The Golden Code: A 2×2 Full-Rate Space–Time Code With Nonvanishing Determinants

Jean-Claude Belfiore, *Member, IEEE*, Ghaya Rekaya, *Student Member, IEEE*, and Emanuele Viterbo, *Senior Member, IEEE*

***Abstract*—In this paper, the Golden code for a 2×2 multiple-input multiple-output (MIMO) system is presented. This is a full-rate 2×2 linear dispersion algebraic space–time code with unprecedented performance based on the Golden number $\frac{1+\sqrt{5}}{2}$.**

***Index Terms*—Cyclic division algebras, number fields, space–time lattices.**

I. Introduction

Full rate and full diversity codes for the 2×2 coherent multiple-input multiple-output (MIMO) systems, were first constructed in [1], using number-theoretical methods. This approach was later generalized for any number of transmit antennas M [2]–[4]. The above constructions satisfy the *rank criterion* and attempt to maximize, for a fixed signal set S, the *coding advantage*, [5]. A general family of 2×2 full-rank and full-rate linear dispersion space–time block codes (LD-STBC) is given in [6], [7], based on cyclic division algebras.

Let $\mathbb{K} = \mathbb{Q}(\theta)$ be a quadratic extension of $\mathbb{Q}(i)$, we define the *infinite code* $\mathcal{C}_\infty$ as the set of matrices of the form

$$\mathcal{C}_\infty = \left\{ \boldsymbol{X} = \begin{bmatrix} a+b\theta & c+d\theta \\ \gamma(c+d\bar{\theta}) & a+b\bar{\theta} \end{bmatrix} : a,b,c,d \in \mathbb{Z}[i] \right\}$$

where $\gamma \in \mathbb{Z}[i]$ is a number carefully chosen [6], [7]. $\mathcal{C}_\infty$ is clearly a linear code, i.e., $\boldsymbol{X}_1 + \boldsymbol{X}_2 \in \mathcal{C}_\infty$ for all $\boldsymbol{X}_1, \boldsymbol{X}_2 \in \mathcal{C}_\infty$. The *finite code* $\mathcal{C}$ is obtained by limiting the *information symbols* to $a,b,c,d \in S \subset \mathbb{Z}[i]$, where we assume the signal constellation S to be a 2^b-QAM, with in-phase and quadrature components equal to $\pm 1, \pm 3, \ldots$ and b bits per symbol.

The code $\mathcal{C}_\infty$ is a discrete subset of a cyclic division algebra over $\mathbb{Q}(i)$, obtained by selecting $\gamma \in \mathbb{Z}[i]$ and $\gamma \neq N_{\mathbb{K}/\mathbb{Q}(i)}(x)$ for any $x \in \mathbb{K}$ [6], [7]. A division algebra naturally yields a structured set of invertible matrices that can be used to construct square LD-STBC, since for any codeword $\boldsymbol{X} \in \mathcal{C}_\infty$, the rank criterion is satisfied as $\det(\boldsymbol{X}) \neq 0$.

We define the *minimum determinant* of $\mathcal{C}_\infty$ as

$$\delta_{\min}(\mathcal{C}_\infty) = \min_{\boldsymbol{X} \in \mathcal{C}_\infty, \boldsymbol{X} \neq 0} |\det(\boldsymbol{X})|^2 \tag{1}$$

and the minimum determinant of the finite code $\mathcal{C}$ as

$$\delta_{\min}(\mathcal{C}) \triangleq \min_{\boldsymbol{X}_1, \boldsymbol{X}_2 \in \mathcal{C}, \boldsymbol{X}_1 \neq \boldsymbol{X}_2} |\det(\boldsymbol{X}_1 - \boldsymbol{X}_2)|^2 \geq 16 \delta_{\min}(\mathcal{C}_\infty). \tag{2}$$

Minimum determinants of $\mathcal{C}_\infty$ in all previous constructions [1]–[4], [7] are nonzero, but vanish as the spectral efficiency b of the signal constellation S is increased. This problem appears because transcendental elements or algebraic elements with a too high degree are used to construct the division algebras. Nonvanishing determinants may be of interest, whenever we want to apply some outer block coded modulation scheme, which usually entails a signal set expansion, if the spectral efficiency has to be preserved.

