{2}\in\mathbb{Q}(\zeta_4)$, i.e., $x^2+px+q=(x-\beta_1)(x-\beta_2)$ is reducible in $\mathbb{Q}(\zeta_4)$. This contradicts with the stated assumption.

Summarizing all the aforementioned discussions yields $|\beta_1-\beta_2|\geq\sqrt{3}$. Therefore, $X(\mathbb{Q}(\zeta_4),\frac{-i+\sqrt{3}}{2},\frac{-i-\sqrt{3}}{2},0)$ is the optimal single-layer Gaussian quadratic space-time block code with minimal determinant 1. This completes the proof of Theorem 2. □

It is important to note that the code $X(\mathbb{Q}(\zeta_4),\frac{-i+\sqrt{3}}{2},\frac{-i-\sqrt{3}}{2},0)$ proposed in [12] is a cyclotomic space-time block code.

Theorem 3: $X(\mathbb{Q}(\zeta_3),\frac{-\zeta_3+\sqrt{\zeta_3^2+4}}{2},\frac{-\zeta_3-\sqrt{\zeta_3^2+4}}{2},0)$ is the optimal single-layer Eisenstein quadratic space-time block code with minimal determinant 1. ■

Proof: Since $\sqrt{\zeta_3^2+4}\notin\mathbb{Q}(\zeta_3)$, polynomial $\left(x-\frac{-\zeta_3+\sqrt{\zeta_3^2+4}}{2}\right)\left(x-\frac{-\zeta_3-\sqrt{\zeta_3^2+4}}{2}\right)=x^2+\zeta_3-1$ is an irreducible polynomial over $\mathbb{Q}(\zeta_3)$. Therefore, $X\left(\mathbb{Q}(\zeta_3),\frac{-\zeta_3+\sqrt{\zeta_3^2+4}}{2},\frac{-\zeta_3-\sqrt{\zeta_3^2+4}}{2},0\right)$ is a single-layer quadratic space-time block code over $\mathbb{Z}[\zeta_3]$. We know from Lemma 2 that the minimal determinant of any single-layer quadratic space-time code over $\mathbb{Q}(\zeta_3)$ is 1. In addition, Lemmas 1 and 2, and Theorem 1 together imply that to prove the optimality of $X\left(\mathbb{Q}(\zeta_3),\frac{-\zeta_3+\sqrt{\zeta_3^2+4}}{2},\frac{-\zeta_3-\sqrt{\zeta_3^2+4}}{2},0\right)$, we only need to prove that for any quadratic minimal polynomial x^2+px+q with $p,\ q\in\mathbb{Z}[\zeta_3]$, $|p|<2$, its two roots β_1 and β_2 satisfy $|\beta_1-\beta_2|=\sqrt{p^2-4q}\geq|\frac{-\zeta_3+\sqrt{\zeta_3^2+4}}{2}-\frac{-\zeta_3-\sqrt{\zeta_3^2+4}}{2}|=|\sqrt{\zeta_3^2+4}|$. Suppose that this is not true. In other words, $|p^2-4q|<|\zeta_3^2+4|$. In the following, we prove that polynomial x^2+px+q is reducible in $\mathbb{Q}(\zeta_3)$. Since $p\in\mathbb{Z}[\zeta_3]$ and $|p|<2$, we have $p\in\{0,\exp(i2k/6),\sqrt{3}i\exp(i2k\pi/6),k=1,\ldots,6\}$. As a result, $p^2\in\{0,\exp(i2k\pi/3),-3\exp(i2k\pi/3),k=1,\ldots,3\}$. Therefore, we consider the following five case.

1) $p=0$. In this case, when $q\neq0$, $|p^2-4q|=4|q|\geq4>|\zeta_3^2+4|$. Therefore, $|p^2-4q|<|\zeta_3^2+4|$ implies that $q=0$. When $q=0$, we have $x^2+px+q=x^2$, which is reducible in $\mathbb{Q}(\zeta_3)$.
2) $p^2=1$. Then, $|p^2-4q|=|1-4q|<|\zeta_3^2+4|$ implies that either $q=1$ or $q=0$. If $q=0$, then $x^2-px+q=x^2-px$ is reducible in $\mathbb{Q}(\zeta_3)$. If $q=1$, then we obtain $\frac{-p\pm\sqrt{p^2-4q}}{2}=\frac{\pm1\pm\sqrt{3}i}{2}\in\mathbb{Q}(\zeta_3)$, and thus, x^2+px+q is also reducible in $\mathbb{Q}(\zeta_3)$.
3) $p^2=\exp(i2\pi/3)$ or $p^2=\exp(i4\pi/3)$. Following the same discussion as Case 2, we can prove that $x^2-px+q=x^2-px$ is reducible in $\mathbb{Q}(\zeta_3)$ in this case.
4) $p^2=-3$. In this situation, $p=\pm\sqrt{3}i$. If $|p^2-4q|=|3+4q|<|\zeta_3^2+4|$, then $q=-1$, and $p^2-4q=1$. Therefore, $\frac{-p\pm\sqrt{p^2-4q}}{2}=\frac{\pm\sqrt{3}i\pm1}{2}\in\mathbb{Q}(\zeta_3)$, i.e., polynomial $x^2+px+q=x^2\pm\sqrt{3}ix-1$ is reducible in $\mathbb{Q}(\zeta_3)$.
5) $p^2=-3\exp(i2\pi/3)$ or $p^2=-3\exp(i4\pi/3)$. Similar to the discussion of Case 4, we can arrive at the fact that polynomial $x^2+px+q=x^2\pm\sqrt{3}ix-1$ is also reducible in $\mathbb{Q}(\zeta_3)$.

