Sobre a construção do reticulado E_8 via álgebras de divisão

Carina Alves

UNESP- Rio Claro

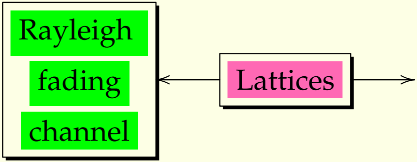
Encontro de Códigos, Reticulados e Informação (EnCoRI) 2023

15 de junho de 2023

Conteúdo

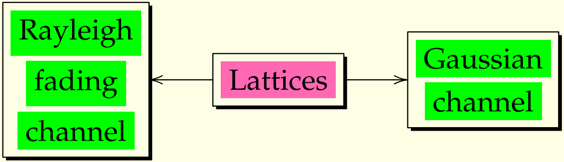
Introduction

- Signal constellations having a lattice structure have been studied as meaningful tools for transmitting data over both Gaussian and single-antenna Rayleigh fading channels.

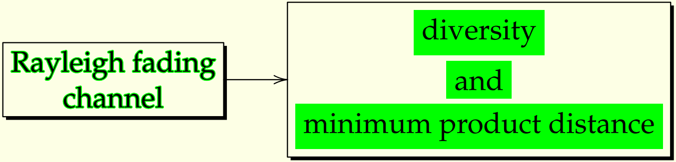


Introduction

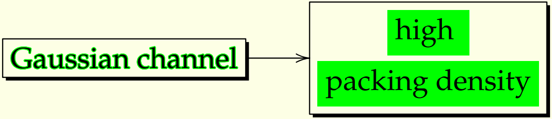
- Signal constellations having a lattice structure have been studied as meaningful tools for transmitting data over both Gaussian and single-antenna Rayleigh fading channels.



Introduction



Introduction



Some References

In order to minimize the probability of error in communication channels with a single antenna there are in the literature many constructions of lattices via number fields.

M. Craig
A Cyclotomic Construction for *Leech′s* Lattice.
Math, 25, pages 236–241, 1978.

M. Craig
Extreme Forms and Cyclotomy
Math, 25, pages 44–56, 1978.

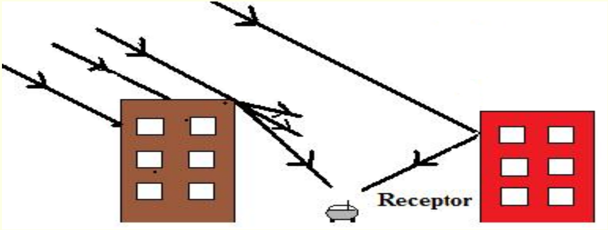
E. Bayer Fluckiger
Lattices and Number Fields
Contemp. Math, 241, pages 69–84, 1999.

	$\mathbb{Q}(\zeta_n)$	*Ideals*
D_4	$\mathbb{Q}(\zeta_8)$	$(2, \zeta_8 + 1)$
E_6	$\mathbb{Q}(\zeta_9)$	$(3, (\zeta_9 + 1)^2)$
E_8	$\mathbb{Q}(\zeta_{20})$	$(5, \zeta_{20} - 2)$
K_{12}	$\mathbb{Q}(\zeta_{21})$	$(7, \zeta_{21} + 3)$
Λ_{16}	$\mathbb{Q}(\zeta_{40})$	$(2, \zeta_{40}^4 + \zeta_{40}^3 + \zeta_{40}^2 + \zeta_{40} + 1)$ $(5, \zeta^2 + 2)$
Λ_{24}	$\mathbb{Q}(\zeta_{39})$	$(3, \zeta_{39}^3 + \zeta_{39}^2 - 1)$ $(3, \zeta_{39}^3 + \zeta_{39}^2 + \zeta_{39} + 1)$ $(13, \zeta_{39} - 3)$

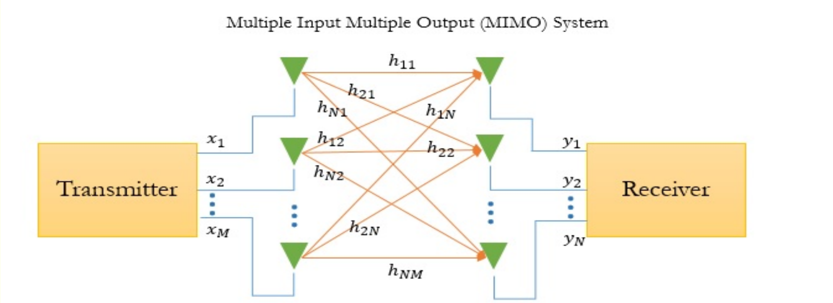
Disadvantages

Transmit data by atmospheric means involving many problems inherent to it, such as:

- meteorological phenomenon
- blockages caused by buildings
- others objects in the signal propagation path



Space-Time Codes



Codes designed for this channel are called space-time codes.

