Golden Space-Time Block Coded Modulation

Laura Luzzi*, Ghaya Rekaya-Ben Othman*, Jean-Claude Belfiore*, and Emanuele Viterbo†

*Télécom ParisTech- École Nationale Supérieure des Télécommunications, 46 Rue Barrault, 75013 Paris, France.
E-mail: {belfiore, rekaya, luzzi}@enst.fr.

† DEIS - Università Della Calabria, Via P. Bucci, 42/C, 87036 Rende (CS), Italy.
E-mail: viterbo@deis.unical.it.

***Abstract*— We consider a block coded modulation scheme for a 2×2 MIMO system over slow fading channels, where the inner code is the Golden Code. The scheme is based on a set partitioning of the Golden Code using two-sided ideals. A lower bound for the minimum determinant is given by the minimum Hamming distance. Performance simulations show that our GC-RS schemes achieve a significant gain over the uncoded Golden Code.**

I. Introduction

The wide diffusion of wireless communications has led to a growing demand for high-capacity, highly reliable transmission schemes over fading channels.
In order to exploit fully the available diversity, a new class of code designs, called *Space-Time Block Codes*, was developed. In the *coherent*, *block fading* model, the fundamental criteria for code design are the *rank* and *determinant criteria* [7].
Codes meeting these two criteria can be constructed using tools from algebraic number theory. In the 2×2 MIMO case, Belfiore et al [1] designed the *Golden Code* $\mathcal{G}$, a full-rate, full-rank and information lossless code satisfying the non-vanishing determinant condition.

In this paper we focus on the *slow block fading* channel, where the fading coefficients are assumed to be constant for a certain number of time blocks L. With slow fading the ergodicity assumption must be dropped and the diversity of the system is reduced, leading to a performance loss.
This loss can be compensated using *coded modulation*: in a general setting, a full-rank space time block code is used as an *inner code* to guarantee full diversity, and is combined with an *outer code* which improves the minimum determinant.
We will take as our inner code the Golden Code: we focus on the problem of designing a *block code* $\{\mathbf{X} = (X_1, \ldots, X_L)\}$, where each component X_i is a Golden codeword.
In order to increase the minimum determinant, one can consider the ideals of $\mathcal{G}$. In [4], Hong et al. describe a *set partitioning* of the Golden Code, based on a chain of left ideals $\mathcal{G}_k$ whose minimum determinant is 2^k times that of $\mathcal{G}$. Their scheme combines two encoders: a trellis encoder whose output belongs to the quotient $\mathcal{G}_k/\mathcal{G}_{k+1}$, and a lattice encoder for $\mathcal{G}_{k+1}$ (*Trellis Coded Modulation*).

The global minimum determinant for a block code is

$$\Delta_{\min} = \min_{\mathbf{X} \neq 0} \det \left(\sum_{i=1}^{L} X_i X_i^H \right) \tag{1}$$

As we will see, the expression $\Delta_{\min}$ is difficult to handle because it involves the Frobenius norm of the codewords and the multiplicative structure of $\mathcal{G}$. The codes described in [4] are designed to maximize the approximate parameter $\Delta'_{\min} = \min_{\mathbf{X} \neq 0} \sum_{i=1}^{L} \det \left(X_i X_i^H \right)$ and so a priori they might be suboptimal; we will here consider the mixed terms and so obtain a tighter bound for $\Delta_{\min}$.
A rough estimate of the coding gain for the block code comes from its minimum "Hamming distance", that is, the minimum number of nonzero components. To increase the Hamming weight, we will take as our outer code an error correcting code over the quotient of $\mathcal{G}$ by one of its ideals.

The paper is organized as follows: in §II, we recall the algebraic construction of the Golden Code and its properties. In §III, we describe the general setting for Golden block codes and the coding gain estimates; in §IV, we study the "good ideals" of $\mathcal{G}$ for binary partitioning. In §V we introduce Reed-Solomon block codes over $\mathcal{G}$ and discuss their performance obtained through simulation results.

