

---

# Le code spatio-temporel d'Aladin-Pythagore

Joseph J. Boutros<sup>1</sup>, Hugues Randriambololona<sup>2</sup>

1. Texas A&M University at Qatar  
Education City, 23874, Doha, Qatar  
boutros@tamu.edu

2. Télécom ParisTech / LTCI CNRS UMR 5141  
46 rue Barrault, 75013 Paris, France  
randriam@enst.fr

---

**RÉSUMÉ.** Dans le cadre des transmissions à antennes multiples, on étudie la construction d'un précodeur linéaire unitaire ayant un déterminant non nul et vérifiant les conditions du génie. Un tel précodeur sera optimisé à la fois pour le décodage à maximum de vraisemblance et pour le décodage probabiliste itératif. En combinant le critère du rang et les conditions du génie, on obtient une nouvelle famille de codes spatio-temporels sur  $\mathbb{Z}[i]$ , construits à partir de triplets pythagoriciens : les codes pythagoriciens. Dans cette famille, le code associé au triplet (3,4,5) – ou encore à l'algèbre de quaternions  $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$  – est optimal. On l'appellera le code d'Aladin-Pythagore, ou plus simplement, le code d'Aladin.

**ABSTRACT.** We study linear unitary precoding for multiple antenna transmissions. Our aim is to find a new precoder satisfying both the genie conditions and the non-vanishing determinant criterion. Such a precoder will be optimized for both maximum likelihood and iterative probabilistic decoding. By combining the rank criterion and the genie conditions, we propose a new family of space-time codes over  $\mathbb{Z}[i]$  defined by Pythagorean triples. In this family, the space-time code associated with the triple (3,4,5) – or with the quaternion algebra  $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$  – is optimal. We will refer to it as Aladdin-Pythagoras, or more simply, Aladdin's Code.

**MOTS-CLÉS :** codage spatio-temporel, décodage itératif probabiliste, conditions du génie, critère du rang, algèbre de quaternions.

**KEYWORDS :** space-time coding, iterative probabilistic decoding, genie conditions, rank criterion, quaternion algebra.

---

DOI:10.3166/TS.27.147-160 © 2010 Lavoisier, Paris

## Extended abstract – The Aladdin-Pythagoras Space-Time Code

High data rates on wireless channels can be attained through multiple antennas installed on both transmitter and receiver sides (Larsson *et al.*, 2003)(Oestges *et al.*, 2007). Multiple antenna systems also offer spatial diversity which is a great means to ensure a low error probability in presence of fading (Tse *et al.*, 2005). At the receiver side, all known combining methods produce a diversity order equal to the number of receive antennas. A transmit diversity order, which is upperbounded by the number of transmit antennas, is achieved if a well designed space-time code is employed at the channel input.

Algebraic constructions of space-time block codes for multiple antenna channels (also referred to as 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 (Guey *et al.*, 1996) (Tarokh *et al.*, 1998), 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 (Richardson *et al.*, 2008).

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 (Boutros *et al.*, 2003) (Gresset *et al.*, 2004). These constraints, known as the *genie conditions*, were mainly used for linear precoding in bit-interleaved coded modulations such as in (Gresset *et al.*, 2008). 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. This is done in the present work.

In this paper, our goal is the design of space-time coding which is optimal under both maximum likelihood and iterative decoding. We focus the study on linear unitary precoders for  $2 \times 2$  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 Section 1.

Section 2 gives a reformulation of the problem and a quadratic form reduction in the  $2 \times 2$  case. Let  $\mathbf{c} \in \mathcal{A}^4 \setminus \{\mathbf{0}\}$  for  $\mathcal{A} = \mathbb{Z}[i]$  be an information vector. The space-time codeword resulting from a linear precoding applied to  $\mathbf{c}$  on a  $2 \times 2$  MIMO channel can be written in matrix form

$$\mathbf{X}_{\mathbf{c}} = \frac{1}{\sqrt{2}}(c_1\mathbf{M}_1 + \dots + c_4\mathbf{M}_4).$$

Our problem can then be reformulated as follows: find  $2 \times 2$  basis matrices  $\mathbf{M}_1, \dots, \mathbf{M}_4$  for the code, satisfying the two conditions

(1) *Shaping*: the  $\mathbf{M}_i$  form a unitary basis of the vector space of all  $2 \times 2$  matrices, equipped with its natural Hermitian scalar product (up to some scaling constant),

(2) *Genie*: the  $\mathbf{M}_i$  are unitary matrices, *i.e.* they lie in the group  $U(2)$

and such that the minimal value of  $|\det \mathbf{X}_{\mathbf{c}}|$  as  $\mathbf{c}$  ranges in  $\mathcal{A}^4 \setminus \{\mathbf{0}\}$  is non-zero, and as large as possible.

It is shown that for  $n = 2$ , matrices satisfying these two conditions can always be put in the form

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

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

for  $\alpha, \beta, \gamma \in \mathbb{C}$  with  $|\alpha| = |\beta| = |\gamma| = 1$ . Taking the determinant, our optimization problem is then to find  $\alpha, \beta, \gamma$  such that the minimum (absolute) value over non-zero  $\mathbf{c}$  of the quadratic form

$$\frac{1}{2}(c_1^2 - \alpha^2 c_2^2 - \beta^2 c_3^2 + \gamma^2 c_4^2)$$

is as large as possible.

