Arithmetic Fuchsian Code

Edson D. de Carvalho, Antonio A. de Andrade, Jozué Vieira Filho and Jaime E. A. Rodriguez

***Resumo*— Neste trabalho apresentaremos uma nova classe de códigos a partir de grupos Fuchsianos. Esta nova classe de códigos é bem similar a obtida pelos códigos de Alamouti. Tem taxa-máxima, porém perde a propriedade de ortogonalidade.**

***Palavras-Chave*— Códigos de Alamouti, Grupos fuchsianos, Álgebra dos quatérnios.**

***Abstract*— In this work we present a new class of codes via Fuchsian groups. These codes are very similar to the ones obtained by Alamouti. This new class of codes has the property of full-rate, but without the property of orthogonality.**

***Keywords*— Alamouti code, Fuchsian group, Quaternion algebra.**

I. Introduction

We focus on the coherent multiple input-multiple output (MIMO) case, i.e., it is assumed that the receiver has recovered the exact information about the state of the channel (this is also known by perfect channel state information). In practice this can be obtained by introducing some pilot symbols that enable accurate channel estimation, so that we can assume that the channel matrix H is known at the receiver. Space Time block codes (STBCs) are used to provide diversity along time and space, and it is possible to consider systems with multiple antennas at both the transmitter and receiver ends, in order to increase the data rates. The coding problem became more complex and the code design criteria for such scenarios showed that the challenge was to construct fully-diversity codes, i.e., sets of matrices such that the difference of any two distinct matrices has full rank. This required new algebraic tools, namely division algebras. Division algebras are non-commutative algebras that naturally yield families of fully-diversity codes, thus enabling to design high rate, highly reliable STBC from a particular family of algebras, namely cyclic algebras built over number fields, for n transmit antennas, $n \times n$ space time codewords that send n^2 information symbols encoded into n^2 signals.

STBCs was originally introduced as orthogonal. The class of codes that satisfies this criterion is called orthogonal space time block codes (OSTBCs). This means that the STBC is designed such that the vectors representing any pair of columns are take from the coding matrix is orthogonal. The result of this is simple, linear, optimal decoding at the receiver. Its most serious disadvantage is that all but one of the codes that satisfy this criterion must sacrifice some proportion of their data rate.

Alamouti code [1] was the first STBC introduced for two transmit antennas, 2×2 space time codewords that send 2 information symbols encoded into 2 signals, i.e., rate $R = 1$. These codewords are obtained by multiplication in the ring of quaternions. As the quaternions form a division algebra, such matrices must be invertible, i.e., the resulting STBC meets the full diversity, and more, theses matrices are orthogonal, i.e., the resulting is an OSTBC.

However, Alamouti code is the only know OSTBCs with rate $R = 1$ used for 2 antennas. Some OSTBCs for higher number of antennas were proposed, but all theses codes are having rate ($R < 1$). To cope up with the increasing demand of high data rate and quality communication we need high date rate codes. High data rate SBTCs have been proposed in the literature using extension of fields and division algebras [2], [3]. These codes are claimed to provide high data rate codes with rate $R > 1$ and better code again for arbitrary number of transmit antennas. But these codes not have property of orthogonality.

In [2], Sethuraman and Rajan showed the Alamouti code is unique from the point of view of division algebras. We propose, here, a new class of codes based on arithmetic Fuchsian groups, which is isomorphic to division algebras. This gives rise to what we call arithmetic Fuchsian codes for this new classes of codes. These codes have the property of full-rate, but without the property of orthogonality. However, these codes matrices are equivalent to code matrices of Alamouti code.

We show that this is possible because the concept of arithmetic Fuchsian groups has two faces. An arithmetic Fuchsian group can be see as a discrete subgroup $\Gamma_{\mathcal{H}^2}$ of $PSL(2,\mathbb{R}) = SL(2,\mathbb{R})/\{\pm \mathrm{I}\}$, where I is the identity matrix, and each matrix is associated to an isometry that preserving orientation on the upper-half plane $\mathcal{H}^2$. Also an arithmetic fuchsian group can be see as a discrete subgroup $\Gamma_{\mathcal{D}^2}$ of $PSL(2,\mathbb{C}) = SL(2,\mathbb{C})/\{\pm \mathrm{I}\}$, where I is the identity matrix, and each matrix is associated to isometric that preserving orientation on the unit disc $\mathcal{D}^2 = \{z \in \mathbb{C} : |z| < 1\}$.

There is a correspondence between these two points of view. We know $\mathcal{H}^2$ and $\mathcal{D}^2$ are two Euclidean models for hyperbolic plane and exists an isometry f between $\mathcal{H}^2$ and $\mathcal{D}^2$. Consequently, we have that the space matrices given by arithmetic Fuchsian group $\Gamma_{\mathcal{H}^2}$ is equivalent to space matrices given by arithmetic Fuchsian group $\Gamma_{\mathcal{D}^2}$. We show that the matrices that belongs to the $\Gamma_{\mathcal{H}^2}$ are identified by elements of Hamilton quaternion, what is used to the construction of Alamouti code. However, we used matrices that belongs to the $\Gamma_{\mathcal{D}^2}$ for the construction of our arithmetic Fuchsian code.