II. The Golden Code

Since we are interested in the partitioning of the Golden Code, we begin by recalling its algebraic construction.
The Golden Code $\mathcal{G}$, introduced in [1], is optimal for the case of 2 transmit and 2 or more receive antennas. It is constructed using the cyclic division algebra $\mathcal{A} = (\mathbb{Q}(i,\theta)/\mathbb{Q}(i), \sigma, \gamma)$ over the number field $\mathbb{Q}(i,\theta)$, where $\theta = \frac{\sqrt{5}+1}{2}$ is the golden number.
The set $\mathcal{A}$ is the $\mathbb{Q}(i,\theta)$-vector space $\mathbb{Q}(i,\theta) \oplus \mathbb{Q}(i,\theta)j$, where j is such that $j^2 = \gamma \in \mathbb{Q}(i)^*$, $xj = j\bar{x}\ \forall x \in \mathbb{Q}(i,\theta)$.
Here we denote by σ the canonical conjugacy sending an element $x = a + b\theta \in \mathbb{Q}(i,\theta)$ to $\bar{x} = a + b\bar{\theta}$, where $\bar{\theta} = 1 - \theta = \frac{1-\sqrt{5}}{2}$, $\quad \theta\bar{\theta} = -1$.
As its degree over its center $\mathbb{Q}(i)$ is 4, $\mathcal{A}$ is also called a *quaternion algebra*.
If we choose $\gamma = i$, γ is not a norm in $\mathbb{Q}(i,\theta)/\mathbb{Q}(i)$, and this implies that $\mathcal{A}$ is a division algebra [1].
Since $\mathbb{Q}(i,\theta)$ is a splitting field for $\mathcal{A}$, $\mathcal{A}$ is isomorphic to a subalgebra of $M_2(\mathbb{Q}(i,\theta))$. The inclusion is given by

$$x \mapsto \begin{pmatrix} x & 0 \\ 0 & \bar{x} \end{pmatrix},\ \forall x \in \mathbb{Q}(i,\theta), \quad j \mapsto \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix} \tag{2}$$

That is, every element $X \in \mathcal{A}$ admits a matrix representation

$$X = \begin{bmatrix} x_1 & x_2 \\ i\bar{x}_2 & \bar{x}_1 \end{bmatrix},\ x_1, x_2 \in \mathbb{Q}(i,\theta) \tag{3}$$

978-1-4244-2270-8/08/$25.00 ©2008 IEEE

If we require that the matrix elements of X belong to the ring of integers $\mathbb{Z}[i,\theta]$ of $\mathbb{Q}(i,\theta)$, then X belongs to the $\mathbb{Z}[i]$-*order*

$$\mathcal{O} = \left\{ \begin{bmatrix} x_1 & x_2 \\ i\bar{x}_2 & \bar{x}_1 \end{bmatrix},\ x_1, x_2 \in \mathbb{Z}[i,\theta] \right\} \tag{4}$$

Since $x \in \mathbb{Z}[i,\theta]$ implies that $N(x) = x\bar{x} \in \mathbb{Z}[i]$, we have $\det(X) \in \mathbb{Z}[i]$, so $|\det(X)| \geq 1$ for every $X \in \mathcal{O} \setminus \{0\}$.
The *Golden Code* is defined as a right principal ideal of $\mathcal{O}$ of the form $\mathcal{G} = \frac{1}{\sqrt{5}}\alpha\mathcal{O}$, where $\alpha = 1 + i\bar{\theta}$. We call A the matrix representation of α.
Every codeword in $\mathcal{G}$ is of the form $X = \frac{1}{\sqrt{5}}AW$, with $W \in \mathcal{O}$:

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

X carries four information symbols $(a,b,c,d) \in \mathbb{Z}[i]^4$: the code is *full-rate*.

Remark 1. We have seen that $\forall W \in \mathcal{O} \setminus \{0\}$, $|\det(W)| \geq 1$. Consequently, $\forall X \in \mathcal{G} \setminus \{0\}$, $|\det(X)|^2 \geq \delta = \frac{1}{5}$.
In fact, if $X = \frac{A}{\sqrt{5}}W$, $|\det(X)| = \frac{|N(\alpha)|}{5}|\det(W)| = \left|\frac{\det(W)}{\sqrt{5}}\right|$, since $|N(\alpha)| = |2 + i| = \sqrt{5}$.

Even though $\mathcal{G}$ is defined as a right ideal, it is easy to see that actually it is a *two-sided ideal*: if $w = w_1 + w_2 j \in \mathcal{O}$, $w_1, w_2 \in \mathbb{Z}[i,\theta]$, $\alpha(w_1 + w_2 j) = w_1\alpha + w_2 j\bar{\alpha} = (w_1 + i\theta w_2 j)\alpha$, observing that $\alpha i\theta = i\theta + 1 = \bar{\alpha}$. But

$$\xi : w_1 + w_2 j \mapsto w_1 + i\theta w_2 j \tag{6}$$

is an homomorphism of $\mathbb{Z}[i]$-modules that maps $\mathcal{O}$ into itself bijectively, therefore $\alpha\mathcal{O} = \mathcal{O}\alpha$.

