COMPUTATIONAL & APPLIED MATHEMATICS

Volume 30, N. 3, pp. 485–498, 2011

ISSN 0101-8205
www.scielo.br/cam

Arithmetic fuchsian groups and space time block codes*

E.D. CARVALHO[1], A.A. ANDRADE[2], R. PALAZZO Jr.[3] and J. VIEIRA FILHO[4]

[1]Department of Mathematics, FEIS-UNESP, Ilha Solteira, SP, Brazil
[2]Department of Mathematics, IBILCE-UNESP, São José do Rio Preto, SP, Brazil
[3]Department of Telematics, FEEC-UNICAMP, Campinas, SP, Brazil
[4]Department of Electrical Engineering, FEIS-UNESP, Ilha Solteira, SP, Brazil
E-mails: edson@mat.feis.unesp.br / andrade@ibilce.unesp.br / palazzo@dt.fee.unicamp.br / jozue@dee.feis.unesp.br

Abstract. In the context of space time block codes (STBCs) the theory of arithmetic Fuchsian groups is presented. Additionally, in this work we present a new class of STBCs based on arithmetic Fuchsian groups. This new class of codes satisfies the property full-diversity, linear dispersion and full-rate.

Mathematical subject classification: 18B35, 94A15, 20H10.

Key words: Arithmetic Fuchsian group, division algebra, quaternion order and space time codes.

1 Introduction

Within the context of digital communication systems, *multiple-input-multiple-output* (MIMO) wireless links, that is, systems that using multiple antennas at the transmitter and the receiver, has emerged. It is used to combat fading from diversity technique, i.e, different replicas of the same information symbol may be transmitted over independent channels and are the available at the receiver side. Notices, in this process, the signal is lost only when all its copies are lost. From

#CAM-196/10. Received: 23/III/10. Accepted: 16/III/11.
*Acknowledgment to FAPESP by financial support 2007/56052-8.

then on, both the data rate and the performance are improved by many orders of magnitude with no extra cost of spectrum. This is also the main reason that the MIMO attracts and motivated much researcher on signal processing. The key feature of a multiple-antenna system is it ability in exploit the turn multiple-path propagation, which is traditionally regarded as a disadvantage to wireless communications, into benefit to the users and result in a diversity again.

In this paper, the diversity can also be obtained at the transmitter by spacing the transmit antennas sufficiently and introducing a code (called *Space Time Block Codes*-STBCs) between the transmitted symbols over M transmit antennas (space) and T symbol periods (time).

Alamouti code [1] was the first practical SBTC proposed in the literature, based with provides full transmit diversity for systems which works with two antennas. The Alamouti code is given by codeword matrices, such that, the matrix operations representing multiplication in the Hamilton quaternions. It is also one of the most successful STBCs because of its simple structure and it is great performance and simple decoding. Tarokh et al. [2] proved that STBC achieves a pairwise error probability (PEP) that is inversely proportional to SNR^{MN}, where SNR denotes the *signal-to-noise ratio*, M the number of transmit antennas and N the number of receive antennas. In this same work, Tarokh showed that the main code design criterion for the STBCs is the rank criterion, i.e, the rank of the difference of two distinct codeword matrices has to be maximal. If this property is satisfied the STBCs is called *fully diverse*.

Full rate (i.e, the number of transmitted signals corresponds to the number of information symbols to be sent) and full diversity codes for the 2×2 MIMO systems, were first constructed by Damen et al. [3], using algebraic number theory. Hassibi in [4] introduced linear dispersion space time block codes (LD-STBCs), i.e, if two codeword matrices X_1, X_2 belong to the code C then $X_1 \pm X_2 \in C$ and $X_1 X_2 \in C$. The idea of LD-STBCs is to spread the information symbols over space and time. Oggier et al. [5] reformulate the rank criterion for LD-STBCs, when the codeword matrices are square, saying the STBC is fully diverse if

$$| \det(X_i - X_j) |^2 \neq 0, \quad \text{for all } X_i \neq X_j \in C.$$

By linearity, it follows that $| \det(X) |^2 \neq 0$ for all nonzero codeword $X \in C$.