As explained in the following, in order to obtain *energy-efficient* codes we need to construct a lattice $M\mathbb{Z}[i]^2$, a rotated version of the complex lattice $\mathbb{Z}[i]^2$, where M is a complex unitary matrix, so that there is no shaping loss in the signal constellation emitted by the transmit antennas. This additional property was never considered before and is the key to the improved performance of our code.

Here we find the Golden Code, a code with nonvanishing $\delta_{\min}$ outperforming all previous constructions. It is interesting to notice that, for this code, $\delta_{\min}$ does not depend on the size of the signal constellation.

After paper submission, the authors became aware that a code isomorphic to the Golden Code was independently found by [8] and [9] by analytical optimization. In [8], it is shown that this code achieves the diversity–multiplexing gain tradeoff [10]. The algebraic approach given here sheds a totally new light over such a code and opens the way to extension to MIMO systems with a higher number of antennas [11].

II. The Golden Code

We first illustrate the construction of the Golden Code, which is related to the Golden number $\theta = \frac{1+\sqrt{5}}{2}$ and yields the best performance. We assume the reader is familiar with the basic definitions in algebraic number theory, for which we suggest [12]–[14].

Consider

$$\mathbb{K} = \mathbb{Q}(i, \sqrt{5}) = \{a + b\theta | a,b \in \mathbb{Q}(i)\}$$

as a relative quadratic extension of $\mathbb{Q}(i)$, with minimal polynomial $\mu_\theta(X) = X^2 - X - 1$. Denote by θ and $\bar{\theta} = 1 - \theta = \frac{1-\sqrt{5}}{2}$,

Manuscript received January 27, 2004; revised August 23, 2004.

J.-C. Belfiore and G. Rekaya are with École Nationale Supérieure des Télécommunications, 75013 Paris, France (e-mail: belfiore@enst.fr; rekaya@enst.fr).

E. Viterbo is with the Department of Electronics, Politecnico di Torino, 10129 Torino, Italy (e-mail: viterbo@ polito.it).

Communicated by Ø. Ytrehus, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2005.844069

0018-9448/$20.00 © 2005 IEEE

the two roots of the minimal polynomial. Let $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i][\theta]$ denote the ring of integers of $\mathbb{K}$, with integral basis $B_{\mathbb{K}} = \{1, \theta\}$. We recall that for any algebraic integer $z = a + b\theta \in \mathcal{O}_{\mathbb{K}}$, with $a, b \in \mathbb{Z}[i]$ (Gaussian integers), the relative norm is

$$N_{\mathbb{K}/\mathbb{Q}(i)}(z) = (a + b\theta)(a + b\bar{\theta}) = a^2 + ab - b^2 \in \mathbb{Z}[i]. \quad (3)$$

Let $\mathbb{L} = \{a + b\,i + c\,\theta + d\,i\theta \mid a, b, c, d \in \mathbb{Q}\}$ be the corresponding absolute extension of $\mathbb{K}$ over $\mathbb{Q}$, with signature $(r_1, r_2) = (0, 2)$, ring of integers $\mathcal{O}_{\mathbb{L}}$, and integral basis $B_{\mathbb{L}} = \{1, i, \theta, i\theta\}$.[1] The relative discriminant of $\mathbb{K}$ is $d_{\mathbb{K}} = 5$, while the absolute discriminant of $\mathbb{L}$ is $d_{\mathbb{L}} = 2^4 \cdot 5^2$.

In order to obtain energy-efficient codes we need to construct a complex lattice $M\mathbb{Z}[i]^2$, where M is a complex unitary matrix, so that there is no shaping loss in the signal constellation. This lattice will derive as an algebraic lattice from an appropriate relative ideal of the ring of integers $\mathcal{O}_{\mathbb{K}}$. The complex lattice $M\mathbb{Z}[i]^2$ can equivalently be seen as a rotated $\mathbb{Z}^4$-lattice: $R\mathbb{Z}^4$, R being an orthogonal matrix, obtained from an ideal of $\mathcal{O}_{\mathbb{L}}$ [13].

