The Aladdin-Pythagoras Space-Time Code

Joseph J. Boutros
Texas A&M University
Department of Electrical Engineering
Education City, Doha, Qatar
boutros@tamu.edu

Hugues Randriambololona
TELECOM ParisTech / LTCI CNRS UMR 5141
Computer Science and Networks Department
Paris, France
randriam@enst.fr

***Abstract*— Our motivation is the design of space-time coding which is optimal under both maximum likelihood and iterative decoding. We describe the construction of new full-rate space-time codes with non-vanishing determinant that satisfy the genie conditions for iterative probabilistic decoding. The problem combining the genie conditions and the rank criterion is rewritten in terms of a quadratic form. The construction over $\mathbb{Z}[i]$ (the cubic lattice) yields a family of codes defined by Pythagorean triples. The space-time code built over $\mathbb{Z}[i]$ and involving the quaternion algebra $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$ is referred to as the *Aladdin-Pythagoras code*. The construction over $\mathbb{Z}[j]$ (the hexagonal lattice) also yields a full-rate non-vanishing determinant code that is suitable for iterative decoding on multiple antenna channels.**

I. Introduction

Algebraic constructions of space-time block codes [12][13] for multiple antenna (MIMO) channels are usually based on design criteria established by analyzing the pairwise error probability under maximum likelihood (ML) decoding. These space-time coding criteria, originally published in [9][17], led to the design of coding for MIMO channels without taking into account the presence of efficient error-correcting codes or the potential use of iterative probabilistic decoding as known in modern coding theory [15].

Some unusual space-time codes, in the context of full-rate unitary linear precoding, have been proposed by applying two constraints to make the code suitable for iterative decoding [3][7]. These constraints, referred to as the *genie conditions*, were mainly used for linear precoding in bit-interleaved coded modulations such as in [8]. The analysis of these codes from a rank/determinant criterion point of view has never been performed. The main difficulty is encountered when trying to satisfy all constraints for both ML and iterative decoding.

In this paper, we propose a new space-time code satisfying the double constraints of ML and iterative decoding. We focus the study in this abstract on linear unitary precoders for 2×2 MIMO channels. The coherence time is assumed to be equal to 2. The channel is supposed to be frequency non-selective and its fading matrix (CSI) is perfectly known by the decoder. There is no CSI at the encoder and no feedback information from the decoder to the encoder. We briefly summarize the method of linear unitary precoding for MIMO channels and the genie conditions in the next section. Section III gives a reformulation of the problem and a quadratic form reduction in the 2×2 case. Section IV shows how to get a non-vanishing determinant under the genie conditions via algebraic number theoretic tools and discusses the optimality of the Aladdin-Pythagoras code. Some experimental results are illustrated in the final section.

II. Space-time linear unitary precoding

Consider a $n \times n$ MIMO channel, i.e., with n transmit and n receive antennas. A space-time codeword $\mathbf{C}$ of length N may be written in matrix form

$$\mathbf{C} = \begin{pmatrix} c_1^1 & c_2^1 & \dots & c_N^1 \\ \vdots & \vdots & & \vdots \\ c_1^n & c_2^n & \dots & c_N^n \end{pmatrix}.$$

Under ML decoding, the pairwise error probability is upper bounded as (e.g., see [5])

$$P(\mathbf{C} \to \mathbf{C}') \quad \leq \quad \left(\frac{1}{\prod_{i=1}^{t}(1+\lambda_i \gamma/4n)} \right)^n \quad \leq \quad \left(\frac{g\gamma}{4n}\right)^{-tn},$$

where γ is the transmitted signal-to-noise ratio per symbol, $t = rank(\mathbf{C} - \mathbf{C}')$, the coding gain is $g = (\lambda_1 \lambda_2 \cdots \lambda_t)^{1/t}$, and $\{\lambda_i\}$ are the eigen values of $(\mathbf{C} - \mathbf{C}')(\mathbf{C} - \mathbf{C}')^*$. Thus, the famous design criteria [9][17] for ML decoding can be recalled as follows:

- Rank: Full diversity is achieved if $t = n$.
- Product distance: Coding gain is maximized by maximizing the determinant.

Full diversity can be attained with $N = n$ if a suitable unitary matrix is applied to the codeword $\mathbf{C}$. Let us write the codeword in a linearized form $\mathbf{c}$ as a row of size n^2, $\mathbf{c} = (c_1, \dots, c_{n^2})$. The new codeword to be transmitted on the MIMO channel is $\mathbf{X} = \mathbf{c}\mathbf{S}$, where $\mathbf{S}$ is unitary. If the components of $\mathbf{c}$ belong to a bidimensional constellation (QAM modulation) and without taking into account a possible error-correcting code, the precoder $\mathbf{S}$ defines a space-time code given by the set of all codewords $\mathbf{X}$.

