An Elementary Condition for Non-Norm Elements

Xiaoyong Guo and Xiang-Gen Xia, *Fellow, IEEE*

***Abstract*—Cyclic division algebra (CDA) has recently become a major technique to construct space–time block codes with nonvanishing determinant (NVD). One of the key steps in this technique is the determination of non-norm elements and a sufficient condition for the determination has been given by Kiran and Rajan lately based on algebraic number theory. In this paper, based on Kiran and Rajan's condition, we present a more elementary condition for non-norm elements when signals are QAM or HEX, which is easier to check. With this elementary condition, non-norm elements with smaller absolute values than the existing ones can be found.**

***Index Terms*—Algebraic number theory, cyclic division algebra, non-norm elements, nonvanishing determinant, space–time block codes.**

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]. Systematic methods to construct STBC with NVD have been presented in [5], [6], [8], [11] based on cyclic division algebra (CDA). In these constructions, one of the key steps is the non-norm element determination and a sufficient condition for a non-norm element has been obtained by Kiran and Rajan in [5] based on algebraic number theory.

In this paper, based on Kiran and Rajan's sufficient condition, we present a more elementary condition for non-norm elements γ, when signals are QAM, i.e., in $\mathbb{Z}[\mathbf{i}]$, where $\mathbf{i} = \sqrt{-1}$, or HEX, i.e., $\mathbb{Z}[\mathbf{j}]$, where $\mathbf{j} = \exp(\frac{\mathbf{i}\pi}{3})$, which is easier to check so that smaller absolute valued non-norm elements than the existing ones can be found. For example, in [6], the non-norm element γ with the smallest absolute value is $2+\mathbf{i}$, while if our newly proposed condition is used, we may show that in many cases, $1+\mathbf{i}$ is also a non-norm element. Since the absolute value of a non-norm element γ may affect the mean signal power and the smaller the absolute value of γ is, the less the mean signal power usually is, non-norm elements with smaller absolute values may be desired. Using simulations, it is illustrated that the STBC with our newly determined non-norm elements indeed perform better than those in [6].

Manuscript received December 12, 2006; revised November 22, 2008. Current version published February 25, 2009. Their work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant FA9550-08-1-0219 and the National Science Foundation under Grant CCR-0325180.

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

Communicated by S. W. McLaughlin, Associate Editor for Coding Techniques.

Color version of Figure 1 is available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2008.2011444

This paper is organized as follows. In Section II, we briefly describe/recall a general construction of full rate NVD STBC based on the CDA approach. In Section III, we present an elementary sufficient condition on non-norm elements γ. In Section IV, we compare the codes with new non-norm elements with the codes proposed in [6]. Throughout this paper, we use $\mathbb{Z}$ and $\mathbb{Q}$ to denote the integer ring and the rational field, respectively.

II. STBC Based on Cyclic Division Algebra

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

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

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

$$M=\begin{bmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & \cdots & \gamma\sigma^{n-1}(x_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \cdots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{bmatrix} \quad (1)$$

where $x_l \in \mathbb{L}, l = 0,1,\ldots,n-1$. 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 $x \in \mathbb{L}$, for $l = 1,2,\ldots,n-1$, 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 the norm condition is said to be a *non-norm element* [16], [17]. We always have $\det(M) \in \mathbb{F}$ and a concise proof is given in [6]. We also have that $\det(M) = 0$ if and only if $x_l = 0$ for all l, i.e., code $\{M\}$ has full diversity. If we choose $\mathbb{F} = \mathbb{Q}(\mathbf{i})$ and $x_l, l = 0,1,\ldots,n-1$, to be algebraic integers in $\mathbb{L}$ with $\prod_{l=0}^{n-1} x_l \neq 0$, and we choose a $\gamma \in \mathbb{Z}[\mathbf{i}]$ which satisfies the norm condition, then $\det(M)$ is clearly a nonzero algebraic integer in $\mathbb{Q}(\mathbf{i})$, i.e., $\det(M) \in \mathbb{Z}[\mathbf{i}]\backslash\{0\}$. Therefore, we have $|\det(M)| \geq 1$. This division algebra property gives us a way to construct NVD STBC [5], [6]. Let $e_l \in \mathcal{O}_{\mathbb{L}}, l = 0,1,\ldots,n-1$, be a relative integer basis of $\mathbb{L}/\mathbb{Q}(\mathbf{i})$, where $\mathcal{O}_{\mathbb{L}}$ is the integer ring of the field $\mathbb{L}$, and let x_l in (1) be

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

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 M, and the resulting STBC is a rate-n (full rate) NVD code.

