Quaternionic Lattices for Space-Time Coding

Jean-Claude Belfiore
École Nat. Sup. des Télécomm.
46, rue Barrault
75013 Paris, France
Email: belfiore@enst.fr

Ghaya Rekaya
École Nat. Sup. des Télécomm.
46, rue Barrault
75013 Paris, France
Email: rekaya@enst.fr

Abstract — **We propose, here, an algebraic framework for studying coherent space-time codes, based on arithmetic lattices on central simple algebras. For two transmit antennas, this algebra is called a quaternion algebra. For this reason, we call these lattices quaternionic lattices. The design criterion is the one described in [1].**

I. Introduction and System Model

In order to achieve high spectral efficiency on wireless channels, we need multiple antennas at both transmitter and receiver ends. We are interested, here, in the coherent case where the receiver perfectly knows channel coefficients. Received signal is

$$\mathbf{Y}_{T\times N} = \mathbf{X}_{T\times M}.\mathbf{H}_{M\times N} + \mathbf{W}_{T\times N} \tag{1}$$

where $\mathbf{X}$ is the transmitted codeword, $\mathbf{H}$ is the channel response, assumed perfectly known at the receiver and $\mathbf{W}$ is the i.i.d. Gaussian noise. Subscripts indicate respective dimensions of the used matrices. M is the number of transmit antennas, N is the number of receive antennas, whereas T is the temporal codelength.

II. Published algebraic Space-Time Codes

In [2], the authors found a square 2×2 space-time code satisfying to the design criteria of [1] and using 2 degrees of freedom per channel use (p.c.u.). Then, generalizations of [2] have been proposed in [3, 4, 5] for any number of transmit antennas. All these codes were square codes (even if an obvious type of rectangular code has been proposed in [5]). They satisfy to the rank criterion and, in some sense, it is possible to maximize the coding advantage of [1] by choosing a good set of parameters. But these codes have a drawback, minimum determinant

$$\delta_{\min}(\mathcal{C}) = \min_{\substack{\mathbf{X}\in\mathcal{C}\\ \mathbf{X}\neq 0}} \det\left(\mathbf{X}^{\dagger}\mathbf{X}\right) \tag{2}$$

vanishes when the spectral efficiency of the code grows up [2, 5]. Here, $\mathcal{C}$ is the space-time code and † is for "transpose conjugate". What we want to present now is a new family of space-time codes whose coding advantage remains constant when the spectral efficiency grows up. In order to do that, we need to use a new algebraic concept : central simple algebras which become quaternion algebras when the number of transmit antennas $M = 2$.

III. The two antennas case

We restrict here to the two antennas case and we present the concept of quaternion algebra.

A. Quaternion algebra

Some definitions A comprehensive treatment of all algebraic stuff needed for this paper can be found in [6]. Now define what a quaternion algebra is. We get inspired from [7].

Definition 1 *Let $\mathbb{F}$ be a field, and β, γ be any non zero elements in $\mathbb{F}$. Then, the corresponding quaternion algebra over $\mathbb{F}$ is the ring*

$$D_{\beta,\gamma}(\mathbb{F}) = \{a + bi + cj + dk \| a, b, c, d \in \mathbb{F}\},$$

where

- addition is obvious
- multiplication is determined by the relations $i^2 = \beta, j^2 = \gamma, k = ij = -ji$

Associated to this definition, there is another one which is very important in the construction of space-time codes, that is

Definition 2 *The reduced norm of $x = a + bi + cj + dk \in D_{\beta,\gamma}(\mathbb{F})$ is*

$$N_{red}(x) = a^2 - \beta b^2 - \gamma c^2 + \beta\gamma d^2 \tag{3}$$

which is also

$$N_{red}(x) = x \cdot \bar{x}$$

with $\bar{x} = a - bi - cj - dk$.