This work is organized as follows. In Section II we present the concepts of division algebra and Alamouti code. In Section

E.D. Carvalho is with the Department of Mathematics, FEIS-UNESP, Ilha Solteira - SP, 15385-000, Brazil (e-mail: edson@mat.feis.unesp.br).

A.A. Andrade is with the Department of Mathematics, IBILCE-UNESP, São José do Rio Preto - SP, 15054-000, Brazil (e-mail: andrade@ibilce.unesp.br).

J. Vieira Filho is with Department of Engenharia Elétrica, FEIS-UNESP, Ilha Solteira - SP, 15385-000, Brazil (e-mail: jozue@dee.feis.unesp.br).

J.E.A. Rodriguez is with the Departamento de Matemática, FEIS-UNESP, Ilha Solteira, 15385-000, Brazil (e-mail: jaime@mat.feis.unesp.br).

III we present the concepts of Fuchsian group and quaternion order. In Section IV we present the quaternion order from a fundamental polygon. In Section V we present a new class of codes via arithmetic Fuchsian groups.

II. Division Algebra and Alamouti Code

Let D be a ring. We say that the ring D is a division ring, if every nonzero element has a multiplicative inverse. A commutative division algebra is just a field, but in this work, we are interested in non-commutative division rings.

Example 1: Hamilton quaternions denoted by $\mathbb{H}$ was the first division algebra proposed. As, we know, $\mathbb{H}$ is an 4-dimensional vector space over the real numbers $\mathbb{R}$ with basis $\{1, i, j, ij\}$, satisfying $i^2 = j^2 = -1$ and $ij = -ji$, that is, $\mathbb{H} = \{x_0 + x_1 i + x_2 j + x_3 ij | x_0, x_1, x_2, x_3 \in \mathbb{R}\}$. The Hamilton quaternions is also denoted by $\mathbb{H} \simeq (-1, -1)_{\mathbb{R}}$. We can be identified the real numbers $\mathbb{R}$ with a subset of $\mathbb{H}$ with $x_1 = x_2 = x_3 = 0$. Also, we can check that the multiplicative inverse x^{-1} of a nonzero quaternion $x = x_0 + x_1 i + x_2 j + x_3 ij$ is the quaternion $x^{-1} = (\frac{x_0}{z}) - (\frac{x_1}{z})i - (\frac{x_2}{z})j - (\frac{x_3}{z})ij$, where $z = x_0^2 + x_1^2 + x_2^2 + x_3^2$. Thus, as every nonzero element has a multiplicative inverse, it follows that $\mathbb{H}$ is indeed a division algebra.

The following proposition gives a very broad principle that can be used to construct full-rate codes from a division algebra.

Proposition 1: [3] Let $f : D \to M_n(F)$ be a rings homomorphism from a division algebra D to the set of $n \times n$ matrices over a field F. If E is any finite subset of the image of D under this map, then E has the property that the difference of any two elements in it will be of full rank.

If D is a division algebra then its center $Z(D)$ is the set $\{x \in D | xd = dx, \forall d \in D\}$. We have that $Z(D)$ is a field, and therefore D has a natural structure of a $Z(D)$-vector space. In this paper, we will only consider division algebras that are finite dimensional as a vector space over its center (see [3] and [4], for more details).

If D is a division algebra over a field F, then its center is F. It is well known that the dimension $[D : F]$ is always a perfect square. Thus, if $[D : F] = n^2$, then the square root of the dimension is n, and is know as the degree or the index of the division algebra. In Example 1, the center of $\mathbb{H}$ is just the real numbers $\mathbb{R}$. Observe that $\mathbb{H}$ is of dimension four over its center $\mathbb{R}$ and therefore $\mathbb{H}$ is of index two.

Now, we describe a fundamental class of division algebras, the class of cyclic division algebras. Recently, several authors constructed STBC from cyclic division algebras.

A cyclic division algebra D over a field F is a division algebra that has a maximal subfield K, where K is Galois over F, with Galois group $Gal(K/F)$ being cyclic.

Example 2: Hamilton quaternions $\mathbb{H}$ is a cyclic division algebra. For instance, observe that the subset of $\mathbb{H}$ given by $\mathbb{H}_1 = \{x_0 1 + x_1 i + 0j + 0ij | x_0, x_1 \in \mathbb{R}\}$ is isomorphic to the complex numbers $\mathbb{C}$. Let us identify the complex numbers $\mathbb{C}$ (by abuse of notation) for this subset. Observe that $\mathbb{C}$ is of dimension 2 over the its center $\mathbb{R}$, that is, $\mathbb{C}$ is a maximal subfield of $\mathbb{H}$. We have that $\mathbb{R} \subseteq \mathbb{C}$ is indeed a Galois extension, whose Galois group is $\{1, \sigma\}$, where σ is a complex conjugation. Thus, $\mathbb{H}$ is a cyclic division algebra.

Let D be a cyclic division algebra with center F, of index n, and with maximal cyclic subfield K, where $F \subseteq K$. If $Gal(K/F)$ is generated by σ, then $\sigma^n = 1$. We have that D is naturally a vector space over F. Also, it is well know that D has the following decomposition as K-spaces

$$D = K \oplus zK \oplus z^2 K \oplus \cdots \oplus z^{n-1} K, \tag{1}$$

where z is an element of D such that

$$kz = z\sigma(k), \tag{2}$$

for all $k \in K$ and $z^n = \gamma$ for some $\gamma \in F^* = F - \{0\}$, and z^i stands for the set of all elements of the form z^k for $k \in K$. The division algebra D, with this decomposition, is often written as $(K/F, \sigma, \gamma)$.