A necessary condition to obtain $R\mathbb{Z}^4$ is that there exists an ideal $\mathcal{I}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{L}}$ of norm 5. In fact, the lattice $\Lambda(\mathcal{O}_{\mathbb{L}})$ has fundamental volume equal to $2^{-r_2}\sqrt{|d_{\mathbb{L}}|} = 5$ and the sublattice $\Lambda(\mathcal{I}_{\mathbb{L}})$ has fundamental volume equal to $2^{-r_2}\sqrt{|d_{\mathbb{L}}|}N(\mathcal{I}_{\mathbb{L}}) = 25$, where the norm of the ideal $N(\mathcal{I}_{\mathbb{L}})$ is equal to the sublattice index. This suggests that the fundamental parallelotope of $\Lambda(\mathcal{I}_{\mathbb{L}})$ could be a hypercube of edge length equal to $\sqrt{5}$, but this needs to be checked explicitly.

An ideal $\mathcal{I}_{\mathbb{L}}$ of norm 5 can be found from the following ideal factorization:

$$5 \cdot \mathcal{O}_{\mathbb{L}} = \mathcal{I}^2 \cdot \overline{\mathcal{I}}^2 = (1 + i - i\theta)^2 \cdot (1 - i + i\theta)^2. \quad (4)$$

Let us take the principal ideal $\mathcal{I}_{\mathbb{L}} = \mathcal{I} = (\alpha)$, where $\alpha = 1 + i - i\theta$.

Following [12], let the canonical embedding of $\mathbb{L}$ be defined by

$$\begin{aligned}&\sigma : \mathbb{L} \mapsto \mathbb{R}^4\\ &\sigma(x) = [\Re(\sigma_1(x)), \Im(\sigma_1(x)), \Re(\sigma_2(x)), \Im(\sigma_2(x))] \quad (5)\end{aligned}$$

where

$$\begin{aligned}&\sigma_1(i\theta) = i\theta && \sigma_2(i\theta) = i\bar{\theta}\\ &\sigma_3(i\theta) = -\,i\theta = \overline{\sigma_1}(i\theta) && \sigma_4(i\theta) = -i\bar{\theta} = \overline{\sigma_2}(i\bar{\theta}) \quad (6)\end{aligned}$$

are the four field homomorphisms. The bi-quadratic nature of $\mathbb{L}$ is reflected by its Galois group

$$\begin{aligned}\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) &= \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}\\ &= \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}) = \mathcal{C}_2 \times \mathcal{C}_2. \quad (7)\end{aligned}$$

The real lattice generator matrix of $\Lambda(\mathcal{O}_{\mathbb{L}})$ is obtained by applying the canonical embedding to the integral basis $B_{\mathbb{L}}$, while the real lattice generator matrix R of the sublattice $\Lambda(\mathcal{I}_{\mathbb{L}})$ is obtained by applying the canonical embedding to the integral basis of the principal ideal $\mathcal{I}_{\mathbb{L}} = (\alpha)$, which is given by $\{\alpha, i\alpha, \alpha\theta, i\alpha\theta\}$. Hence,

$$R = \begin{bmatrix} 1 & -1+\theta & \theta & 1\\ 1-\theta & 1 & -1 & \theta\\ 1 & -1+\bar{\theta} & \bar{\theta} & 1\\ 1-\bar{\theta} & 1 & -1 & \bar{\theta}\end{bmatrix}.$$

By straightforward calculations we may verify that $R^TR = 5I$, which corresponds to the $\sqrt{5}\,\mathbb{Z}^4$-lattice.