Now, let us briefly establish the genie conditions for iterative decoding [3][7]. For simplicity, take $n = 2$. The MIMO channel is defined by its fading matrix

$$\mathbf{H_0} = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix},$$

where h_{ij} are iid and $\mathbb{C}\mathcal{N}(0,1)$ distributed. The non-noisy part of the signal observed by the decoder is $\mathbf{XH}$, where

$$\mathbf{H} = \begin{pmatrix} \mathbf{H_0} & 0 \\ 0 & \mathbf{H_0} \end{pmatrix}.$$

The genie condition is equivalent to perfect extrinsic information (or a priori) generated by the error-correcting decoder. Under perfect a priori information, the performance depends on the squared Euclidean metric $D^2 = \|\mathbf{XH} - \mathbf{X'H}\|^2 = \|(\mathbf{c} - \mathbf{c}')\mathbf{SH}\|^2$ where $(\mathbf{c} - \mathbf{c}') = (\Delta, 0, 0, 0)$, i.e., only one component is different between the two codewords. Here, we assumed that this difference is in the first position. If $s = (s_{11}, s_{12}, s_{13}, s_{14})$ denotes the first row of the precoder $\mathbf{S}$, then the squared Euclidean metric becomes

$$D^2 = \Delta^2 \left[|s_{11}h_{11} + s_{12}h_{21}|^2 + |s_{11}h_{12} + s_{12}h_{22}|^2 \right. \\ \left. + |s_{13}h_{11} + s_{14}h_{21}|^2 + |s_{13}h_{12} + s_{14}h_{22}|^2 \right].$$

From the properties of χ^2 distributions [18][19], the best situation is encountered when all complex gaussians within the χ^2 are independent and have equal variance. These properties are translated into

- First genie condition: (s_{11}, s_{12}) must be orthogonal to (s_{13}, s_{14})
- Second genie condition: (s_{11}, s_{12}) and (s_{13}, s_{14}) must have equal norms.

Of course, the 4 rows of the precoder should satisfy the genie conditions as announced above for the first row. In the sequel, the property of $\mathbf{S}$ being unitary will be referred to as a *shaping* condition. Also, following [14], a space-time code defined by a unitary $\mathbf{S}$ will be called *perfect* if it has a non-vanishing determinant.

III. Matrix preliminaries

A. Intrinsic reformulation of the Genie conditions

For any integer n, we endow $M_n(\mathbb{C})$, the space of square $n \times n$ matrices, with the Hermitian scalar product

$$< \mathbf{A}, \mathbf{B} >_n = \frac{1}{n} \operatorname{tr} \mathbf{AB}^* = \frac{1}{n} \sum a_{ij} \overline{b_{ij}}$$

for $\mathbf{A} = (a_{ij})$ and $\mathbf{B} = (b_{ij})$ in $M_n(\mathbb{C})$. Notice the $\frac{1}{n}$ normalization.

We recall also that the unitary group $U(n)$ is the subset of the elements $\mathbf{V} \in M_n(\mathbb{C})$ satisfying

$$\mathbf{VV}^* = \mathbf{I}_n.$$

Thus any such V has norm

$$\|\mathbf{V}\|_n = 1.$$

Consider now a linear space-time code of order n. In linearized form, as described in the previous section, the codeword associated to symbols $(c_1, \ldots, c_{n^2})$ is $\mathbf{X} = (c_1, \ldots, c_{n^2})\mathbf{S}$ where $\mathbf{S} = (s_{ij})$ is the square $n^2 \times n^2$ matrix of the precoder.

Alternatively, for any such matrix $\mathbf{S}$, let $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ be the square $n \times n$ matrices whose linearizations are the rows of $\mathbf{S}$, scaled by a factor $\sqrt{n}$. Explicitly, the (j,k) entry of $\mathbf{M}_i$ is $\sqrt{n}s_{i,(j-1)n+k}$. Then in matrix form the codeword associated to $\mathbf{c} = (c_1, \ldots, c_{n^2})$ is $\mathbf{X_c} = \frac{1}{\sqrt{n}}(c_1\mathbf{M}_1 + \cdots + c_{n^2}\mathbf{M}_{n^2})$.

Proposition 1: With $\mathbf{S}$ and the $\mathbf{M}_i$ as defined, we can reformulate the shaping and genie conditions as follows:

1) The matrix $\mathbf{S}$ is unitary (that is, in $U(n^2)$) if and only if $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ form a unitary basis for the Hermitian product $< .,. >_n$ in $M_n(\mathbb{C})$.
2) The matrix S satisfies the genie conditions if and only if $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ are in $U(n)$.

Putting all this together:

Definition 1: We say $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ satisfy (S+G) if they are in $U(n)$ and are mutually orthogonal in $M_n(\mathbb{C})$.