From the above discussions we reach the conclusion that if $|p^2-4q|<|\zeta_3^2+4|$, then polynomial x^2+px+q is reducible in $\mathbb{Q}(\zeta_3)$. This completes the proof of Theorem 3. ■

We can observe from Theorem 3 that since $|\frac{-\zeta_3+\sqrt{\zeta_3^2+4}}{2}|\neq1$ and $|\frac{-\zeta_3-\sqrt{\zeta_3^2+4}}{2}|\neq1$, the optimal code $X(\mathbb{Q}(\zeta_3),\frac{-\zeta_3+\sqrt{\zeta_3^2+4}}{2},\frac{-\zeta_3-\sqrt{\zeta_3^2+4}}{2},0)$ is not a cyclotomic space-time block code. Therefore, the optimal single-layer quadratic space-time time code does not belong to the cycloctomic code family. In addition, by Lemma 1, we know that $X(\mathbb{Q}(\zeta_3),\frac{-\zeta_3+\sqrt{\zeta_3^2+4}}{2},\frac{-\zeta_3-\sqrt{\zeta_3^2+4}}{2},0)$ has better performance than $X(\mathbb{Q}(\zeta_4),\frac{-i+\sqrt{3}}{2},\frac{-i-\sqrt{3}}{2},0)$ in terms of the diversity product criterion. Therefore, we have the following theorem.

Theorem 4: Among all the single-layer Gaussian and Eisenstein quadratic space-time block codes, $X(\mathbb{Q}(\zeta_3),\frac{-\zeta_3+\sqrt{\zeta_3^2+4}}{2},\frac{-\zeta_3-\sqrt{\zeta_3^2+4}}{2},0)$ is the optimal single-layer quadratic space-time block code with minimal determinant 1. ■

IV. Optimal Full-Rate Quadratic Space-Time Block Codes

The primary purpose of this section is to design the optimal full-rate and nonvanishing quadratic space-time block codes with large diversity products for two-transmitter antennas.

Theorem 5: $X\left(\mathbb{Q}(\zeta_4), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, \sqrt{1+i}\right)$ is the optimal full-rate Gaussian quadratic space-time block code with minimal determinant 1. ■

To prove Theorem 5, we first establish the following Proposition.

Proposition 1: The complex number $1+i$ is not a relative algebraic norm of any element in $\mathbb{Q}(\zeta_4, \frac{i+\sqrt{3}}{2})$ over $\mathbb{Q}(\zeta_4)$. ■

Proof: Suppose that there exist $x = x_1 + x_2\alpha_1 \in \mathbb{Z}[\zeta_4, \alpha_1]$ and $y = y_1 + y_2\alpha_2 \in \mathbb{Z}[\zeta_4, \alpha_1]$ with $x_k,\ y_k \in \mathbb{Z}[\zeta_4],\ k = 1, 2,\ \alpha_1 = \frac{i+\sqrt{3}}{2}$ such that

$$\mathbb{N}_{\mathbb{Q}(\zeta_4,\alpha_1)/\mathbb{Q}(\zeta_4)}(x) = (1+i)\mathbb{N}_{\mathbb{Q}(\zeta_4,\alpha_1)/\mathbb{Q}(\zeta_4)}(y). \tag{10}$$

Since $\alpha_1 = \zeta_{12},\ \mathbb{Q}(\zeta_4, \alpha_1) = \mathbb{Q}(\zeta_{12})$, we know that $\{1, \zeta_{12}\}$ is a basis of $\mathbb{Q}(\zeta_{12})$ over $\mathbb{Q}(\zeta_4)$. Hence, any element x in $\mathbb{Z}[\zeta_{12}]$ can be expressed by $x = x_1 + x_2\zeta_{12}$ with $x_1, x_2 \in \mathbb{Z}[\zeta_4]$. From the definition of the relative algebraic norm, we have $\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(x) = \sigma_1(x)\sigma_2(x)$, where σ_1 and σ_2 are the embedding of $\mathbb{Q}(\zeta_{12})$ to $\mathbb{C}$ with $\sigma_1(z) = \sigma_2(z) = z$ for any $z \in \mathbb{Q}(\zeta_4)$ and $\sigma_1(\zeta_{12}) = \zeta_{12},\ \sigma_2(\zeta_{12}) = \zeta_{12}^5$. Therefore, it can be verified by calculation that

$$\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(x) = \sigma_1(x)\sigma_2(x) = x_1^2 - x_1^2 + ix_1x_2. \tag{11}$$

Similarly, for any $y \in \mathbb{Z}[\zeta_{12}]$ with $y = y_1 + y_2\zeta_{12}$ and $y_1, y_2 \in \mathbb{Z}[\zeta_4]$, we have

$$\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(y) = y_1^2 - y_2^2 + iy_1y_2. \tag{12}$$

Since $(1+i)\mathbb{Z}[\zeta_4]$ is an ideal of ring $\mathbb{Z}[\zeta_4]$, there is an integer l_0 such that

$$x_k = \sum_{l=1}^{l_0} \rho^{l-1}x_{k,l} \text{ and } y_k = \sum_{l=1}^{l_0} \rho^{l-1}y_{k,l} \tag{13}$$

for $k = 1, 2$, where $\rho = 1 + i$, and $x_{k,l}, y_{k,l} \in \{0, \exp(j2p\pi/4), p = 1, \ldots, 4\}$. Combining (10)--(12) with (13) yields