The corresponding complex lattice $\Lambda(\mathcal{I}_{\mathbb{K}})$ can be obtained by applying the complex canonical embedding

$$\begin{aligned}&\sigma : \mathbb{K} \mapsto \mathbb{C}^2\\ &\sigma(x) = [\sigma_1(x), \sigma_2(x)] \quad (8)\end{aligned}$$

to the relative basis $\{\alpha, \alpha\theta\}$ of $\mathcal{I}_{\mathbb{K}}$

$$M = \begin{bmatrix}\sigma_1(\alpha) & \sigma_1(\alpha\theta)\\ \sigma_2(\alpha) & \sigma_2(\alpha\theta)\end{bmatrix} = \begin{bmatrix}1 + i(1-\theta) & \theta - i\\ 1 + i(1-\bar{\theta}) & \bar{\theta} - i\end{bmatrix}.$$

If we consider the cyclic division algebra

$$\mathcal{A} = (\mathbb{K}/\mathbb{Q}(i), \sigma, \gamma)$$

over $\mathbb{K}$, we can represent all its elements by 2 × 2 matrices

$$\begin{aligned}\boldsymbol{X} &= \begin{bmatrix}x_1 & 0\\ 0 & x_2\end{bmatrix} + \begin{bmatrix}x_3 & 0\\ 0 & x_4\end{bmatrix} \cdot \begin{bmatrix}0 & 1\\ \gamma & 0\end{bmatrix}\\ &= \begin{bmatrix}x_1 & x_3\\ \gamma x_4 & x_2\end{bmatrix} \quad (9)\end{aligned}$$

where $x_1, x_2, x_3, x_4 \in \mathbb{K}$ and $\gamma \in \mathbb{Q}(i)$ is not an algebraic norm of any element of $\mathbb{K}$ (see [6], [7]).

In our case, we define $\mathcal{C}_\infty = (\mathcal{A}, \mathcal{I}_{\mathbb{K}})$ as an order of $\mathcal{A}$, obtained by restricting $x_1, x_2, x_3, x_4 \in \mathcal{I}_{\mathbb{K}}$. Codewords of $\mathcal{C}_\infty$ are given by

$$\begin{aligned}\boldsymbol{X} &= \mathrm{diag}\left(\frac{1}{\sqrt{5}}M\begin{bmatrix}a\\ b\end{bmatrix}\right) + \mathrm{diag}\left(\frac{1}{\sqrt{5}}M\begin{bmatrix}c\\ d\end{bmatrix}\right)\begin{bmatrix}0 & 1\\ \gamma & 0\end{bmatrix}\\ &= \frac{1}{\sqrt{5}}\begin{bmatrix}\alpha(a + b\theta) & \alpha(c + d\theta)\\ \gamma\bar{\alpha}(c + d\bar{\theta}) & \bar{\alpha}(a + b\bar{\theta})\end{bmatrix} \quad (10)\end{aligned}$$

where $a, b, c, d \in \mathbb{Z}[i]$, $\bar{\alpha} = 1 + i(1 - \bar{\theta})$, and the factor $\frac{1}{\sqrt{5}}$ is necessary to normalize M in order to obtain a unitary matrix.

Division algebras guarantee that $\det(\boldsymbol{X}) \neq 0$ for all codewords. But how can we choose γ to avoid vanishing determinants and preserve energy efficiency?

The numerically optimized codes in [1] take $\gamma = e^{i\phi} \in \mathbb{C}$, such that it is transcendental over $\mathbb{K}$. The fact that γ is transcendental guarantees nonzero determinants. From (10), we have

$$\begin{aligned}&\det(\boldsymbol{X}) = \frac{1}{5}\left(N_{\mathbb{K}/\mathbb{Q}(i)}(z_1) - \gamma N_{\mathbb{K}/\mathbb{Q}(i)}(z_2)\right) \neq 0\\ &\quad\forall\, z_1 = \alpha(a + b\theta) \in \mathcal{I}_{\mathbb{K}}, \quad z_2 = \bar{\alpha}(c + d\bar{\theta}) \in \mathcal{I}_{\mathbb{K}}. \quad (11)\end{aligned}$$

The idea is to choose a $\gamma \in \mathbb{Z}(i)$ (hence, not transcendental) which is not a norm of elements of $\mathcal{I}_{\mathbb{K}}$ as proposed in [6] and also such that $|\gamma| = 1$, which guarantees that the same average

[1] The fields $\mathbb{K}$ and $\mathbb{L}$ coincide abstractly, it is only for convenience of exposition that we use distinct notation

