Partitionning the Golden Code: A framework to the design of Space-Time coded modulation

David Champion, Jean-Claude Belfiore, Ghaya Rekaya and Emanuele Viterbo

***Abstract*— This paper presents a method of set partitionning for the Golden code. This space-time block code has been introduced in [1]. We show how to construct the Gosset lattice E_8 as well as the Leech lattice Λ_{24}. The same set partitionning is finally used to construct a trellis-coded modulation that outperforms the Golden code.**

***Index Terms*— Set partitionning, reduced norm, coded modulation**

I. Introduction

IN [1], the 2×2 Golden code was presented. It outperformed all previous 2×2 constructions. Moreover, its minimum determinant remains constant when the spectral efficiency increases. We propose here to construct new space-time coded modulations based on a set partitionning of the Golden code that increases both the minimum Euclidean distance and the minimum determinant.

II. The Golden Code

We first recall the construction of the Golden Code, which is related to the Golden number $\theta = \frac{1+\sqrt{5}}{2}$ and yields excellent performance [1]. We assume the reader is familiar with the basic definitions in algebraic number theory, for which we suggest [2], [3], [4].

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 $\bar{\theta} = 1 - \theta = \frac{1-\sqrt{5}}{2}$, 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 consider the cyclic division algebra

$$\mathcal{A} = (\mathbb{K}/\mathbb{Q}(i), \sigma, i) = \{z_1 + z_2 \cdot e, z_1, z_2 \in \mathbb{K}\}$$

where the operating rules are $e^2 = i$, $z \cdot e = e \cdot \sigma(z), \forall z \in \mathbb{K}$. A matrix representation of an element of this algebra is

$$\begin{bmatrix} z_1 & z_2 \\ i\sigma(z_2) & \sigma(z_1) \end{bmatrix}$$

The reduced norm of an element of this algebra, denoted $N_r(\cdot)$ is the determinant of the matrix representation. Let $\alpha = 1 + i - i\theta$ and $\mathcal{I}_{\mathbb{K}}$ be the principal ideal generated by α. We define the infinite Golden code $\mathcal{C}_\infty = (\mathcal{A}, \mathcal{I}_{\mathbb{K}})$ as an order of $\mathcal{A}$, obtained by restricting $z_1, z_2 \in \mathcal{I}_{\mathbb{K}}$. Codewords of $\mathcal{C}_\infty$ are given by

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(a + b\theta) & \alpha(c + d\theta) \\ \gamma\bar{\alpha}(c + d\bar{\theta}) & \bar{\alpha}(a + b\bar{\theta}) \end{bmatrix} \quad (1)$$

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 for energy normalizing purpose. We recall that the minimum squared determinant of the Golden code is

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

III. A Quaternary Set Partitionning for the Golden Code

A. The set partitioning

We recall that a cyclic algebra of order 2 is a quaternion algebra [5] and its elements are called quaternions. Thanks to KANT software [6], we can find, in the algebra defined by the Golden code, a quaternion with reduced norm $1 + i$. Namely, this quaternion is

$$\beta = i\,(1 - \theta) + (1 - \theta)\,e$$

with matrix representation

$$\begin{bmatrix} i\,(1 - \theta) & 1 - \theta \\ i\,(1 - \bar{\theta}) & i\,(1 - \bar{\theta}) \end{bmatrix}.$$

The infinite Golden code $\mathcal{G}$ is a quaternionic order. Let $\mathfrak{I}_\beta$ be the right ideal defined by

$$\mathfrak{I}_\beta = \{\mathbf{X} \cdot \beta, \mathbf{X} \in \mathcal{G}\}.$$

In fact, since $N_r(\beta) = 1 + i$, we have $|\mathcal{G} / \mathfrak{I}_\beta| = |1 + i|^4 = 4$ (in fact, this quotient ring is equal to the finite field $\mathbb{F}_4$). So, we get a quaternary partition of the Golden code that can be iterated by considering powers of the ideal $\mathfrak{I}_\beta$.

B. Identification of lattices in the partitionning chain

Figure 1 shows the quaternary partition chain of the Golden code when using $\mathfrak{I}_\beta$ as the partitionning ideal (see [7] for more details). What is surprising is that we can construct the Gosset lattice E_8 which is the densest one in dimension 8 for the Euclidean distance. The minimum squared determinant $\delta_{\min}$ is multiplied by $2 = |N_r(\beta)|^2$ at each step. But the problem is that the determinant increase just compensates the constellation expansion as can be seen in figure 2. On the Gaussian channel, we see the well-known asymptotic gain of $3dB$ whereas, on the Rayleigh quasi-static channel, there is no gain for the Golden E_8 code compared to the Golden code.

$$\begin{tikzcd}
\mathbb{Z}[i]^4 \cong \mathbb{Z}^8 \arrow[r, dashed] \arrow[d] & \mathcal{G} \\
D_4^2 \arrow[r, dashed] \arrow[d] & \mathfrak{I}_\beta \\
E_8 \arrow[r, dashed] \arrow[d] & \mathfrak{I}_\beta^2 \\
(1+i)\, D_4^2 \arrow[r, dashed] \arrow[d] & \mathfrak{I}_\beta^3 \\
2\mathbb{Z}^8 \arrow[r, dashed] & \mathfrak{I}_\beta^4 = (2)
\end{tikzcd}$$