III. Golden Block Codes

We now focus on the case of a *slow block fading* channel, meaning that the channel coefficients remain constant during the transmission of L codewords. The transmitted signal $\mathbf{X} = (X_1, \ldots, X_L)$ will be a vector of Golden codewords in a block code $\mathcal{S} \subset \mathcal{G}^L$. The received signal is

$$\mathbf{Y} = H\mathbf{X} + \mathbf{W}, \qquad \mathbf{X}, \mathbf{Y}, \mathbf{W} \in \mathbb{C}^{2\times 2L}, \tag{7}$$

where the entries of $H \in \mathbb{C}^{2\times 2}$ are i.i.d. complex Gaussian random variables with zero mean and variance per real dimension equal to $\frac{1}{2}$, and $\mathbf{W}$ is the Gaussian noise with i.i.d. entries of zero mean and variance N_0. We consider the coherent case, where the channel matrix H is known at the receiver.
The pairwise error probability is bounded by [7]

$$P(\mathbf{X} \mapsto \mathbf{X}') \leq \frac{1}{\left(\sqrt{\Delta_{\min}}\frac{E_{\mathcal{S}}}{N_0}\right)^4}, \tag{8}$$

In the above formula, $E_{\mathcal{S}}$ is the average energy per symbol of $\mathcal{S}$ and $\Delta_{\min} = \min_{\mathbf{X}\neq 0} \det\left(\sum_{i=1}^{L} X_i X_i^H\right)$. In order to minimize the PEP for a given SNR, we should maximize $\Delta_{\min}$.
To compare the error probability of a block code with that of the uncoded Golden Code of equal length L with the same data rate, we can employ the *asymptotic coding gain* [4]:

$$\gamma_{\text{as}} = \frac{\sqrt{\Delta_{\min}}/E_{\mathcal{S}}}{\sqrt{\Delta_{\min,U}}/E_{\mathcal{S},U}}, \tag{9}$$

where $\Delta_{\min}, \Delta_{\min,U}$ and $E_{\mathcal{S}}, E_{\mathcal{S},U}$ are the minimum determinants and average constellation energies of the block code and the uncoded case respectively.

A. Estimates of the minimum determinant

First of all, we give a more explicit expression for $\det(\mathbf{X}\mathbf{X}^H)$.
We define the quaternionic conjugacy in the algebra $\mathcal{A}$:

$$X = \begin{bmatrix} x_1 & x_2 \\ i\bar{x}_2 & \bar{x}_1 \end{bmatrix} \quad \mapsto \quad \widetilde{X} = \begin{bmatrix} \bar{x}_1 & -x_2 \\ -i\bar{x}_2 & x_1 \end{bmatrix}$$

$\forall X \in \mathcal{A}$, $\widetilde{X}X = \det(X)\mathbb{1}$ and $\det(X) = \det(\widetilde{X})$, where $\mathbb{1}$ denotes the identity matrix.
Recall that the *Frobenius norm* of a matrix $M = (m_{i,j})$ is $\|M\|_F = \sqrt{\sum_{i,j}|m_{i,j}|^2}$. Then $\forall \mathbf{X} = (X_1, \ldots, X_L) \in \mathcal{A}^L$, the following formula holds:

$$\det(\mathbf{X}\mathbf{X}^H) = \sum_{i=1}^{L} |\det(X_i)|^2 + \sum_{j>i} \left\|\widetilde{X}_j X_i\right\|_F^2 \tag{10}$$

These simple properties of the quaternionic conjugate and of the Frobenius norm will be useful in the sequel:

a) If $W \in \mathcal{O}$, $\|W\|_F^2 \in \mathbb{Z}$.
b) Let X, Y be two 2×2 complex-valued matrices. Then

$$\begin{aligned} \|X\|_F^2 &\geq 2\,|\det(X)|\,, \\ \left\|\widetilde{X}Y\right\|_F^2 &\geq 2\,|\det(X)|\,|\det(Y)| \end{aligned} \tag{11}$$

c) If $X_1, X_2 \in \mathcal{G} \setminus \{0\}$,

$$\left\|\widetilde{X}_2 X_1\right\|_F^2 \geq \frac{2}{5} = 2\delta \tag{12}$$

From equation (11), it follows that the determinant is bounded from below by the squared Hamming weight:

Lemma 1. *Let* $\mathbf{X} = (X_1, \ldots, X_L) \in \mathcal{G}^L$. *Then*

$$\det(\mathbf{X}\mathbf{X}^H) \geq \left(\sum_{i=1}^{L} |\det(X_i)|\right)^2 \geq (w_H(\mathbf{X}))^2\delta,$$

where $w_H(\mathbf{X}) = \#\{i \in \{1, \ldots, L\} \mid X_i \neq 0\}$ *is the Hamming weight of the block* $\mathbf{X}$.