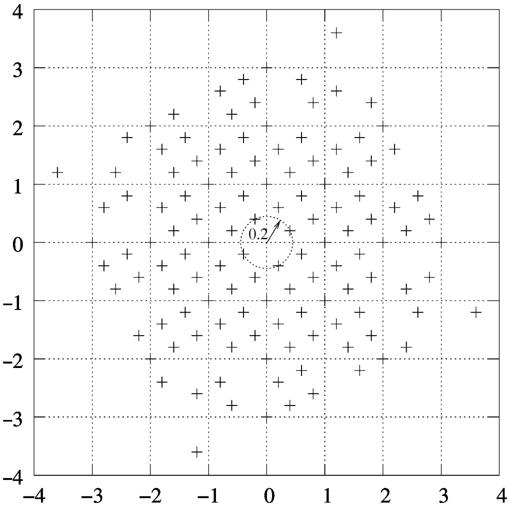

Fig. 1. Some determinants for the codewords of $\mathcal{C}_\infty$ (see (13)).

energy is transmitted from each antenna at each channel use. This limits the choice to $\gamma = \pm 1, \pm i$.

In order to satisfy the nonvanishing determinant condition in (11), we choose $\gamma = i$ and verify that it is never a norm of an element of $\mathbb{K}$ (see the Appendix). Hence, by choosing $\gamma = i$, we ensure that the determinants in (11) only take values in the discrete set $\frac{1}{5}\mathbb{Z}[i]$. In Fig. 1, we plot the first few terms of the *determinant spectrum* in the complex plane. In this plot, we can see an empty disk around the origin whose square radius is exactly $\delta_{\min}(\mathcal{C}_\infty)$. Let us relate this to the algebraic structure of the code. From (11) we have

$$\det(\boldsymbol{X}) = \frac{1}{5}N_{\mathbb{K}/\mathbb{Q}(i)}(\alpha)(N_{\mathbb{K}/\mathbb{Q}(i)}(a+b\theta) - \gamma N_{\mathbb{K}/\mathbb{Q}(i)}(c+d\theta)), \qquad \forall\, a,b,c,d \in \mathbb{Z}[i]. \quad (12)$$

As the second term in (12) only takes values in $\mathbb{Z}[i]$ and its minimum modulus is equal to 1 (take $a = 1$ and $b = c = d = 0$), we conclude that

$$\delta_{\min}(\mathcal{C}_\infty) = \frac{1}{25}|N_{\mathbb{K}/\mathbb{Q}(i)}(\alpha)|^2 = \frac{1}{25}|2+i|^2 = \frac{1}{5}. \quad (13)$$

III. Simulation Results

The numerically optimized 2 × 2 full-rate codes in [1] have vanishing determinants and are equivalent to

$$\left\{ \boldsymbol{X} = \frac{1}{\sqrt{2}} \begin{bmatrix} a+b\theta & c+d\theta \\ \gamma(c-d\theta) & a-b\theta \end{bmatrix} a,b,c,d \in \mathbb{Z}[i] \right\}$$

with $\gamma = \theta = e^{i\phi}$.

The first 2 × 2 code proposed in [1] falls in the general scheme of (10), where we take the cyclotomic field

$$\mathbb{K} = \mathbb{Q}(i,\theta) = \mathbb{Q}(\theta)$$

with $\theta = e^{i\pi/4}$, $\alpha = 1$ and $\gamma = \theta = \sqrt{i} \notin \mathbb{Z}[i]$. We will denote this code by $\mathcal{C}_a$.

Further optimization of $\delta_{\min}$ yields different codes with a similar structure to $\mathcal{C}_a$ with $\gamma = \theta$ transcendental or algebraic. In the case γ is transcendental, as explained in [7, Proposition 12], $\mathbb{K} = \mathbb{Q}(i,\gamma)$ is not necessarily a finite extension [15].

We will denote these codes for the 4-QAM by $\mathcal{C}_{b4}$, where $\gamma = e^{i/2}$, and for the 16-QAM by $\mathcal{C}_{b16}$, where $\gamma = e^{i\pi/6}$.