$$\begin{aligned} &x_{1,1}^2 - x_{2,1}^2 + ix_{1,1}x_{2,1} \\ &= \rho\left(y_1^2 - y_2^2 + iy_1y_2\right) - \rho(\rho\bar{x}_{1,1}^2 - \rho\bar{x}_{2,1}^2 + i\rho\bar{x}_{1,1}\bar{x}_{2,1}) \\ &\quad -2\rho(x_{1,1}\bar{x}_{1,1} - x_{2,1}\bar{x}_{2,1}) - i\rho(x_{1,1}\bar{x}_{2,1} + x_{2,1}\bar{x}_{1,1}) \end{aligned} \tag{14}$$

where $\bar{x}_{k,1} = \sum_{l=2}^{l_0} \rho^{l-2}x_{k,l} \in \mathbb{Z}[\zeta_4],\ k = 1, 2$. Since the term on the right-hand side of (14) belongs to $\rho\mathbb{Z}[\zeta_4]$, the term on the left-hand side of (14) also belongs to $\rho\mathbb{Z}[\zeta_4]$, i.e.,

$$x_{1,1}^2 - x_{2,1}^2 + ix_{1,1}x_{2,1} \in \rho\mathbb{Z}[\zeta_4]. \tag{15}$$

After examining (15) with $x_{1,1}, x_{2,1} \in \{0, \exp(i2p\pi/4), p = 1, \ldots, 4\}$, we find that (15) holds only when $x_{1,1} = x_{2,1} = 0$. In this case, (14) becomes

$$y_1^2 - y_1^2 + iy_1y_2 - \rho(\bar{x}_{1,1}^2 - \bar{x}_{2,1}^2 + i\bar{x}_{1,1}\bar{x}_{2,1}) = 0 \tag{16}$$

i.e.,

$$\begin{aligned} &y_{1,1}^2 - y_{2,1}^2 + iy_{1,1}y_{2,1} \\ &= \rho\left(\bar{x}_{1,1}^2 - \bar{x}_{2,1}^2 + i\bar{x}_{1,1}\bar{x}_{2,1}\right) \\ &- \rho\left\{\rho(\bar{y}_{1,1}^2 - \bar{y}_{2,1}^2) + i\rho\bar{x}_{1,1}\bar{x}_{2,1}\right\} \\ &- 2\rho(y_{1,1}\bar{y}_{1,1} - y_{2,1}\bar{y}_{2,1} + iy_{1,1}\bar{y}_{2,1} + iy_{2,1}\bar{y}_{1,1}) \end{aligned}$$

where $\bar{y}_{k,1} = \sum_{l=2}^{l_0} \rho^{l-2}y_{k,l} \in \mathbb{Z}[\zeta_6],\ k = 1, 2$. Following the discussion much similar to the proof for $x_{1,1}$ and $x_{2,1}$ in (15), we can attain $y_{1,1} = y_{2,1} = 0$. Continue this procedure until $x_{1,l_0} = x_{2,l_0} = 0$ and $y_{1,l_0} = y_{2,l_0} = 0$. Finally, we obtain $x = y = 0$. This completes the proof of Proposition 1. □

Proof of Theorem 5: First, we know from Proposition 1 and Lemma 2 that $X(\mathbb{Q}(\zeta_4), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, \sqrt{1+i})$ is a full-rate quadratic space-time block code with determinant 1. In the following, we prove the optimality of the code $X\left(\mathbb{Q}(\zeta_4), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, \sqrt{1+i}\right)$ among all the full-rate Gaussian quadratic space-time block codes. To this end, we only need to prove that for any two-layer Gaussian quadratic space-time code $X(\mathbb{Q}(\zeta_4), \beta_1, \beta_2, \rho)$ with $\rho^2 \in \mathbb{Z}[\zeta_4]$ and $d_{\min} \geq 1$, we have $|\det(\bar{G})\rho| \geq \sqrt{3}\sqrt{|1+i|}$, where

$$\bar{G} = \begin{bmatrix} 1 & \beta_1 \\ 1 & \beta_2 \end{bmatrix}. \tag{17}$$

To proceed, let us consider a quadratic polynomial $x^2 + px + q$ with $p, q \in \mathbb{Z}[\zeta_4]$. By Theorem 1, we can always assume that $|p| < 2$, i.e., $p \in \{0, \pm 1, \pm i, \pm 1 \pm i\}$ without loss of generality. Suppose that there exists a two-layer quadratic space-time block code with minimal determinant 1 based on $x^2 + px + q$ such that

$$|\det(\bar{G})\rho| < \sqrt{3}\sqrt{|1+i|} \tag{18}$$

where $\bar{G}$ is defined in (17) and β_1, β_2 are the two roots of polynomial $x^2 + px + q$. Since $\det(\bar{G}) = \beta_2 - \beta_1$, inequality (18) is equivalent to

$$|\beta_1 - \beta_2|^2|\rho^2| = |p^2 - 4q||\rho^2| < 3|1+i| = 3\sqrt{2}. \tag{19}$$

From the proof of Theorem 2, we can observe that when $|p^2 - 4q| < 3$, the polynomial $x^2 + px + q$ is reducible in $\mathbb{Q}(\zeta_4)$. As a consequence, it cannot be used to generate a quadratic space-time block code. Therefore, we only need to consider the case when $|p^2 - 4q| \geq 3$. In this case, since $\rho^2 \in \mathbb{Z}[\zeta_4], \rho \neq 0$, and $p^2 - 4q \in \mathbb{Z}[\zeta_4]$, we have $|\rho| \geq 1$, and thus, inequality (19) implies

$$\left(|p^2 - 4q|, |\rho^2|\right) \in \{(3, 1), (4, 1)\}. \tag{20}$$

This leads us to consider the following two situations.