Example 1 *It is quite easy to give an example of quaternion algebra. It is the field of Hamilton quaternions $\mathbb{H}$ with $\mathbb{F} = \mathbb{R}$, and $\beta = \gamma = -1$. But this example is not very interesting for our application. The code that it generates is simply the Alamouti code [8], in its complex version.*

Another definition is very usefull,

Example 2

Definition 3 *A quaternion algebra $D_{\beta,\gamma}(\mathbb{F})$ is a division algebra iff there are no zero-divisors in $D_{\beta,\gamma}(\mathbb{F})$.*

Proposition 1 *$D_{\beta,\gamma}(\mathbb{F})$ is a division algebra iff*

$$\forall x \in D^{\star}_{\beta,\gamma}(\mathbb{F}), N_{red}(x) \neq 0$$

$$A=\left\{x\in M_{d\times d}(\mathbb{L})\,\|x=\begin{pmatrix} x_1 & x_2 & \cdots & \cdots & x_d\\ \gamma\sigma(x_d) & \sigma(x_1) & \sigma(x_2) & & \sigma(x_{d-1})\\ \gamma\sigma^2(x_{d-1}) & \gamma\sigma^2(x_d) & \sigma^2(x_1) & & \sigma^2(x_{d-2})\\ \vdots & & \vdots & \ddots & \vdots\\ \gamma\sigma^{d-1}(x_2) & \gamma\sigma^{d-1}(x_3) & \gamma\sigma^{d-1}(x_4) & \cdots & \sigma^{d-1}(x_1)\end{pmatrix}\right\} \tag{4}$$

Representation In fact, elements in $D_{\beta,\gamma}(\mathbb{F})$ have a matrix representation in $\mathbb{R}^{2\times 2}$ or in $\mathbb{C}^{2\times 2}$. We can see in eq. (5) the basis elements of $D_{\beta,\gamma}(\mathbb{F})$.

$$i=\begin{pmatrix}\sqrt{\beta} & 0\\ 0 & -\sqrt{\beta}\end{pmatrix} \qquad j=\begin{pmatrix}0 & 1\\ \gamma & 0\end{pmatrix} \tag{5}$$

$$k=ij=\begin{pmatrix}0 & \sqrt{\beta}\\ -\gamma\sqrt{\beta} & 0\end{pmatrix}$$

Remark that an element of $D_{\beta,\gamma}(\mathbb{F})$ is

$$x=a+bi+cj+dk=\begin{pmatrix}a+b\sqrt{\beta} & c+d\sqrt{\beta}\\ \gamma\left(c-d\sqrt{\beta}\right) & a-b\sqrt{\beta}\end{pmatrix} \tag{6}$$

giving the determinant $\det(x)=a^2-\beta b^2-\gamma c^2+\beta\gamma d^2=N_{\text{red}}(x)$.

B. Full rate code for $M=2$ antennas

In [2], a code has been presented, which satisfied to the rank criterion. Codewords determinant can be written as $\det(x)=\left(s_1^2-is_2^2\right)-\theta\left(s_3^2-is_4^2\right)$ with $s_i\in\mathbb{Z}[i]$ are the 4 information QAM symbols, $i=\sqrt{-1}$ and $\theta=\exp\left(i\frac{\pi}{4}\right)$. When the spectral efficiency of QAM modulation grows up, then $\min\det(x)$ vanishes. Here we propose a code with a very similar structure to code of [2], but with $|\det(x)|^2$ taking its values in $\mathbb{Z}$.

B.1 The quaternion algebra

Construct the quaternion algebra $D_{\beta,\gamma}(\mathbb{F})$ with $\mathbb{F}=\mathbb{Q}(i)$, $\beta=i$ and $\gamma\in\mathbb{Q}(i)$. We denote $\theta=\exp\left(i\frac{\pi}{4}\right)=\sqrt{\beta}$. So, elements of $D_{\beta,\gamma}(\mathbb{F})$ are

$$x=\begin{pmatrix}a+b\theta & c+d\theta\\ \gamma(c-d\theta) & a-b\theta\end{pmatrix}\mid a,b,c,d\in\mathbb{Q}(i).$$