Division algebras have been proposed [5], [6], [7], [8] as a new tool for con-

structing STBCs, since they are non-commutative algebras that naturally yield linear fully diverse codes. However, for determining precisely these algebras are division algebras can be a nontrivial problem. Katok [9] characterized some particular classes of 2×2 matrices space $M_2(\mathbb{R})$ isomorphic to Hamilton quaternion (division algebra). The construction of this matrix space are based on the existence of the *arithmetic Fuchsian groups*, i.e, discrete subgroups of $PSL(2, \mathbb{R})$ obtained by some arithmetic construction in the hyperbolic plane.

From then on, we proposed one arithmetic construction of the arithmetic Fuchsian Groups Γ from the self-dual tessellations $\{4g, 4g\}$, with $g \geq 2$, where g denotes the genus of the compact surface, it has the hyperbolic plane as universal covering. This systematic procedure anable us to construction new class of 2×2 STBCs. Additionally, we will show this new class STBCs satisfies the properties of linear dispersion, full rate and full diversity codes. In fact, according to our best knowledge the theory of arithmetic Fuchsian groups required for giving this notion has never been considered before in this area.

This work is organized as follows. In Section 2, we present the concepts of Fuchsian group and quaternion order. In Section 3, we determine the Fuchsian groups Γ_{4g} from hyperbolic tessellation. In section 4, we shown the Fuchsian groups Γ_{4g} are derived from quaternion algebras. In Section 5, we present a new class of codes via arithmetic Fuchsian groups. Some conclusions are presented in Section 6.

2 Arithmetic Fuchsian Groups and Quaternion Order

Let F be a totally real number field of degree $n \geq 2$ over $\mathbb{Q}$ and $\mathcal{O}_F$ be the ring of algebraic integers of F. Let $\{\sigma_1, \ldots, \sigma_n\}$ the n different embedding F into $\mathbb{R}$.

The *quaternion algebra* $\mathcal{A} = (t, s)_F$ is defined as the 4-dimensional vector space over F, with a basis $\{1, i, j, ij\}$, satisfying the conditions $i^2 = t$, $j^2 = s$, $ij = -ji$ and $(ij)^2 = -ts$, where $t, s \in \dot{F} = F - \{0\}$. The quaternion algebra $\mathcal{A} = (t, s)_F$ can be embedded in $M\left(2, F\left(\sqrt{t}\right)\right)$, i.e, there is a linear map such that

$$i \mapsto \begin{bmatrix} \sqrt{t} & 0 \\ 0 & -\sqrt{t} \end{bmatrix} \qquad \text{and} \qquad j \mapsto \begin{bmatrix} 0 & r_1 \\ r_2 & 0 \end{bmatrix},$$

where $s = r_1 r_2$. There exists $\mathbb{R}$-isomorphism ρ_i,

$$\rho_1 : A^{\sigma_1} \otimes \mathbb{R} \to M(2, \mathbb{R}), \qquad \rho_i : A^{\sigma_i} \otimes \mathbb{R} \to \mathbb{H} \tag{1}$$

with $2 \leq i \leq n$, where A is *non-ramified* in ρ_1 and *ramified* in the remaining ρ_i's.

The element $\overline{x} = x_0 - x_1 i - x_2 j - x_3 ij \in \mathcal{A}$ is called *conjugate* of the element $x = x_0 + x_1 i + x_2 j + x_3 ij \in \mathcal{A}$. The *reduced trace* and the *reduced norm* of an element $x \in \mathcal{A}$ are defined as $\mathrm{Trd}(x) = x + \overline{x}$ and $\mathrm{Nrd}(x) = x\overline{x}$, respectively. Thus the norm $\mathrm{Nrd}(x)$ is a quadratic form over F given by $Nrd(x\overline{x}) = x_0^2 - tx_1^2 - sx_2^2 + tsx_3^2$. An *order* $\mathcal{O}$ *in* $\mathcal{A}$ *over* F is a subring of $\mathcal{A}$ containing $\mathcal{O}_F$, which is finitely generated as an $\mathcal{O}_F$-module such that $F\mathcal{O} = \mathcal{A}$.