1) $|p^2 - 4q| = 3$ and $|\rho^2| = 1$. From $|\rho^2| = 1$ and $\rho^2 \in \mathbb{Z}[\zeta_4]$, we can derive that $\rho^2 = \{\pm 1, \pm i\}$. In addition, $|p^2 - 4q| = 3$ with $p, q \in \mathbb{Z}[\zeta_4]$ and $|p| < 2$ implies that

$$(p, q) \in \{(\pm 1, 1), (\pm i, -1)\}$$

and thus

$$(p, \sqrt{p^2 - 4q}) \in \{(\pm 1, \sqrt{3}i), (\pm i, \sqrt{3})\}.$$

Therefore, either the field $\mathbb{Q}(\zeta_4,\beta_1) = \mathbb{Q}(\zeta_4, \frac{-p\pm\sqrt{p^2-4q}}{2}) = \mathbb{Q}(\zeta_4, \frac{1\pm\sqrt{3}i}{2})$ or $\mathbb{Q}(\zeta_4,\beta_1) = \mathbb{Q}(\zeta_4, \frac{i\pm\sqrt{3}}{2})$. However, in this case, it can be directly verified that $\rho^2 \in \{\pm 1, \pm i\}$ is an algebraic norm of $\mathbb{Q}(\zeta_4,\beta_1)$ over $\mathbb{Q}(\zeta_4)$, which means that the minimal determinant of $X(\mathbb{Q}(\zeta_4),\beta_1,\beta_2,\rho)$ is 0.

2) $|p^2-4q| = 4$ and $|\rho^2| = 1$. In this case, $p = 0$ and $q \in \{\pm 1, \pm i\}$ because of $|p| < 2$. Hence, we have $x^2+px+q = x^2+q$. If $q = \pm 1$, then x^2+q is reducible in $\mathbb{Q}(\zeta_4)$. If $q = \pm i$, then the roots of x^2+q are $\pm\sqrt{\pm i}$. However, it can be directly verified that in this case, $\rho^2 \in \{\pm 1, \pm i\}$ is an algebraic norm of $\mathbb{Q}(\zeta_4, \pm\sqrt{\pm i})$ over $\mathbb{Q}(\zeta_4)$.

The aforementioned discussion leads to a common conclusion that inequality (18) cannot hold. This completes the proof of Theorem 5. □

Theorem 6: $X\left(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_{12}\right)$ is the optimal full-rate Eisenstein quadratic space-time block code with minimal determinant 1, where $p = -1-\zeta_6$ and $q = \sqrt{3}i$.

Before proving Theorem 6, we first develop the following Proposition.

Proposition 2: The complex number ζ_6 is not a norm of any element of $\mathbb{Q}(\zeta_3,\alpha_1)$ over $\mathbb{Q}(\zeta_3)$, where $\alpha_1 = \frac{-p+\sqrt{p^2-4q}}{2}$ with $p = -1-\zeta_6$ and $q = \sqrt{3}i$. ■

Proof: We first prove that if there exist $x = x_1 + x_2\alpha_1$ and $y = y_1 + y_2\alpha_1$ with $x_k, y_k \in \mathbb{Z}[\zeta_3]$ for $k = 1, 2$ such that

$$\mathbb{N}_{\mathbb{Q}(\zeta_3,\alpha_1)/\mathbb{Q}(\zeta_3)}(x) = \zeta_6 \mathbb{N}_{\mathbb{Q}(\zeta_3,\alpha_1)/\mathbb{Q}(\zeta_3)}(y) \tag{21}$$

then we must have $x = y = 0$. From the definition of the relative norm, we have

$$\begin{aligned}\mathbb{N}_{\mathbb{Q}(\zeta_3,\alpha_1)/\mathbb{Q}(\zeta_3)}(x) &= (x_1+x_2\alpha_1)(x_1+x_2\alpha_2)\\ &= x_1^2 - px_1x_2 + qx_2^2\\ &= x_1^2 + (1+\zeta_6)x_1x_2 + \sqrt{3}ix_2^2\end{aligned} \tag{22}$$

and

$$\begin{aligned}\mathbb{N}_{\mathbb{Q}(\zeta_3,\alpha_1)/\mathbb{Q}(\zeta_3)}(y) &= (y_1+y_2\alpha_1)(y_1+y_2\alpha_2)\\ &= y_1^2 - py_1y_2 + qy_2^2\\ &= y_1^2 + (1+\zeta_6)y_1y_2 + \sqrt{3}iy_2^2.\end{aligned} \tag{23}$$

Now, substituting (22) and (23) into (21) yields

$$\begin{aligned}x_1^2 + (1+\zeta_6)x_1x_2 - \zeta_6\{y_1^2 + (1+\zeta_6)y_1y_2\}\\ = \sqrt{3}i(\zeta_6y_2^2 - x_2^2).\end{aligned} \tag{24}$$

On the other hand, notice that $\sqrt{3}i\mathbb{Z}[\zeta_6]$ is an ideal of ring $\mathbb{Z}[\zeta_6]$. Therefore, there exists an integer l_0 such that the elements x_k and y_k in $\mathbb{Z}[\zeta_3]$ can be represented by

$$x_k = \sum_{l=1}^{l_0} x_{k,l}(\sqrt{3}i)^{l-1},\ y_k = \sum_{l=1}^{l_0} y_{k,l}(\sqrt{3}i)^{l-1} \tag{25}$$

with $x_{k,l}, y_{k,l} \in \mathcal{S} = \{0, \exp(i2m\pi/6), m = 1,\ldots,6\}$. Plugging (25) into (24) results in