This last task is done in Section 3 via algebraic number theoretic tools (the underlying ideas belong to the theory of generalized quaternion algebras). We obtain a family of codes with non-vanishing determinant that satisfy the genie conditions. The quadratic form expressing their determinant involves Pythagorean triples, hence their name, *Pythagorean codes*.

The simplest code in this family is the one associated with the triple (3,4,5). For reasons explained below, we named it the Aladdin-Pythagoras space-time code, or more simply, *Aladdin's code*. It is found to be given by

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

where  $\mathbf{c} \in \mathbb{Z}[i]^4$ , and  $\alpha = \frac{1+i}{\sqrt{2}}$ ,  $\beta = \frac{2+i}{\sqrt{5}}$ ,  $\gamma = \frac{1+3i}{\sqrt{10}}$ .

This code is a perfect  $2 \times 2$  space-time code satisfying the genie conditions and admitting a minimum determinant equal to  $\frac{1}{2\sqrt{5}}$ , which is shown to be optimal. A careful examination also shows this code admits strong algebraic relations with the so-called golden code (Belfiore *et al.*, 2005): although different, both are  $\mathbb{Z}[i]$ -lattices in the same generalized quaternion algebra  $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$ . To summarize, this code is (somewhat) golden and contains a genie, hence its name.

Experimental results are illustrated in the final section with error rate comparisons (at least under iterative probabilistic decoding) to some famous space-time codes given in the literature.

## 1. Le précodage spatio-temporel

Les constructions algébriques de codes en blocs spatio-temporels (Larsson *et al.*, 2003)(Oestges *et al.*, 2007) pour les canaux numériques à antennes multiples (MIMO) sont généralement basées sur un critère établi après analyse de la probabilité d'erreur par paire avec un décodage à maximum de vraisemblance (MV). Ce critère de conception, connu sous le nom de *critère du rang* ou *critère du déterminant*, publié à l'origine par (Guey *et al.*, 1996) et (Tarokh *et al.*, 1998) ne tient pas compte de la présence de codes correcteurs d'erreurs puissants utilisant le décodage itératif probabiliste (Richardson *et al.*, 2008). De manière peu habituelle, certains codes spatio-temporels construits à l'aide d'un précodage linéaire unitaire ont été proposés pour le décodage itératif (Boutros *et al.*, 2003) (Gresset *et al.*, 2008) en imposant deux contraintes dites *contraintes du génie*. Le déterminant minimal de ces codes n'a jamais été étudié. Il était très difficile de mettre ensemble les contraintes MV et celles du décodage itératif.

Dans ce travail, nous décrivons un nouveau code spatio-temporel vérifiant les contraintes doubles du décodage MV et itératif. L'étude se limite au précodage linéaire unitaire pour les canaux MIMO  $2 \times 2$  non sélectif en fréquence (Oestges *et al.*, 2007) (voir la section 5.5 de cette référence pour une liste détaillée de précodeurs unitaires connus dans la littérature). Le temps de cohérence du canal est supposé être supérieur ou égal à 2. La matrice des coefficients du canal est parfaitement connue par le récepteur. Enfin, nous supposons que l'émetteur ne connaît pas les coefficients du canal et ne dispose pas d'un canal de retour le liant au récepteur. Le mot de code de longueur  $N$  pour un canal MIMO  $n \times n$  s'écrit sous la forme matricielle

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

Après décodage à maximum de vraisemblance, la probabilité d'erreur par paire pourrait être majorée comme suit (e.g., voir (El Gamal *et al.*, 2003b))

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

où  $\gamma$  est le rapport signal-à-bruit par symbole à l'émission,  $t = \text{rang}(\mathbf{C} - \mathbf{C}')$ , le gain de codage est  $g = (\lambda_1 \lambda_2 \dots \lambda_t)^{1/t}$ , et les  $\{\lambda_i\}$  sont les valeurs propres de  $(\mathbf{C} - \mathbf{C}')(\mathbf{C} - \mathbf{C}')^*$ . Ainsi, le fameux critère de conception (Guey *et al.* 1996) (Tarokh *et al.*, 1998) pour le décodage MV se résume par :

- rang : la diversité maximale est atteinte si  $t = n$ .
- distance produit : le meilleur gain de codage est obtenu en maximisant le déterminant.