III. Design of Non-Norm Elements γ

In this section, we discuss how to find a non-norm element γ of a cyclic extension $\mathbb{L}/\mathbb{Q}(\mathbf{i})$. Although the following discussions are for the case when the cyclic extension $\mathbb{L}$ over $\mathbb{Q}(\mathbf{i})$ is a composition of a real cyclic extension $\mathbb{K}$ over $\mathbb{Q}$ and the field $\mathbb{Q}(\mathbf{i})$, i.e., $\mathbb{L} = \mathbb{K}(\mathbf{i})$, (note that all the cyclic extensions $\mathbb{L}$ over $\mathbb{Q}(\mathbf{i})$ constructed in [6] belong to this case), they can be easily generalized to $\mathbb{Q}(\mathbf{j})$ if $\mathbf{i}$ is replaced by $\mathbf{j}$.

We first present a theorem below.

Theorem 1: 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 $\mathbb{Q}(\mathbf{i})$. Let p be a prime in $\mathbb{Z}$ and $p\mathcal{O}_\mathbb{K}$ remain prime in $\mathcal{O}_\mathbb{K}$. Then

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

In order to prove the above theorem, let us introduce the following theorem by Kiran and Rajan.

Theorem 2 (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 $\mathfrak{p}\backslash\mathfrak{p}^2$, then $\gamma^j \notin N_{\mathbb{L}/\mathbb{F}}(\mathbb{L})$ for any $j = 1, 2, \ldots, f-1$.

Let $\mathbb{F} = \mathbb{Q}(\mathbf{i})$. We know that $\mathcal{O}_{\mathbb{Q}(\mathbf{i})} = \mathbb{Z}[\mathbf{i}]$ is a principal ideal domain. Thus, every prime ideal in $\mathbb{Z}[\mathbf{i}]$ can be written as $\langle p \rangle$ for some prime p in $\mathbb{Z}[\mathbf{i}]$. Let $\langle p \rangle$ be a prime ideal in $\mathbb{Z}[\mathbf{i}]$ 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 $p \in \langle p \rangle \backslash \langle p \rangle^2$, according to Theorem 2, $p^j \notin N_{\mathbb{L}/\mathbb{Q}(\mathbf{i})}(\mathbb{L}), j = 1, 2, \ldots, n-1$, namely, p is a non-norm element in $\mathbb{L}/\mathbb{Q}(\mathbf{i})$. This leads to the following lemma, which will be used in the Proof of Theorem 1.

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

Now we give a Proof of Theorem 1.

Proof: Since $p\mathcal{O}_\mathbb{K}$ is a prime ideal, we have $f(p\mathcal{O}_\mathbb{K}/\langle p \rangle) = n$. Due to the fact that $m_\alpha(x)$ is irreducible in $\mathbb{Q}(\mathbf{i})$, we have $[\mathbb{K}(\mathbf{i}) : \mathbb{Q}(\mathbf{i})] = n$. Since

$$\begin{aligned}[\mathbb{K}(\mathbf{i}) : \mathbb{Q}] &= [\mathbb{K}(\mathbf{i}) : \mathbb{Q}(\mathbf{i})][\mathbb{Q}(\mathbf{i}) : \mathbb{Q}] \\ &= [\mathbb{K}(\mathbf{i}) : \mathbb{K}][\mathbb{K} : \mathbb{Q}], \end{aligned} \tag{3}$$

we obtain $[\mathbb{K}(\mathbf{i}) : \mathbb{K}] = 2$. Let $\mathfrak{P}_1$ be the prime ideal above $\langle p \rangle$ in $\mathbb{Q}(\mathbf{i})$, let $\mathcal{P}$ be the prime ideal above $\langle p \rangle$ in $\mathbb{K}(\mathbf{i})$. Let $f(\mathfrak{P}_1/\langle p \rangle) = c$, $f(\mathcal{P}/\mathfrak{P}_1) = b$, $f(\mathcal{P}/p\mathcal{O}_\mathbb{K}) = a$. The following diagram shows the relationship of these fields, prime ideals and the corresponding extension degrees and inertial degrees:

$$\begin{tikzcd}
\mathbb{K}(\mathbf{i}) \arrow[r, phantom, "\supset"] & \mathcal{P} \\
\mathbb{Q}(\mathbf{i}) \arrow[u, "n"'] \arrow[r, phantom, "\supset"] & \mathfrak{P}_1 \arrow[u, "b"] \\
\mathbb{Q} \arrow[u, "2"'] \arrow[r, phantom, "\supset"] & \langle p \rangle \arrow[u, "c"]
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{P} \arrow[r, phantom, "\subset"] & \mathbb{K}(\mathbf{i}) \\
p\mathcal{O}_\mathbb{K} \arrow[u, "a"'] \arrow[r, phantom, "\subset"] & \mathbb{K} \arrow[u, "2"] \\
\langle p \rangle \arrow[u, "n"'] \arrow[r, phantom, "\subset"] & \mathbb{Q} \arrow[u, "n"]
\end{tikzcd}$$