TABLE I
Comparison of $\sqrt{\delta_{\min}}$

γ	$\sqrt{\delta_{\min}}$ 4–QAM	$\sqrt{\delta_{\min}}$ 16–QAM	$\sqrt{\delta_{\min}}$ 64–QAM
$\gamma = e^{i\pi/4}$	0.0858	0.0272	0.0147
$\gamma = e^{i/2}$	0.2369	0.0137	0.0137
$\gamma = e^{i\pi/6}$	0.1895	0.0508	0.0186
$\gamma = i$	1.7889	1.7889	1.7889

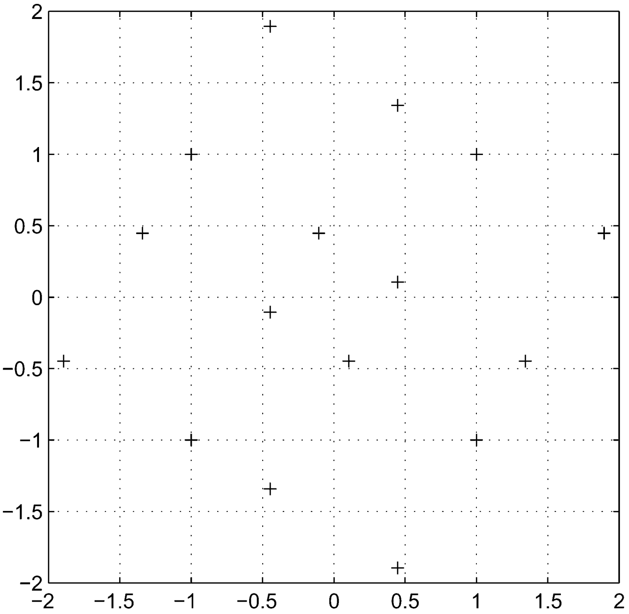

Fig. 2. Transmitted constellation for 4-QAM (Golden Code).

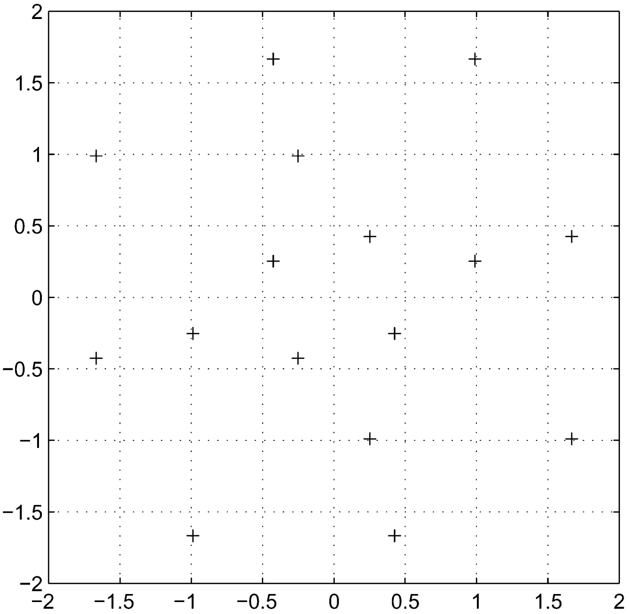

Fig. 3. Transmitted constellation for 4-QAM (best previously known code).

The Golden Code $\mathcal{C}_g$ has $\delta_{\min}(\mathcal{C}_g) = 16/5$, for any size of the constellation S and is always larger than the previous ones (see Table I).

The symbols per transmit antenna (i.e., the elements of the matrix codewords) are drawn from a "coded" constellation S_c plotted in Figs. 2 and 3 and for the Golden Code and the best