Example 3: If $\mathbb{H}$ is the Hamilton quaternions, then $\mathbb{H}$ can be regrouped as $\{x_0 + x_1 i | x_0, x_1 \in \mathbb{R}\} + \{x_2 j + x_3 ij | x_2, x_3 \in \mathbb{R}\} = \{x_0 + x_1 i | x_0, x_1 \in \mathbb{R}\} + j\{x_2 + x_3 i | x_2, x_3 \in \mathbb{R}\}$. In Example 2, we saw the subset $\mathbb{H}_1 = \{x_0 + x_1 i | x_0, x_1 \in \mathbb{R}\}$ was identified by the complex numbers $\mathbb{C}$. Similarly to Example 2, it is easy to show the subset $\{x_2 + x_3 i | x_2, x_3 \in \mathbb{R}\}$ of $\mathbb{H}$ is identified by the complex numbers $\mathbb{C}$. Thus, $\mathbb{H} = \mathbb{C} \oplus i\mathbb{C}$, i.e., $\mathbb{H}$ has a decomposition in $\mathbb{C}$-vector spaces. Moreover, if $\gamma = -1$, then $\mathbb{H}$ is a cyclic algebra of kind $(\mathbb{C}/\mathbb{R}, \sigma, -1)$.

A. Alamouti Code

In this subsection, we show how to build the Alamouti code. For this we consider the linear map $\tau : \mathbb{H} \to M_2(\mathbb{R})$ that associates the basis elements $1, i, j, ij$ to the matrices $M_0, M_1, M_2, M_3 \in M_(2, \mathbb{R})$, respectively, where

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad M_1 = \begin{bmatrix} l & 0 \\ 0 & -l \end{bmatrix}$$

$$M_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad M_3 = \begin{bmatrix} 0 & l \\ l\sqrt{t} & 0 \end{bmatrix},$$

and $l^2 = -1$. Thus τ is an embedding of $\mathbb{H}$ in $M_2(\mathbb{R})$, and therefore

$$\tau(x_0 + x_1 i + x_2 j + x_3 ij) = \begin{bmatrix} x_0 + lx_1 & x_2 + lx_3 \\ -(x_2 - lx_3) & x_0 - lx_1 \end{bmatrix} \tag{3}$$

where $x = x_0 + x_1 i + x_2 j + x_3 ij \in \mathbb{H}$.

We have that τ is a ring homomorphism and $\tau(\mathbb{H}) = E = M_2(\mathbb{R})$. By Proposition 1, we conclude the matrices space E has the property that the differences of any two elements of E has full-rank. Thus the matrices that belongs to the matrices space E form an Alamouti code.

III. Arithmetic Fuchsian Group and Quaternion Order

A Fuchsian group Γ is a discrete subgroup of $PSL(2, \mathbb{R}) = SL(2, \mathbb{R})/\{\pm \mathrm{I}\}$, where I is the identity matrix, that is, Γ consists of isometries on $\mathcal{H}^2 = \{z = x + iy \in \mathbb{C} : y > 0\}$, upper half-plane Euclidean model for the hyperbolic plane, endowed with the Riemannian metric $ds^2 = (dx^2 + dy^2)/y^2$,

preserving orientation and action on $\mathcal{H}^2$ by homomorphism [5], given by Möbius transformation $T_A(z) = \dfrac{az+b}{cz+d}$, where

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

$a, b, c, d \in \mathbb{R}$ and $det(T_A) = ad - bc = 1$.

We will use also the Poincare disc model (another Euclidean model for hyperbolic plane), $\mathcal{D}^2 = \{z \in \mathbb{C} | \, |z| < 1\}$, with the Riemmanian metric $ds^2 = dz/|z|$, where the Möbius transformations is given by $T_A(z) = \dfrac{az+c}{\overline{c}z+\overline{a}}$, with $a, c \in \mathbb{C}$ and $|a|^2 - |c|^2 = 1$. Moreover, the mapping $f(z) = \dfrac{zi+1}{z+i}$, is an isometry between $\mathcal{H}^2$ and $\mathcal{D}^2$.

In this work, associated with the Fuchsian group Γ, we show that there is a fundamental region $\mathcal{P}$ (polygonal shape containing $4g$ edges). Therefore, the quotient space $\mathcal{H}^2/\Gamma$ with the metric of Riemann surface with genus $g \geq 2$ may be modeled in the hyperbolic plane [5]. The pairing of the $4g$ edges of hyperbolic polygon $\mathcal{P}_{4g}$, considered in Section IV, leads to an oriented compact surface $\mathcal{H}^2/\Gamma_{4g}$, with genus g, where Γ_{4g} is the Fuchsian group associated with a self-dual hyperbolic tessellation $\{4g, 4g\}$. Also, for each g, the Fuchsian group is co-compact, and therefore the hyperbolic area $\mu(\mathcal{P}_{4g}) = \mu(\mathcal{H}^2/\Gamma_{4g})$ is finite.