Since inertial degree is multiplicative in tower [18], we must have

$$\begin{aligned} f(\mathcal{P}/\langle p \rangle) &= f(\mathcal{P}/\mathfrak{P}_1) f(\mathfrak{P}_1/\langle p \rangle) \\ &= f(\mathcal{P}/p\mathcal{O}_\mathbb{K}) f(p\mathcal{O}_\mathbb{K}/\langle p \rangle) \end{aligned} \tag{4}$$

i.e.,

$$na = bc \tag{5}$$

and since inertial degree must be smaller than or equal to the extension degree, we also have

$$a \le [\mathbb{K}(\mathbf{i}) : \mathbb{K}] = 2, \quad b \le [\mathbb{K}(\mathbf{i}) : \mathbb{Q}(\mathbf{i})] = n. \tag{6}$$

For the case when p remains prime in $\mathbb{Z}[\mathbf{i}]$ and n is odd, $\mathfrak{P}_1 = p\mathbb{Z}[\mathbf{i}] = \langle p \rangle$. $c = f(\mathfrak{P}_1/\langle p \rangle) = [\mathbb{Q}(\mathbf{i}) : \mathbb{Q}] = 2$. Since n is an odd number, by (6) and (5), $a = 2, f(\mathcal{P}/p\mathcal{O}_\mathbb{K}) = b = n$, i.e., $p\mathcal{O}_{\mathbb{K}(\mathbf{i})} = \mathcal{P}$ remains prime in $\mathbb{K}(\mathbf{i})$. According to Lemma 1, we have $p^j \notin N_{\mathbb{K}/\mathbb{Q}}(\mathbb{K}), j = 1, 2, \ldots, n-1$, i.e., p is a non-norm element in $\mathbb{K}(\mathbf{i})/\mathbb{Q}(\mathbf{i})$.

If p is reducible in $\mathbb{Z}[\mathbf{i}]$, according to the algebraic number theory, p can be factorized as $p = p_o p_o^*$, and p_o is a prime in $\mathbb{Z}[\mathbf{i}]$. In this case $\mathfrak{P}_1 = \langle p_o \rangle$ or $\mathfrak{P}_1 = \langle p_o^* \rangle$. Without loss of generality, we assume $\mathfrak{P}_1 = \langle p_o \rangle$. Since $p = p_o p_o^*$, the inertial degree $c = f(\mathfrak{P}_1/p) = 1$. The only solution for a, b satisfying both (5) and (6) is $a = 1, b = f(\mathcal{P}/\langle p_o \rangle) = n$. i.e., $p_o\mathcal{O}_{\mathbb{K}(\mathbf{i})} = \mathcal{P}$ remains prime in $\mathbb{K}(\mathbf{i})$. Thus, by Lemma 1, $p_o^j \notin N_{\mathbb{K}(\mathbf{i})/\mathbb{Q}(\mathbf{i})}(\mathbb{K}(\mathbf{i})), j = 1, 2, \ldots, n-1$, i.e., p_o is a non-norm element in $\mathbb{K}(\mathbf{i})/\mathbb{Q}(\mathbf{i})$. ■

In order to use Theorem 1 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* [19], which tells us the relationship between the factorization of $\mathfrak{p}\mathcal{O}_\mathbb{L}$ 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 3 (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:

$$m_\alpha(x) = \prod_{j=1}^{g} m_j^{e_j}(x) \tag{7}$$

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

$$\mathfrak{p}\mathcal{O}_\mathbb{L} = \prod_{j=1}^{g} \mathfrak{p}_j^{e_j} \tag{8}$$

where $\mathfrak{p}_j = \langle \mathfrak{p}, m_j(\alpha) \rangle$.We next only consider the case when $\mathbb{F} = \mathbb{Q}$. As a consequence of the *prime ideal factorization theorem*, we have the following corollary.