Il est possible d'atteindre la diversité maximale avec  $N = n$  (Larsson *et al.*, 2003) (Oestges *et al.*, 2007) si une matrice unitaire bien choisie est appliquée à  $\mathbf{C}$ . Écrivons le mot de code de manière linéaire sous la forme d'un vecteur de longueur  $n^2$ ,  $\mathbf{c} = (c_1, \dots, c_{n^2})$ . Le nouveau mot de code à transmettre sur le canal est  $\mathbf{X} = \mathbf{c}\mathbf{S}$ , où  $\mathbf{S}$  est une matrice  $n^2 \times n^2$  unitaire. Nous allons restreindre les composantes de  $\mathbf{c}$  à  $\mathcal{A} = \mathbb{Z}[i]$  (constellations QAM finies ou infinies). Rappelons brièvement les conditions du génie pour le décodage itératif (Boutros *et al.*, 2003) (Gresset *et al.*, 2004). Simplifions la situation en prenant  $n = 2$ . Le canal MIMO est défini par la matrice des évanouissements suivante

$$\mathbf{H}_0 = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix},$$

où les coefficients d'évanouissement  $h_{ij}$  sont iid et distribués selon une loi gaussienne complexe  $\mathcal{CN}(0,1)$  à symétrie circulaire. La partie utile (sans le bruit) du signal observé par le décodeur est  $\mathbf{X}\mathbf{H}$ , avec

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_0 & 0 \\ 0 & \mathbf{H}_0 \end{pmatrix}.$$

Les conditions du génie sont déterminées en supposant que le code correcteur d'erreurs génère des informations extrinsèques parfaites, ces informations étant vues comme information *a priori* pour le détecteur spatio-temporel. En présence d'information *a priori* parfaite, le détecteur produit une information extrinsèque  $\xi$  associée à un élément binaire du mot  $\mathbf{X}$ , ou à une composante complexe de ce mot, à l'aide de l'expression

$$\xi = \frac{\exp(-\|\mathbf{Y} - \mathbf{X}\mathbf{H}\|^2/2\sigma^2)}{\exp(-\|\mathbf{Y} - \mathbf{X}\mathbf{H}\|^2/2\sigma^2) + \exp(-\|\mathbf{Y} - \mathbf{X}'\mathbf{H}\|^2/2\sigma^2)},$$

où  $\mathbf{Y}$  est la sortie du canal,  $\sigma^2$  est la variance (par dimension réelle) du bruit additif blanc gaussien du canal. Les mots  $\mathbf{X}$  et  $\mathbf{X}'$  du message  $\xi$  diffèrent par une seule composante, c-à-d,  $\mathbf{X} = \mathbf{c}\mathbf{S}$  et  $\mathbf{X}' = \mathbf{c}'\mathbf{S}$  avec  $(\mathbf{c} - \mathbf{c}') = (\Delta, 0, 0, 0)$ . Ici, nous supposons que cette différence est en première position. La probabilité d'erreur par bit ou par composante mesurée à la sortie du détecteur et basée sur la valeur de  $\xi$  dépend de la métrique euclidienne  $D^2 = \|\mathbf{X}\mathbf{H} - \mathbf{X}'\mathbf{H}\|^2 = \|(\mathbf{c} - \mathbf{c}')\mathbf{S}\mathbf{H}\|^2$ .

Soit  $s = (s_{11}, s_{12}, s_{13}, s_{14})$  la première ligne du précodeur  $\mathbf{S}$ , alors la distance euclidienne devient

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

D'après les propriétés de la loi de  $\chi^2$  (Tse *et al.*, 2005) (Veeravalli, 2001), le cas minimisant la probabilité d'erreur après détection est celui où toutes les gaussiennes complexes de la  $\chi^2$  sont indépendantes et possèdent la même variance. Ces propriétés se traduisent donc en deux conditions (Boutros *et al.*, 2003) (Gresset *et al.*, 2004) :

- Première condition du génie :  $(s_{11}, s_{12})$  est orthogonal à  $(s_{13}, s_{14})$ .
- Deuxième condition du génie :  $(s_{11}, s_{12})$  et  $(s_{13}, s_{14})$  ont la même norme.

Les conditions annoncées ci-dessus pour la première ligne de  $\mathbf{S}$  devraient également être vérifiées par toutes ses lignes.

## 2. Reformulation du problème

Mettons chaque ligne de  $\mathbf{S}$  dans une matrice  $n \times n$  avec un facteur d'échelle  $\sqrt{n}$ , pour obtenir un ensemble de matrices  $\mathbf{M}_1, \dots, \mathbf{M}_{n^2}$ . L'équation de codage  $\mathbf{X} = \mathbf{cS}$  devient alors  $\mathbf{X}_{\mathbf{c}} = \frac{1}{\sqrt{n}}(c_1\mathbf{M}_1 + \dots + c_{n^2}\mathbf{M}_{n^2})$ . Pour une constellation  $\mathcal{A}$  de  $\mathbb{C}$ , nous définissons le déterminant minimal du code engendré comme la valeur minimale de  $|\det \mathbf{X}_{\mathbf{c}-\mathbf{c}'}|$  où  $\mathbf{c}, \mathbf{c}' \in \mathcal{A}^{n^2}$ ,  $\mathbf{c} \neq \mathbf{c}'$ .

Les conditions que l'on impose à  $\mathbf{S}$  peuvent alors se reformuler en termes des  $\mathbf{M}_i$ . Tout d'abord, la condition que  $\mathbf{S}$  est unitaire (*shaping*) devient :

(S) Les  $\mathbf{M}_i$  forment une base unitaire (à un facteur d'échelle près) de l'espace  $M_n(\mathbb{C})$  muni de son produit scalaire hermitien naturel.

Quant aux conditions du génie, elles se reformulent ainsi :

(G) Les  $\mathbf{M}_i$  sont des matrices unitaires, *i.e.* appartiennent au groupe  $U(n)$ .