Proposition 2 *$D_{\beta,\gamma}(\mathbb{F})$ is a division algebra iff $\gamma\notin N_{\mathbb{Q}(\theta)/\mathbb{Q}(i)}(\mathbb{Q}(\theta))$, where $N_{\mathbb{Q}(\theta)/\mathbb{Q}(i)}(p)$ is the algebraic norm of $p\in\mathbb{Q}(\theta)$ [9].*

We calculate the reduced norm of x, $N_{\text{red}}(x)=N(a+b\theta)-\gamma N(c+d\theta)$ where $N(p)$ is for $N_{\mathbb{Q}(\theta)/\mathbb{Q}(i)}(p)$. So, $N_{\text{red}}(x)=0\Leftrightarrow N(a+b\theta)=\gamma N(c+d\theta)$, which gives that γ must be the norm of an element in $\mathbb{Q}(\theta)$.

B.2 The 2×2 code

Information symbols are supposed to be QAM symbols, that means that to construct a 2×2 code for its use with 2 receive antennas, we need to use 2 degrees of freedom p.c.u. which gives 4 information symbols $(s_1,s_2,s_3,s_4)\in\mathbb{Z}[i]^4$. For the construction, we use the quaternion algebra $D_{i,p}(\mathbb{Q}(i))$. The code will be a subset of this algebra, obtained by not considering all possible numbers in $\mathbb{Q}(i)$, but only those which are Gaussian integers. That gives the following codewords,

$$x=\begin{pmatrix}s_1+s_2\theta & s_3+s_4\theta\\ p(s_3-s_4\theta) & s_1-s_2\theta\end{pmatrix}\mid s_1,s_2,s_3,s_4,p\in\mathbb{Z}(i).$$

Now, in order to be fully diverse, we must have $\det x=0\Leftrightarrow x=0$. So it means that $D_{i,p}(\mathbb{Q}(i))$ must be a division algebra, hence, p does not have to be the algebraic norm of any number in $\mathbb{Q}(\theta)$. For example $p=1+2i$ works. We deduce a lower bound on the minimal determinant (see eq. (2)) of the code, whatever the spectral efficiency of the QAM constellation is,

$$\delta_{\min}(\mathcal{C})\geq 1$$

giving a non vanishing determinant.

C. Quaternionic lattices

The construction of a 2 antennas code is closely related to the construction of arithmetic lattices on $GL_2(\mathbb{C})$ (the group of 2×2 invertible matrices with coefficients in $\mathbb{C}$). These lattices are called quaternionic lattices. Now we generalize this concept.

IV. Central Cyclic algebras

We need, in order to generalize the 2×2 code to the $T\times M$ case, the notion of central cyclic algebras. It is, in fact, the generalization to dimensions >2 of quaternion algebras. There is in [6] a good introduction on this topic. We give, first, a definition of a central cyclic algebra.

Definition 4 *Let $\mathbb{F}$ be a field and $\mathbb{L}$ a cyclic extension of degree d on $\mathbb{F}$. That means that the Galois group Gal$(\mathbb{L}/\mathbb{F})$is cyclic. We denote σ the generator of this Galois group. Now, take $\gamma\in\mathbb{F}^\star$. We form the algebra generated by $\mathbb{L}$ and an element e such that*

$$\begin{cases} e^d=\gamma\\ e\cdot\bar{z}=\bar{z}\cdot\sigma(e),\forall\bar{z}\in\mathbb{L}\end{cases} \tag{7}$$

Thus, this algebra is

$$A=(\mathbb{L}/\mathbb{F},\sigma,\gamma)\doteq\mathbb{L}\oplus e\cdot\mathbb{L}\oplus\cdots\oplus e^{d-1}\cdot\mathbb{L} \tag{8}$$

This algebra can be constructed as a subalgebra of $M_d(\mathbb{L})$ by setting

$$e=\begin{pmatrix}0 & 1 & & 0\\ \vdots & & \ddots & \\ 0 & & \ddots & 1\\ \gamma & 0 & \cdots & 0\end{pmatrix} \qquad \bar{z}=diag\left(\sigma^i(z)\right) \tag{9}$$

$$i=0,\cdots,d-1$$

which gives equation (4). The codeword "architecture" is very similar to the one of [5], but the small difference makes the determinant non vanishing. Now, in order to construct a space-time code satisfying to the rank criterion, we need to use a cyclic division algebra. There is a simple condition ensuring that A is a division algebra.