We consider the upper-half plane $\mathcal{H}^2 = \{z \in \mathbb{C} : Im\,(z) > 0\}$ equipped with a Riemannian metric

$$ds = \frac{\sqrt{dx^2 + dy^2}}{y}.$$

With this metric, $\mathcal{H}^2$ is a model of the hyperbolic plane.

Let G be the group formed of all Möubius transformations, $T : \mathbb{C} \to \mathbb{C}$, given by $T(z) = \frac{az+b}{cz+d}$, where $a, b, c, d \in \mathbb{R}$ and $ad - bc = 1$. To this transformation the following pair of matrices are associated

$$A_T = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Hence,

$$PSL(2, \mathbb{R}) \simeq \frac{SL(2, \mathbb{R})}{\{\pm I_2\}},$$

where $SL(2, \mathbb{R})$ is the group of real matrices with determinant equal to 1 and I_2 denotes the 2×2 identity matrix. A Fuchsian group Γ is a discrete subgroup of $PSL(2, \mathbb{R})$, that is, Γ consists of isometries that preserving orientation and acting on $\mathcal{H}^2$ by homeomorphisms [9] and [12].

For each order $\mathcal{O}$ in $\mathcal{A}$, consider $\mathcal{O}^1$ as the set $\mathcal{O}^1 = \{x \in \mathcal{O} : Nrd(x) = 1\}$. Note that $\mathcal{O}^1$ is a multiplicative group. We observe that a Fuchsian group may be obtained by the isomorphism ρ_1 given by the Equation (1) applied in $\mathcal{O}^1$. In fact, if $x \in \mathcal{O}^1$, then $Nrd\,(x) = \det\,(\rho_1\,(x)) = 1$. From this, it follows that $\rho_1\left(\mathcal{O}^1\right)$ is a subgroup of $SL(2, \mathbb{R})$. Therefore, the derived group from the quaternion algebra $\mathcal{A} = (t, s)_F$ whose order is $\mathcal{O}$, denoted by $\Gamma(\mathcal{A}, \mathcal{O})$, is given by

$$\Gamma(\mathcal{A}, \mathcal{O}) = \frac{\rho_1\left(\mathcal{O}^1\right)}{\{\pm I_2\}} < \frac{SL(2, \mathbb{R})}{\{\pm I_2\}} \simeq PSL(2, \mathbb{R}).$$

The group $\Gamma(\mathcal{A}, \mathcal{O})$ is a Fuchsian group [10]. If Γ is a subgroup of $\Gamma(\mathcal{A}, \mathcal{O})$ with finite index, then Γ is a Fuchsian group derived from a quaternion algebra $\mathcal{A}$, also called *Arithmetic Fuchsian Group*. The Möubius transformation is given by $f(z) = \dfrac{zi+1}{z+i}$, whose matrix associated is given by

$$P = \begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix}, \tag{2}$$

maps $\mathcal{H}^2$ to the Poincaré disc $\mathcal{D}^2$ (another Euclidean model for the hyperbolic plane). The action of $PSL(2, \mathbb{R})$ on $\mathcal{H}^2$ transforms to an action of $PSU(1, 1)$ on $\mathcal{H}^2$, since

$$PSU(1, 1) = f.PSL(2, \mathbb{R}).f^{-1}. \tag{3}$$

The group $PSU(1, 1)$ consists of orientations preserving isometries T: $\mathcal{D}^2 \to \mathcal{D}^2$, acting on $\mathcal{D}^2$ by homomorphisms. The isometries T are given by $T(z) = \dfrac{az+c}{\overline{c}z+\overline{a}}$, where $a, c \in \mathbb{C}$ and $|a|^2 - |c|^2 = 1$. For each of these transformations the following pair of matrices are associated

$$A_T = \pm \begin{bmatrix} a & c \\ \overline{c} & \overline{a} \end{bmatrix}.$$

Theorem 2.1. [9] *Let Γ be a Fuchsian group. 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 $\mathcal{O}_F$, the ring of algebraic integers of F.*