On est donc ramené au problème suivant :

*Trouver des matrices  $\mathbf{M}_1, \dots, \mathbf{M}_{n^2}$  vérifiant les conditions (S+G) et telles que le déterminant minimal du code qu'elles engendrent soit aussi grand que possible.*

On remarque que les conditions (S+G) ainsi que la valeur du déterminant minimal sont préservées lorsque l'on multiplie à droite ou à gauche toutes les  $\mathbf{M}_i$  par une même matrice unitaire. On déduit de ceci une notion naturelle d'*équivalence* pour les systèmes de  $\mathbf{M}_i$ . Dans le cas  $n = 2$ , cette notion d'équivalence permet de mettre les  $\mathbf{M}_i$  sous une forme particulièrement simple :

**THÉORÈME 1.** — *Tout ensemble de matrices  $\mathbf{M}_1, \dots, \mathbf{M}_4$  dans  $M_2(\mathbb{C})$  vérifiant (S+G) est équivalent à*

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

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

*pour un certain choix de  $\alpha, \beta, \gamma \in \mathbb{C}$  vérifiant  $|\alpha| = |\beta| = |\gamma| = 1$ .*

*Preuve.* Quitte à tout multiplier par  $\mathbf{M}_1^{-1}$ , on peut supposer  $\mathbf{M}_1 = \mathbf{I}$ . Le théorème de diagonalisation des matrices unitaires permet de se ramener au cas où  $\mathbf{M}_2$  est diagonale, en préservant  $\mathbf{M}_1 = \mathbf{I}$ . De plus  $\mathbf{M}_2$  et  $\mathbf{M}_1 = \mathbf{I}$  sont orthogonales (condition (S)), ce qui implique que  $\mathbf{M}_2$  est bien de la forme indiquée. Cela étant,  $\mathbf{M}_3$  et  $\mathbf{M}_4$  sont orthogonales à  $\mathbf{M}_1$  et  $\mathbf{M}_2$ , donc anti-diagonales, et en conjuguant par une matrice anti-diagonale convenablement choisie (ce qui préserve  $\mathbf{M}_1$  et  $\mathbf{M}_2$ ), on les met finalement sous la forme indiquée.

Soient  $u, v, w \in \mathbb{C}$  avec  $|u| = |v| = |w| = 1$ , considérons la forme quadratique (Lam, 2004)

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

où  $\mathbf{z} = (z_1, z_2, z_3, z_4) \in \mathbb{C}^4$ . Pour toute constellation  $\mathcal{A}$  de  $\mathbb{C}$ , définissons

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

**COROLLAIRE.** — Avec les notations ci-dessus, la valeur maximale du déterminant minimal d'un code espace-temps linéaire  $2 \times 2$  défini sur  $\mathcal{A}$  et satisfaisant les conditions (S+G) est

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

En particulier, un code espace-temps  $2 \times 2$  parfait (unitaire + déterminant non nul) sur  $\mathcal{A}$  et vérifiant les conditions du génie existe si et seulement si  $\maxqmin(\mathcal{A}) > 0$ . De plus, si  $\maxqmin(\mathcal{A}) > 0$  est atteint pour des valeurs spécifiques de  $u, v, w$ , alors, il existe un code ayant un gain de codage optimal, dont la construction se déduit explicitement de ces valeurs.

Ce corollaire résulte du théorème 1 et de l'expression

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

où  $u = \alpha^2, v = \beta^2, w = \gamma^2$ .

Nous recherchons une borne inférieure à  $\maxqmin(\mathcal{A})$  pour  $\mathcal{A} = \mathbb{Z}[i]$ . Une condition suffisante serait de trouver des valeurs convenables de  $u, v, w$  et borner  $|q_{u,v,w}(\mathbf{c})|$  pour  $\mathbf{c} \in \mathcal{A}^4 \setminus \{\mathbf{0}\}$ . Pour atteindre cet objectif dans la section suivante, nous utilisons des outils de la théorie algébrique des nombres (Samuel, 1967) (Weil, 1995).

### 3. Une minoration donnée par la théorie des nombres

Soient  $\mathcal{A} = \mathbb{Z}[i]$  et  $K = \mathcal{A}_{\mathbb{Q}} = \mathbb{Q}(i)$ . On commence par remarquer que si on choisit  $u, v, w \in K$ , et si  $d \in \mathcal{A}$  est un dénominateur commun de  $u, v, w$ , on a  $q_{u,v,w}(\mathbf{c}) \in \frac{1}{d} \mathcal{A}$  pour  $\mathbf{c} \in \mathcal{A}^4$ , de sorte que :

- ou bien  $q_{u,v,w}(\mathbf{c}) = 0$ ,
- ou bien  $|q_{u,v,w}(\mathbf{c})| \geq \frac{1}{|d|}$ .