A. Quaternion Order

Hamilton quaternions is a special example of a quaternion algebra. Now, we give a general definition. We say the set $\mathcal{A}$ denoted by $\mathcal{A} = (t, s)_F$ is a quaternion algebra, where $\mathcal{A}$ is a 4-dimensional vector space over a number field F with basis $\{1, i, j, ij\}$, satisfying $i^2 = t, j^2 = s, ij = -ji$, and $(ij)^2 = -ts$, where $t, s \in F^*$. If $x \in \mathcal{A}$, then $x = x_0 + x_1 i + x_2 j + x_3 ij$, with $x_0, x_1, x_2, x_3 \in F$, and $\overline{x} = x_0 - x_1 i - x_2 j - x_3 ij$ is the conjugate of x. The *reduced trace* and the *reduced norm* of x, denoted, respectively, by $\mathrm{Trd}(x)$ and $\mathrm{Nrd}(x)$, are defined as $\mathrm{Trd}(x) = x\overline{x}$ and $Nrd(x\overline{y}) = x_0^2 - tx_1^2 - sx_2^2 + tsx_3^2$.

There is a linear map $\tau : \mathcal{A} \to M_2(F(\sqrt{t}))$ (see [6] and [7]) that associates the basis elements $1, i, j, ij$ to the matrices $M_0, M_1, M_2, M_3 \in M_2(F(\sqrt{t}))$, respectively, where

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad M_1 = \begin{bmatrix} \sqrt{t} & 0 \\ 0 & -\sqrt{t} \end{bmatrix},$$

$$M_2 = \begin{bmatrix} 0 & r_1 \\ r_2 & 0 \end{bmatrix}, \qquad M_3 = \begin{bmatrix} 0 & r_1\sqrt{t} \\ -r_2\sqrt{t} & 0 \end{bmatrix},$$

$s = r_1 r_2$ and τ is an embedding of $\mathcal{A}$ in $M_2(F(\sqrt{t}))$. Thus

$$\tau(x_0 + x_1 i + x_2 j + x_3 ij) = \begin{bmatrix} x_0 + x_1\sqrt{t} & r_1(x_2 + x_3\sqrt{t}) \\ r_2(x_2 - x_3)\sqrt{t} & x_0 - x_1\sqrt{t} \end{bmatrix}$$

where $x = x_0 + x_1 i + x_2 j + x_3 ij \in \mathcal{A}$.

Moreover, since τ satisfies the conditions $\tau(i^2) = (\tau(i))^2, \tau(j^2) = (\tau(j))^2$ and $\tau(ij) = \tau(i)\tau(j)$, it follows that τ is an algebra homomorphism. Also, τ is onto $M_2(F)$ if and only if $t = k^2$, for some $k \in F^*$.

This shows that there are two possibilities for a quaternion algebra $\mathcal{A}$ over F. Either it is isomorphic to the matrix algebra $M_2(F)$ (in this case we say that $\mathcal{A}$ is *non-ramified*), or to a sub-algebra of $M_2(F(\sqrt{t}))$, with $\sqrt{t} \notin F$, having the structure of a division algebra isomorphic to Hamilton quaternions $\mathbb{H}$. In this case, we say that $\mathcal{A}$ is *ramified* for some $t \in F$.

If $\mathcal{A} \simeq (t, s)_F$ is quaternion algebra over a number field F, and $\sigma : F \to K$ is an homomorphism of F into another field K, we define $\mathcal{A}^\sigma = (\sigma(t), \sigma(s))_{\sigma(F)}$, and $\mathcal{A}^\sigma \oplus K = (\sigma(t), \sigma(s))_K$.

In what follow, F will be a totally real number field of degree n. This means that F is a field extension of $\mathbb{Q}$ of degree n, so that all n distinct embedding of F into $\mathbb{C}$ are embedding φ_i, for $i = 1, 2, \cdots, n$, into $\mathbb{R}$, where φ_1 is the identity. Let $\mathcal{A}$ be a quaternion algebra over F such that for $i = 1, 2, \cdots, n$ there exists $\mathbb{R}$-isomorphisms ρ_i defined by

$$\rho_1 : \mathcal{A}^{\varphi_1} \oplus \mathbb{R} \to M_2(\mathbb{R}) \quad \text{and} \quad \rho_i : \mathcal{A}^{\varphi_i} \oplus \mathbb{R} \to \mathbb{H}, \tag{4}$$

where $i = 2, \cdots, n$.

In this case, we say $\mathcal{A}$ is *non-ramified* in ρ_1 and *ramified* in the remaining ρ_i's. We denote by $Nrd_{\mathbb{H}}$ and $Trd_{\mathbb{H}}$, the reduced norm and the reduced trace of $\mathbb{H}$, respectively. Thus, if $x \in \mathcal{A}$, then

$$Nrd_{\mathbb{H}}(x) = det(\rho_1(x)), \qquad Trd_{\mathbb{H}}(x) = tr(\rho_1(x)). \tag{5}$$

$$\varphi_i(Nrd_{\mathbb{H}}(x)) = Nrd_{\mathbb{H}}(\rho_i(x)), \varphi_i(Trd_{\mathbb{H}}(x)) = Trd_{\mathbb{H}}(\rho_i(x)). \tag{6}$$

B. Arithmetic Fuchsian Group

Let $\mathcal{O}_F$ be the ring of integers of F. An *order $\mathcal{O}$ in $\mathcal{A}$ over F* is a free $\mathcal{O}_F$-module containing 1 with rank $4n$.