Code design criteria (Coherent case)

- The pairwise probability of error is bounded by

$$P(X \to \hat{X}) \leq \frac{\text{const}}{|\det(X - \hat{X})|^{2M}},$$

where M is the number of received antennas.

- $\det(X_i - X_j) \neq 0,\ \forall X_i \neq X_j,\ X_i, X_j \in \mathcal{C}$.
- If $\mathcal{C}$ is taken inside an algebra of matrices, the problem simplifies to $\det(X) \neq 0,\ \ 0 \neq X \in \mathcal{C}$.
- Division algebras are rings which every nonzero element has a multiplicative inverse.

Example 1: Codes built from quaternion division algebras

- **Alamouti Code:** $\mathcal{HA} = (-1,-1)_{\mathbb{R}},\ i^2 = j^2 = -1.$
- **Silver Code:** $\mathcal{SA} = (-1,-1)_{\mathbb{Q}(\sqrt{-7})},\ i^2 = -1,\ j^2 = -1.$
- **Golden Code:** $\mathcal{GA} = (5,i)_{\mathbb{Q}(i)},\ i^2 = 5,\ j^2 = i.$

Lattice

- A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$ generated by integer combinations of n linearly independents vectors $v_1, \cdots, v_n \in \mathbb{R}^n$.
- A matrix M whose rows are these vectors is said to be a generator matrix for Λ and the matrix

$$G = MM^t = (< v_i, v_j >)_{i,j=1}^m$$

is called a Gram matrix for the lattice Λ. The determinant of Λ is given by $det\Lambda = detG$.

Quaternion Algebras

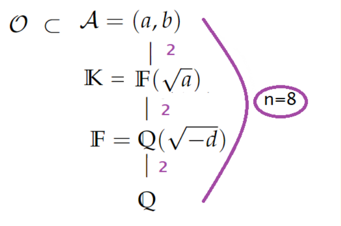
- A quaternion algebra $\mathcal{A} = (a, b)_{\mathbb{F}}$ over a number field $\mathbb{F}$ is a algebra of dimension 4 with basis $\{1, i, j, k\}$ satisfying $i^2 = a$, $j^2 = b$ and $k = ij = -ji$, where $a, b \in \mathbb{F} \setminus \{0\}$.

Quaternion Algebras

- A quaternion algebra $\mathcal{A} = (a, b)_{\mathbb{F}}$ over a number field $\mathbb{F}$ is a algebra of dimension 4 with basis $\{1, i, j, k\}$ satisfying $i^2 = a$, $j^2 = b$ and $k = ij = -ji$, where $a, b \in \mathbb{F} \setminus \{0\}$.

Quaternion Algebras

- A quaternion algebra $\mathcal{A} = (a, b)_{\mathbb{F}}$ over a number field $\mathbb{F}$ is a algebra of dimension 4 with basis $\{1, i, j, k\}$ satisfying $i^2 = a$, $j^2 = b$ and $k = ij = -ji$, where $a, b \in \mathbb{F} \setminus \{0\}$.



Division Algebras

When a quaternion algebra is a division algebra?

Division Algebras

When a quaternion algebra is a division algebra?

Division Algebras

When a quaternion algebra is a division algebra?

Proposition 2.

A quaternion algebra $\mathcal{A} = (a, b)_{\mathbb{F}}$ is a division algebra if only if $b \notin N_{\mathbb{F}(\sqrt{a})/\mathbb{F}}(\mathbb{F}(\sqrt{a}))$.

- $|b| = 1$, guarantees that the same average energy is transmitted from each antenna.

Algebraic Reduction

- Space-Time Codes based on an order of a quaternion algebra such that the volume of the Dirichlet's polyhedron of the group of units is small, are better suited for decoding using the method of algebraic reduction since the approximation error is smaller.