On dit que  $q_{u,v,w}$  ne représente pas zéro sur  $\mathcal{A}$  si  $q_{u,v,w}(\mathbf{c}) \neq 0$  pour  $\mathbf{c} \neq \mathbf{0}$  dans  $\mathcal{A}$ . L'alternative précédente nous montre alors que, si cette condition est vérifiée, on a

$$|q_{u,v,w}(\mathbf{c})| \geq \frac{1}{|d|}$$

pour tout  $\mathbf{c} \neq \mathbf{0}$  dans  $\mathcal{A}$ , d'où

$$\max_{\mathbf{c} \in \mathcal{A}} \min_{\mathbf{c} \neq \mathbf{0}} |q_{u,v,w}(\mathbf{c})| \geq \frac{1}{|d|}.$$

Il s'agit donc maintenant de trouver  $u, v, w \in K$ , avec  $|u| = |v| = |w| = 1$ , ayant un dénominateur commun aussi petit que possible, et tels que  $q_{u,v,w}$  ne représente pas zéro. Un cas facile à analyser est celui où  $w = uv$ , de sorte que

$$q_{u,v,uv}(\mathbf{z}) = (z_1^2 - uz_2^2) - v(z_3^2 - uz_4^2).$$

LEMME 1. — *Une condition nécessaire et suffisante pour que la forme  $q_{u,v,uv}$  ci-dessus ne représente pas zéro sur  $\mathcal{A}$  est que  $u$  et  $v$  vérifient :*

- $u$  n'est pas un carré dans  $K$
- $v$  n'est pas une norme de  $K(\sqrt{u})$  dans  $K$ , i.e. il n'existe pas de  $x, y \in K$  tels que  $v = N(x + y\sqrt{u}) = x^2 - uy^2$ .

*Preuve.* Si  $u$  n'est pas un carré dans  $K$ , on ne peut pas avoir  $z_1^2 - uz_2^2 = 0$  sauf à avoir  $z_1 = z_2 = 0$  (sinon  $u = (z_1/z_2)^2$  serait un carré). De même on ne peut pas avoir  $z_3^2 - uz_4^2 = 0$  sauf à avoir  $z_3 = z_4 = 0$ . Si maintenant  $q_{u,v,uv}$  représentait zéro, on aurait  $(z_1^2 - uz_2^2) - v(z_3^2 - uz_4^2) = 0$  avec  $z_3^2 - uz_4^2 \neq 0$  par ce qui précède, donc

$$v = (z_1^2 - uz_2^2)/(z_3^2 - uz_4^2) = N((z_1 + z_2\sqrt{u})/(z_3 + z_4\sqrt{u}))$$

en contradiction avec la seconde condition.

REMARQUE. — Ce qui précède est intimement lié à la théorie des algèbres de quaternions généralisés. Rappelons que si  $K$  est un corps et  $u, v \in K$ , l'algèbre de quaternions généralisés  $(\frac{u,v}{K})$  est l'algèbre sur  $K$  de base  $1, e, f, g$  vérifiant  $e^2 = u$ ,  $f^2 = v$ , et  $ef = -fe = g$  (ce qui implique  $g^2 = -w$ ). La forme  $q_{u,v,uv}$  est alors la « norme réduite » de cette algèbre, exprimée dans cette base, et le fait que  $q_{u,v,uv}$  ne représente pas zéro équivaut à demander que cette algèbre de quaternions soit une algèbre à division, i.e. qu'elle n'admette pas de diviseurs de zéro. Comme cas particulier de cette théorie, pour  $K = \mathbb{R}$  et  $u = v = -1$ , on retrouve la construction classique de l'algèbre  $(\frac{-1,-1}{\mathbb{R}})$  des quaternions de Hamilton. En effet, les quaternions



de Hamilton forment une algèbre sur  $\mathbb{R}$  de base  $1, i, j, k$  vérifiant  $i^2 = j^2 = -1$  et  $ij = -ji = k$ . Si  $h = a + bi + cj + dk$  est un tel quaternion, sa norme réduite est  $|h|^2 = a^2 + b^2 + c^2 + d^2 = q_{-1, -1, 1}(a, b, c, d)$ , qui ne représente pas zéro sur  $\mathbb{R}$ .

Il s'agit maintenant de trouver  $u, v \in K$ , avec  $|u| = |v| = 1$ , vérifiant les conditions du lemme, et de dénominateur le plus petit possible (idéalement, on voudrait prendre  $u$  et  $v$  des *unités* de  $K$ ).

Les unités de  $K = \mathbb{Q}(i)$  sont  $\{\pm 1, \pm i\}$ . Elles sont bien de norme complexe 1, et on vérifie facilement que parmi celles-ci,  $i$  et  $-i$  ne sont pas des carrés dans  $K$ . Ainsi on peut choisir  $u = i$ . Pour  $v$ , on va choisir un nombre premier  $p \equiv 1 \pmod{4}$ , se factorisant sous la forme  $p = x_p \overline{x_p}$  dans  $K$ , et poser  $v = x_p / \overline{x_p} = x_p^2 / p$ . Ainsi on a bien  $|v| = 1$ , et on montre :

LEMME 2. — Si  $K = \mathbb{Q}(i)$ ,  $u = i$ , et  $p = x_p \overline{x_p}$  dans  $K$ , une condition nécessaire et suffisante pour que  $v = x_p / \overline{x_p}$  ne soit pas une norme de  $K(\sqrt{u})$  dans  $K$  est que  $p \equiv 5 \pmod{8}$ .