Theorem 1 *A cyclic algebra as in definition 4 is a division algebra iff $\gamma, \gamma^2, \cdots, \gamma^{d-1}$ are not algebraic norms of elements in $\mathbb{L}$ ($\gamma, \gamma^2, \cdots, \gamma^{d-1} \notin N_{\mathbb{L}/\mathbb{F}}(\mathbb{L})$).*

The proof is quite difficult and can be found in [6].

V. Space-time Codes from cyclic division algebras

The construction of space-time codes for $M > 2$ transmit antennas is the same as the one for 2 antennas. Simply replace quaternion algebra with cyclic algebra. As it was the case in section III, in order to have a full rank code, we need a division algebra, which means that in eq. (4), γ and all its powers have to be outside $N_{\mathbb{L}/\mathbb{F}}(\mathbb{L})$.

A. Construction of the space-time code

In order to construct a space-time code, we need a complex alphabet which can be, for example a finite part of $\mathbb{Z}[i]$ (QAM symbols) or a finite part of $\mathbb{Z}[j]$ with $j = (-1)^{\frac{1}{3}}$ [10]. That means that we need to take $\mathbb{F} = \mathbb{Q}(i)$ or $\mathbb{F} = \mathbb{Q}(j)$ and then a cyclic extension $\mathbb{L}$ of degree M over $\mathbb{F}$. Symbols x_i of eq. (4) are elements of the ring of integers $\mathcal{O}$ of $\mathbb{L}$. The most difficult part now is to find a good element γ in $\mathbb{Z}[i]$ or $\mathbb{Z}[j]$ such that γ and its powers $\notin N_{\mathbb{L}/\mathbb{F}}(\mathbb{L})$. Such a choice will be treated in different examples. We can now claim the main theorem of this paper.

Theorem 2 *Let $\mathbb{F} = \mathbb{Q}(i)$ if $M = 2^r$ or $\mathbb{F} = \mathbb{Q}(j)$ for $M = 3 \cdot 2^r$. Consider $\mathbb{L}$ a cyclotomic extension of degree M over $\mathbb{F}$ (it is always a cyclic extension) and $\mathcal{O}$ the ring of integers in $\mathbb{L}$. Take γ an integer of $\mathbb{F}$ such that $\gamma, \gamma^2, \ldots, \gamma^{M-1} \notin N_{\mathbb{L}/\mathbb{F}}(\mathbb{L})$. With the notations of eq. (8), construct the order [9]*

$$\mathcal{O}_A(\mathbb{L}/\mathbb{F}, \sigma, \gamma) \doteq \mathcal{O} \oplus e \cdot \mathcal{O} \oplus \cdots \oplus e^{d-1} \cdot \mathcal{O} \tag{10}$$

Construct the space-time code $\mathcal{CA}(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ as being equal to a finite part of $\mathcal{O}_A(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ defined by using for example QAM constellations as symbols x_i if $M = 2^r$ (see eq. (4)). Then $\mathcal{CA}(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ satisfies to the following properties

1. $\mathcal{CA}(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ uses M degrees of freedom p.c.u.
2. $\mathcal{CA}(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ is fully diverse
3. $\min |\det \mathcal{CA}(\mathbb{L}/\mathbb{F}, \sigma, \gamma)|^2$ does not vanish when the spectral efficiency grows up. Moreover, $\{\det(x), x \in \mathcal{O}_A(\mathbb{L}/\mathbb{F}, \sigma, \gamma)\}$ is a discrete subset of $\mathbb{C}$.