(2) *If σ is an embedding of F in $\mathbb{C}$ different from the identity, then $\sigma(tr(\Gamma))$ is bounded in $\mathbb{C}$.*

3 Fuchsian Groups from Fundamental Polygon $\mathcal{P}_{4g}$

Let S_g be the fundamental group of a compact closed surface of genus g. The presentation of Fuchsian group is given by

$$S_g = \langle a_1, b_1, a_2, b_2, \ldots, a_g, b_g | \prod_{i=1}^{g} [a_i, b_i] = \mathrm{I} \rangle,$$

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 between adjacent edges equal to $2\pi/4g$. Hence, the corresponding fundamental region of self-dual tessellations $\{4g, 4g\}$ of the hyperbolic plane. Considering the Poincaré model $\mathcal{D}^2$, and assuming that $0 \in \mathcal{D}^2$ is the barycenter of $\mathcal{P}_g$. Now, we determine the generators of the Fuchsian group $\Gamma_{\mathcal{D}^2}$, 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 $\mathcal{D}^2/\Gamma_{\mathcal{D}^2}$, and whose hyperbolic area is $\mu(\mathcal{D}^2/\Gamma_{\mathcal{D}^2}) = 4\pi(g-1)$. If T_{A_i}, T_{B_i}, where $i = 1, \ldots, g$, 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 $i = 1, \ldots, g$, is canonically isomorphic to S_{4g} [9]. 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 $i = 1, \ldots, g$. Following exactly the same procedures done by Katok [9] for the case $g = 2$ we have the following result.

Proposition 3.1. *The elements a, c of the 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 the remaining 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 $i = 1, \ldots, g$, 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 3.1. 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 3.2. 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 corresponding real matrices of $PSL(2,\mathbb{R})$ by isometries $f : \mathcal{H}^2 \longrightarrow \mathcal{D}^2$ given by $f(z) = \dfrac{zi+1}{z+i}$, we obtain the following isomorphism

$$\Gamma_{\mathcal{H}^2} \simeq P^{-1}\Gamma_{\mathcal{D}^2}P, \tag{4}$$

where P is the invertible matrix given by the Equation (2). Then by consequence of the Equation (4), it follows that there is an equivalence between the matrix spaces $\Gamma_{\mathcal{H}^2}$ and $\Gamma_{\mathcal{D}^2}$. Thus, $f(\Gamma_{\mathcal{H}^2}) = P^{-1}\Gamma_{\mathcal{D}^2}P$ 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, if $A_1 \in f(\Gamma_8)$ 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 $A_1 \in f(\Gamma_{12})$ 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 3.1. If we compute all the generator matrices $M = D_i$ or $M = E_i$, for $i = 1, \ldots, g$, of $f(\Gamma_{4g})$ it is easy to check that

(1) if $g = 2$, then

$$M = \frac{1}{2}\begin{bmatrix} a+b\sqrt{t} & c+d\sqrt{t} \\ -(c-d\sqrt{t}) & a-b\sqrt{t} \end{bmatrix}, \tag{5}$$

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

$$M = \frac{1}{2}\begin{bmatrix} a + b\sqrt{t} & c + d\sqrt{t} \\ -(c - d\sqrt{t}) & a - b\sqrt{t} \end{bmatrix}, \tag{6}$$

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 the type M and belong to the group $f(\Gamma)$.

4 Fuchsian Groups derived from Quaternion Algebras

In this section, we present a construction that is similar to ones given by Katok [9]. Let $F = \mathbb{Q}(\theta)$ field extension of degree 2 and $\sigma_2 : F \to \mathbb{R}$ be the non-identity homomorphism belong to Galois group $Gal(F/\mathbb{Q})$ given by $\sigma_2(\theta) = -\theta$. Thus, $\psi_2 : K \to \mathbb{C}$, defined by $\psi_2(\sqrt{\theta}) = i\sqrt{\theta}$ is an isomorphism, where $K = F(\sqrt{\theta})$. We consider now a quaternion algebra $\mathcal{A}[\Gamma]$ over $F = \mathbb{Q}(\theta)$ given by

$$\mathcal{A}[\Gamma] = \left\{ \sum_{i=1}^{\lambda} a_i T_i : a_i \in F, \quad T_i \in \Gamma \right\}.$$