$$\begin{aligned}&x_{1,1}^2 + (1+\zeta_6)x_{1,1}x_{2,1} - \zeta_6(y_{1,1}^2 + (1+\zeta_6)y_{1,1}y_{2,1})\\ &= \sqrt{3}i(\zeta_6y_2^2 - x_2^2) - \sqrt{3}i(2x_{1,1}\bar{x}_{1,1}\\ &\quad + (1+\zeta_6)(\bar{x}_{1,1}x_2 + x_{1,1}\bar{x}_{2,1}) + \sqrt{3}i\bar{x}_{1,1}^2)\\ &\quad + \sqrt{3}i\zeta_6(2y_{1,1}\bar{y}_{1,1} + (1+\zeta_6)(\bar{y}_{1,1}y_2 + y_{1,1}\bar{y}_{2,1})\\ &\quad + \sqrt{3}i\bar{y}_{1,1}^2)\end{aligned} \tag{26}$$

where $\bar{x}_{k,1} = \sum_{l=2}^{l_0} x_{k,l}(\sqrt{3}i)^{l-2}$ and $\bar{y}_{k,1} = \sum_{l=2}^{l_0} y_{k,l}(\sqrt{3}i)^{l-2}$. The term on the right-hand side of (26) belongs to $\sqrt{3}i\mathbb{Z}[\zeta_3]$, so does the term on the left-hand side of (26), i.e.,

$$\begin{aligned}x_{1,1}^2 + (1+\zeta_6)x_{1,1}x_{2,1} - \zeta_6\{y_{1,1}^2 + (1+\zeta_6)y_{1,1}y_{2,1}\}\\ \in \sqrt{3}i\mathbb{Z}[\zeta_3].\end{aligned} \tag{27}$$

After checking (27) for each $x_{k,1}, y_{k,1} \in \mathcal{S}$, we find that (27) is true only when $x_{1,1} = y_{1,1} = 0$. In this case, (26) is reduced to

$$\begin{aligned}&x_{2,1}^2 + (1+\zeta_6)x_{2,1}x_{1,2} - \zeta_6(y_{2,1}^2 + (1+\zeta_6)y_{2,1}y_{1,2})\\ &= \sqrt{3}i(\zeta_6\bar{y}_{1,1}^2 - \bar{x}_{1,1}^2) - \sqrt{3}i(2x_{2,1}\bar{x}_{2,1}\\ &\quad + (1+\zeta_6)(\bar{x}_{2,1}\bar{x}_{1,1} + x_{2,1}\bar{x}_{1,2}) + \sqrt{3}i\bar{x}_{2,1}^2)\\ &\quad + \sqrt{3}i(2y_{2,1}\bar{y}_{2,1} + (1+\zeta_6)(\bar{y}_{2,1}\bar{y}_{1,1} + y_{2,1}\bar{y}_{1,2})\\ &\quad + \sqrt{3}i\bar{y}_{2,1}^2)\end{aligned} \tag{28}$$

i.e.,

$$\begin{aligned}x_{2,1}^2 + (1+\zeta_6)x_{2,1}x_{1,2} - \zeta_6\{y_{2,1}^2 + (1+\zeta_6)y_{2,1}y_{1,2}\}\\ \in \mathbb{Z}[\zeta_3]\end{aligned} \tag{29}$$

where $\bar{x}_{k,2} = \sum_{l=2}^{l_0} x_{k,l}(\sqrt{3}i)^{l-3}$ and $\bar{y}_{k,2} = \sum_{l=2}^{l_0} y_{k,l}(\sqrt{3}i)^{l-3}$. Similarly, by testing (29) with each $x_{1,2}, x_{2,1}, y_{1,2}, y_{2,1} \in \mathcal{S}$, we realize that (29) is true only when $x_{2,1} = y_{2,1} = 0$. Continue this process until $x = y = 0$. This completes the proof of Proposition 2. □

Proof of Theorem 6: Similar to the proof of Theorem 5, it suffices to prove that for any quadratic polynomial x^2+px+q with $p,\ q \in \mathbb{Z}[\zeta_3],\ |p| < 2$, and any $\rho^2 \in \mathbb{Z}[\zeta_3]$, such that

$$|\det(\bar{G})\rho| = |\sqrt{p^2-4q}||\rho| < |\sqrt{(1+\zeta_6)^2 - 4\sqrt{3}i}| \tag{30}$$

we have that $X(\mathbb{Q}(\zeta_3),\beta_1,\beta_2,\rho)$ is not a full-rate space-time code with minimal determinant 1, where $\beta_1 = \frac{-p+\sqrt{p^2-4q}}{2}$, $\beta_2\frac{-p-\sqrt{p^2-4q}}{2}$ are roots of x^2+px+q, and

$$\bar{G} = \begin{bmatrix}1 & \beta_1\\ 1 & \beta_2\end{bmatrix}. \tag{31}$$

Since $|p| < 2$, we have $p \in \{0, \exp(i2k\pi/6), \sqrt{3}i\exp(i2k\pi/6), k = 1,\ldots,6\}$. In addition, (30) implies that

$$\begin{aligned}|p^2-4q| \in \{0, 1, \sqrt{3}, 2, |2+\zeta_6|, 3, 2|1+\zeta_6|,\\ |3+\zeta_6|, |3+2\zeta_6|\}.\end{aligned} \tag{32}$$

However, from the proof of Theorem 3, it is evident that when $|p^2-4q| < |\zeta_3^2+4| = |3+\zeta_6|$, the polynomial x^2+px+q becomes reducible in field $\mathbb{Q}(\zeta_3)$. Hence, we need to only consider the case

$$|p^2-4q| \in \{|3+\zeta_6|, |3+2\zeta_6|\}. \tag{33}$$

Now, let us discuss each individual case.