IV. The quotient ring $\mathcal{G}/2\mathcal{G}$

The choice of a good block code of length L will be based on a partition of the Golden Code. To obtain a binary partition, which is simpler to use for coding and fully compatible with the choice of a QAM constellation, we must use ideals whose index is a power of 2, that is, whose norm is a power of $1 + i$. A similar construction appears in [4] and employs one-sided ideals. However, in order to have good estimates of the coding gain, because of the mixed terms in the minimum determinant

formula (10), we need to take the ring structure into account: we will choose *two-sided ideals* to ensure that the ideals are invariant with respect to the quaternionic conjugacy and multiplication on both sides, and that the quotient group is also a ring.

A. Two-sided ideals of $\mathcal{G}$

The existence of two-sided ideals is related to the ramification of primes over the base field. We refer the reader to [8] and [6] for an exposition of these topics.
As we have seen in §II, $\mathcal{O} = \mathbb{Z}[i, \theta] \oplus \mathbb{Z}[i, \theta]j$ is a $\mathbb{Z}[i]$-order of $\mathcal{A}$, and $\overline{\mathcal{G}} = \sqrt{5}\mathcal{G} = \alpha\mathcal{O}$ is a two-sided principal ideal of $\mathcal{O}$. $\sqrt{5}\mathcal{G}$ is also a prime ideal since $\sqrt{5}\mathcal{G} \cap \mathbb{Z}[i] = (2+i)$ is a prime ideal of $\mathbb{Z}[i]$.
Observe that the prime ideals $(2+i)$ and $(2-i)$ of $\mathbb{Z}[i]$ are both ramified in $\mathcal{A}$: in fact

$$(2+i) = (\alpha)^2, \text{ and } (2-i) = (\alpha')^2, \text{ where } \alpha' = 1 - i\bar{\theta}$$

(Remark that $\alpha = i\theta\bar{\alpha}$, $\alpha' = -i\bar{\theta}\bar{\alpha'}$).
By computing the reduced discriminant $d(\mathcal{O}) = \sqrt{|\det(\mathrm{tr}(w_k w_l))|}\mathbb{Z}[i]$, where $\{w_1 = 1,\ w_2 = \theta, w_3 = j,\ w_4 = \theta j\}$ is the basis of $\mathcal{O}$ over $\mathbb{Z}[i]$, one can show that $\mathcal{O}$ is a *maximal order* of $\mathcal{A}$, and that $(2+i)$ and $(2-i)$ are the only ramified primes in $\mathcal{A}$.

Then the prime two-sided ideals of $\mathcal{O}$ are either of the form $p\mathcal{O}$, where p is prime in $\mathbb{Z}[i]$, or belong to $\{\alpha\mathcal{O}, \alpha'\mathcal{O}\}$. In fact, the following theorem holds:

Theorem 2. *The two-sided ideals of a maximal R-order $\mathcal{O}$ of a quaternion algebra form a commutative group with respect to multiplication, which is generated by the ideals of R and the ideals of reduced norm P, where P varies over the prime ideals of R that are ramified in the algebra.*

It follows that the only two-sided ideals of $\mathcal{G}$ whose norm is a power of $1+i$ are the trivial ideals of the form $(1+i)^k\mathcal{G}$.

B. The quotient ring $\overline{\mathcal{G}}/2\overline{\mathcal{G}}$

Consider the ideal $2\mathcal{O}$. It is easy to check that $\overline{\mathcal{G}} = \sqrt{5}\mathcal{G}$ and $2\mathcal{O}$ are *coprime* ideals, that is $\overline{\mathcal{G}} + 2\mathcal{O} = \mathcal{O}$ and as a consequence, $\overline{\mathcal{G}} \cap 2\mathcal{O} = \overline{\mathcal{G}}2\mathcal{O} = 2\overline{\mathcal{G}}$. Recall the following basic result:

Theorem 3 (third isomorphism theorem for rings). *Let I and J be ideals in a ring R. Then $\frac{I}{I\cap J} \cong \frac{I+J}{J}$.*

If $I = \overline{\mathcal{G}}$ and $J = 2\mathcal{O}$, we get $\frac{\overline{\mathcal{G}}}{2\overline{\mathcal{G}}} \cong \frac{\mathcal{O}}{2\mathcal{O}}$.
If $\pi_{\overline{\mathcal{G}}} : \overline{\mathcal{G}} \to \overline{\mathcal{G}}/2\overline{\mathcal{G}}$ and $\pi_{\mathcal{O}} : \mathcal{O} \to \mathcal{O}/2\mathcal{O}$ are the canonical projections on the quotient, the ring isomorphism is simply given by $\pi_{\overline{\mathcal{G}}}(g) \mapsto \pi_{\mathcal{O}}(g)$.
We denote the image of $x \in \mathcal{O}$ through $\pi_{\mathcal{O}}$ with $[x]$.