L. Luzzi, G. R-B. Othman, J-C. Belfiore,
Algebraic Reduction for the Golden Code.
IEEE Information Theory Workshop on Information Theory (ITW 2010, Cairo), v.6, n.1, pp. 1–5, 2010.

The volume of this Dirichlet's polyhedron is given by the Tamagawa formula and is called the Tamagawa volume.

Let $\mathcal{O}^1$ be the group of units of the maximal order $\mathcal{O}$ and $\mathcal{P}$ a compact fundamental polyhedron.

Theorem (Tamagawa Volume Formula)

Let $\mathcal{A}$ be a quaternion algebra over K such that $\mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{C})$. Let $\mathcal{O}$ be a maximal order of $\mathcal{A}$. Then the hyperbolic volume is given by,

$$Vol(\mathcal{P}_{\mathcal{O}^1}) = \frac{1}{4\pi^2}\zeta_{\mathbb{F}}(2)|D_{\mathbb{F}}|^{3/2}\prod_{p|\delta_{\mathcal{O}}}(N_p - 1),$$

where I varies among the proper ideals of $O_{\mathbb{F}}$ relative to the field $\mathbb{F}$, $D_{\mathbb{F}}$ is the discriminant of $\mathbb{F}$, $\delta_{\mathcal{O}}$ is the discriminant of $\mathcal{O}$, p varies among the primes of $O_{\mathbb{F}}$, and $N_p = [O_{\mathbb{F}} : pO_{\mathbb{F}}]$.

Maximal order of the Silver Algebra

Consider the quaternion algebra $\mathcal{A} = (a,b)_{\mathbb{F}}$. Then $\mathcal{O} = \mathbb{O}_{\mathbb{F}} \oplus \mathbb{O}_{\mathbb{F}} i \oplus \mathbb{O}_{\mathbb{F}} j \oplus \mathbb{O}_{\mathbb{F}} k$ is an $\mathbb{O}_{\mathbb{F}}$-order. We refer to this order as the **natural order**.

Example

Here, the natural order is not maximal order. By using the MAGMA software, we compute a maximal order $\mathcal{O}$ for the Silver code algebra $\mathcal{A} = (-1,-1)_{\mathbb{Q}(\sqrt{-7})}$ with basis $\{1,i,j,k\}$. This maximal order $\mathcal{O}$ can be written as

$$\mathcal{O} = \mathbb{Z}[\theta] \oplus i\mathbb{Z}[\theta] \oplus j\mathbb{Z}[\theta] \oplus \left(\frac{1+i+j+k}{2}\right)\mathbb{Z}[\theta].$$

- An order $\mathcal{M}$ in a quaternion algebra $\mathcal{A}$ is maximal if $\mathcal{M}$ is not properly contained in another order of $\mathcal{A}$.

Motivation

Y. Hong, E. Viterbo, J-C. Belfiore,
Golden Space-Time Trellis Code Modulation,
IEEE Trans. Inform. Theory, 53, pages 1689–1705, 2007.

The E_8 lattice was constructed by considering a left ideal of the maximal order of the quaternion division algebra

$$\mathcal{A} = (5, \sqrt{-1})_{\mathbb{Q}(\sqrt{-1})}.$$

Goal

Construct the E_8-lattice via quaternion division algebra over imaginary quadratic field with small Tamagawa volume.

C. Alves, J-C. Belfiore,
Lattices from maximal orders into quaternion algebras,
Journal of Pure and Applied Algebra, 219, pages 687–702, 2014.

$$\begin{array}{c} (-3,-1)_{\mathbb{K}} \\ \Big|\, 4 \\ \mathbb{K} = \mathbb{Q}(\sqrt{-2}) \\ \Big|\, 2 \\ \mathbb{Q} \end{array} \qquad \begin{array}{c} (-7,-1)_{\mathbb{K}} \\ \Big|\, 4 \\ \mathbb{K} = \mathbb{Q}(\sqrt{-3}) \\ \Big|\, 2 \\ \mathbb{Q} \end{array} \qquad \begin{array}{c} (-1,-1)_{\mathbb{K}} \\ \Big|\, 4 \\ \mathbb{K} = \mathbb{Q}(\sqrt{-7}) \\ \Big|\, 2 \\ \mathbb{Q} \end{array}$$

The E_8-lattice was constructed using quaternion division algebras over some imaginary quadratic fields .