Fig. 1. Partitionning the Golden code

C. Construction of the Leech lattice

A construction of the Leech lattice Λ_{24} similar to the Tits's one [8] is proposed. First, we define the conjugate of a quaternion $q = x + y \cdot e$ with $x, y \in \mathbb{K}$ as $\bar{q} = \sigma(x) - y \cdot e$. We get the following relation,

$$q \cdot \bar{q} = N_r(q) = N_{\mathbb{K}/\mathbb{Q}(i)}(x) - i N_{\mathbb{K}/\mathbb{Q}(i)}(y).$$

Now, define the lattice

$$\Lambda = \Big\{ (x_1, x_2, x_3) \text{ with } x_i \in \mathfrak{I}_\beta^2 \Big| \\ \forall i \neq j \quad x_i \equiv x_j \bmod \mathfrak{I}_\beta^3 \text{ and } x_1 + x_2 + x_3 \equiv 0 \bmod \mathfrak{I}_\beta^2 \cdot \mathfrak{I}_{\bar{\beta}} \Big\}$$

It can be shown that this lattice is the Leech lattice (see [9, Chap. 8, pp. 210-211]). But, as it has been remarked in subsection III-B, we do not know the effective coding gain of this lattice compared to the Golden code, for the Rayleigh quasi-static channel.

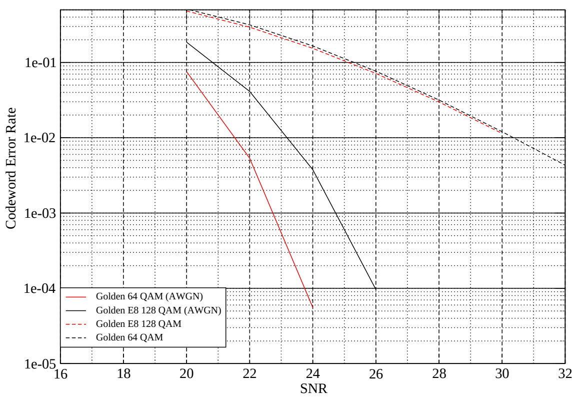

Fig. 2. The Golden code and the Golden E_8 lattice on Gaussian and Rayleigh quasi-static channels (12 bits p.c.u.)

IV. Increasing the coding gain

With this formalism, we should be able to construct non-square space-time codes with larger coding gains than the square Golden code as described in figure 3. For a codeword

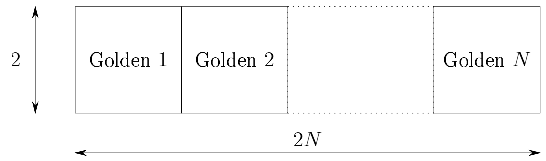

Fig. 3. Rectangular codeword based on the Golden code

whose components are quaternions from the Golden code $C = (g_1, g_2, \ldots g_N)$, the determinant of the Gram matrix is

$$\det\left(CC^\dagger\right) = \sum_{i=1}^{N} \det\left(g_i g_i^\dagger\right) + \text{ positive crossed terms }.$$

In fact, the coding gain is in the "crossed terms" and is difficult to evaluate. In figure 4, we give, as an example, the performance of the Golden code both uncoded and trellis-coded by using the set partitionning of figure 1.

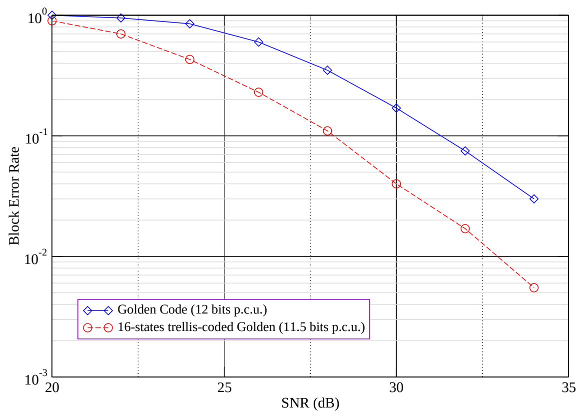

Fig. 4. 16−states trellis-coded Golden code vs. the Golden Code

References

[1] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The Golden Code: A 2 × 2 full rate Space-Time Code with non vanishing Determinants." to appear in *IEEE Trans. on Inf. Theory*, April 2005. http://www.enst.fr/~belfiore/publi.html .
[2] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good Lattice Constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. Inform. Theory*, vol. 42, pp. 502–518, March 1996.
[3] F. Oggier and E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels," in *Foundations and Trends in Communications and Information Theory*, vol. 1, pp. 333–415, 2004.
[4] H. Cohn, *Advanced Number Theory*. Dover Publications Inc. New York, 1980.
[5] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The Book of Involutions*, vol. 44. American Mathematical Society Colloquium Publications, 1998.
[6] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, and K. Wildanger, "KANT V4," *J. Symbolic Comp.*, vol. 24, pp. 267–283, 1997.
[7] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Trans. Inform. Theory*, vol. 43, pp. 938–952, May 1997.
[8] J. Tits, "Quaternions over $\mathbb{Q}(\sqrt{5})$, Leech's lattice and the sporadic group of Hall-Janko," *Journal of Algebra*, vol. 63, pp. 56–75, 1980.
[9] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. Grundlehren der mathematischen Wissenschaften, New York Berlin: Springer-Verlag, 2nd ed., 1988.