Given an order $\mathcal{O}$ in $\mathcal{A}$, we define its *group of units* $\mathcal{O}^1 = \{x \in \mathcal{O} | \mathrm{Nrd}(x) = 1\}$ and set $\Gamma(\mathcal{A}, \mathcal{O}) = \rho_1(\mathcal{O}^1) / \{\pm \mathrm{I}\}$. It is known (and proved by Takeushi in 1975, [8]) that $\Gamma(\mathcal{A}, \mathcal{O})$ is a Fuchsian group, that is, a discrete subgroup of $PSL(2, \mathbb{R})$. Since every Fuchsian group may be obtained in such a way, we say the a Fuchsian group Γ is *derived from a quaternion algebra* if there is a quaternion algebra $\mathcal{A}$ and an order $\mathcal{O} \subset \mathcal{A}$ such that Γ has finite index in $\Gamma(A, \mathcal{O})$. The group Γ is called *arithmetic Fuchsian group*.

The next theorem is important to characterize the Fuchsian groups that are derived from a quaternion algebra.

Theorem 1: [5] If Γ is a Fuchsian group associated to a fundamental region with finite hyperbolic area, then Γ is derived from a quaternion algebra $\mathcal{A}$ over a totally real number field F if and only if Γ satisfies the following conditions

1) if $F = \mathbb{Q}(tr(T))$, where $T \in \Gamma$, then F is a number field of finite degree and $tr(\Gamma)$ is in $\mathcal{O}_F$, and
2) if φ is an embedding of F in $\mathbb{C}$ different from the identity, then $\varphi(tr(\Gamma))$ is bounded in $\mathbb{C}$.

IV. Quaternion Order from Fundamental Polygon $\mathcal{P}_{4g}$

Let S_g be the fundamental group of a compact closed surface of genus g. It has a presentation as $S_g =$

$\langle a_1, b_1, a_2, b_2, \cdots, a_g, b_g | \prod_{i=1}^{g}[a_i, b_i] = \mathrm{I} \rangle$ with $[a_i, b_i] = a_i b_i a_i^{-1} b_i^{-1}$. Let us consider a regular polygon $\mathcal{P}_g$ with $4g$ edges and angles with measure equal to $2\pi/4g$. Hence, the corresponding fundamental region of self-dual tessellations of the hyperbolic plane is denoted by $\{4g, 4g\}$.

Now, we determine the generators of Fuchsian group Γ_{4g}, where edge-pairing generators of a regular polygon $\mathcal{P}_g$ with $4g$ edges (fundamental region of Γ_{4g}) are hyperbolic transformations, T_i (whose trace $tr(T_i)$ associated to T_i is such that $tr(T_i) > 2$), where g is the genus of compact surface $\mathcal{H}^2/\Gamma$, and whose hyperbolic area is $\mu(\mathcal{H}^2/\Gamma_{4g}) = 4\pi(g-1)$.

If T_{A_i}, T_{B_i}, where $i = 1, \cdots, g$, are the hyperbolic transformations determined by matrices A_i, B_i, such that $T_{A_i}(u_i) = u_i^{'}$ and $T_{B_i}(v_i) = v_i^{'}$, then the group Γ_{4g} generated by T_{A_i}, T_{B_i}, where $i = 1, \cdots, g$, is canonically isomorphic to S_{4g} (see [5], p. 94). Considering the Poincare model $\mathcal{D}^2$, and assuming that $0 \in \mathcal{D}^2$ is the barycenter of $\mathcal{P}_g$, we can find an explicit formula for the matrices A_i and B_i that generates the transformations T_{A_i} and T_{B_i}, for $i = 1, \cdots, g$. Following exactly the same kind of procedures done by Katok for the case $g = 2$ (see [5, Example C, p. 95]), we have the following result.

Proposition 1: The elements a, c of matrix $A_1 = \begin{bmatrix} a & c \\ \overline{c} & \overline{a} \end{bmatrix}$ are given by

$$|a| = \tan\left(\frac{(2g-1)\pi}{4g}\right) \quad \text{and} \quad arg(a) = -\frac{(g-1)\pi}{2g},$$

$$|c| = \sqrt{\tan^2\left[\frac{(2g-1)\pi}{4g}\right] - 1} \quad \text{and} \quad arg(c) = -\frac{(g-1)\pi}{4g},$$

and other generator matrices are given by $A_i = C^{4i} A_1 C^{-4i}$ and $B_i = C^{4i+1} A_1 C^{4i+1}$, for all $i = 1, \cdots, g$, where C is the rotation matrix given by

$$C = \begin{bmatrix} e^{2\pi i/4g} & 0 \\ 0 & e^{-2\pi i/4g} \end{bmatrix}.$$

Example 4: If $g = 2$, then the matrix A_1 associated to generator transformation $T_{A_1} \in \Gamma_8$ is given by

$$A_1 = \begin{bmatrix} \frac{(2+\sqrt{2})(1+i)}{2} & \frac{-\sqrt[4]{2}((2+\sqrt{2})+i(2+\sqrt{2}))}{2} \\ \frac{-\sqrt[4]{2}((2+\sqrt{2})-i(2+\sqrt{2}))}{2} & \frac{(2+\sqrt{2})(1-i)}{2} \end{bmatrix},$$

and the other matrices A_2, B_1 and B_2 are given by conjugation.