TABLE I
NON-NORM ELEMENTS γ FOR SIGNALS IN $\mathbb{Z}[\mathbf{i}]$

n	Cyclotomic Field	Minimal Polynomial $m_\alpha(x)$	$\mathrm{disc}(m_\alpha(x))$	γ	
				new	in [6]
2	$\mathbb{Q}(\omega_8)$	x^2-2	8	$2+\mathbf{i}$	$2+\mathbf{i}$
3	$\mathbb{Q}(\omega_7)$	x^3+x^2-2x-1	49	$1+\mathbf{i}$	$2+\mathbf{i}$
4	$\mathbb{Q}(\omega_{16})$	x^4-4x^2+2	2048	$2+\mathbf{i}$	$2+\mathbf{i}$
4	$\mathbb{Q}(\omega_5)$	$x^4+x^3+x^2+x+1$	125	$1+\mathbf{i}$	-
5	$\mathbb{Q}(\omega_{11})$	$x^5+x^4-4x^3-3x^2+3x+1$	11^4	$1+\mathbf{i}$	$3+2\mathbf{i}$
6	$\mathbb{Q}(\omega_{13})$	x^6+x^3+1	-3^9	$1+\mathbf{i}$	-
7	$\mathbb{Q}(\omega_{29})$	$x^7+x^6-12x^5-7x^4$ $+28x^3+14x^2-9x+1$	$17^2\cdot 29^6$	$1+\mathbf{i}$	$6+\mathbf{i}$
8	$\mathbb{Q}(\omega_{32})$	$x^8+8x^6+20x^4+16x^2+2$	2^{31}	$2+\mathbf{i}$	$2+\mathbf{i}$
9	$\mathbb{Q}(\omega_{19})$	$x^9+x^8-8x^7-7x^6+21x^5$ $+15x^4-20x^3-10x^2+5x+1$	19^8	$1+\mathbf{i}$	$5+2\mathbf{i}$
10	$\mathbb{Q}(\omega_{11})$	$x^{10}+x^9+x^8+x^7+x^6+x^5$ $+x^4+x^3+x^2+x+1$	-11^9	$1+\mathbf{i}$	-
11	$\mathbb{Q}(\omega_{23})$	$x^{11}+x^{10}-10x^9-9x^8$ $+36x^7+28x^6-56x^5-35x^4$ $+35x^3+15x^2-6x-1$	23^{10}	$1+\mathbf{i}$	$2+\mathbf{i}$
12	$\mathbb{Q}(\omega_{13})$	$x^{12}+x^{11}+x^{10}+x^9+x^8$ $+x^7+x^6+x^5+x^4+x^3$ $+x^2+x+1$	11^{13}	$1+\mathbf{i}$	-
13	$\mathbb{Q}(\omega_{53})$	$x^{13}+x^{12}-24x^{11}-19x^{10}$ $+190x^9+116x^8-601x^7-246x^6$ $+738x^5+215x^4-291x^3$ $-68x^2+10x+1$	$23^4\cdot 53^{12}$ $\cdot 83^2\cdot 317^2$ $\cdot 719^2$	$1+\mathbf{i}$	$2+\mathbf{i}$
14	$\mathbb{Q}(\omega_{29})$	$x^{14}+x^{13}-13x^{12}-12x^{11}+66x^{10}$ $+55x^9-165x^8-120x^7+210x^6$ $+126x^5-126x^4-56x^3$ $+28x^2+7x-1$	23^9	$1+\mathbf{i}$	-
15	$\mathbb{Q}(\omega_{31})$	$x^{15}+x^{14}-28x^{13}-23x^{12}$ $+276x^{11}+182x^{10}-1193x^9$ $-592x^8+2307x^7+956x^6-1721x^5$ $-908x^4+316x^3+262x^2+42x+1$	$11^{14}\cdot 61^{14}$ $\cdot 599^2$	$1+\mathbf{i}$	$7+2\mathbf{i}$
16	$\mathbb{Q}(\omega_{64})$	$x^{16}+16x^{14}+104x^{12}+352x^{10}$ $+660x^8+672x^6+336x^4+64x^2+2$	2^{79}	$2+\mathbf{i}$	$2+\mathbf{i}$
17	$\mathbb{Q}(\omega_{103})$	$x^{17}+x^{16}-48x^{15}-105x^{14}+763x^{13}$ $+2579x^{12}-3653x^{11}-23311x^{10}$ $-11031x^9+74838x^8+107759x^7$ $-50288x^6-198615x^5-102976x^4$ $+58507x^3+75722x^2+25763x+2837$	$47^4\cdot 103^{16}$ $\cdot 149^4\cdot 983^2$ $\cdot 2677^2\cdot 5413^2$	$1+\mathbf{i}$	$2+\mathbf{i}$
18	$\mathbb{Q}(\omega_{19})$	$x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}$ $+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7$ $+x^6+x^5+x^4+x^3+x^2+x+1$	-19^{17}	$1+\mathbf{i}$	-
19	$\mathbb{Q}(\omega_{191})$	$x^{19}+x^{18}-90x^{17}-57x^{16}+3044x^{15}$ $+1124x^{14}-51184x^{13}-4822x^{12}$ $+474003x^{11}-90110x^{10}-2465084x^9$ $+1153239x^8+6854098x^7$ $-5023125x^6-8711114x^5$ $+8950277x^4+2600136x^3$ $-5125792x^2+1553447x-117649$	$7^{52}\cdot 109^2$ $\cdot 191^{18}\cdot 383^2$ $\cdot 389^2\cdot 421^2$ $\cdot 431^2\cdot 491^2$ $\cdot 1567^2\cdot 9161^2$ $\cdot 6883^2\cdot 1801^2$	$1+\mathbf{i}$	$5+2\mathbf{i}$
20	$\mathbb{Q}(\omega_{25})$	$x^{20}+x^{15}+x^{10}+x^5+1$	5^{35}	$1+\mathbf{i}$	-