Let now $\mathcal{A}$ be any constellation (finite or infinite) in $\mathbb{C}$. We define the minimum determinant of $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ on $\mathcal{A}$ as the infimum value of $|\det \mathbf{X}_{\mathbf{c}-\mathbf{c}'}|$ for $\mathbf{c}, \mathbf{c}' \in \mathcal{A}^{n^2}$, $\mathbf{c} \neq \mathbf{c}'$.

Our problem is then to find $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ satisfying (S+G) and with minimum determinant non-zero, and ideally as large as possible.

Definition 2: We say that two families $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ and $\mathbf{M}'_1, \ldots, \mathbf{M}'_{n^2}$ are equivalent if there exist $\mathbf{V}, \mathbf{W} \in U(n)$ such that $\mathbf{M}'_i = \mathbf{VM}_i\mathbf{W}$ for all i.

Proposition 2: Suppose $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ and $\mathbf{M}'_1, \ldots, \mathbf{M}'_{n^2}$ are equivalent. Then:

1) $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ satisfy (S+G) if and only if $\mathbf{M}'_1, \ldots, \mathbf{M}'_{n^2}$ do.
2) $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$ and $\mathbf{M}'_1, \ldots, \mathbf{M}'_{n^2}$ have the same minimum determinant.

Proof: Since $U(n)$ is a group, if $\mathbf{M}_i$ is in $U(n)$, then $\mathbf{M}'_i = \mathbf{VM}_i\mathbf{W}$ also. If $\mathbf{M}_i \perp \mathbf{M}_j$ in $M_n(\mathbb{C})$, then $\mathbf{M}'_i \perp \mathbf{M}'_j$ also because $\mathbf{M}'_i{\mathbf{M}'_j}^* = \mathbf{VM}_i\mathbf{WW}^*\mathbf{M}_j^*\mathbf{V}^* = \mathbf{VM}_i\mathbf{M}_j^*\mathbf{V}^*$ so that $\operatorname{tr}\mathbf{M}'_i{\mathbf{M}'_j}^* = \operatorname{tr}\mathbf{VM}_i\mathbf{M}_j^*\mathbf{V}^* = \operatorname{tr}\mathbf{M}_i\mathbf{M}_j^*\mathbf{V}^*\mathbf{V} = \operatorname{tr}\mathbf{M}_i\mathbf{M}_j = 0$. Finally for $\mathbf{c}, \mathbf{c}' \in \mathcal{A}^{n^2}$ one has $\mathbf{X}'_{\mathbf{c}-\mathbf{c}'} = \mathbf{VX}_{\mathbf{c}-\mathbf{c}'}\mathbf{W}$ so they have same determinant. ■

B. The 2×2 MIMO case: Reduction to a quadratic form approach

We are now interested in the case $n = 2$.

Theorem 1: Any $\mathbf{M}_1, \ldots, \mathbf{M}_4$ in $M_2(\mathbb{C})$ satisfying (S+G) are equivalent to some

$$\mathbf{M}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{M}_2 = \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix},$$

$$\mathbf{M}_3 = \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix}, \qquad \mathbf{M}_4 = \begin{pmatrix} 0 & \gamma \\ -\gamma & 0 \end{pmatrix},$$

for $\alpha, \beta, \gamma \in \mathbb{C}$ with $|\alpha| = |\beta| = |\gamma| = 1$.

Proof: After replacing each $\mathbf{M}_i$ with $\mathbf{M}_1^{-1}\mathbf{M}_i$, we can suppose $\mathbf{M}_1 = \mathbf{I}_2$. Now by the diagonalization theorem for unitary matrices we can find $\mathbf{V} \in U(2)$ such that $\mathbf{VM}_2\mathbf{V}^*$ is diagonal. After replacing each $\mathbf{M}_i$ with $\mathbf{VM}_i\mathbf{V}^*$ (which does not modify $\mathbf{M}_1$), we can suppose $\mathbf{M}_2$ is diagonal, and since $\mathbf{M}_2 \perp \mathbf{M}_1$, it is of the form $\mathbf{M}_2 = \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}$.