Lemma 4. *$\mathcal{O}/2\mathcal{O}$ is isomorphic to the ring $M_2(\mathbb{F}_2[i])$ of 2×2 matrices over the ring $\mathbb{F}_2[i]$.*

Proof. We use the well-known lemma [5]:

Lemma 5. *Let R be a ring with identity, I a proper ideal of R, M a free R-module with basis X and $\pi : M \to M/IM$ the canonical projection. Then M/IM is a free R/I-module with basis $\pi(X)$ and $|\pi(X)| = |X|$.*

This Lemma implies that $\mathcal{O}/2\mathcal{O}$ is a free $\mathbb{Z}[i]/2$-module, that is a free $\mathbb{F}_2[i]$-module, of dimension 4. We can construct an explicit homomorphism of $\mathbb{F}_2[i]$-modules $\phi : \mathcal{O}/2\mathcal{O} \to M_2(\mathbb{F}_2[i])$ by specifying the image of the basis $\{1, \theta, j, \theta j\}$:

$$\phi([1]) = \mathbb{1}, \quad \phi([\theta]) = \begin{pmatrix} 1+i & 1 \\ i & i \end{pmatrix},$$
$$\phi([j]) = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}, \quad \phi([\theta j]) = \phi([\theta])\phi([j])$$

One can easily check that ϕ is bijective (the images of the basis elements being linearly independent) and that it is a ring homomorphism. □

In order to find an explicit isomorphism between $\overline{\mathcal{G}}/2\overline{\mathcal{G}}$ and $M_2(\mathbb{F}_2)$, consider the following diagram, where $\pi_{\overline{\mathcal{G}}} : \overline{\mathcal{G}} \to \overline{\mathcal{G}}/2\overline{\mathcal{G}}$ is the projection on the quotient, φ comes from the third isomorphism theorem for rings, and $\phi : \mathcal{O}/2\mathcal{O} \to M_2(\mathbb{F}_2[i])$ is the mapping defined in Lemma 4:

$$\overline{\mathcal{G}} \xrightarrow{\pi_{\overline{\mathcal{G}}}} \overline{\mathcal{G}}/2\overline{\mathcal{G}} \xrightarrow{\varphi} \mathcal{O}/2\mathcal{O} \xrightarrow{\phi} M_2(\mathbb{F}_2[i])$$

The basis $\{\alpha, \alpha\theta, \alpha j, \alpha\theta j\}$ of $\overline{\mathcal{G}}$ as a $\mathbb{Z}[i]$-module is also a basis of $\overline{\mathcal{G}}/2\overline{\mathcal{G}}$ as an $\mathbb{F}_2[i]$-module. The isomorphism φ is simply the composition of the inclusion $\overline{\mathcal{G}} \hookrightarrow \mathcal{O}$ and the quotient mod $2\mathcal{O}$. We can compute the images through ϕ of the basis vectors: observing that $\alpha = 1+i-i\theta$, $\alpha\theta = \theta - i$, $\alpha j = (1+i-i\theta)j$, $\alpha\theta j = (\theta - i)j$, we get the basis

$$\mathcal{B}_{M_2(\mathbb{F}_2[i])} = \left\{ \begin{pmatrix} 0 & i \\ 1 & i \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ i & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} i & 1 \\ 0 & i \end{pmatrix} \right\} \quad (13)$$

Observe that the lifts to $\overline{\mathcal{G}}$ of non-invertible elements have a higher determinant:

Remark 2. If $M \in M_2(\mathbb{F}_2[i]) \setminus \{0\}$ is non-invertible,

$$\min_{X\in\mathcal{G},\ \pi_{\overline{\mathcal{G}}}(\sqrt{5}X)=M} |\det(X)|^2 \geq 2\delta$$

C. The encoder

The codes that we consider follow the outline of Forney's *coset codes*, taking advantage of the decomposition $\mathcal{G} = [\mathcal{G}/I]+I$, where I is a two-sided ideal of $\mathcal{G}$, and $[\mathcal{G}/I]$ denotes a set of coset leaders.

- a binary $(n, k, d_{\min})$ encoder operates on some of the information data, and these coded bits are used to select $(C_1, \ldots, C_L) \in (\mathcal{G}/I)^L$.
- the remaining information bits are left uncoded and used to select $(Z_1, \ldots, Z_L) \in I^L$.
- the corresponding block codeword is $\mathbf{X} = (c_1 + Z_1, \ldots, c_L + Z_L) \in \mathcal{G}^L$, where c_i is the coset leader of C_i.