1) $|p^2-4q| = |3+\zeta_6|$. Since $p \in \{0, \exp(i2k\pi/6), \sqrt{3}i\exp(i2k\pi/6), k=1,\ldots,6\}$, the condition $|p^2-4q| = |3+\zeta_6|$ implies that

$$(p,q) \in \{(\zeta_6\zeta_6^k, -\zeta_3^k), ((2-\zeta_6)\zeta_6^k, -\zeta_6\zeta_3^k),\ k=1,\ldots,6\}. \tag{34}$$

If $|\rho^2|>1$, then we have $|\rho^2| \geq \sqrt{3}$, since $\rho^2 \in \mathbb{Z}[\zeta_3]$. In this case, we attain $|\rho^2(3+\zeta_6)| > 6.24 > |(1+\zeta_6)^2 - 4\sqrt{3}i|$. Therefore, inequality (30) implies that $|\rho|=1$. It can be directly verified that $\rho^2 \in \{\exp(i2ki\pi/6),\ k=1,\ldots,6\}$ is an algebraic norm of $\mathbb{Q}(\zeta_3, \frac{p\pm\sqrt{p^2-4q}}{2})$ over $\mathbb{Q}(\zeta_3)$ with p and q belonging to the set given in (34).

2) $|p^2-4q| = |3+2\zeta_6|$. In fact, it is impossible to have p and q in $\mathbb{Z}[\zeta_3]$ with $|p|<2$ such that $|p^2-4q| = |3+2\zeta_6|$.

The above discussion completes the proof of Theorem 6. □

Theorem 7: Among all the two-layer Gaussian and Eisenstein quadratic space-time block codes, $X\left(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_{12}\right)$ is the optimal full-rate quadratic space-time block code with minimal determinant 1 in terms of the diversity product criterion, where $p=-1-\zeta_6$, $q=\sqrt{3}i$.

Proof: To prove this theorem, by Lemma 1, we only need to compare the diversity product of the optimal two-layer Gaussian quadratic space-time block code $X\left(\mathbb{Q}(\zeta_4), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, \sqrt{1+i}\right)$ designed by Theorem 5 with that of the optimal two-layer Eisenstein quadratic space-time block code $X\left(\mathbb{Q}(\zeta_3), \frac{1+\zeta_6+\sqrt{(1+\zeta_6)^2-4\sqrt{3}i}}{2}, \frac{1+\zeta_6+\sqrt{(1-\zeta_6)^2-4\sqrt{3}i}}{2}, \zeta_{12}\right)$ designed by Theorem 6. Since the minimal determinants of both codes are 1, by Lemma 1 we only need to compare the determinants of their generating matrices. On one hand, the determinant of the generating matrix of the code $X\left(\mathbb{Q}(\zeta_3), \frac{1+\zeta_6+\sqrt{(1+\zeta_6)^2-4\sqrt{3}i}}{2}, \frac{1+\zeta_6+\sqrt{(1-\zeta_6)^2-4\sqrt{3}i}}{2}, \zeta_{12}\right)$ is given by

$$\begin{aligned}&|\det(G_{\text{opt}-\text{Eisenstein}})\det(\Lambda_{\zeta_3})^2\\ &= |\zeta_{12}^2((1+\zeta_6)^2-4\sqrt{3}i)\det(\Lambda_{\zeta_3})^2|\\ &= |(1+\zeta_6)^2-4\sqrt{3}i)|\frac{3}{4} < 3.44\end{aligned}$$

where $\det(\Lambda_{\zeta_3}) = \frac{\sqrt{3}}{2}$. On the other hand, the determinant of the generating matrix of the code $X\left(\mathbb{Q}(\zeta_4), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, \sqrt{1+i}\right)$ is given by

$$\begin{aligned}&|\det(G_{\text{opt}-\text{Gaussian}})\det(\Lambda_{\zeta_4})^2|\\ &= |(1+i)3\det(\Lambda_{\zeta_4})^2| = 3\sqrt{2} > 4.24\end{aligned}$$

where $\det(\Lambda_{\zeta_4}) = 1$. Therefore, we have

$$\begin{aligned}&|\det(G_{\text{opt}-\text{Gaussian}})\det(\Lambda_{\zeta_4})^2|\\ &> |\det(G_{\text{opt}-\text{Eisenstein}})\det(\Lambda_{\zeta_3})^2|\end{aligned}$$

and thus, the code $X\left(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_{12}\right)$ with $p=-1-\zeta_6$, $q=\sqrt{3}i$ is the optimal among all the two-layer Gaussian and Eisenstein full-rate quadratic space-time block codes. This completes the proof of Theorem 7. □

The following two comments on Theorems 5 and 6 are in order.

1) Since $\left|\frac{-p+\sqrt{p^2-4q}}{2}\right| \neq 1$ and $\left|\frac{-p-\sqrt{p^2-4q}}{2}\right| \neq 1$, the code $X\left(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_6\right)$ given in Theorem 6 is not a cyclotomic code. However, it was proven in [20] that the code $X\left(\mathbb{Q}(\zeta_4), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, \sqrt{1+i}\right)$ in Theorem 5 is the optimal cyclotomic space-time block code. In addition, Theorem 7 shows us that the cyclotomic space-time block code does not enable the optimality of the quadratic space-time block codes. In addition, in the optimal cyclotomic space-time code $X\left(\mathbb{Q}(\zeta_4), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, \sqrt{1+i}\right)$, since $|\rho| = |\sqrt{1+i}| > 1$, the average power in different layers is different. However, in the optimal quadratic space-time block code $X\left(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_{12}\right)$, since $|\rho| = |\zeta_{12}| = 1$, the average power in different layers is the same, thus resulting in a low peak-to-average power ratio.