Example 5: If $g = 3$, then the matrix A_1 associated to generator transformation $T_{A_1} \in \Gamma_{12}$ is given by

$$A_1 = \begin{bmatrix} \frac{(2+\sqrt{3})+i(3+2\sqrt{3})}{2} & \frac{q[(-1+\sqrt{3})+i(1+\sqrt{3})]}{2} \\ \frac{q[(-1+\sqrt{3})-i(1+\sqrt{3})]}{2} & \frac{(2+\sqrt{3})-i(3+2\sqrt{3})}{2} \end{bmatrix},$$

where $q = \sqrt{3+2\sqrt{3}}$ and the other matrices A_2, A_3, B_1, B_2 and B_3 are given by conjugation.

Now, taking the correspondent real matrices of $PSL(2, \mathbb{R})$ by isometries $f : \mathcal{H}^2 \longrightarrow \mathcal{D}^2$ given by $f(z) = \frac{zi+1}{z+i}$, we have the following equality

$$\Gamma = P^{-1}\Gamma_{4g}P, \tag{7}$$

where P is the invertible matrix associated to the isometry f and is given by

$$P = \begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix}.$$

Thus, $\Gamma = P^{-1}\Gamma_{4g}P$ is a subgroup of $PSL(2, \mathbb{R})$, where $g = 2, 3$, and the generator matrices are given by $P^{-1}A_iP = D_i$ and $P^{-1}B_iP = E_i$. In particular, we have that if $A_1 \in \Gamma_8$ then

$$P^{-1}A_1P = D_1 = \begin{bmatrix} \frac{(2+\sqrt{2})+(-2-\sqrt{2})\sqrt[4]{2}}{2} & \frac{(2+\sqrt{2})-(\sqrt{2})(\sqrt[4]{2})}{2} \\ \frac{(-2-\sqrt{2})+(\sqrt{2})(\sqrt[4]{2})}{2} & \frac{(2+\sqrt{2})+(2+\sqrt{2})\sqrt[4]{2}}{2} \end{bmatrix},$$

and if $A_1 \in \Gamma_{12}$ then

$$P^{-1}A_1P = D_1 = \begin{bmatrix} \frac{(2+\sqrt{3})+p(1+\sqrt{3})}{2} & \frac{(3+2\sqrt{3})+p(-1+\sqrt{3})}{2} \\ \frac{-(3+2\sqrt{3})+p(-1+\sqrt{3})}{2} & \frac{(2+\sqrt{3})-p(1+\sqrt{3})}{2} \end{bmatrix},$$

where $p = \sqrt{3+2\sqrt{3}}$.

Remark 1: If we compute all the generator matrices $M = D_i$ or $M = E_i$, for $i = 1, \cdots, g$, of Γ_{4g} it is easy to check that the matrices are given by

1) if $g = 2$, then

$$M = \frac{1}{2}\begin{bmatrix} a+b\sqrt{t} & c+d\sqrt{t} \\ -(c-d\sqrt{t}) & a-b\sqrt{t} \end{bmatrix}, \tag{8}$$

where, $a, b, c, d \in \mathbb{Z}[\sqrt{2}]$ and $\sqrt{t} = \sqrt{\sqrt{2}} = \sqrt[4]{2}$, and

2) if $g = 3$, then

$$M = \frac{1}{2}\begin{bmatrix} a+b\sqrt{t} & c+d\sqrt{t} \\ -(c-d\sqrt{t}) & a-b\sqrt{t} \end{bmatrix}, \tag{9}$$

where, $a, b, c, d \in \mathbb{Z}[\sqrt{3}]$ and $\sqrt{t} = \sqrt{3+2\sqrt{3}}$.

Also, it is easy to show the product of these matrices are of type M and belong to group Γ.

Remark 2: We have that a geometric equivalence between the Euclidean models $\mathcal{H}^2$ and $\mathcal{D}^2$ and also an equivalence between the matrices space Γ and Γ_{4g}, where P is an invertible matrix by consequence of Equation (7).

Lemma 1: [5] If $\mathbb{H} \simeq (-1,-1)_{\mathbb{R}}$ and $\mathbb{H}^1 = \{x \in \mathbb{H} : Nrd_{\mathbb{H}}(x) = 1\}$ then $Trd_{\mathbb{H}}(\mathbb{H}^1)$ is bound in $\mathbb{C}$.

Proof: If $x = x_0 + x_1 i + x_2 j + x_3 ij \in \mathbb{H}^1$, where $i^2 = j^2 = (ij)^2 = -1$, and $Nrd_{\mathbb{H}}(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1$, then $|x_0| \leq 1$, and hence $Trd_{\mathbb{H}}(x) = 2x_0 \in [-2, 2]$. Since the converse statement is obviously true it follows that $Trd_{\mathbb{H}}(x) = 2x_0 \in [-2, 2]$.

Theorem 2: If $g = 2$, then the group Γ_8 is derived from quaternion algebra A over a totally real number field $\mathbb{Q}(\sqrt{2})$.