For a coset code, $\Delta_{\min}$ is bounded by the minimum determinant of I and the minimum distance $d_{\min}$ of the binary code:

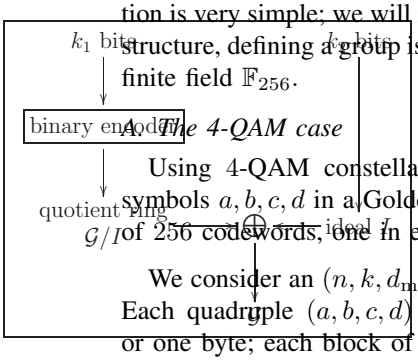
$$\Delta_{\min} \geq \min\left(\min_{X\in I\setminus\{0\}} |\det(X)|^2, d_{\min}^2\delta \right) \quad (14)$$

Fig. 1. The general structure of the encoder.

In fact, if $(c_1, \ldots, c_L) = \mathbf{0}$, then $\mathbf{X} \in I^L$, and for $\mathbf{X} \neq \mathbf{0}$, $\det(\mathbf{X}\mathbf{X}^H) \geq \min_{X \in I \setminus \{0\}} |\det(X)|^2$. If on the contrary $(c_1, \ldots, c_L) \neq \mathbf{0}$, there are at least $d_{\min}$ components of $\mathbf{X}$ which do not belong to I, and consequently are nonzero, and $\det(\mathbf{X}\mathbf{X}^H) \geq \delta w_H(\mathbf{X})^2 \geq \delta d_{\min}^2$.
So the performance of a coset code will be always limited by the minimum determinant of I, except if the code on I^L is the zero code.
If $I = 2\mathcal{G}$, the set of coset leaders *coincides* with the (4-QAM)^4 constellation, making it easier to implement coset codes with high Hamming distance.

V. Golden Reed-Solomon Codes

To exploit fully the ring structure of the quotient, one should use as the outer code an error-correcting code based on $M_2(\mathbb{F}_2[i])$; but at present very little is known about codes over non-commutative rings.
We choose shortened Reed-Solomon codes instead because they are maximum distance separable and their implementation is very simple; we will restrict our attention to the additive structure, defining a group isomorphism between $\mathcal{G}/2\mathcal{G}$ and the finite field $\mathbb{F}_{256}$.



A. The 4-QAM case

Using 4-QAM constellations to modulate each of the 4 symbols a, b, c, d in a Golden codeword (5), we obtain a total of 256 codewords, one in each coset of $2\mathcal{G}$.

We consider an $(n, k, d_{\min})$ Reed-Solomon code over $\mathbb{F}_{256}$. Each quadruple (a, b, c, d) of 4-QAM signals carries 8 bits or one byte; each block of n Golden codewords will carry n bytes, corresponding to k information bytes.
The encoding and decoding procedure involves several steps:

a) *Reed-Solomon encoding:* Each information byte can be seen as a binary polynomial of degree ≤ 8, that is, an element of the Galois field $\mathbb{F}_{256}$. An information message of k bytes, seen as a vector $\mathbf{U} = (U_1, \ldots, U_k) \in \mathbb{F}_{256}^k$, is encoded into a codeword $\mathbf{V} = (V_1, \ldots, V_n) \in \mathbb{F}_{256}^n$ using the RS$(n, k, d_{\min})$ shortened code $\mathcal{C}$.

b) *From the Galois field $\mathbb{F}_{256}$ to the matrix ring $M_2(\mathbb{F}_2[i])$:* We can represent the elements of $M_2(\mathbb{F}_2[i])$ as bytes, simply by vectorising each matrix and separating real and imaginary parts. Since we are only working with the additive structure, we can identify $\mathbb{F}_{256}$ and $M_2(\mathbb{F}_2[i])$, which are both $\mathbb{F}_2$-vector spaces of dimension 8.

c) *From the matrix ring $M_2(\mathbb{F}_2[i])$ to the quotient ring $\overline{\mathcal{G}}/2\overline{\mathcal{G}}$:* For this step we make use of the isomorphism of $\mathbb{F}_2[i]$-modules $(\varphi \circ \phi)^{-1} : \overline{\mathcal{G}}/2\overline{\mathcal{G}} \to M_2(\mathbb{F}_2[i])$ described in §IV-B that relates the coordinates with respect to the bases (13) and $\mathcal{B}_{\overline{\mathcal{G}}} = \{\alpha, \alpha\theta, \alpha j, \alpha\theta j\}$. Let $(a, b, c, d) \in \mathbb{Z}_2[i]^4$ be the coordinates of our codeword in the basis $\mathcal{B}_{\overline{\mathcal{G}}}$.

d) *Golden Code encoding*: For each of the n vector components, the symbols a,b,c,$d \in \mathbb{Z}_2[i]$ correspond to four 4-QAM signals, and can be encoded into a Golden codeword of the form (5). Thus we have obtained a Golden block $\mathbf{X} = \xi(\mathbf{V})$, where $\xi : \mathbb{F}_{256}^n \to \mathcal{G}^n$ is injective.