Point 1 is obvious. Point 2 is proved by the fact that $\mathcal{CA}(\mathbb{L}/\mathbb{F}, \sigma, \gamma) \subset A(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ which is a division algebra. So all determinants of the matrix representation of $A(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ are non zero. Because $A(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ is an algebra, that means that if x and y are in $A(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$, then $x - y$ is in $A(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$, so its determinant is also non zero. That means that the rank criterion of [1] is satisfied by $A(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ hence by $\mathcal{CA}(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$. Point 3 is more difficult to prove. The idea is to show that the determinant is a sum of algebraic norms and traces taking their values in $\mathbb{Z}[i]$ or $\mathbb{Z}[j]$ which are discrete subsets of $\mathbb{C}$. And because $\det(x) = 0 \Leftrightarrow x = 0$, then $\delta_{\min} \geq 1$ whatever the size of the constellation in $\mathbb{Z}[i]$ or in $\mathbb{Z}[j]$ can be. That proves the non-vanishing determinant property of this code.

B. The case $M = 3$ antennas

In that case, we take $\mathbb{F} = \mathbb{Q}(j)$ and $\mathbb{L} = \mathbb{Q}(\zeta_9)$ with ζ_9 being the ninth root of unity $\exp\left(i\frac{2\pi}{9}\right)$. $\mathcal{O}$ is the ring of integers in $\mathbb{L}$. The problem is now to find element $\gamma \in \mathbb{Z}[j]$ such that $\gamma, \gamma^2 \notin N_{\mathbb{L}/\mathbb{F}}(\mathbb{L})$. We used KANT software [11] in order to find it. First, we found that the ideal $7 \cdot \mathbb{Z}[j]$ factorized in $\mathbb{Z}[j]$ as

$$7 \cdot \mathbb{Z}[j] = (7, 3 + j) \cdot (7, 5 + j)$$

where notation (a, b) means the ideal generated by a and b. Furthermore, if we denote $\mathfrak{I} = 7 \cdot \mathcal{O} \oplus (3 + j) \cdot \mathcal{O}$, then $\mathfrak{I}$ is a prime, principal ideal. So, $3 + j$ and $(3 + j)^2$ are not algebraic norms of elements in $\mathcal{O}$. Take $\gamma = 3 + j$, $\theta = \zeta_9$, $(s_{pq})_{\substack{p=0,1,2 \\ q=0,1,2}}$ be the nine information symbols carved from $\mathbb{Z}[j]$. Denote $x_i = s_{i0} + s_{i1}\theta + s_{i2}\theta^2$, then the generator σ of Gal $(\mathbb{L}/\mathbb{F})$ transforms θ in that way

$$\sigma : \theta \longmapsto j\theta$$

Because it is a field morphism, it transforms x_i in that way

$$\sigma : s_{i0} + s_{i1}\theta + s_{i2}\theta^2 \longmapsto s_{i0} + js_{i1}\theta + j^2 s_{i2}\theta^2$$

So we get codewords

$$x = \begin{pmatrix} x_1 & x_2 & x_3 \\ \gamma\sigma(x_3) & \sigma(x_1) & \sigma(x_2) \\ \gamma\sigma^2(x_2) & \gamma\sigma^2(x_3) & \sigma^2(x_1) \end{pmatrix} \tag{11}$$

The set of all these codewords x with s_{pq} taking all values of $\mathbb{Z}[j]$ is called an arithmetic lattice of $GL_M(\mathbb{C})$.