Lemma [3]

Let $\mathbb{F}$ be an imaginary quadratic field of discriminant $D_{\mathbb{F}}$. Let $\mathcal{I}$ be a left ideal of a maximal order $\mathcal{O}$ of $\mathcal{A}$, with discriminant $\delta_{\mathcal{O}}$. $nr_{\mathcal{Q}/\mathbb{F}}(\mathcal{I})$ denotes the reduced norm of $\mathcal{I}$. Then

$$\det(\Lambda_{\mathcal{I}}) = (D_{\mathbb{F}})^4 \cdot N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) \cdot N_{\mathbb{F}/\mathbb{Q}}(nr_{\mathcal{A}/\mathbb{F}}(\mathcal{I}))^4. \tag{1}$$

- $\Lambda_{\mathcal{I}}$
- $\sqrt{c}E_8$, $c \in \mathbb{Z}$.

Necessary condition: $\det(\Lambda_{\mathcal{I}}) = \det(\sqrt{c}E_8)$.

$$D_{\mathbb{F}}^4 \cdot N_{\mathbb{F}/\mathbb{Q}} \underbrace{(\delta_{\mathcal{O}})}_{\delta_{\mathcal{O}}=?} \cdot N_{\mathbb{F}/\mathbb{Q}}(nr_{\mathcal{A}/\mathbb{F}}(\mathcal{I}))^4 = c^8.$$

Theorema. [4]

Assume that $\mathbb{F}$ is a totally complex number field, and that P_1 and P_2 are the two smallest distinct prime ideals in $O_{\mathbb{F}}$. Then the smallest possible discriminant of all central division algebras over $\mathbb{F}$ of index n is

$$(P_1 P_2)^{n(n-1)}$$

In our case, $n = 2$.

- $\delta_{\mathcal{O}} = (P_1 P_2)^2$, P_1 and P_2 distinct prime ideals of $O_{\mathbb{F}}$.

$$P_1 \cdot P_2 = pO_{\mathbb{F}}$$

for some prime $p \in \mathbb{Z}$.

$$N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) = p^4$$

Replacing in the necessary condition:

$$(D_{\mathbb{F}}p)^4 \cdot \underbrace{N_{\mathbb{F}/\mathbb{Q}}(nr_{\mathcal{Q}/\mathbb{F}}(\mathcal{I}))^4} = c^8$$

$$P_1 \cdot P_2 = pO_{\mathbb{F}}$$

for some prime $p \in \mathbb{Z}$.

$$N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) = p^4$$

Replacing in the necessary condition:

$$(D_{\mathbb{F}}p)^4 \cdot \underbrace{N_{\mathbb{F}/\mathbb{Q}}(nr_{\mathcal{Q}/\mathbb{F}}(\mathcal{I}))^4} = c^8$$

$$\Downarrow$$

$$N_{\mathbb{F}/\mathbb{Q}}(nr_{\mathcal{Q}/\mathbb{F}}(\mathcal{I})) = D_{\mathbb{F}}p$$

$$\mathcal{I} = ?$$

- Subfields of $\mathcal{A}$ are of the form $\mathbb{K} = \mathbb{F}\left(\sqrt{ax_1^2 - bx_2^2 - abx_3^2}\right)$. Consider the subfields $\mathbb{K}_1$ and $\mathbb{K}_2$ of $\mathcal{A}$ and find ideals $\mathcal{I}_1$ and $\mathcal{I}_2$ in $O_{\mathbb{K}_1}$ and $O_{\mathbb{K}_2}$ with absolute norm

$$N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{K}_1/\mathbb{F}}(\mathcal{I}_1)) = N_{\mathbb{K}_1/\mathbb{Q}} = p.$$

and

$$N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{K}_2/\mathbb{F}}(\mathcal{I}_2)) = N_{\mathbb{K}_2/\mathbb{Q}} = D_{\mathbb{F}}.$$

- Embedding $\mathcal{I}_1$ and $\mathcal{I}_2$ in $\mathcal{A}$.
- Ideal that we are looking for: $\mathcal{I} = \mathcal{I}_1\mathcal{I}_2$.

We detail in the table below, the computation of the Tamagawa volume for all addressed cases.