B. Decoding

ML decoding consists in the search for the minimum of the Euclidean distance $\sum_{i=1}^n \|HZ_i - Y_i\|^2$ over all the images $\mathbf{Z} = \xi(\mathbf{V}')$ of Reed-Solomon codewords.
One can first compute and store in memory the distances

$$d(i, j) = \left\| HZ^{(j)} - Y_i \right\|^2 \tag{15}$$

for every component $i = 1, \ldots, n$ of the received vector $\mathbf{Y}$ and for all the Golden codewords $Z^{(j)}, j = 0, .., 255$ that can be obtained from a quadruple $U^{(j)}$ of 4-QAM symbols. The search for the minimum can be carried out using the Viterbi algorithm or a tree search algorithm.

One can replace ML decoding with n separate Sphere Decoders on each of the components of $\mathbf{Y}$, followed by Reed-Solomon decoding. This "hard" decoding has the advantage of speed. However it is highly suboptimal: performance simulations show that with this method the coding gain is almost entirely cancelled out (see figure 2).

C. Simulation results

In the 4-QAM case, the spectral efficiency of the Golden Reed-Solomon codes is

$$\frac{8k \text{ bits}}{2n \text{ channel uses}} = \frac{4k}{n} \text{ bpcu}$$

From Lemma 1, we get a lower bound for $\Delta_{\min}$: using an $(n, k, d_{\min})$ Reed-Solomon code, we have $\Delta_{\min} \geq \delta d_{\min}^2$.
If $k = \frac{n}{2}$, the spectral efficiency is 2bpcu. Comparing the 4-QAM, $(n, k, d_{\min})$ Golden-RS design ($E_{\mathcal{S}} = 0.5$) with the uncoded Golden Code using BPSK ($E_{\mathcal{S},U} = 0.25$), we get an asymptotic coding gain of:

$$\gamma_{\text{as}} = \frac{\sqrt{\Delta_{\min}}/E_{\mathcal{S}}}{\sqrt{\Delta_{\min,U}}/E_{\mathcal{S},U}} = \frac{d_{\min}/0.5}{1/0.25} = \frac{d_{\min}}{2} \tag{16}$$

Figure 2 shows the performance comparison of the Golden-RS code $(4, 2, 3)$ with the uncoded scheme at 2bpcu. Assuming the channel to be constant for 4 blocks, the Golden-RS code outperforms the uncoded scheme by 6.1 dB.
This gain is unexpectedly high compared with the theoretical coding gain (16) for $d_{\min} = 3$, that is $10 \log_{10}\left(\frac{3}{2}\right)$ dB $=$

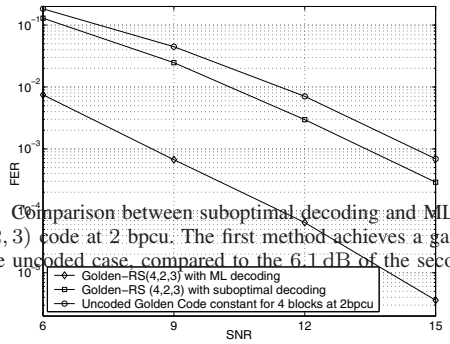


Fig. 2. Comparison between suboptimal decoding and ML decoding for the RS$(4,2,3)$ code at 2 bpcu. The first method achieves a gain of only $1.1\,\mathrm{dB}$ over the uncoded case, compared to the $6.1\,\mathrm{dB}$ of the second.

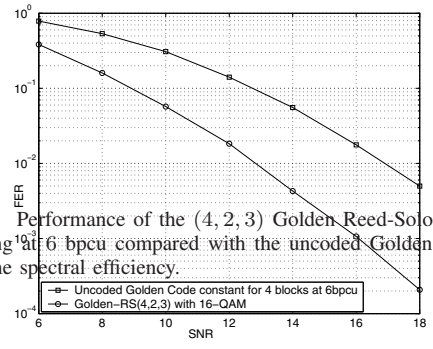


Fig. 3. Performance of the $(4,2,3)$ Golden Reed-Solomon code with soft decoding at 6 bpcu compared with the uncoded Golden Code scheme with the same spectral efficiency.

$1.7\,\mathrm{dB}$. Also for the $(6,3,4)$ code, the actual gain ($7.0\,\mathrm{dB}$) is higher than the theoretical gain ($10\log_{10}2\,\mathrm{dB} = 3.0\,\mathrm{dB}$).

D. The 16-QAM case

If we use a 16-QAM constellation for each symbol a, b, c, d in a Golden codeword, we have 2^{16} available Golden codewords, or 256 words for each of the 256 cosets of $2\mathcal{G}$ in $\mathcal{G}$. As in the 4-QAM case, we consider coset codes where the outer code is an $(n, k, d_{\min})$ Reed-Solomon code $\mathcal{C}$ on the quotient $\mathcal{G}/2\mathcal{G}$. The total information bits transmitted are $8k + 8n$; they will be encoded into $8n + 8n = 16n$ bits.