Thus,

$$\mathcal{A}[\Gamma] = \left\{ \begin{pmatrix} a_1 & b_1 \\ -b_1' & a_1' \end{pmatrix} : a, b \in K \right\}.$$

Therefore,

$$\mathcal{A}^{\psi_2} = \Psi(\mathcal{A}[\Gamma]) = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} : a, b \in \psi_2(K), \right\}$$

where

$$\Psi : \mathcal{A}[\Gamma] \to M(2, \mathbb{C}),$$

is an embedding given by

$$\Psi(\alpha) = \begin{pmatrix} \psi_2(a_1) & \psi_2(b_1) \\ -\psi_2(b_1') & \psi_2(a_1') \end{pmatrix}.$$

Consequently, $\mathcal{A}^{\psi_2} \otimes \mathbb{R} \simeq \mathcal{H}$, [9].

Lemma 4.1. *If* $\mathbb{H} \simeq (-1, -1)_{\mathbb{R}}$ *and* $\mathbb{H}^1 = \{x \in \mathbb{H} : Nrd(x) = 1\}$ *then* $Trd(\mathbb{H}^1)$ *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 $Nrd(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1$, then $|x_0| \leq 1$, and hence $Trd(x) = 2x_0 \in [-2, 2]$. Since the converse statement is obviously true it follows that $Trd(x) = 2x_0 \in [-2, 2]$.

Theorem 4.1. *If $g = 2$, then the group $f(\Gamma_8)$ is derived from the quaternion algebra $\mathcal{A}$ over the totally real number field $\mathbb{Q}(\sqrt{2})$.*

Proof. Following the same procedures done by Katok [9] for the case $g = 2$, we first show that the conditions (1) and (2) of Theorem 2.1 are satisfied by the elements of $f(\Gamma_8)$. From Remark 3.1, the elements of $f(\Gamma_8)$ 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 $x_0, x_1, x_3, x_4 \in \mathbb{Z}[\sqrt{2}]$ and $tr(M) = x_0 = a_1 + a_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. In this way, it follows that $\mathbb{Q}(tr(f(\Gamma_8))) = \mathbb{Q}(a_1 + a_2\sqrt{2}) = \mathbb{Q}(\sqrt{2})$, 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 2.1 is satisfied. Let $\sigma_2 : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ be the non-identity embedding defined by $\sigma_2(\sqrt{2}) = -\sqrt{2}$. From Remark 3.1, it follows that the generators of Γ_8 and therefore all elements of $f(\Gamma_8)$ are embedded into $M_2(K)$, where $K = \mathbb{Q}(\sqrt{2})(\sqrt{\sqrt{2}})$. Thus, σ_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 procedures done by Katok [9], the elements of $f(\Gamma_8)$ are mapped into 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 $\mathcal{A}^{\Psi_2} \oplus \mathbb{R} \approx \mathbb{H}$. Now, if $T \in f(\Gamma)$, then $tr(T) = a + \overline{a}$ and by Lemma 4.1, it follows that $\Psi_2(a) + \Psi_2(\overline{a}) \in [-2, 2]$. However, $a + \overline{a} \in K$. In this way, $\Psi_2(a) + \Psi_2(\overline{a}) = \Psi_2(a + \overline{a}) = \sigma_2(a + \overline{a})$, that is, $\sigma_2(a + \overline{a}) \in [-2, 2]$. Therefore $\sigma_2(tr(f(\Gamma)))$ is bound in $\mathbb{C}$.

Similarly to the previous case, we have the next theorems.