On ne donnera pas la preuve de ce lemme, qui repose sur différents outils de théorie algébrique des nombres (plongement  $p$ -adique, théorie du corps de classes).

Choisissant un tel  $p$ , on aura alors  $|q_{u, v, uv}(\mathbf{c})| \geq \frac{1}{|x_p|} = \frac{1}{\sqrt{p}}$  pour tout  $\mathbf{c} \neq \mathbf{0}$  dans  $\mathcal{A}$ , de sorte que  $\max \text{qmin}(\mathcal{A}) \geq \frac{1}{\sqrt{p}}$ . Le plus petit  $p$  qui convienne est  $p = 5$ , et on a ainsi obtenu la preuve que

$$\max \text{qmin}(\mathbb{Z}[i]) \geq \frac{1}{\sqrt{5}}.$$

#### 4. Le code d'Aladin-Pythagore

Explicitons la famille de codes construits par la méthode décrite ci-dessus. Soit  $p$  un nombre premier vérifiant

$$p \equiv 5 \pmod{8}.$$

On écrit

$$p = a^2 + b^2 = x_p \overline{x_p}$$

où  $x_p = a + ib$ . En élevant au carré on trouve  $x_p^2 = c + id$  où  $c = a^2 - b^2$  et  $d = 2ab$ . En prenant la norme au carré on obtient enfin

$$p^2 = c^2 + d^2$$

de sorte que  $(c, d, p)$  est un triplet pythagoricien.

En choisissant comme indiqué  $u = i$ ,  $v = x_p/\overline{x_p} = x_p^2/p$  et  $w = uv$ , la forme quadratique est donnée par

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

et la construction s'effectue en prenant les matrices  $\mathbf{M}_i$  données par le théorème 1 avec :  $\alpha = \sqrt{u} = e^{i\pi/4}$ ,  $\beta = \sqrt{v} = x_p/\sqrt{p}$  et  $\gamma = \sqrt{w} = \alpha\beta$ .

Le déterminant minimal de ces codes, que nous nommerons *codes pythagoriciens*, est au moins  $\frac{1}{2|x_p|} = \frac{1}{2\sqrt{p}}$ .

Dans le cas particulier  $p = 5$ , ce qui correspond au triplet (3,4,5), on prend  $x_5 = 2 + i$ , ce qui donne :

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

La matrice du précodeur devient

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

et pour  $\mathbf{c} \in \mathbb{Z}[i]^4$ , on a

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

avec le déterminant

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

toujours supérieur ou égal à  $\frac{1}{2\sqrt{5}}$  pour  $\mathbf{c}$  non nul. En fait,  $|\det \mathbf{X}_{\mathbf{c}}| = \frac{1}{2\sqrt{5}}$  est atteinte pour  $\mathbf{c} = (0, i, 1, i)$ , cette valeur est donc la valeur exacte du déterminant minimal.

Remarquons que ce code est construit comme un réseau dans l'algèbre  $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$ , qui se trouve être la même (seul le choix du réseau diffère) que celle du code en or, ou *Golden code* (Belfiore *et al.*, 2005) ; et de plus notre code contient les conditions du *génie*. Nous l'avons donc nommé le *code d'Aladin*.

En sens inverse, on peut aussi par un calcul explicite obtenir une borne supérieure sur le déterminant minimal d'un code vérifiant les conditions (S+G) lorsqu'on restreint les symboles à une constellation finie, par exemple à une 16-QAM. Ceci donne a fortiori une borne supérieure pour la constellation infinie  $\mathbb{Z}[i]$ , et cette borne se trouve coïncider avec la valeur du déterminant du code d'Aladin, ce qui conduit finalement au résultat d'optimalité suivant :

THÉORÈME 2. — *Le code d'Aladin(-Pythagore) est un code spatio-temporel  $2 \times 2$  parfait défini sur  $\mathbb{Z}[i]$  et satisfaisant les conditions du génie, avec un déterminant minimal égal à  $\frac{1}{2\sqrt{5}}$ . De plus, son gain de codage est optimal : tout code vérifiant ces propriétés possède un déterminant minimal strictement inférieur à  $\frac{1}{2\sqrt{5}}$ , sauf s'il est équivalent à Aladin. (Mieux, ce résultat d'optimalité est déjà valable lorsque l'on restreint les symboles à une 16-QAM.)*