2) The golden code proposed in [19] is another space-time block code for two-transmitter antennas with full rate, high diversity product, nonvanishing minimal determinant, and the same average power at different layers. In addition, the minimal determinant of the golden code is $d_{\min}(\text{golden code}) = 1$ and the determinant of the generating matrix of the golden code is

$$\begin{aligned}&|\det(G_{\text{golden}})\det(\Lambda_{\zeta_4})^2| = 5 > 3.44\\ &> |\det(G_{\text{opt}-\text{Eisenstein}})\det(\Lambda_{\zeta_3})^2|.\end{aligned} \tag{35}$$

Therefore, in terms of the diversity product criterion, the optimal full-rate quadratic space-time block code is better than the golden code.

V. Simulation Results

In this section, we perform computer simulations and examine the error performance of the optimal quadratic space-time block code proposed in this paper and the golden code [19] for a 2-by-2 MIMO system with flat Rayleigh fading. The codewords used are the Golden space-time code proposed in [19] and the optimal quadratic space-time code $X\left(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_{12}\right)$ with $p=-1-\zeta_6$, $q=\sqrt{3}i$ proposed in this paper. The transmission bit rate of the codes in this simulation is 3 bits per Hz, per channel use, i.e., 2^6 codewords are used. These 2^6 codewords are chosen based

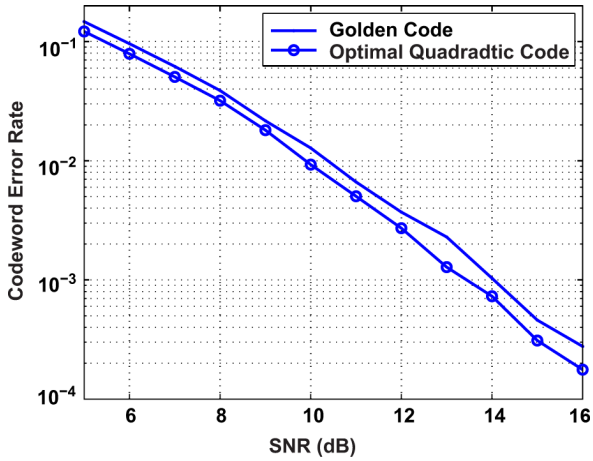

Fig. 1. Error performance comparison of the optimal quadratic space-time block code and the golden code.

on the diversity product criterion proposed in [20] or Lemma 1. The simulation result shows that the codeword error rate of the optimal quadratic space-time block code is superior to that of the golden code with about 0.5 dB gain. The reason is that the diversity product of optimal quadratic space-time block code is larger than that of the golden code, which is explained by (35).

VI. Conclusion

[1]In this paper, we have considered the systemic design of nonvanishing determinant space-time block codes for the two-transmitter antennas. A novel coding scheme has been proposed based on quadratic field extensions. Using the diversity product as a design criterion, we have attained the optimal space-time block code and shown that the diversity product of the optimal quadratic space-time block code is larger than the best-known full-rate space-time block codes such as the golden and optimal cyclotomic space-time block codes for the two-transmitter antennas. In addition, like the golden space-time block code, the optimal full-rate (two layers) quadratic space-time block code has the property that the average powers at different layers are the same, therefore, resulting in a low peak-to-average power ratio. However, we must point out that a major difference between the proposed optimal quadratic space-time block code and the golden code is that the golden code is unitary and, thus, information lossless.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[1]During the course of this paper revision, quite a few of good nonvanishing determinant space-time block code designs based on algebraic number theory, cyclic division algebra, and Hasse invariants from class field theory have been developed. For example, see [31]–[35].

[5] 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.

[6] M. O. Damen and N. C. Beaulieu, "On two high-rate algebraic space-time codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 1059–1063, Apr. 2003.

[7] H. El Gamal and M. O. Damen, "Universal space-time coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1097–1119, May 2003.

[8] 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.

[9] S. Galliou and J. C. Belfiore, "A new family of full rate, fully diversity space-time codes based on Galois theory," in *Proc. Int. Symp. Inf. Theory*, Lausanne, Switzerland, Jul. 5, 2002, p. 419.

[10] 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.

[11] 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.

[12] G. Wang, H. Liao, H. Wang, and X.-G. Xia, "Systematic and optimal cyclotomic space-time code designs based on high dimensional lattices," in *Proc. Globecom*, San Francisco, CA, Dec. 1–5, 2003, pp. 631–635.

[13] 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.

[14] 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.

[15] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1473–1484, Jun. 2002.

[16] R. W. Heath and A. J. Paulraj, "Linear dispersion codes for MIMO systems based on frame theory," *IEEE Trans. Signal Processing*, vol. 50, no. 10, pp. 2429–2441, Oct. 2002.

[17] H. Yao and G. W. Wornell, "Achieving the full MIMO diversity-multiplexing frontier with rotation-based space-time codes," in *Proc. Allerton Conf. Commun., Cont., and Computing*, IL, Oct. 2003, pp. 400–409.

[18] J. C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," in *Proc. Inf. Theory Workshop*, Paris, France, Mar. 2003, pp. 267–270.

[19] J. C. Belfiore, G. Pekaya, and E. Viterbo, "The Golden Coden: A 2×2 full rate space-time code with nonvanishing determinants," in *Proc. Int. Symp. Information Theory*, Jun. 2004, pp. 310–313.

[20] G. Wang and X.-. G. Xia, "On optimal multi-layer cyclotomic space-time code designs," in *Proc. Int. Symp. Inf. Theory*, Jun. 2004, pp. 318–322.

[21] 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. 1999, pp. 136–140.

[22] 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.

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

[24] 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.

[25] A. A. Albert, *Structure of Algebras*. Providence, RI: AMS Colloqium Pub., 1961, vol. 24.

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

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

[28] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, 3rd ed. Natick, MA: A. K. Peters, 2002.