Corollary 1: 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 $\mathcal{O}_\mathbb{Q}=\mathbb{Z}$, which cannot divide $\mathrm{disc}(m_\alpha(x))$. 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, $\mathrm{disc}(m_\alpha(x))$ is the discriminant of the minimal polynomial $m_\alpha(x)$ [20]. Write $m_\alpha(x)=\prod(x-r_i)$, then $\mathrm{disc}(m_\alpha(x))$ is defined as

$$\mathrm{disc}(m_\alpha(x))=\prod_{i<j}(r_i-r_j)^2. \quad (9)$$

Proof: From algebraic number theory, we know $|\mathcal{O}_\mathbb{K}/\mathcal{O}_\mathbb{Q}[\alpha]|^2=|\mathrm{disc}(m_\alpha(x))/\mathrm{disc}(\mathbb{K})|$ [21], where $\mathrm{disc}(\mathbb{K})$ is the discriminant of the field $\mathbb{K}$. If p is not a factor of $\mathrm{disc}(m_\alpha(x))$, then p cannot divide $|\mathcal{O}_\mathbb{K}/\mathcal{O}_\mathbb{Q}[\alpha]|$. By Theorem 3, 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 1 and Theorem 1, we immediately have the following theorem on a sufficient condition for a non-norm element, which is more elementary and easier to understand than the existing ones.

Theorem 4: 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 $\mathbb{Q}(\mathbf{i})$. Let p be a prime in $\mathbb{Z}$, which cannot divide $\mathrm{disc}(m_\alpha(x))$. If $m_\alpha(x)$ is irreducible over $\mathbb{Z}/\langle p\rangle$, then

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

Although all the above discussions are based on the QAM signals in $\mathbb{Z}[\mathbf{i}]$, the result in Theorem 1 holds when $\mathbf{i}$ is replaced by $\mathbf{j}$, i.e., for HEX signals in $\mathbb{Z}[\mathbf{j}]$. In fact, from the proof of Theorem 1, one can see that if $\mathbf{i}$ is replaced by β where β satisfies two conditions: $\mathbb{Q}(\beta)$ is a degree-2 field extension over $\mathbb{Q}$ and $\mathbb{Z}(\beta)$ is a principal ideal domain (when $\beta = \mathbf{j}$, these two conditions are certainly satisfied), then the above theorem holds.

In Table I, we list non-norm elements from $n_t = 2$ to $n_t = 20$, where the second column indicates the cyclotomic fields which contain the real cyclic extensions. We use ω_k to denote the k-th root of unity, i.e., $\omega_k \triangleq \exp(2\mathbf{i}\pi/k)$. Most of the resulting cyclic extensions $\mathbb{L}$ over $\mathbb{Q}(\mathbf{i})$ are the same as in [6] as listed in Table I except for $n = 6, 10, 12, 14, 18, 20$ and the second example of $n = 4$ case.

For $n = 2$, $\mathbb{L} = \mathbb{Q}(\exp(\mathbf{i}\pi/4))$, so $\mathbb{K} = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{2}$. The minimal polynomial for α is $m_\alpha(x) = x^2 - 2$. $m_\alpha(x) = x^2 - 2$ is irreducible over the finite field $\mathbb{Z}/\langle 5\rangle$, and $\mathrm{disc}(m_\alpha(x)) = 8$, since 5 is not a factor of 8. By applying the second case in Theorem 4, we know that $2 + \mathbf{i}$ is a non-norm element.