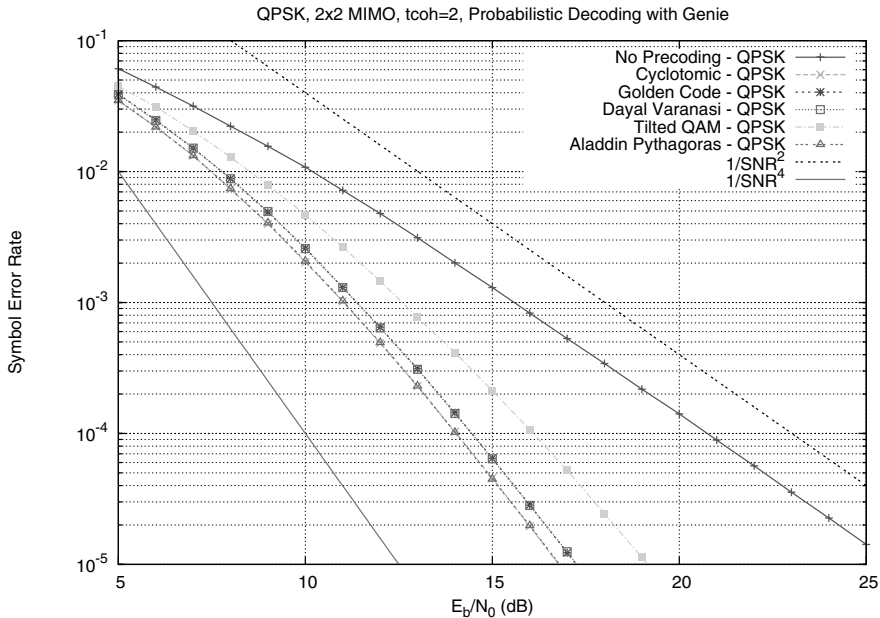


Figure 1. Constellation QPSK avec différents types de précodeurs spatio-temporels

## 5. Résultats numériques

Dans cette section, nous montrons les résultats du décodage probabiliste avec un génie, dans les figures 1 et 2. Le codage et décodage spatio-temporel sont simulés sur ordinateur avec la modulation  $\mathcal{A} = QPSK$ . Il n'est pas nécessaire d'utiliser une version à sortie souple du décodeur de réseaux de points par sphères (Viterbo *et al.*, 1999), il suffit de faire varier un seul symbole pour calculer les métriques de décodage.

Nous comparons plusieurs types de précodeurs linéaires : la rotation cyclotomique provenant de (Boutros *et al.*, 1998) et modifiée comme dans (Boutros *et al.*, 2003) (Gresset *et al.*, 2004) afin de satisfaire les conditions du génie, le code Golden défini dans (Belfiore *et al.*, 2005), le code de Dayal-Varanasi construit dans (Dayal *et al.*, 2005), le code dit tilted-QAM proposé par (Yao *et al.*, 2003), et enfin

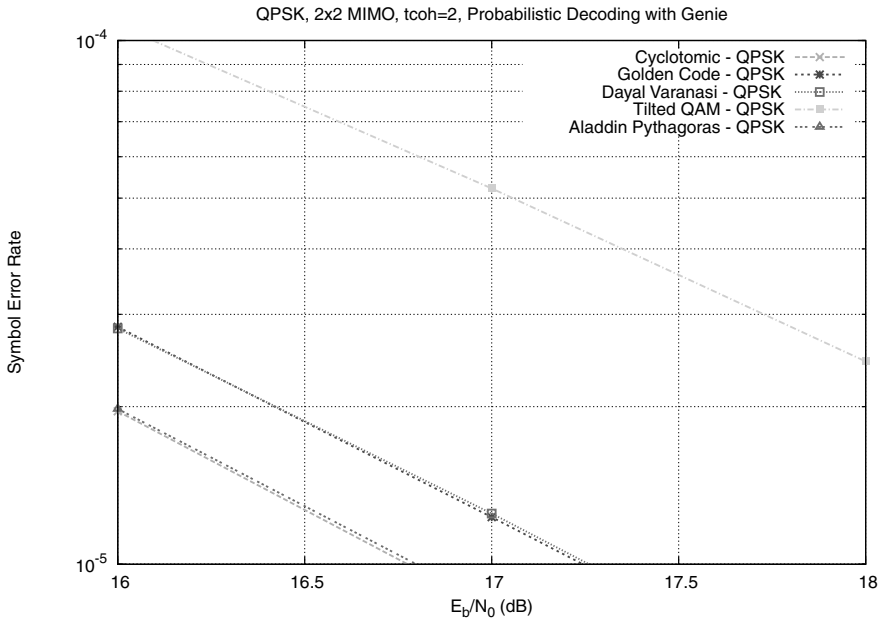


Figure 2. Constellation QPSK avec différents types de précodeurs spatio-temporels (agrandissement de la figure 1)

notre code d'Aladin-Pythagore. Nous citons aussi d'autres précodeurs spatio-temporels intéressants comme le GIOM (Genie + Information Outage Minimization) (Kraidy *et al.*, 2005) et le TAST (El Gamal *et al.*, 2003a). Comme prévu, la différence entre tous ces précodeurs en terme de rapport signal-à-bruit est très faible (par exemple, une sélection aléatoire de 2000 matrices du type GIOM produit un excellent précodeur). Les codes Golden et Dayal-Varanasi ont les mêmes performances (Oestges *et al.*, 2007). Le code tilted-QAM est dépassé par tous les autres précodeurs. Idem, comme prévu, la rotation cyclotomique et le code d'Aladin-Pythagore ont des performances équivalentes (l'optimalité du déterminant n'intervient pas dans ce scénario).