Proof: In this prove we will adopt exactly the same kind of procedures done by Katok for the case $g = 2$ (see [5, Example

C, p. 95]). Thus, first we shown that the conditions (1) and (2) of Theorem 1 are satisfied for elements of Γ_8. By, Remark 1, the elements of Γ_8 are given by

$$M = \frac{1}{2}\begin{bmatrix} x_0 + x_1\sqrt[4]{2} & x_2 + x_3\sqrt[4]{2} \\ -(x_2 - x_3)\sqrt[4]{2} & x_0 - x_1\sqrt[4]{2} \end{bmatrix},$$

where x_0, x_1, x_3 and $x_4 \in \mathbb{Z}[\sqrt{2}]$ and $tr(M) = x_0 = a_1 + a_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. In this way, we have that $\mathbb{Q}(tr(\Gamma_8)) = \mathbb{Q}(a_1 + a_2\sqrt{2}) = \mathbb{Q}(\sqrt{2})$, and $tr(M) \in \mathbb{Z}[\sqrt{2}]$. Since $\mathbb{Q}(\sqrt{2})$ is a totally real quadratic extension of $\mathbb{Q}$, it follows that the condition (1) of Theorem 1 is satisfied. Let $\varphi_2 : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ be non-identity embedding seeding $\varphi_2(\sqrt{2}) = -\sqrt{2}$. By Remark 1, the generators of Γ_8 and therefore all elements of Γ_8 are embedded into $M_2(K)$, where $K = \mathbb{Q}(\sqrt{2})(\sqrt{\sqrt{2}})$. Thus, φ_2 extends to an isomorphism $\Psi_2 : K \longrightarrow \mathbb{C}$, where

$$\Psi_2(\sqrt[4]{2}) = \sqrt{-\sqrt{2}} = i\sqrt[4]{2}.$$

Following exactly the same kind of procedures done by Katok, the elements of Γ_8 are mapped in matrices in $M_2(\mathbb{C})$ of type

$$M = \begin{bmatrix} \Psi_2(a) & \Psi_2(b) \\ \Psi_2(-\overline{b}) & \Psi_2(\overline{a}) \end{bmatrix}, \text{ with } a, b \in \Psi_2(K),$$

where we denote this set by $\mathcal{A}^{\Psi_2} \oplus \mathbb{R} \approx \mathbb{H}$ (see [5, Example C, p. 149]). Now, if $T \in \Gamma$, then $tr(T) = a + \overline{a}$ and by Lemma 1, we have that $\Psi_2(a) + \Psi_2(\overline{a}) \in [-2, 2]$. However, $a + \overline{a} \in K$. In this way, $\Psi_2(a) + \Psi_2(\overline{a}) = \Psi_2(a + \overline{a}) = \varphi_2(a + \overline{a})$, this is, $\varphi_2(a + \overline{a}) \in [-2, 2]$. Therefore $\varphi_2(tr(\Gamma))$ are bound in $\mathbb{C}$.

Similarly we have the next theorem.

Theorem 3: If $g = 3$, then the group Γ_{12} is derived from quaternion algebra A over a totally real number field $\mathbb{Q}(\sqrt{3})$.

Theorem 4: If Γ is a Fuchsian group whose generators are matrices in $PSL(2, \mathbb{R})$ of the type

$$M = \frac{1}{2}\begin{bmatrix} a + b\sqrt{t} & r_1(c + d\sqrt{t}) \\ r_2(a - d\sqrt{t}) & a - b\sqrt{t} \end{bmatrix},$$

where $a, b, c, d \in \mathcal{O}_F$, with $\sqrt{t} \notin \mathcal{O}_{\mathbb{F}}, r_1 = 1$ and $r_2 = -1$, then, Γ is identified by quaternion order $\mathcal{O} \simeq (t, s)_{\mathcal{O}_F}$ of quaternion algebra $A \simeq (t, s)_F$, where $s = r_1 r_2$.

The product of two matrices of Theorem IV assumes the same form M. Furthermore, all the elements of Γ may be obtained directly by relation of the products of the generator matrices and this fact guarantee that all the elements of Γ assume the same form M.

Example 6: If we applied the Theorem 4 and the Remark 1 over matrices belongs to the Γ_8, we have $\Gamma_8 \simeq \mathcal{A}_8 = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$.

Example 7: If we applied the Theorem 4 and the Remark 1 over matrices belongs to the Γ_{12}, we have that $\Gamma_{12} \simeq \mathcal{A}_{12} = (3 + 2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$.

Also, we have that $Z[\mathcal{A}_8] = \mathbb{Q}(\sqrt{2})$ and $Z[\mathcal{A}_{12}] = \mathbb{Q}(\sqrt{3})$, and by Equation (6) there exists an $\mathbb{R}$-isomorphisms ρ_2 defined by $\rho_2 : \mathcal{A}^{\varphi_i} \oplus \mathbb{R} \to \mathbb{H}$.

V. Arithmetic Fuchsian Codes

Based on the previous sections, we now explain how to build a new class of codes that we will call arithmetic fuchsian codes from arithmetic fuchsian groups.

If $g \in \Gamma \subset PSL(2, \mathbb{R})$, where

$$g = \frac{1}{2}\begin{bmatrix} x & y \\ z & w \end{bmatrix},$$

then

$$P^{-1}gP = \begin{bmatrix} (x + w) + i(y - z) & (y + z) + i(x - w) \\ y + z) - i(x - w) & (x + w) - i(y - z) \end{bmatrix}$$

(see [9] for more details).