For $n = 3$, $\mathbb{L} = \mathbb{Q}(\mathbf{i}, \cos(2\pi/7))$, $\mathbb{K} = \mathbb{Q}(\cos(2\pi/7))$, the minimal polynomial for α is $m_\alpha(x) = x^3 + x^2 - 2x - 1$, and $\mathrm{disc}(m_\alpha(x)) = 49$. $m_\alpha(x)$ is irreducible over the finite field $\mathbb{Z}/\langle 2\rangle$. Noting that 2 is not a factor of 49, by Theorem 4, $1 + \mathbf{i}$ is a non-norm element. By a similar procedure we can also show that $2 + \mathbf{i}$ is a non-norm element since 5 cannot divide 49 too.

For the remaining of the non-norm γ in Table I, we briefly discuss as follows. For the second example of $n = 4$ and $n = 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20$, the discriminants of the minimal polynomials are all odd numbers, see Table I, 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 4, we conclude that $\gamma = 1 + \mathbf{i}$ satisfies the norm condition for all these cases.

For the first example of $n = 4$ and $n = 8, 16$, 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 4, $\gamma = 2 + \mathbf{i}$ is a non-norm element for these three cases.

Note that the last column in Table I has some of the non-norm elements presented in [6] and the empty spaces mean that the cyclotomic fields in the corresponding rows in Table I are different from those in [6].

IV. Comparison With an Existing Code

In this section, 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

$$\zeta(\mathcal{C}) = \frac{\delta(\mathcal{C}_\infty)}{E^n}, \tag{10}$$

where $\delta(\mathcal{C}_\infty)$ is the *minimum determinant* as defined in [2], [8]. 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 M in (1) can be written as

$$M = \mathrm{diag}[Ax_0] + \mathrm{diag}[Bx_1]S_1 + \mathrm{diag}[Cx_2]S_2 \tag{11}$$

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

$$A = \begin{bmatrix} 1 & 2\cos(2\pi/7) & 2\cos(4\pi/7) \\ 1 & 2\cos(4\pi/7) & 2\cos(8\pi/7) \\ 1 & 2\cos(8\pi/7) & 2\cos(2\pi/7) \end{bmatrix} \tag{12}$$

$$B = \begin{bmatrix} 1 & 2\cos(2\pi/7) & 2\cos(4\pi/7) \\ 1 & 2\cos(4\pi/7) & 2\cos(8\pi/7) \\ 2+\mathbf{i} & (2+\mathbf{i})2\cos(8\pi/7) & (2+\mathbf{i})2\cos(2\pi/7) \end{bmatrix} \tag{13}$$

$$C = \begin{bmatrix} 1 & 2\cos(2\pi/7) & 2\cos(4\pi/7) \\ 2+\mathbf{i} & (2+\mathbf{i})2\cos(4\pi/7) & (2+\mathbf{i})2\cos(8\pi/7) \\ 2+\mathbf{i} & (2+\mathbf{i})2\cos(8\pi/7) & (2+\mathbf{i})2\cos(2\pi/7) \end{bmatrix}. \tag{14}$$

the total energy of the generator matrices of all three layers is 103.1957, the minimum determinant $\delta(\mathcal{C}_\infty) = 1$, so the normalized diversity product is $\frac{1}{103.1957^3}$.

The generator matrices of the code constructed using our method are

$$A = \begin{bmatrix} 1 & 2\cos(2\pi/7) & 2\cos(4\pi/7) \\ 1 & 2\cos(4\pi/7) & 2\cos(6\pi/7) \\ 1 & 2\cos(6\pi/7) & 2\cos(2\pi/7) \end{bmatrix} \tag{15}$$

$$B = \begin{bmatrix} 1 & 2\cos(2\pi/7) & 2\cos(4\pi/7) \\ 1 & 2\cos(4\pi/7) & 2\cos(6\pi/7) \\ 1+\mathbf{i} & (1+\mathbf{i})2\cos(6\pi/7) & (1+\mathbf{i})2\cos(2\pi/7) \end{bmatrix} \tag{16}$$

$$C = \begin{bmatrix} 1 & 2\cos(2\pi/7) & 2\cos(4\pi/7) \\ 1+\mathbf{i} & (1+\mathbf{i})2\cos(4\pi/7) & (1+\mathbf{i})2\cos(6\pi/7) \\ 1+\mathbf{i} & (1+\mathbf{i})2\cos(6\pi/7) & (1+\mathbf{i})2\cos(2\pi/7) \end{bmatrix}. \tag{17}$$