Now $\mathbf{M}_3$ is orthogonal to $\mathbf{M}_1$ and $\mathbf{M}_2$, so it must be anti-diagonal, say $\mathbf{M}_3 = \begin{pmatrix} 0 & \beta \\ \beta' & 0 \end{pmatrix}$. Then we put $\mathbf{W} =$

$\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{\beta/\beta'} \end{pmatrix}$, and after replacing each $\mathbf{M}_i$ with $\mathbf{W}\mathbf{M}_i\mathbf{W}^*$ (which does not modify $\mathbf{M}_1$ nor $\mathbf{M}_2$), we can suppose $\beta = \beta'$. Finally, $\mathbf{M}_4$ is orthogonal to $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3$ so it must be as indicated. ■

For $u, v, w \in \mathbb{C}$ with $|u| = |v| = |w| = 1$, consider the quadratic form [11]

$$q_{u,v,w}(\mathbf{z}) = z_1^2 - uz_2^2 - vz_3^2 + wz_4^2,$$

for $\mathbf{z} = (z_1, z_2, z_3, z_4) \in \mathbb{C}^4$. Now for any constellation $\mathcal{A}$ in $\mathbb{C}$, put

$$\operatorname{maxqmin}(\mathcal{A}) = \sup_{|u|=|v|=|w|=1} \left(\inf_{\substack{\mathbf{c},\mathbf{c}' \in \mathcal{A}^4 \\ \mathbf{c} \neq \mathbf{c}'}} |q_{u,v,w}(\mathbf{c} - \mathbf{c}')| \right).$$

In particular if $\mathcal{A}$ is an additive subgroup of $\mathbb{C}$,

$$\operatorname{maxqmin}(\mathcal{A}) = \sup_{|u|=|v|=|w|=1} \left(\inf_{\mathbf{c} \in \mathcal{A}^4 \setminus \{\mathbf{0}\}} |q_{u,v,w}(\mathbf{c})| \right).$$

Corollary 1: With these notations, the supremum value of the minimum determinant of 2×2 linear space-time codes on $\mathcal{A}$ satisfying the shaping and genie conditions is

$$\frac{1}{2} \operatorname{maxqmin}(\mathcal{A}).$$

In particular, a perfect 2×2 space-time code for $\mathcal{A}$ satisfying the genie conditions exists if and only if $\operatorname{maxqmin}(\mathcal{A}) > 0$.

Moreover, if $\operatorname{maxqmin}(\mathcal{A}) > 0$ is attained for a particular value of u, v, w, then there exists a corresponding code with optimal coding gain.

Proof: This is a consequence of propositions 1 and 2, theorem 1, and the following observation:

For $\mathbf{M}_1, \ldots, \mathbf{M}_4$ as in the theorem and for $\mathbf{c} \in \mathcal{A}^4$, one has $\mathbf{X_c} = \frac{1}{\sqrt{2}} \begin{pmatrix} c_1 + \alpha c_2 & \beta c_3 + \gamma c_4 \\ \beta c_3 - \gamma c_4 & c_1 - \alpha c_2 \end{pmatrix}$ so that

$$\det \mathbf{X_c} = \frac{1}{2}(c_1^2 - \alpha^2 c_2^2 - \beta^2 c_3^2 + \gamma^2 c_4^2) = \frac{1}{2} q_{u,v,w}(\mathbf{c}),$$

where $u = \alpha^2$, $v = \beta^2$, $w = \gamma^2$. To conclude, remark then that u, v, w can take any values independently in the circle $|z| = 1$ when α, β, γ do so. ■

IV. The Aladdin-Pythagoras space-time code construction

A. Number theoretic considerations

Having corollary 1 in mind, we search for a lower bound on $\operatorname{maxqmin}(\mathcal{A})$ for $\mathcal{A} = \mathbb{Z}[i]$ or $\mathbb{Z}[j]$. In order to achieve that, a sufficient condition is to pick some convenient value for u, v, w and then give a lower bound on $|q_{u,v,w}(\mathbf{c})|$ for $\mathbf{c} \in \mathcal{A}^4 \setminus \{\mathbf{0}\}$. This will be done using algebraic number theory [16][21].

Let $K = \mathcal{A}_{\mathbb{Q}} = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$. Observe that if we take $u, v \in K$ and $w = uv$, then $q_{u,v,w}$ is the reduced norm form of the generalized quaternion algebra $\left(\frac{u,v}{K}\right)$ in the naturally associated basis. If this quaternion algebra is a division algebra, then $q_{u,v,w}$ does not represent 0. Moreover, if $d \in \mathcal{A}$ is a common denominator for u, v, w, then $q_{u,v,w}(\mathbf{c}) \in \frac{1}{d}\mathcal{A}$ for $\mathbf{c} \in \mathcal{A}^4$, so that if it is non-zero, one has $|q_{u,v,w}(\mathbf{c})| \geq \frac{1}{|d|}$. This will give our lower bound.

Our task is then to find $u, v \in K$, with $|u| = |v| = 1$, and such that $\left(\frac{u,v}{K}\right)$ is a division algebra, that is such that u is not a square in K and v is not a norm from $K(\sqrt{u})$ to K. It would also be pleasant to keep their denominators as small as possible.

Lemma 1: For each prime p in $\mathbb{Z}$ that splits in K (that is $p \equiv 1 \mod 4$ for $\mathcal{A} = \mathbb{Z}[i]$ and $p \equiv 1 \mod 3$ for $\mathcal{A} = \mathbb{Z}[j]$) chose a factorization $p = x_p \overline{x_p}$ in K.