[29] R. A. Mollin, *Algebraic Number Theory*. London: Chapman & Hall/CRC, 1999.

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

[31] 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. Inf. Theory*, vol. 52, no. 9, pp. 3869–3884, Sep. 2006.

[32] F. E. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space-time block codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3885–3902, Sep. 2006.
[33] C.-P. Xing, "Diagonal lattice space-time codes from number fields and asymptotic bounds," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, Nov. 2007.
[34] J. Lahtonen and R. Vehkalahti, "Dense MIMO matrix lattices—A meeting point for class field theory and invariant theory," in *Proc. 17th Symp. Applied algebra, Algebraic algorithms and Error Correcting Codes*, Dec. 16–20, 2007, pp. 247–256.
[35] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "Optimal matrix lattices for MIMO codes from division algebras," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 9–14, 2006, pp. 783–787.

Genyuan Wang received the B.Sc. and M.S. degrees in Mathematics from Shaanxi Normal University, Xi'an, China, in 1985 and 1988, respectively, and his Ph.D. degree in Electrical Engineering from Xidian University, Xi'an, in 1998. From July 1988 to September 1994, he worked at Shaanxi Normal University as an Assistant Professor and then as an Associate Professor. From September 1994 to May 1998, he worked at Xidian University as a Research Assistant. From June 1988 to December 2003, he was a Postdoctoral Fellow at the Department of Electrical and Computer Engineering, University of Delaware. From January 2004 to April 2006, he was a Research Associate at the Center for Advanced Communications, Villanova University. From May 2006 to September 2011, he worked with Cisco Systems as a Senior System Engineer. Since October 2011, he has been with Ruckus Wireless as a Senior System Engineer. He is a recipient of the paper which received the IEEE Signal Processing Society Best Award in 2009. His research interests are radar imaging and radar signal processing, adaptive filter, OFDM system, channel equalization, and space-time coding.

Jian-Kang Zhang (M'04–SM'11) received the B.S. degree in Information Science (Math.) from Shaanxi Normal University, Xi'an, China, the M.S. degree in Information and Computational Science (Math.) from Northwest University, Xi'an, and the Ph.D. degree in Electrical Engineering from Xidian University, Xi'an, in 1983, 1988, and 1999, respectively.

He is now an Assistant Professor in the Department of Electrical and Computer Engineering at McMaster University, Hamilton, ON, Canada. He has hold research positions in McMaster University and Harvard University. He is the co-author of the paper which received the "IEEE Signal Processing Society Best Young Author Award" in 2008. He is currently serving as an Associate Editor for the IEEE SIGNAL PROCESSING LETTERS and the *Journal of Electrical and Computer Engineering*.

His research interests include multirate filterbanks, wavelet and multiwavelet transforms and their applications, number theory transform and their applications in signal processing. His current research focuses on random matrices, channel capacity, and coherent and noncoherent MIMO communication systems.

Moeness Amin (F'01) received his Ph.D. degree in 1984 from University of Colorado in Electrical Engineering. He has been on the Faculty of the Department of Electrical and Computer Engineering at Villanova University since 1985. In 2002, he became the Director of the Center for Advanced Communications, College of Engineering.

Dr. Amin is the Recipient of the 2009 Individual Technical Achievement Award from the European Association of Signal Processing, and the Recipient of the 2010 NATO Scientific Achievement Award. He is a Fellow of the Institute of Electrical and Electronics Engineers (IEEE), 2001; Fellow of the International Society of Optical Engineering, 2007; and a Fellow of the Institute of Engineering and Technology (IET), 2010. Dr. Amin is a Recipient of the IEEE Third Millennium Medal, 2000; Recipient of the Chief of Naval Research Challenge Award, 2010; Distinguished Lecturer of the IEEE Signal Processing Society, 2003–2004; Member of the Franklin Institute Committee on Science and the Arts; Recipient Villanova University Outstanding Faculty Research Award, 1997; and the Recipient of the IEEE Philadelphia Section Award, 1997. He is a member of the SPIE, EURASIP, ION, Eta Kappa Nu, Sigma Xi, and Phi Kappa Phi.

Dr. Amin has over 500 journal and conference publications in the areas of Wireless Communications, Time-Frequency Analysis, Smart Antennas, Waveform Design and Diversity, Interference Cancellation in Broadband Communication Platforms, Anti-Jam GPS, Target Localization and Tracking, Direction Finding, Channel Diversity and Equalization, Ultrasound Imaging and Radar Signal Processing. He is a recipient of seven best paper awards.

Dr. Amin currently serves on the Overview Board of the IEEE TRANSACTIONS ON SIGNAL PROCESSING. He also serves on the Editorial Board of the IEEE SIGNAL PROCESSING MAGAZINE and the EURASIP *Signal Processing Journal*. He was a Plenary Speaker at ICASSP 2010. Dr. Amin was the Special Session Co-Chair of the 2008 IEEE International Conference on Acoustics, Speech, and Signal Processing. He was the Technical Program Chair of the 2nd IEEE International Symposium on Signal Processing and Information Technology, 2002. Dr. Amin was the General and Organization Chair of the IEEE Workshop on Statistical Signal and Array Processing, 2000. He was the General and Organization Chair of the IEEE International Symposium on Time-Frequency and Time-Scale Analysis, 1994. He was an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING during 1996–1998. He was a member of the IEEE Signal Processing Society Technical Committee on Signal Processing for Communications during 1998–2002. He was a Member of the IEEE Signal Processing Society Technical Committee on Statistical Signal and Array Processing during 1995–1997. He has given several keynote and plenary talks, and served as a Session Chair in several technical meetings. Dr. Amin organized five Workshops for the Franklin Institute Medal Program.