Example 8: If $g \in \Gamma_8 \subset PSL(2, \mathbb{R})$, where

$$g = \frac{1}{2}\begin{bmatrix} a + b\sqrt[4]{2} & c + d\sqrt[4]{2} \\ -(c - d\sqrt[4]{2}) & a - b\sqrt[4]{2} \end{bmatrix},$$

for $a = a_1 + a_2\sqrt{2}$, $b = b_1 + b_2\sqrt{2}$, $c = c_1 + c_2\sqrt{2}$ and $d = d_1 + d_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, then

$$P^{-1}gP = \begin{bmatrix} m_1 & \sqrt[4]{2}m_2 \\ \sqrt[4]{2}m_3 & m_4 \end{bmatrix}, \tag{10}$$

where $m_1 = (a_1 + ic_1) + \sqrt{2}(a_2 + ic_2)$, $m_4 = \overline{m_1}$, $m_2 = (d_1 + ib_1) + \sqrt{2}(d_2 + ib_2))$, $m_3 = \overline{m_2}$, where $\overline{m}$ denotes the complex conjugation of the element m, and $a_1 + ic_1, a_2 + ic_2, d_1 + ib_1, d_2 + ib_2 \in \mathbb{Z}[i]$.

Example 9: If $g \in \Gamma_{12} \subset PSL(2, \mathbb{R})$, where

$$g = \frac{1}{2}\begin{bmatrix} a + b\sqrt{3 + 2\sqrt{3}} & (c + d\sqrt{3 + 2\sqrt{3}}) \\ -(c - d\sqrt{3 + 2\sqrt{3}}) & a - b\sqrt{3 + 2\sqrt{3}} \end{bmatrix},$$

for $a = a_1 + a_2\sqrt{3}$, $b = b_1 + b_2\sqrt{3}$, $c = c_1 + c_2\sqrt{3}$ and $d = d_1 + d_2\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, then

$$P^{-1}gP = \begin{bmatrix} m_1 & \sqrt{3 + 2\sqrt{3}}m_2 \\ \sqrt{3 + 2\sqrt{3}}m_3 & m_4 \end{bmatrix}, \tag{11}$$

where $m_1 = (a_1 + ic_1) + \sqrt{3}(a_2 + ic_2)$, $m_4 = \overline{m_1}$, $m_2 = (d_1 + ib_1) + \sqrt{3}(d_2 + ib_2))$, $m_3 = \overline{m_2}$, and $a_1 + ic_1, a_2 + ic_2, d_1 + ib_1, d_2 + ib_2 \in \mathbb{Z}[i]$.

VI. Conclusions

In this work we have combined the ideas of the Alamouti code with the arithmetic Fuchsian groups. We used concept of arithmetic Fuchsian groups to show that the groups Γ_8 and Γ_{12} are isomorphic to Hamilton quaternions $\mathbb{H}$. We identified $\mathbb{H}$ by the matrices space E, whose elements are codewords of Alamouti code. However, by Equation (7), we have that the matrices space Γ is equivalent to the matrices space Γ_{4g} (for case $g = 2, 3$). In Section II we presented the construction of Alamouti code from elements of E (remember E is the image of $\mathbb{H}$ by an onto map). We have that the finite set of matrices given by matrices in the Equations (10) and (11) are equivalents to finite set of matrices (codeword) of Alamouti code. However, the Alamouti code has rate 1, and the new code has 4 information symbols belongs to the $\mathbb{Z}[i]$ given by $a_1 + ic_1, a_2 + ic_2, d_1 + ib_1, d_2 + ib_2$ what are encode, and therefore this code has full-rate. But this code has not the property of orthogonality.

ACKNOWLEDEGEMENT

The authors would to like to thank the FAPESP by financial support 2007/56052-8.

REFERÊNCIAS

[1] S.M. Alamouti, “A simple transmit diversity thecnique for wireless communication”, IEEE J. on Select. Areas in Commun., vol. 16, no. 8, pp. 1451-1458, October 1998.

[2] B.A. Sethuraman and B.S. Rajan, “An algebraic description of orthogonal designs and the uniqueness of the alamouti code”, Proc. IEEE GLOBECOM 2002, Taipai, Nov. 17-21, 2002, pp. 1088-1092.

[3] B.A. Sethuraman and B.S. Rajan, “Full-diversity, hight-rate space-time block codes from division algebras”, IEEE Trans. Inform. Theory, vol. 49, pp. 2596-2616, October 2003.

[4] O.T. *O′* Meara, *Introduction to Quadratic Forms*, Spring-Verlag, New York, 1973.

[5] S. Katok, *Fuchsian Groups*, The University of Chicago Press, Chicago, 1992.

[6] S. Johansson, “On Fundamental Domains of Arithmetic Fuchsian Groups”, *Math. Comp.*, vol. 69, no. 229, pp. 339-349, 2000.

[7] S. Johansson, “Genera of Arithmetic Fuchsian Groups”, Acta Arith., vol. 86, no. 2, pp. 171-191, 1998.

[8] K. Takeuchi, “A characterization of arithmetic Fuchsian groups”, J. Math. Soc. Japan, vol. 27, pp. 600-612, 1975.

[9] M.L. Macasieb, “Derived arithmetic fuchsian groups of genus two”, Experimental Mathematics, vol. 17, no. 3, pp. 347-369, 2008.

[10] P.A. Firby and C.F. Gardiner *Surface Topology*, Ellis Horwood, New York, 1991.