Then the subgroup $|z| = 1$ of $K^\times$ is the direct sum of the group of units in $\mathcal{A}$ (that is $\{\pm 1, \pm i\}$ for $\mathbb{Z}[i]$ and $\{\pm 1, \pm j, \pm j^2\}$ for $\mathbb{Z}[j]$) and of the free cyclic groups generated by the $x_p/\overline{x_p}$.

Proof: Consequence of the unique factorization in $\mathcal{A}$. ■

Lemma 2: The units in $\mathcal{A}$ that are not squares in K are $\{\pm i\}$ for $\mathcal{A} = \mathbb{Z}[i]$ and $\{-1, -j, -j^2\}$ for $\mathcal{A} = \mathbb{Z}[j]$.

If we take u such a unit, then all other units are norms from $K(\sqrt{u})$ to K.

Proof: Direct (and easy) computation. ■

Since we want to keep denominators as small as possible, the first part of this lemme allows us to take $u = i$ for $\mathcal{A} = \mathbb{Z}[i]$ and $u = -1$ for $\mathcal{A} = \mathbb{Z}[j]$. However, because of the second part of this same lemma, we cannot take v a unit, so we will take it as $v = x_p/\overline{x_p}$ for p a small convenient prime. This will give the lower bound $|q_{u,v,w}(\mathbf{c})| \geq \frac{1}{|\overline{x_p}|} = \frac{1}{|\sqrt{p}|}$ (when non-zero).

Lemma 3: With these notations, a necessary and sufficient condition for v not to be a norm from $K(\sqrt{u})$ to K, is that $p \equiv 5 \mod 8$ for $\mathcal{A} = \mathbb{Z}[i]$, or $p \equiv 7 \mod 12$ for $\mathcal{A} = \mathbb{Z}[j]$.

Proof: We treat only the case $\mathcal{A} = \mathbb{Z}[i]$, and we prove only the 'sufficient' part since this is the only one that will be used in the sequel (for completeness, one proof of the 'necessary' part, using Hensel's lifting and Hasse's norm theorems, will be given in a forthcoming paper).

So let $K = \mathbb{Q}(i)$ and $u = i$. Suppose $p \equiv 5 \mod 8$ and $v = x_p/\overline{x_p}$ is a norm from $K(\sqrt{u})$ to K. Then $p = \overline{x_p}^2 v$ also is a norm, so there are $x, y \in K$ with $x^2 - iy^2 = p$. Since $p \equiv 1 \mod 4$, the polynomial $X^2 + 1$ is split in $\mathbb{F}_p$, so it admits a root $\overline{I}$ there, and by Hensel lifting it admits a root I in $\mathbb{Z}_p$. We thus get an embedding of K in $\mathbb{Q}_p$ by sending i to I, and we get $x', y' \in \mathbb{Q}_p$ satisfying $x'^2 - Iy'^2 = p$. Since $I \in \mathbb{Z}_p$ and $v_p(p) = 1$, one cannot have both $v_p(x')$ and $v_p(y') > 0$. Let thus $m = -\min(v_p(x'), v_p(y')) \geq 0$, so that $x'' = p^m x'$ and $y'' = p^m y'$ are in $\mathbb{Z}_p$, one of them at least is a unit, and they satisfy $x''^2 - Iy''^2 = p^{2m+1}$. Then in $\mathbb{F}_p$ one has $\overline{x''}^2 - \overline{I}\,\overline{y''}^2 = 0$, so that $\overline{x''}$ and $\overline{y''}$ both are non-zero and $\overline{I} = (\overline{x''}/\overline{y''})^2$ is a square in $\mathbb{F}_p$. But $\overline{I}$ has order 4 in $\mathbb{F}_p^\times$, so its square root has order 8, and by Lagrange's theorem $p \equiv 1 \mod 8$, a contradiction. ■

Taking $p = 5$, we have proved:

$$\operatorname{maxqmin}(\mathbb{Z}[i]) \geq \frac{1}{\sqrt{5}} \tag{1}$$

and in the same way $\operatorname{maxqmin}(\mathbb{Z}[j]) \geq \frac{1}{\sqrt{7}}$.