- The code $\mathcal{C}$ outputs $8n$ bits, which are used to encode the first two bits of $4n$ 16-QAM constellations, which identify one of the four cosets of $2\mathbb{Z}[i]$ in $\mathbb{Z}[i]$; each byte corresponds to a different coset configuration of (a, b, c, d).
- the other $8n$ bits, left uncoded, are used to choose the last two bits of each 16-QAM signal.

In total, we have $4n$ 16-QAM symbols, that is n Golden codewords $\mathbf{X} = (X_1, \ldots, X_n)$. The resulting spectral efficiency is

$$\frac{8(k+n)\text{ bits}}{2n\text{ channel uses}} = \frac{4(k+n)}{n}\text{ bpcu}$$

We have seen in (14) that

$$\Delta_{\min} \geq \min\left(\min_{X\in 2\mathcal{G}\setminus\{0\}} |\det(X)|^2, d^2_{\min}\delta\right) = \min(16\delta, d^2_{\min}\delta)$$

With an error-correcting code of rate $k = \frac{n}{2}$, we obtain a spectral efficiency of 6 bpcu.

- If $d_{\min} \geq 4$, we have $\gamma_{\mathrm{as}} = \frac{4/2.5}{1/1.5} = 2.4$, leading to an approximate gain of $3.8\,\mathrm{dB}$.
- If $d_{\min} = 3$, $\gamma_{\mathrm{as}} = \frac{3/2.5}{1/1.5} = 1.8$, giving a gain of $2.5\,\mathrm{dB}$.

Decoding

The ML decoding procedure for the 16-QAM case requires only a slight modification with respect the one illustrated in §V-B. In the first phase, for each component $i = 1, \ldots, n$ and for each coset leader W_j, $j = 0, \ldots, 255$, we find the closest point in that coset to the received component Y_i, that is

$$\hat{Z}_{i,j} = \operatorname*{argmin}_{Z\in 2\mathcal{G}} \|Y_i - H(Z + W_j)\|^2$$

Computing HZ and HW_j separately allows to carry out only 512 products instead of 256^2. The second phase can be performed as in the 4-QAM case, and the search is limited to the "closest points" $\hat{Z}_{i,j} + W_j$ found previously:

$$\hat{\mathbf{X}} = \operatorname*{argmin}_{(\hat{Z}_{1,j_1}+W_{j_1},\ldots,\hat{Z}_{n,j_n}+W_{j_n})} \sum_{i=1}^{n} \left\| H(\hat{Z}_{i,j_i} + W_{j_i}) - Y_i \right\|^2$$

over all the images $(W_{j_1}, \ldots, W_{j_n})$ of Reed-Solomon codewords.

Simulation results

In the 16-QAM case, the $(4,2,3)$ Golden Reed-Solomon code achieves a gain of $3.8\,\mathrm{dB}$ over the uncoded scheme at 6 bpcu at the frame error rate of 10^{-2} (see figure 3).

VI. Conclusions

In this paper we have presented Golden-RS codes, a coded modulation scheme for 2×2 slow fading MIMO channels, where the inner code is the Golden Code.
We use a simple binary partitioning, whose set of coset leaders coincides with a QAM symbol constellation. With a Reed-Solomon code as the outer code in order to increase the minimum Hamming distance among the codewords, we obtain a significant performance gain with respect to the uncoded case.

References

[1] J-C. Belfiore, G. Rekaya, E. Viterbo, "The Golden Code: a 2×2 full-rate Space-Time Code with non-vanishing determinants", *IEEE Trans. Inform. Theory*, vol 51 n. 4, 2005

[2] S. Benedetto, E. Biglieri, "Principles of Digital Transmission with Wireless Applications", Kluwer 1999

[3] G. D. Forney, "Coset codes- Part I: Introduction and geometrical classification", *IEEE Trans. Inform. Theory*, vol 34 n. 5, 1988

[4] Y. Hong, E. Viterbo, J.-C. Belfiore, "Golden Space-Time trellis coded modulation", *IEEE Trans. Inform. Theory*, vol 53 n. 5, 2007

[5] T. W. Hungerford, "Algebra", Springer-Verlag 1974

[6] I. Reiner, "Maximal Orders", Clarendon Press, Oxford 2003

[7] V. Tarokh, N. Seshadri, A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction", *IEEE Trans. Inform. Theory*, vol. 44 n. 2, 1998

[8] M-F. Vignéras, "Arithmétique des Algèbres de Quaternions", Lecture Notes in Mathematics, Springer Verlag 1980