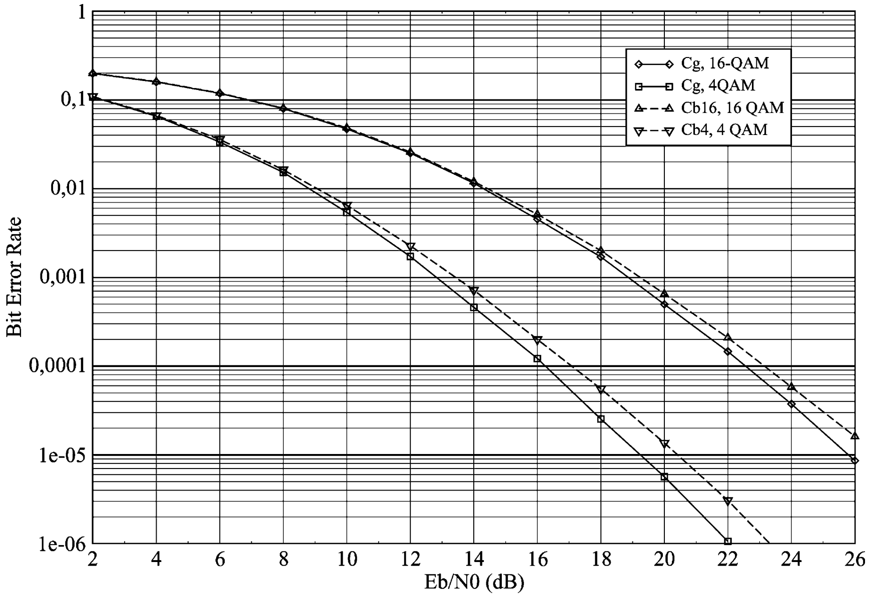

Fig. 4. Performance comparison of the new codes versus those of [1] and [15].

previously known one [1], respectively. We can observe that, for the Golden Code, S_c is almost a rotated regularly spaced quadrature amplitude modulation (QAM) constellation with 2^{2b} distinct points with same average energy as S, whereas it is the union of three phase-shift keying (PSK) constellations for the other code. We conjecture that this property of the S_c constellation along with the minimum value of $\delta_{\min}$ are the key factors to explain the good performance of the Golden Code in the medium signal-to-noise (SNR) range.

In Fig. 4, we show the bit-error rates for the codes $\mathcal{C}_{b4}$, $\mathcal{C}_{b16}$, and the Golden Code $\mathcal{C}_g$ as a function of E_b/N_0 for the standard block-fading 2 × 2 MIMO channel. The maximum-likelihood sphere decoder [16], [17] is used at the receiver. We can observe that the Golden Code gains 0.9 dB in the 16-QAM case and 1.2 dB in the 4-QAM case with respect to the best previously known codes.

IV. Conclusion

We presented a new 2 × 2 LD-STBC with full rate and full diversity, energy efficient, and with nonvanishing determinants. This outperforms all previously known codes. Moreover, it is possible to show that a family of codes similar to the Golden Code can be generated using $\mathbb{K} = \mathbb{Q}\left(i, \sqrt{p}\right)$ for all primes $p \equiv 5 \bmod 8$ [18]. For these codes, $\delta_{\min} = 1/p$. Hence, the Golden code gives the largest $\delta_{\min}$ within this family.

Appendix

We show, in this appendix, that the cyclic algebra $\mathcal{A}$ defined in (9) is a division algebra.

Proposition 1: Let $\mathbb{K} = \mathbb{Q}\left(i, \sqrt{5}\right)$, then the element $\gamma = i$ is not a relative norm of any $x \in \mathbb{K}$, i.e., $N_{\mathbb{K}/\mathbb{Q}(i)}(x) \neq i, \forall x \in \mathbb{K}$.

Proof: Let $\boldsymbol{Q}_5$ denote the field of 5-adic numbers, and $\boldsymbol{Z}_5 = \{x \in \boldsymbol{Q}_5 | \nu_5(x) \geq 0\}$ its valuation ring [19]. The complex rationals $\mathbb{Q}(i)$ can be embedded in $\boldsymbol{Q}_5$ by

$$i \mapsto 2 + 5\boldsymbol{Z}_5.$$

Let $x = a + b\sqrt{5} \in \mathbb{K}$ with $a, b \in \mathbb{Q}(i)$, then we must show that

$$N_{\mathbb{K}/\mathbb{Q}(i)}(x) = a^2 - 5b^2 = i$$

has no solution for $a, b \in \mathbb{Q}(i)$. We can lift this equation in the 5-adic field $\boldsymbol{Q}_5$