## Bibliographie

- Belfiore J.-C., Rekaya G., Viterbo E. (2005). « The golden code : a 2x2 full-rate space-time code with non-vanishing determinants », *IEEE Trans. on Inf. Theory*, vol. 51, n° 4, p. 1432-1436.
- Boutros J., Gresset N., Brunel L. (2003). « Turbo coding and decoding for multiple antenna channels », *Int. Symp. on Turbo Codes*, (<http://www.josephboutros.org/coding/>), Brest, Sept.
- Boutros J., Viterbo E. (1998). « Signal space diversity : a power and bandwidth efficient diversity technique for the Rayleigh fading channel », *IEEE Trans. on Inf. Theory*, vol. 44, n° 4, p. 1453-1467.

- Dayal P., Varanasi M. (2005). « An optimal two transmit antenna space-time code and its stacked extensions », *IEEE Trans. on Inf. Theory*, vol. 51, n° 12, p. 4348-4355.
- El Gamal H., Damen M. (2003a). « Universal space-time coding », *IEEE Trans. on Inf. Theory*, vol. 49, n° 5, p. 1097-1119.
- El Gamal H., Hammons, Jr A. (2003b). « On the design of algebraic space-time codes for MIMO blockfading channels », *IEEE Trans. on Inf. Theory*, vol. 49, n° 1, p. 151-163.
- Gresset N., Boutros J., Brunel L. (2004). « Optimal linear precoding for BICMoverMIMO channels », *IEEE Int. Symp. on Inf. Theory*, Chicago, IL, p. 66, June.
- Gresset N., Brunel L., Boutros J. (2008). « Space-time coding techniques with bit-interleaved coded modulations for MIMO block-fading channels », *IEEE Trans. on Inf. Theory*, vol. 54, n° 5, p. 2156-2178.
- Guey J.-C., Fitz M., Bell M., Kuo W.-Y. (1996). « Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels », *Vehicular Technology Conf. (VTC'96)*, Atlanta, GA, Apr.
- Kraidy G., Gresset N., Boutros J. (2005). « Information theoretical versus algebraic constructions of linear unitary precoders for non-ergodic multiple antenna channels », *The Ninth Canadian Workshop on Information Theory*, Montréal, Canada, p. 406-409, June.
- Lam T. (2004). *Introduction to Quadratic Forms over Fields*, American Mathematical Society.
- Larsson E., Stoica P. (2003). *Space-Time Block Coding for Wireless Communications*, Cambridge University Press.
- Oestges C., Clerckx B. (2007). *MIMO Wireless Communications : from real-world propagation to space-time code design*, Academic Press, Elsevier.
- Richardson T., Urbanke R. (2008). *Modern Coding Theory*, Cambridge University Press.
- Samuel P. (1967). *Théorie Algébrique des Nombres*, Hermann.
- Tarokh V., Seshadri N., Calderbank A. (1998). « Space-time codes for high data rate wireless communication: performance criterion and code construction », *IEEE Trans. on Inf. Theory*, vol. 44, n° 2, p. 744-765.
- Tse D., Viswanath P. (2005). *Fundamentals of Wireless Communication*, Cambridge University Press.
- Veeravalli V. (2001). « On performance analysis for signaling on correlated fading channels », *IEEE Trans. on Comm.*, vol. 49, n° 11, p. 1879-85.
- Viterbo E., Boutros J. (1999). « A universal lattice code decoder for fading channels », *IEEE Trans. on Inf. Theory*, vol. 45, n° 5, p. 1639-1642.
- Weil A. (1995). *Basic Number Theory*, Springer, reprinted.
- Yao H., Wornell G. (2003). « Structured space-time block codes with optimal diversity-multiplexing tradeoff and minimum delay », *Globecom 2003*, San Francisco, CA, p. 1941-1945, Dec.



**Joseph Jean Boutros** a obtenu le diplôme d'ingénieur en 1992 de l'École Nationale Supérieure des Télécommunications (ENST ou Télécom ParisTech), spécialité Conception des Systèmes de Transmission. Il a soutenu sa thèse de doctorat en 1996 dans la même école sur le thème des réseaux de points pour les canaux à évanouissements. Maître de conférence au département Communications et électronique de l'ENST de 1996 à 2006, il est aussi membre de l'unité UMR-5141 du CNRS. En 2007, il est devenu professeur au département Electrical Engineering de l'Université Texas A&M au Qatar. Joseph Boutros a été consultant scientifique pour Alcatel Espace, Centre de Recherche Philips, Motorola Semiconducteurs, et membre de l'équipe traitement du signal de Juniper Networks Cable. Ses domaines de recherche scientifique sont les codes sur les graphes, le décodage itératif, le codage conjoint source-canal, le codage espace-temps, ainsi que les réseaux de points de manière générale.



**Hugues Randriambololona** est ancien élève de l'École normale supérieure et a soutenu une thèse en géométrie arithmétique à l'Université Paris-Sud Orsay en 2002. Ses principaux domaines de recherche sont la géométrie algébrique et la théorie des nombres. Actuellement Maître de conférences en mathématiques au sein du département Informatique et Réseaux à Télécom ParisTech, il s'intéresse aussi dans ce cadre à divers problèmes de mathématiques discrètes, théorie de l'information, et communications numériques (combinatoire, codes correcteurs d'erreurs, cryptographie, information quantique, etc.), notamment via des méthodes algébriques ou géométriques.