B. *Optimality of the Aladdin-Pythagoras code*

We explicit the codes so constructed for $\mathcal{A} = \mathbb{Z}[i]$. Let $p \equiv 5 \mod 8$ be prime. Then one has $p = a^2 + b^2$ for $x_p = a + ib$. Let also $x_p^2 = c + id$, so $c = a^2 - b^2$ and $d = 2ab$. Then $p^2 = c^2 + d^2$, and (c, d, p) is known as a Pythagorean triple. For $u = i$, $v = x_p/\overline{x_p} = x_p^2/p$ and $w = uv$ the quadratic form $q_{u,v,w}$ is given by

$$q_{u,v,w}(\mathbf{z}) = (z_1^2 - iz_2^2) - \tfrac{c+id}{p}(z_3^2 - iz_4^2),$$

and the code can be constructed by putting in theorem 1 $\alpha = \sqrt{u} = e^{i\pi/4}$, $\beta = \sqrt{v} = x_p/\sqrt{p}$ and $\gamma = \sqrt{w} = \alpha\beta$. It has minimum determinant at least $\frac{1}{2|\overline{x_p}|} = \frac{1}{2\sqrt{p}}$.

Since the construction of these codes involves Pythagorean triples, they could be named Pythagorean codes.

For the particular case $p = 5$ one can take $x_5 = 2 + i$ (with associated triple $(3, 4, 5)$) so that

- $\alpha = \frac{1+i}{\sqrt{2}} = e^{i\pi/4}$
- $\beta = \frac{2+i}{\sqrt{5}} = e^{i\,\mathrm{atan}(1/2)}$
- $\gamma = \frac{1+3i}{\sqrt{10}} = e^{i\,\mathrm{atan}(3)}$.

The precoder matrix is

$$\mathbf{S} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ \alpha & 0 & 0 & -\alpha \\ 0 & \beta & \beta & 0 \\ 0 & \gamma & -\gamma & 0 \end{pmatrix}$$

and for $\mathbf{c} \in \mathbb{Z}[i]^4$, one has

$$\mathbf{X_c} = \frac{1}{\sqrt{2}} \begin{pmatrix} c_1 + \alpha c_2 & \beta c_3 + \gamma c_4 \\ \beta c_3 - \gamma c_4 & c_1 - \alpha c_2 \end{pmatrix}$$

with determinant

$$\begin{aligned} \det \mathbf{X_c} &= \tfrac{1}{2}((c_1^2 - ic_2^2) - \tfrac{2+i}{2-i}(c_3^2 - ic_4^2)) \\ &= \tfrac{1}{2}((c_1^2 - ic_2^2) - \tfrac{3+4i}{5}(c_3^2 - ic_4^2)) \end{aligned}$$

always at least $\frac{1}{2\sqrt{5}}$ for non-zero $\mathbf{c}$. In fact $|\det \mathbf{X_c}| = \frac{1}{2\sqrt{5}}$ is attained for $\mathbf{X_c} = (0, i, 1, i)$, so this is the exact value of its minimum determinant.

Observe that the quaternion algebra involved in the construction of this code is $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$, the same as for the Golden Code [1] (although we use a different lattice in this algebra). Since this code contains a genie and is somewhat Golden, it could be named Aladdin-Pythagoras Code.

Theorem 2: Aladdin-Pythagoras Code is a perfect 2 × 2 space-time code over $\mathbb{Z}[i]$ satisfying the genie conditions, with minimum determinant $\frac{1}{2\sqrt{5}}$. Moreover, it has optimal coding gain: any code satisfying these properties has minimum determinant strictly less than $\frac{1}{2\sqrt{5}}$, unless it is equivalent to Aladdin-Pythagoras Code.

In fact, this optimality property already holds when restricted to a 16-QAM.

Proof: We compute $\mathrm{maxqmin}(16\text{-QAM})$. This is a finite optimization problem: maximize

$$\min_{\substack{\mathbf{c},\mathbf{c}' \in (16\text{-QAM})^4 \\ \mathbf{c} \neq \mathbf{c}'}} |q_{u,v,w}(\mathbf{c} - \mathbf{c}')|,$$

for $|u| = |v| = |w| = 1$. This can be performed exactly, and find a unique solution (up to obvious changes of variables), which is as before $u = i = e^{i\pi/2}$, $v = \frac{3+4i}{5} = e^{i\,\mathrm{atan}(4/3)}$, $w = uv$, with $|q_{u,v,w}|$ minimum equal to $\frac{1}{\sqrt{5}}$ for $\mathbf{c} - \mathbf{c}' = (0, i, 1, i)$. Thus

$$\frac{1}{\sqrt{5}} = \mathrm{maxqmin}(16\text{-QAM}) \geq \mathrm{maxqmin}(\mathbb{Z}[i]) \geq \frac{1}{\sqrt{5}},$$

so all these inequalities are equalities, and we conclude with corollary 1. ■

In the same way, one can construct a perfect 2 × 2 space-time code over $\mathbb{Z}[j]$ satisfying the genie conditions, with optimal coding gain. Its minimum determinant is $\frac{1}{2\sqrt{7}}$. At first sight this looks worse than the $\frac{1}{2\sqrt{5}}$ obtained before, however comparing the performances of these two codes would require a closer analysis, since one should keep in mind that $\mathbb{Z}[j]$ has higher density than $\mathbb{Z}[i]$.