C. The case $M = 4$ antennas

Here, information symbols are in $\mathbb{Z}[i]$ (QAM symbols). $\mathbb{L} = \mathbb{Q}(\zeta_{16})$ with ζ_{16} being the 16^{th} root of unity $\exp\left(i\frac{\pi}{8}\right)$. $\mathcal{O}$ is the ring of integers in $\mathbb{L}$. The problem is now to find an element $\gamma \in \mathbb{Z}[i]$ such that $\gamma, \gamma^2, \gamma^3 \notin N_{\mathbb{L}/\mathbb{F}}(\mathbb{L})$. First, we found that the ideal $5 \cdot \mathbb{Z}[i]$ factorized in $\mathbb{Z}[i]$ as

$$5 \cdot \mathbb{Z}[i] = (5, 2 + i) \cdot (5, 3 + i)$$

Furthermore, if we denote $\mathfrak{I} = 5 \cdot \mathcal{O} \oplus (2 + i) \cdot \mathcal{O}$, then $\mathfrak{I}$ is a prime, principal ideal. So, $2 + i$, $(2 + i)^2$ and $(2 + i)^3$ are not algebraic norms of elements in $\mathcal{O}$. Take $\gamma = 2 + i$, $\theta = \zeta_{16}$, $(s_{pq})_{\substack{p=0,\ldots,3 \\ q=0,\ldots,3}}$ be the 16 information symbols carved from $\mathbb{Z}[i]$. Denote $x_i = \sum_{j=0}^{3} s_{ij}\theta^j$, then the generator σ of Gal $(\mathbb{L}/\mathbb{F})$ transforms θ in that way

$$\sigma : \theta \longmapsto i\theta$$

$$x=\begin{pmatrix} x_1 & \gamma^{\frac{1}{d}}x_2 & \cdots & \cdots & \gamma^{\frac{d-1}{d}}x_d \\ \gamma^{\frac{d-1}{d}}\sigma\left(x_d\right) & \sigma\left(x_1\right) & \gamma\sigma\left(x_2\right) & & \gamma^{\frac{d-2}{d}}\sigma\left(x_{d-1}\right) \\ \gamma^{\frac{d-2}{d}}\sigma^2\left(x_{d-1}\right) & \gamma^{\frac{d-1}{d}}\sigma^2\left(x_d\right) & \sigma^2\left(x_1\right) & & \gamma^{\frac{d-3}{d}}\sigma^2\left(x_{d-2}\right) \\ \vdots & & \vdots & \ddots & \vdots \\ \gamma^{\frac{1}{d}}\sigma^{d-1}\left(x_2\right) & \gamma^{\frac{2}{d}}\sigma^{d-1}\left(x_3\right) & \gamma^{\frac{3}{d}}\sigma^{d-1}\left(x_4\right) & \cdots & \sigma^{d-1}\left(x_1\right) \end{pmatrix} \tag{12}$$

Because it is a field morphism, it transforms x_p in that way

$$\sigma:\sum_{q=0}^{3}s_{pq}\theta^q\longmapsto\sum_{q=0}^{3}i^q s_{pq}\theta^q$$

So we get codewords

$$x=\begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ \gamma\sigma\left(x_3\right) & \sigma\left(x_0\right) & \sigma\left(x_1\right) & \sigma\left(x_2\right) \\ \gamma\sigma^2\left(x_2\right) & \gamma\sigma^2\left(x_3\right) & \sigma^2\left(x_0\right) & \sigma^2\left(x_1\right) \\ \gamma\sigma^3\left(x_1\right) & \gamma\sigma^3\left(x_2\right) & \gamma\sigma^3\left(x_3\right) & \sigma^3\left(x_0\right) \end{pmatrix} \tag{13}$$

When all information symbols s_{pq} go through $\mathbb{Z}[i]$, then we get an arithmetic lattice of $GL_4(\mathbb{C})$.

VI. Improvement of the codes

Performances of the codes found in sections III and V can be improved by better distributing the symbols energies in a codeword without changing the codewords determinant. Now codewords have the expression of eq. (12). Determinant of these codewords are equal to the determinants of codewords in $\mathcal{CA}(\mathbb{L}/\mathbb{F},\sigma,\gamma)$, but symbols average energies are lower. We give in figures 1 and 2 simulation results for the 2 antennas case. Results for the modified code based on quaternionic lattices are better than those of code found in [2].