$\mathbb{F}$	$\zeta_{\mathbb{F}}(2)$	$\lvert D_{\mathbb{F}} \rvert$	$(a,b)_{\mathbb{F}}$	$\prod_{p \mid \delta_{\mathcal{O}}} (N_p - 1)$	$vol(\mathcal{P}_{\mathcal{O}^1})$
$\mathbb{Q}(\sqrt{-1})$	$1.5067\cdots$	4	$(5,i)_{\mathbb{F}}$	16	$4.885\cdots$
$\mathbb{Q}(\sqrt{-2})$	$1.7514\cdots$	8	$(-3,-1)_{\mathbb{F}}$	4	$4.015\cdots$
$\mathbb{Q}(\sqrt{-3})$	$1.2851\cdots$	3	$(-7,-1)_{\mathbb{F}}$	36	$6.089\cdots$
$\mathbb{Q}(\sqrt{-7})$	$1.8948\cdots$	7	$(-1,-1)_{\mathbb{F}}$	1	$0.888\cdots$

We detail in the table below, the computation of the Tamagawa volume for all addressed cases.

$\mathbb{F}$	$\zeta_{\mathbb{F}}(2)$	$\lvert D_{\mathbb{F}}\rvert$	$(a,b)_{\mathbb{F}}$	$\prod_{p\mid\delta_{\mathcal{O}}}(N_p-1)$	$vol(\mathcal{P}_{\mathcal{O}^1})$
$\mathbb{Q}(\sqrt{-1})$	$1.5067\cdots$	4	$(5,i)_{\mathbb{F}}$	16	$4.885\cdots$
$\mathbb{Q}(\sqrt{-2})$	$1.7514\cdots$	8	$(-3,-1)_{\mathbb{F}}$	4	$4.015\cdots$
$\mathbb{Q}(\sqrt{-3})$	$1.2851\cdots$	3	$(-7,-1)_{\mathbb{F}}$	36	$6.089\cdots$
$\mathbb{Q}(\sqrt{-7})$	$1.8948\cdots$	7	$(-1,-1)_{\mathbb{F}}$	1	$0.888\cdots$

Quite recently, Kim and Lee presented reduction algorithms for arbitrary Euclidean domains ($d=-1,-2,-3,-7,-11$ are Euclidean)

- T. Kim and C. Lee, “Lattice reductions over Euclidean rings with applications to cryptanalysis,” in Proc. Cryptography Coding - 16th IMA Int. Conf., IMACC 2017, vol. 10655, Springer, pp. 371–391, 2017.

Results and Next Steps

Lattices in $4n-$ dimensional Eclidean space.

$$\mathcal{A} = (a,b)_{\mathbb{K}} \quad \rightsquigarrow \quad \text{quaternion division algebra}$$

$$\Big|\ 4$$

$$\mathbb{F} = \mathbb{Q}(\zeta_s + \zeta_s^{-1}) \quad \rightsquigarrow \quad \text{maximal real subfield of } \mathbb{Q}(\zeta_s)$$

$$\Big|\ n=\frac{\phi(s)}{2}$$

$$\mathbb{Q}$$

C.W.O. Benedito, C. Alves, N.G. Brasil Jr., S.I.R. Costa
Algebraic construction of lattices via maximal quaternion orders,
Journal of Pure and Applied Algebra, v.224 (5), 2020.

Results and Next Steps

Lattices in $4n-$ dimensional Eclidean space.

$\mathcal{A} = (a, b)_{\mathbb{K}}$ $\rightsquigarrow$ **quaternion division algebra**

$\Big|\, 4$

$\mathbb{F} = \mathbb{Q}(\zeta_s + \zeta_s^{-1})$ $\rightsquigarrow$ **maximal real subfield of $\mathbb{Q}(\zeta_s)$**

$\Big|\, n = \frac{\phi(s)}{2}$

$\mathbb{Q}$

$$det(\Lambda) = D_{\mathbb{K}}^4 N(\alpha)^4 N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) N_{\mathbb{K}}(nr_{\mathcal{A}/\mathbb{F}}(\mathcal{I}))^4$$

Results and Next Steps

Lattices in 8− dimensional Eclidean space.