V. Experimental results

In this section, probabilistic decoding in presence of a genie is simulated on a computer with both $\mathcal{A} = QPSK$ and $\mathcal{A} = 256 - QAM$ modulations. There is no need for a soft-output version of the Sphere Decoder [20], flipping one symbol is sufficient while computing the decoding metrics. Different precoders are compared: The cyclotomic rotations found in [2] and modified as in [3][7] to match the genie conditions, the Golden code as defined in [1], the Dayal-Varanasi code [4], the Tilted QAM proposed in [22], and our Aladdin-Pythagoras code. Other interesting precoders can be found in the literature such as the GIOM (Genie+Information Outage Minimization) [10] and the TAST code [6]. As expected, the SNR difference between the best precoders is negligible (even a random selection among 2000 matrices as for GIOM yields a relatively excellent precoder). As known, the Golden code and Dayal-Varanasi exhibit equivalent performance. The tilted QAM is outperformed by the other precoders. Also as expected, the cyclotomic rotation shows performance similar to Aladdin-Pythagoras code. In the future work, deeper comparisons should be made between unitary space-time codes, mainly we should look for more equivalences and determine unknown determinant value for some codes in the non-vanishing case.

References

[1] J.-C. Belfiore, G. Rekaya, and E. Viterbo,"The golden code: a 2x2 full-rate space-time code with non-vanishing determinants," *IEEE Trans. on Inf. Theory*, vol. 51, no. 4, pp. 1432-1436, Apr. 2005.

[2] J.J. Boutros and E. Viterbo, "Signal space diversity: a power and bandwidth efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. on Inf. Theory*, vol. 44, no. 4, pp. 1453-1467, Jul. 1998.

[3] J.J. Boutros, N. Gresset, and L. Brunel,"Turbo coding and decoding for multiple antenna channels," *Int. Symp. on Turbo Codes*, Brest, Sept. 2003. Downloadable at *http://www.josephboutros.org/coding*

[4] P. Dayal and M.K. Varanasi,"An optimal two transmit antenna space-time code and its stacked extensions," *IEEE Trans. on Inf. Theory*, vol. 51, no. 12, pp. 4348-4355, Dec. 2005.

[5] H. El Gamal and A.R. Hammons,Jr., "On the design of algebraic space-time codes for MIMO block-fading channels," *IEEE Trans. on Inf. Theory*, vol. 49, no. 1, pp. 151-163, Jan. 2003.

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

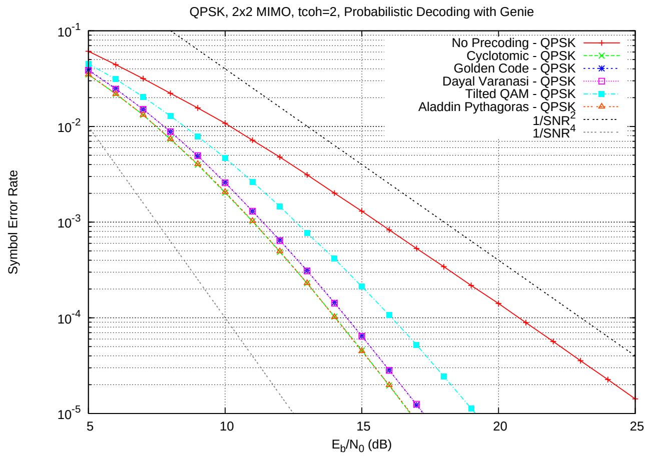

Fig. 1. QPSK with different space-time precoders.

[7] N. Gresset, J.J. Boutros, and L. Brunel, “Optimal linear precoding for BICM over MIMO channels,” In Proc. *IEEE Int. Symp. on Inf. Theory*, Chicago, IL, pp. 66, June 2004.

[8] N. Gresset, L. Brunel, and J.J. Boutros, “Space-time coding techniques with bit-interleaved coded modulations for MIMO block-fading channels,” *IEEE Trans. on Inf. Theory*, vol. 54, no. 5, pp. 2156-2178, May 2008.

[9] J.-C. Guey, M.P. Fitz, M.R. Bell, and W.-Y. Kuo, “Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels,” In Proc. *Vehicular Technology Conf. (VTC’96)*, Atlanta, GA, Apr. 1996.

[10] G.M. Kraidy, N. Gresset, and J.J. Boutros, “Information theoretical versus algebraic constructions of linear unitary precoders for non-ergodic multiple antenna channels”, In Proc. *The Ninth Canadian Workshop on Information Theory*, Montréal, Canada, pp. 406-409, June 2005.

[11] T.Y. Lam, Introduction to Quadratic Forms over Fields, American Mathematical Society, 2004.