Theorem 4.2. *If $g = 3$, then the group $f(\Gamma_{12})$ is derived from quaternion algebra $\mathcal{A}$ over the totally real number field $\mathbb{Q}(\sqrt{3})$.*

Theorem 4.3. *If $f(\Gamma)$ is a Fuchsian group whose generators are matrices in $PSL(2,\mathbb{R})$ of the type*

$$M = \frac{1}{2}\begin{bmatrix} a + b\sqrt{t} & (c + d\sqrt{t}) \\ -(a - d\sqrt{t}) & a - b\sqrt{t} \end{bmatrix}, \tag{7}$$

where $a, b, c, d \in \mathcal{O}_F$, with $\sqrt{t} \notin \mathcal{O}_{\mathbb{F}}$, then the matrices belong to $f(\Gamma)$ are identified by the elements of the quaternion order $\mathcal{O} \simeq (t,-1)_{\mathcal{O}_F}$ of the quaternion algebra $\mathcal{A} \simeq (t,-1)_F$.

The product of two matrices in Theorem 4.3 assumes the same form M. Furthermore, all the elements of $f(\Gamma)$ may be obtained directly as the product of the generator matrices and this fact guarantee that all the elements of $f(\Gamma)$ assume the same form M.

Example 4.1. Applying Theorem 4.3 and Remark 3.1 to the matrices belonging to $f(\Gamma_8)$, it follows that these matrices are identified by the elements of quaternion order $\mathcal{A}_8 = (\sqrt{2},-1)_{\mathbb{Z}[\sqrt{2}]}$.

Example 4.2. Applying Theorem 4.3 and Remark 3.1 to the matrices belonging to $f(\Gamma_{12})$, it follows that these matrices are identified by the elements of quaternion order $\mathcal{A}_{12} = (3 + 2\sqrt{3},-1)_{\mathbb{Z}[\sqrt{3}]}$.

We will denoted by $\mathcal{A}_8(2)$ and $\mathcal{A}_{12}(2)$ the matrix spaces associated to quaternion order $\mathcal{A}_8$ and $\mathcal{A}_{12}$, respectively. As consequence of Equation (4) and by Theorems 4.1 and 4.2, it follows that the matrix spaces $\mathcal{A}_8(2)$ and $\mathcal{A}_{12}(2)$ are division algebras. Similarly, by Equation (4), it follows that $M_{\mathcal{A}_{4g}}(2) \simeq P^{-1}\mathcal{A}_{4g}(2)$ for $g = 2, 3$ and P is the invertible matrix given by the Equation (2).

5 Space-Time Codes From Division Algebra

In this section, we will characterize algebraically the matrix spaces $M_{\mathcal{A}_{4g}}(2)$. First, we notice each element of matrix space $\mathcal{A}_{4g}(2)$ can written as

$$M = \frac{1}{2}\begin{bmatrix} x + y\theta' & z + w\theta' \\ -(z - w\theta') & x - y\theta' \end{bmatrix},$$

with x, y, z and $w \in \mathbb{Z}[\theta]$, where $\theta = \sqrt{2}$ if $M \in \mathcal{A}_8(2)$ and $\theta = 3 + 2\sqrt{3}$ if $M \in \mathcal{A}_{12}(2)$.

Proposition 5.1. *If $M \in \mathcal{A}_{4g}(2)$ is given by*

$$M = \frac{1}{2}\begin{bmatrix} x + y\theta' & z + w\theta' \\ -(z - w\theta') & x - y\theta' \end{bmatrix}, \tag{8}$$

with $x = a_1 + a_2\theta$, $y = b_1 + b_2\theta$, $w = c_1 + c_2\theta$, $z = d_1 + d_2\theta \in \mathbb{Z}[\theta]$, where $\theta = \sqrt{2}, \theta' = \sqrt[4]{2}$ if $M \in \mathcal{A}_8(2)$ and $\theta = \sqrt{3}, \theta' = 3 + 2\sqrt{3}$ if $M \in \mathcal{A}_{12}(2)$, then

$$N = P^{-1}MP = \frac{1}{2}\begin{bmatrix} (a_1 + ic_1) + \theta[(a_2 + ic_2)] & \theta'[(d_1 + ib_1) + (d_2 + ib_2)] \\ \theta'[(d_1 - ib_1) + (d_2 - ib_2)] & (a_1 - ic_1) + \theta[(a_2 - ic_2)] \end{bmatrix}, \tag{9}$$

where $a_1 + ic_1, a_2 + ic_2, d_1 + ib_1, d_2 + ib_2 \in \mathbb{Z}[i]$.