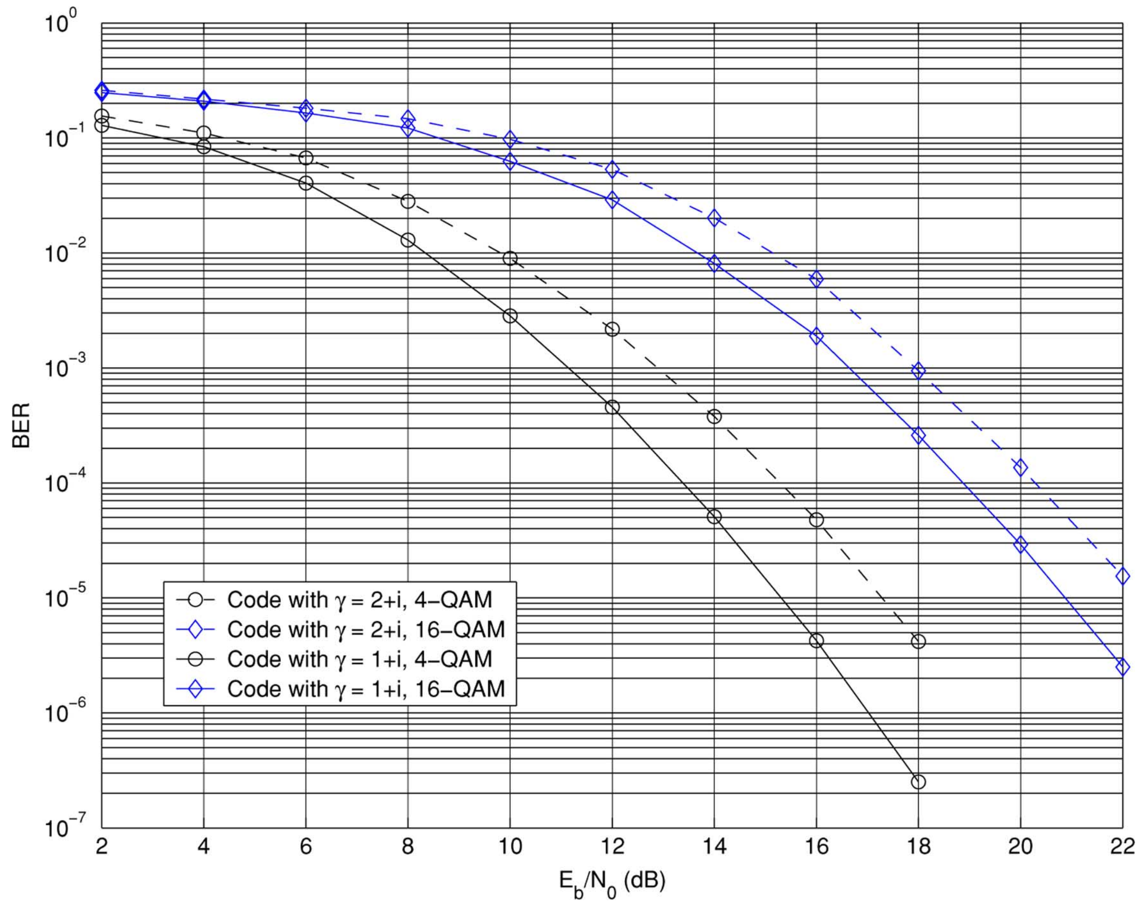

Fig. 1. Comparison of the codes with $\gamma = 2 + \mathbf{i}$ and $\gamma = 1 + \mathbf{i}$.

the total energy of the generator matrices of all three layers is 55.0489, the minimum determinant $\delta(\mathcal{C}_\infty) = 1$, so 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 a smaller absolute value than the γ presented in [6] does. The simulation results in Fig. 1 show that for 4-QAM and 16-QAM constellations, the code with $\gamma = 1 + \mathbf{i}$ is about 2 and 1.5 dB better than the code with $\gamma = 2 + \mathbf{i}$, respectively.

V. Conclusion

In this paper, we have obtained a more elementary sufficient condition for a non-norm element when signals are QAM, i.e., in $\mathbb{Z}[\mathbf{i}]$, or HEX, i.e., $\mathbb{Z}[\mathbf{j}]$. Using the newly proposed sufficient condition, non-norm elements γ with smaller absolute values than the existing ones have been found.

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*, Monticello, IL, 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. Inf. 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. Inf. 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. Inf. Theory*, vol. 51, no. 3, pp. 1102–1135, Mar. 2005.

[5] T. Kiran and B. S. Rajan, "STBC-scheme with nonvanishing determinant for certain number of transmit antennas," *IEEE Trans. Inf. 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. Inf. Theory*, vol. 52, no. 9, pp. 3869–3884, Sep. 2006.