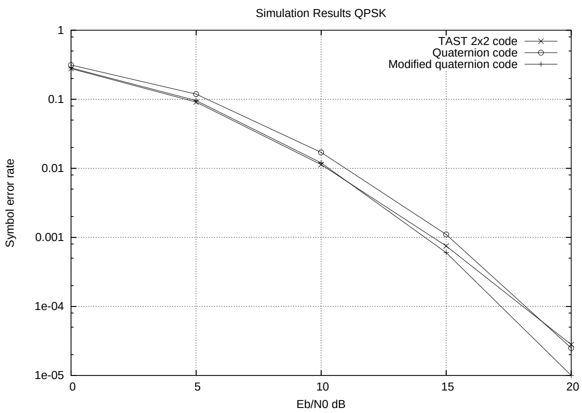

Figure 1: Simulation results $M=2$ QPSK Symbols (4 bits p.c.u.)

VII. Conclusion

Quaternionic lattices and more generally arithmetic lattices based on division algebras are fantastic tools to build space-time codes. The large number of degrees of freedom they offer to us will also permit to build more general codes as rectangular codes, non coherent codes, etc ...

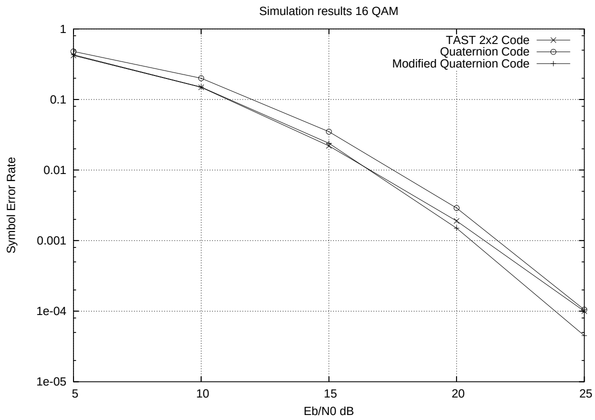

Figure 2: Simulation results $M=2$ 16-QAM Symbols (8 bits p.c.u.)

References

[1] V. Tarokh, N.Seshadri, and A. Calderbank, "Space-time codes for high data rate wireless communication : Performance criterion and code construction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 744–765, March 1998.

[2] M. O. Damen, A. Tewfi k, and J.-C. Belfi ore, "A construction of a space-time code based on the theory of numbers," *IEEE Trans. Inform. Theory*, vol. 48, no. 3, pp. 753–760, March 2002.

[3] S. Galliou and J.-C. Belfi ore, "A new family of full rate, fully diverse space-time codes based on Galois theory," in *Proceedings IEEE International Symposium on Information Theory*. IEEE, June 30-July 5 2002, p. 419.

[4] H. E. Gamal and M. O. Damen, "An algebraic number theoretic framework for space-time coding," in *Proceedings IEEE International Symposium on Information Theory*. IEEE, June 30-July 5 2002, p. 132.

[5] H. El Gamal and M. O. Damen, "Universal space-time coding," January 2002, submitted to *IEEE Trans. on Inform. Theory*.

[6] A. A. Albert, "Structure of Algebras," AMS Colloqium Pub. XXIV, 1961, AMS, Providence.

[7] S. Johansson, "A description of quaternion algebra," http://math.chalmers.se/∼sj/forskning.

[8] S. Alamouti, "Space-time block coding: A simple transmitter diversity technique for wireless communications," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 1451–1458, Oct. 1998.

[9] S. Lang, *Algebraic Number Theory*, 2nd ed., ser. Graduate Texts in Mathematics. Springer-Verlag, 1994.

[10] G. D. Forney, Jr, R. G. Gallager, G. R. Lang, F. M. Longstaff, and S. U. Qureshi, "Effi cient modulation for band-limited channels," *IEEE J. Select. Areas Commun.*, vol. 2, pp. 632–647, September 1984.

[11] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, and K. Wildanger, "KANT V4," *J. Symbolic Comp.*, vol. 24, pp. 267–283, 1997.