Le code spatio-temporel d'Aladin-Pythagore

Joseph J. Boutros[1] et Hugues Randriambololona[2]

[1]Texas A&M University at Qatar
Education City, 23874, Doha, Qatar

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

Résumé – Dans le cadre des transmissions à antennes multiples, nous étudions le précodage linéaire unitaire ayant un déterminant non nul et vérifiant les conditions du génie pour le décodage probabiliste itératif. Nous proposons la construction d'un nouveau code spatio-temporel combinant le critère du rang et les conditions du génie. Le résultat de l'étude est une famille de codes construite sur $\mathbb{Z}[i]$ et faisant appel à des triplets de Pythagore. Dans cette famille, le code associé à l'algèbre de quaternions $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$ est dit code d'Aladin-Pythagore.

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 optimal under 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. The space-time code involving the quaternion algebra $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$ is referred to as the *Aladdin-Pythagoras* code.

1 Le précodage spatio-temporel

Les constructions algébriques de codes en blocs spatio-temporels [1][2] 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 [3] et [4] ne tient pas compte de la présence de codes correcteurs d'erreurs puissants utilisant le décodage itératif probabiliste [5]. De manière peu habituelle, certains codes spatio-temporels construits à l'aide d'un précodage linéaire unitaire ont été proposés pour le décodage itératif [6][7] 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 2×2 non sélectif en fréquence [2] (voir la section 5.5 de cette référence pour une liste détaillée de précodeurs unitaires connus dans la litérature). Le temps de cohérence du canal est supposé être supérieur ou égal à 2. La matrice des cofficients 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 [8])

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

où γ est le rapport signal-à-bruit par symbole à l'émission, $t = rang(\mathbf{C}-\mathbf{C}')$, le gain de codage est $g = (\lambda_1\lambda_2\cdots\lambda_t)^{1/t}$, et les $\{\lambda_i\}$ sont les valeurs propres de $(\mathbf{C}-\mathbf{C}')(\mathbf{C}-\mathbf{C}')^*$. Ainsi, le fameux critère de conception [3][4] pour le décodage MV se résume par :

- Le Rang : la diversité maximale est atteinte si $t = n$.
- La Distance Produit : le meilleur gain de codage est obtenu en maximisant le déterminant.

Il est possible d'atteindre la diversité maximale avec $N = n$ [1][2] si une matrice unitaire bien choisie est appliquée à $\mathbf{C}$. Ecrivons 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 $\mathbf{X} = \mathbf{cS}$, où 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 [6][9]. 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 $\mathbb{C}\mathcal{N}(0,1)$. La partie utile (sans le bruit) du signal observé par le décodeur est $\mathbf{XH}$, 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. Les performances de ce dernier lorsque l'information a priori est parfaite dépendent de la métrique euclidienne $D^2 = \|\mathbf{XH} - \mathbf{X'H}\|^2 = \|(\mathbf{c}-\mathbf{c'})\mathbf{SH}\|^2$ avec $(\mathbf{c}-\mathbf{c'}) = (\Delta, 0, 0, 0)$, c-à-d, les deux mots de code diffèrent d'une seule composante. Ici, nous supposons que cette différence est en première position. Soit $s = (s_{11}, s_{12}, s_{13}, s_{14})$ la première ligne du précodeur $\mathbf{S}$, alors la distance euclidienne devient

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

D'après les propriétés de la loi de χ^2 [10][11], le cas optimal est celui où toutes les gaussiennes complexes de la χ^2 sont indépendantes et possèdent la même variance. Ces propriétés se traduisent donc en deux conditions :

- 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 Formulation à l'aide d'une forme quadratique

Mettons chaque ligne de S dans une matrice $n \times n$ avec un facteur d'échelle $\sqrt{n}$, pour obtenir un ensemble de matrices $\mathbf{M}_1, \ldots, \mathbf{M}_{n^2}$. L'équation de codage $\mathbf{X} = \mathbf{cS}$ devient alors $\mathbf{X_c} = \frac{1}{\sqrt{n}}(c_1\mathbf{M}_1 + \cdots + c_{n^2}\mathbf{M}_{n^2})$. Pour une constellation $\mathcal{A}$ de $\mathbb{C}$, nous définissons le déterminant minimal comme la valeur minimale de $|\det \mathbf{X_{c-c'}}|$ où $\mathbf{c}, \mathbf{c'} \in \mathcal{A}^{n^2}$, $\mathbf{c} \neq \mathbf{c'}$. Les conditions sur la matrice S seront notées (S+G), (S) revient à imposer que S soit unitaire et (G) correspond aux deux conditions du génie citées ci-dessus. Nous pouvons ainsi énoncer le théorème suivant :