$$a^2 - 5b^2 = 2 + 5x, \qquad a, b \in \mathbb{Q}(i), \ x \in \boldsymbol{Z}_5 \tag{14}$$

and show that it has no solution there. We take the valuations of both sides of (14)

$$\nu_5(a^2 - 5b^2) = \nu_5(2 + 5x)$$

to show that a and b must be in $\boldsymbol{Z}_5$. In fact, since $x \in \boldsymbol{Z}_5$

$$\nu_5(2 + 5x) \geq \min\{\nu_5(2), \nu_5(x) + 1\} = 0$$

and we have equality as both valuations are distinct. Now

$$\nu_5(a^2 - 5b^2) = \min\{2\nu_5(a), 2\nu_5(b) + 1\}$$

must be 0, hence, $\nu_5(a) = 0$ which implies $a \in \boldsymbol{Z}_5$ and consequently $b \in \boldsymbol{Z}_5$.

We conclude by showing that

$$a^2 - 5b^2 = 2 + 5x, \qquad a, b, x \in \boldsymbol{Z}_5$$

has no solution. Reducing modulo $5\boldsymbol{Z}_5$ we find that 2 should be a square in GF(5), which is a contradiction. □

Acknowledgment

The authors would like to thank the anonymous reviewers for their comments that helped to improve the presentation of this paper. They particularly thank Frédérique Oggier for her help in establishing the proof of the Appendix.

References

[1] M. O. Damen, A. Tewfik, and J.-C. Belfiore, “A construction of a space-time code based on the theory of numbers,” *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 753–760, Mar. 2002.

[2] H. El Gamal and M. O. Damen, “An algebraic number theoretic framework for space-time coding,” in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, Jun./Jul. 2002, p. 132.

[3] S. Galliou and J.-C. Belfiore, “A new family of full rate, fully diverse space-time codes based on galois theory ,” in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, Jun./Jul. 2002, p. 419.

[4] H. El Gamal and M. O. Damen, “Universal space–time coding,” *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 1097–1119, May 2003.

[5] V. Tarokh, N. Seshadri, and A. 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.

[6] J.-C. Belfiore and G. Rekaya, “Quaternionic lattices for space-time coding,” in *Proc. IEEE Information Theory Workshop*, Paris, France, Mar./Apr. 2003, pp. 267–270.

[7] 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.

[8] H. Yao and G. W. Wornell, “Achieving the full MIMO diversity-multiplexing frontier with rotation-based space-time codes,” in *Proc. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Oct. 2003.

[9] P. Dayal and M. K. Varanasi, “An optimal two transmit antenna space-time code and its stacked extensions,” in *Proc. Asilomar Conf. on Signals, Systems and Computers*, Monterey, CA, Nov. 2003, pp. 987–991.

[10] L. Zheng and D. N. C. Tse, “Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels,” *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[11] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, “Perfect space-time block codes,” *IEEE Trans. Inf. Theory*, submitted for publication.

[12] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, “Good lattice constellations for both Rayleigh fading and Gaussian channels,” *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 502–518, Mar. 1996.

[13] F. Oggier and E. Viterbo, “Algebraic number theory and code design for Rayleigh fading channels,” in *Foundations and Trends in Communications and Information Theory*, The Netherlands: Now Publishers Inc., 2004, vol. 1, pp. 333–415.

[14] H. Cohn, *Advanced Number Theory*. New York: Dover, 1980.

[15] 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.

[16] M. O. Damen, A. Chkeif, and J.-C. Belfiore, “Lattice codes decoder for space-time codes,” *IEEE Commun. Lett.*, vol. 4, no. 5, pp. 161–163, May 2000.

[17] E. Viterbo and J. Boutros, “A universal lattice code decoder for fading channels,” *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1639–1642, Jul. 1999.

[18] F. Oggier, private communication, 2004.

[19] F. Q. Gouvêa, *P-Adic Numbers: An Introduction*, 2nd ed. Berlin, Germany: Springer-Verlag, 1997, Universitext.