[12] E.R. Larsson and P. Stoica, *Space-Time Block Coding for Wireless Communications*, Cambridge University Press, 2003.

[13] C. Oestges and B. Clerckx, MIMO Wireless Communications: from real-world propagation to space-time code design, Academic Press, Elsevier, 2007.

[14] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, “Perfect space-time block codes,” *IEEE Trans. on Inf. Theory*, vol. 52, no. 9, pp. 3885-3902, Sept. 2006.

[15] T.J. Richardson and R.L. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008.

[16] P. Samuel, *Théorie Algébrique des Nombres*, Hermann, 1967.

[17] V. Tarokh, N. Seshadri, and A.R. Calderbank, “Space-time codes for high data rate wireless communication: performance criterion and code construction,” *IEEE Trans. on Inf. Theory*, vol. 44, no. 2, pp. 744-765, Mar. 1998.

[18] D.N.C. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, Cambridge University Press, 2005.

[19] V.V. Veeravalli,”On performance analysis for signaling on correlated fading channels,” *IEEE Trans. on Comm.*, vol. 49, no. 11, pp. 1879-85, Nov. 2001.

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

[21] A. Weil, *Basic Number Theory*, Springer, 1995.

[22] H. Yao and G.W. Wornell,“Structured space-time block codes with optimal diversity-multiplexing tradeoff and minimum delay,” In Proc. *Globecom 2003*, San Francisco, CA, vol. 4, pp. 1941-1945, Dec. 2003.

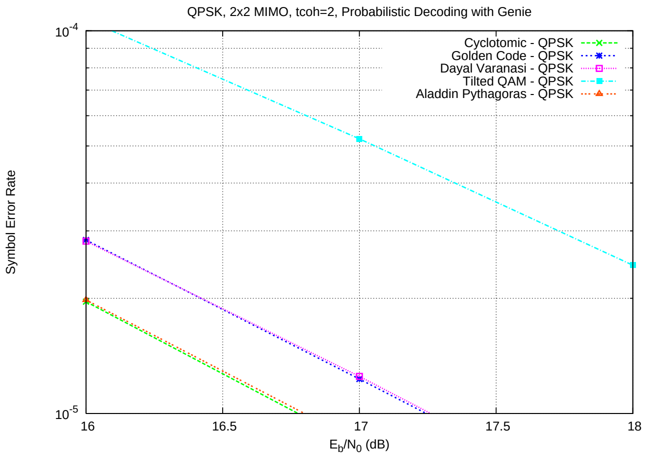

Fig. 2. QPSK with different space-time precoders (Zoom on Fig. 1).

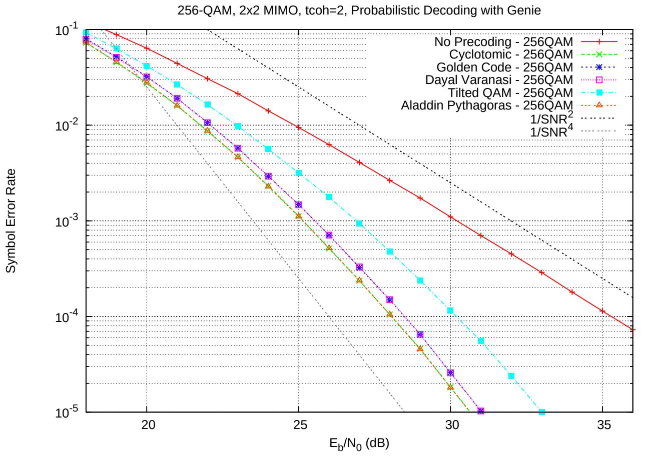

Fig. 3. 256-QAM with different space-time precoders.

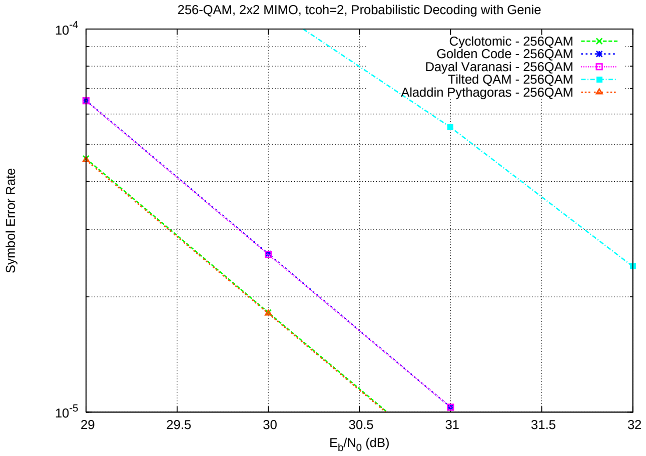

Fig. 4. 256-QAM with different space-time precoders (Zoom on Fig. 3).