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

$$\mathbf{M}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \mathbf{M}_2 = \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}$$
$$\mathbf{M}_3 = \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix} \quad \mathbf{M}_4 = \begin{pmatrix} 0 & \gamma \\ -\gamma & 0 \end{pmatrix}$$

où $\alpha, \beta, \gamma \in \mathbb{C}$ avec $|\alpha| = |\beta| = |\gamma| = 1$.

Soient $u, v, w \in \mathbb{C}$ avec $|u| = |v| = |w| = 1$, considérons la forme quadratique [12]

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

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

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

Corollaire 1 *Avec les notations ci-dessus, la valeur maximale du déterminant minimal d'un code espace-temps linéaire 2×2 défini sur $\mathcal{A}$ et satisfaisant les conditions (S+G) est*

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

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

Ce corollaire résulte du théorème 1 et de l'expression

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

où $u = \alpha^2$, $v = \beta^2$, $w = \gamma^2$. Nous recherchons une borne inférieure à $\text{maxqmin}(\mathcal{A})$ 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 [13][14].

3 Le code d'Aladin-Pythagore

Soit $K = \mathcal{A}_{\mathbb{Q}} = \mathbb{Q}(i)$. Remarquons que si $u, v \in K$ et $w = uv$, alors $q_{u,v,w}$ est une norme réduite de l'algèbre de quaternions généralisés $\left(\frac{u,v}{K}\right)$, dans sa base naturelle. Si cette algèbre est une algèbre à division, la forme $q_{u,v,w}$ ne représentera pas 0. De plus, 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 $\mathbf{c} \in \mathcal{A}^4$. Nous aurons donc $|q_{u,v,w}(\mathbf{c})| \geq \frac{1}{|d|}$ dans le cas non nul. Trouvons donc $u, v \in K$, avec $|u| = |v| = 1$, tels que $\left(\frac{u,v}{K}\right)$ soit une algèbre à division, c-à-d, u n'est pas un carré dans K et v n'est pas une norme de $K(\sqrt{u})$ dans K. Il serait préférable de les choisir avec le dénominateur le plus petit possible.

Lemme 1 *Pour tout nombre premier p dans $\mathbb{Z}$ qui se factorise dans K (c-à-d $p \equiv 1 \mod 4$) choisir une factorisation $p = x_p\overline{x_p}$. Alors, le sous-groupe $|z| = 1$ de $K^\times$ est la somme directe du groupe des unités dans $\mathcal{A}$ et des groupes cycliques libres engendrés par les $x_p/\overline{x_p}$.*

Lemme 2 *Les unités de $\mathcal{A}$ qui ne sont pas des carrés dans K sont $\{\pm i\}$ lorsque $\mathcal{A} = \mathbb{Z}[i]$. Si on prend une telle unité comme u, alors toutes les autres unités sont des normes de $K(\sqrt{u})$ dans K.*

D'après ce dernier lemme, nous prenons $u = i$, mais alors on ne peut pas prendre v une unité. On choisit donc $v = x_p/\overline{x_p}$ où p un nombre premier (petit de préférence). On obtient ainsi la borne inférieure (lorsque la forme est non nulle) $|q_{u,v,w}(\mathbf{c})| \geq \frac{1}{|\overline{x_p}|} = \frac{1}{|\sqrt{p}|}$.

Lemme 3 *Une condition nécessaire et suffisante pour que v ne soit pas une norme de $K(\sqrt{u})$ dans K est $p \equiv 5 \mod 8$ lorsque $\mathcal{A} = \mathbb{Z}[i]$.*

En prenant $p = 5$, on obtient la preuve que

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

La famille de codes construite avec la méthode décrite ci-dessus correspond donc à $\mathcal{A} = \mathbb{Z}[i]$ et $p \equiv 5 \mod 8$. Nous avons $p = a^2 + b^2$ si $x_p = a + ib$. Soit $x_p^2 = c + id$, donc $c = a^2 - b^2$ et $d = 2ab$. On a enfin $p^2 = c^2 + d^2$. Le triplet (c, d, p) est dit triplet de Pythagore.
Dans le cas $u = i$, $v = x_p/\overline{x_p} = x_p^2/p$ et $w = uv$, la forme quadratique est donnée par