$$\mathcal{A} = (a,b)_{\mathbb{K}} \quad \rightsquigarrow \quad \text{quaternion division algebra}$$

$$\Big| \, 4$$

$$\mathbb{F} = \mathbb{Q}(\sqrt{-d}) \quad \rightsquigarrow \quad \text{d=1,2,3,7}$$

$$\Big| \, 2$$

$$\mathbb{Q}$$

$$det(\Lambda) = D_{\mathbb{F}}^4 \cdot N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) \cdot N_{\mathbb{F}/\mathbb{Q}}(nr_{\mathcal{A}/\mathbb{F}}(\mathcal{I}))^4.$$

Results and Next Steps

Lattices in 8− dimensional Eclidean space.

$$\mathcal{A} = (a, b)_{\mathbb{K}} \quad \rightsquigarrow \quad \text{quaternion division algebra}$$

$$\Big|\, 4$$

$$\mathbb{F} = \mathbb{Q}(\sqrt{-d}) \quad \rightsquigarrow \quad d=1,2,3,7, \ldots ??$$

$$\Big|\, 2$$

$$\mathbb{Q}$$

Recently, the LLL algorithm has also been generalized to lattices over imaginary quadratic fields.

- K. Arimoto and Y. Hirano, "A generalization of LLL lattice basis reduction over imaginary quadratic fields," Scientiae Mathematicae Japonicae, vol. 82, no. 1, pp. 1–6, 2019.
- K. Arimoto, "On LLL lattice basis reduction over imaginary quadratic fields by introducing reduction parameters," Int. J. Math. Comput. Sci., vol. 15, no. 2, pp. 611–619, 2020.

Results and Next Steps

Lattices in $4\phi(n)-$ dimensional Eclidean space.

$$\mathcal{A} = (a,b)_{\mathbb{K}} \quad \rightsquigarrow \quad \textbf{quaternion division algebra}$$

$$\begin{array}{c} \mathcal{A} = (a,b)_{\mathbb{K}} \\ \Big| \; 4 \\ \mathbb{F} = \mathbb{Q}(\zeta_n) \\ \Big| \; \phi(n) \\ \mathbb{Q} \end{array}$$

Results and Next Steps

Lattices in $4\phi(n)-$ dimensional Eclidean space.

$$\mathcal{A} = (a,b)_{\mathbb{K}} \quad \rightsquigarrow \quad \textbf{quaternion division algebra}$$

$$\begin{array}{c} \mathcal{A} = (a,b)_{\mathbb{K}} \\ \Big| \, 4 \\ \mathbb{F} = \mathbb{Q}(\zeta_n) \\ \Big| \, \phi(n) \\ \mathbb{Q} \end{array}$$

$$det(\Lambda) = ??$$

References I

[1] **E. Bayer-Fluckiger, Lattices and number fields, Contemporary Mathematics, 241, (1999) 69–84.**

[2] **F.-T. Tu and Y. Yang, Lattice packing from quaternion algebras,** *RIMS Kôkyûroku Bessatsu* **(2012) 229–237.**

[3] **C. Alves and J.-C. Belfiore, Lattices from maximal orders into quaternion algebras,** *J. Pure Appl. Algebra*, **219 (4) (April 2015) 687–702.**

[4] **I. Reiner,** *Maximal Orders*, **(Academic Press, London, 1975).**

[5] **C. Maclachlan and A. W. Reid,** *The arithmetic of hyperbolic 3-manifolds*. **Springer-Verlag, New York, 2003.**

References II

[6] **J.H. Conway and N.J.A. Sloane,** *Sphere Packings, Lattices and Groups*. **Springer-Verlag, 1998.**

[7] **E. Biglieri, Y. Hong, and E. Viterbo,** *On fast-decodable space-time block codes, IEEE Trans. Information Theory, v. 55, n. 2, February 2009.*

[8] **J.-C. Belfiore, G. Rekaya and E. Viterbo,** *The Golden Code: A* 2×2 *Full Rate Space-Time Code with Non-vanishing Determinant property, IEEE Trans. Inform. Theory, v. 51, n. 4, April 2005.*

[9] **C. Hollanti, J. Lahtonen, K. Ranto, R. Vehkalahti, and E. Viterbo,** *On the Algebraic Structure of the Silver Code, IEEE Information Theory Workshop, Porto, Portugal, May 2008.*

References III

[10] **L. Luzzi, G. R-B. Othman, J-C. Belfiore,** *Algebraic Reduction for the Golden Code, Advances in Mathematics of Communications, v.6, n.1, pp. 1–26, 2012.*

Obrigada!