[7] G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Algebraic 3×3, 4×4, 6×6 space-time codes with non-vanishing determinants," in *Proc. IEEE Int. Symp. Inf. Theory Its Appli.*, 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. Inf. Theory*, vol. 52, no. 9, pp. 3885–3902, Sep. 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. Acoust., Speech Signal Processing*, Philadelphia, PA, 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. Acoust., Speech Signal Processing*, Philadelphia, PA, 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," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 3853–3868, Nov. 2007.

[12] P. V. Kumar, "Achieving the D-MG and DMD tradeoffs of MIMO fading channels," in *Proc. Inf. Theory Appli. Workshop*, San Diego, CA, 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," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 569–583, Feb. 2009.

[14] H. Liao and X.-G. Xia, "Some designs of full rate space-time codes with non-vanishing determinant," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2898–2908, Aug. 2007.

[15] L. Zheng and D. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073–1096, Mar. 2003.

[16] J. H. M. Wedderburn, "A type of primitive algebra," *Trans. Amer. Math. Soc.*, vol. 15, no. 2, pp. 162–166, Apr. 1914.

[17] 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.

[18] L. C. Washington, *Introduction to Cyclotomic Fields*, ser. Graduate Texts in Mathematics, 2nd ed. New York: Springer-Verlag, 1990, vol. 83.

[19] W. Stein, A Brief Introduction to Classical and Adelic Algebraic Number Theory 2004, Lecture Notes.

[20] H. Cohen, *Resultants and Discriminants*. New York: Springer-Verlag, 1993.

[21] D. A. Marcus, *Number Fields*. New York: Springer-Verlag, Jan. 1995.

[22] J. J. Rotman, *Galois Theory*, ser. Graduate Texts in Mathematics, 4th ed. : Springer-Verlag, 1999, vol. 148.

[23] J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," in *Proc. IEEE Inf. Theory Workshop*, Paris, France, Mar. 31–Apr. 4 2003, pp. 267–270.

[24] S. Lang, *Algebraic Number Theory*, ser. Graduate Texts in Mathematics 110, 2nd ed. New York: Springer-Verlag, 1994.

[25] P. Dayal and M. K. Varanasi, "An algebraic family of complex lattices for fading channels with application to space-time codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4184–4202, Dec. 2005.

[26] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. New York: Dover, 1964.

[27] J. H. M. Wedderburn, "On division algebra," *Trans. American Math. Soc.*, vol. 22, no. 2, pp. 129–135, Apr. 1921.

Xiaoyong Guo received the B.S. degree in mathematics from Xi'an Jiaotong University, Xi'an, China, in 2003. He is currently pursuing the Ph.D. degree at the University of Delaware, Newark.

His current research interests are space–time coding for MIMO and cooperative systems.

Xiang-Gen Xia (M'97–SM'00–F'09) received the B.S. degree in mathematics from Nanjing Normal University, Nanjing, China, and the M.S. degree in mathematics from Nankai University, Tianjin, China, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1983, 1986, and 1992, respectively.

He was a Senior/Research Staff Member at Hughes Research Laboratories, Malibu, CA, during 1995–1996. In September 1996, he joined the Department of Electrical and Computer Engineering, University of Delaware, Newark, Delaware, where he is the Charles Black Evans Professor. He was a Visiting Professor at the Chinese University of Hong Kong during 2002–2003, where he is an Adjunct Professor. Before 1995, he held visiting positions in a few institutions. His current research interests include space-time coding, MIMO and OFDM systems, and SAR and ISAR imaging. He has over 180 refereed journal articles published and accepted, and seven U.S. patents awarded and is the author of the book *Modulated Coding for Intersymbol Interference Channels* (New York: Marcel Dekker, 2000).

Dr. Xia received the National Science Foundation (NSF) Faculty Early Career Development (CAREER) Program Award in 1997, the Office of Naval Research (ONR) Young Investigator Award in 1998, and the Outstanding Overseas Young Investigator Award from the National Nature Science Foundation of China in 2001. He also received the Outstanding Junior Faculty Award of the Engineering School of the University of Delaware in 2001. He is currently an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, *Signal Processing (EURASIP)*, and the *Journal of Communications and Networks (JCN)*. He was a guest editor of Space-Time Coding and Its Applications in the *EURASIP Journal of Applied Signal Processing* in 2002. He served as an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING during 1996 to 2003, the IEEE TRANSACTIONS ON MOBILE COMPUTING during 2001 to 2004, the IEEE *Signal Processing Letters* during 2003 to 2007, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY during 2005 to 2008, and the *EURASIP Journal of Applied Signal Processing* during 2001 to 2004. He is also a Member of the Sensor Array and Multichannel (SAM) Technical Committee in the IEEE Signal Processing Society. He was the General Co-Chair of ICASSP 2005 in Philadelphia, PA.