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

et la construction s'effectue en prenant dans le th. 1 :
$\alpha = \sqrt{u} = e^{i\pi/4}$, $\beta = \sqrt{v} = x_p/\sqrt{p}$ and $\gamma = \sqrt{w} = \alpha\beta$.
Le déterminant minimal de ces codes, que nous nommerons *codes de Pythagore*, est au moins $\frac{1}{2|\overline{x_p}|} = \frac{1}{2\sqrt{p}}$.
Dans le cas particulier $p = 5$, on prend $x_5 = 2 + i$ (avec le triplet $(3, 4, 5)$) tel que

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

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

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

avec le déterminant

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

toujours supérieur ou égal à $\frac{1}{2\sqrt{5}}$ pour $\mathbf{c}$ non nul. En effet, $|\det \mathbf{X_c}| = \frac{1}{2\sqrt{5}}$ est atteinte pour $\mathbf{X_c} = (0, i, 1, i)$, cette valeur est donc la valeur exacte du déterminant minimal. Remarquons que la construction de ce code implique l'algèbre $\left(\frac{i,5}{\mathbb{Q}(i)}\right)$, la même que celle du code Golden [15] mais avec un réseau différent, et de plus notre code contient les conditions du génie, nous l'avons donc nommé le code d'Aladin-Pythagore.

Theorème 2 *Le code d'Aladin-Pythagore est un code spatio-temporel 2×2 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 Aladdin-Pythagore.*

4 Résultats numériques

Dans ce paragraphe, 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 [16], 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 [17] et modifiée comme dans [6][9] afin de satisfaire les conditions du génie, le code Golden défini dans [15], le code de Dayal-Varanasi construit dans [18], le code dit tilted-QAM proposé par [19], et enfin notre code d'Aladin-Pythagore. Nous citerons aussi d'autres précodeurs spatio-temporels intéressants comme le GIOM (Genie+Information Outage Minimization) [20] et le TAST [21]. 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 [2]. 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.

Références

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

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

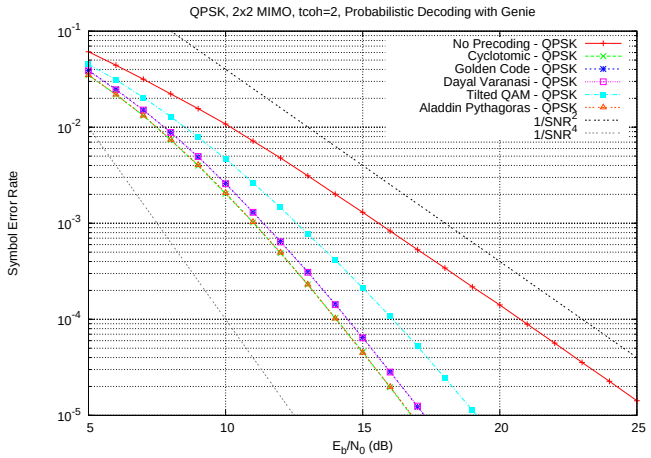

FIG. 1 – Constellation QPSK avec différents types de précodeurs spatio-temporels.

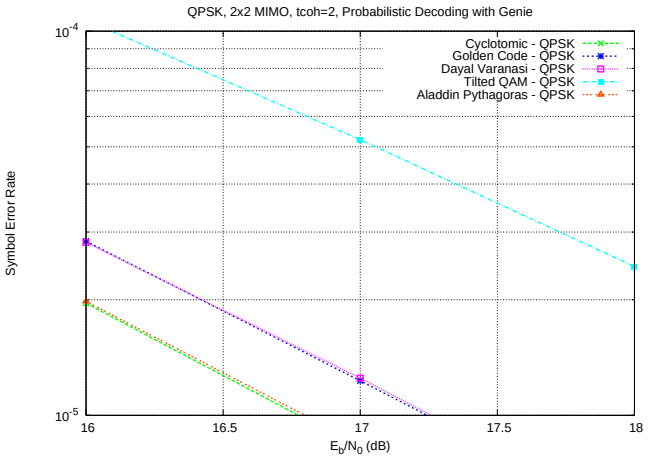

FIG. 2 – Constellation QPSK avec différents types de précodeurs spatio-temporels (agrandissement de la figure 1).

[3] 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.

[4] 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.

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

[6] 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*

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

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

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

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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.