Proof. If $H \in \mathcal{A}_{4g}(2)$, where $H = \frac{1}{2}\begin{pmatrix} x & y \\ z & w \end{pmatrix}$, then

$$P^{-1}HP = \begin{pmatrix} (x + w) + i(y - z) & (y + z) + i(x - w) \\ (y + z) - i(x - w) & (x + w) - i(y - z) \end{pmatrix}, \tag{10}$$

which concludes the proof.

Example 5.1. If $M \in \mathcal{A}_8(2)$, where

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

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

$$N = P^{-1}MP = \begin{bmatrix} m_1 & \sqrt[4]{2}m_2 \\ \sqrt[4]{2}m_3 & m_4 \end{bmatrix}, \tag{11}$$

with $m_1 = (a_1 + ic_1) + \sqrt{2}(a_2 + ic_2)$, $m_4 = \overline{m_1}$, $m_2 = (d_1 + ib_1) + \sqrt{2}(d_2 + ib_2))$, $m_3 = \overline{m_2}$, 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 5.2. If $M \in \mathcal{A}_{12}(2)$, where

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

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

$$N = P^{-1}MP = \begin{bmatrix} m_1 & \sqrt{3+2\sqrt{3}}m_2 \\ \sqrt{3+2\sqrt{3}}m_3 & m_4 \end{bmatrix}, \tag{12}$$

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 $a_1+ic_1, a_2+ic_2, d_1+ib_1, d_2+ib_2 \in \mathbb{Z}[i]$.

5.1 Construction of Space Time Codes

In order to construction a space time code, we need a complex alphabet which can be for example belong to ring of algebraic integers $\mathbb{Z}[i]$ (*QAM* symbols). In the next theorem we given a construction of a space time codes $C \subseteq M_{\mathcal{A}_{4g}}(2)$.

Theorem 5.1. *Let $F = \mathbb{Q}(i)$ and $K = F(\theta')$, where $\theta' = \sqrt[4]{2}$ or $\sqrt{3+2\sqrt{3}}$. We consider the set $C \subseteq \mathcal{M}_{4g}(2)$. Then the set C is a space time code, that satisfies the following properties:*

(1) *C is linear dispersion space time code,*

(2) *C is full rate, and*

(3) *C is full diversity.*

Proof.

(1) If $X, Y \in C$, it is easy to see $X \pm Y, XY \in C$. Then C is a linear dispersion space time code.

(2) Notice, for each codematrix $N \in C$ given by the matrix of the Equation (11), it follows that 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 they are encoded. Then C is full rate.

(3) If $N \in C \subseteq \mathcal{M}_{4g}(2)$, then N is given by

$$N = \frac{1}{2}\begin{bmatrix} (a_1 + ic_1) + \theta[(a_2 + ic_2)] & \theta'[(d_1 + ib_1) + (d_2 + ib_2)] \\ \theta'[(d_1 - ib_1) + (d_2 - ib_2)] & (a_1 - ic_1) + \theta[(a_2 - ic_2)] \end{bmatrix}, \quad (13)$$

where $a_1 + ic_1, a_2 + ic_2, d_1 + ib_1, d_2 + ib_2 \in \mathbb{Z}[i]$. Now, if $H \in \mathcal{M}_{4g}(2)$, where $H = \frac{1}{2}\begin{pmatrix} n_1 & n_2 \\ \overline{n_2} & \overline{n_1} \end{pmatrix}$, then

$$f^{-1}(H) = \begin{pmatrix} Re(n_1) + Im(n_2) & Im(n_1) + Re(n_2) \\ -(Im(n_1) - Re(n_2)) & Re(n_1) - Im(n_2) \end{pmatrix}. \quad (14)$$

Therefore

$$f^{-1}(H) = \frac{1}{2}\begin{bmatrix} x + y\theta' & z + w\theta' \\ -(z - w\theta') & x - y\theta' \end{bmatrix}, \quad (15)$$

with $x, y, z, w \in \mathbb{Z}[\theta]$, where $\theta = \sqrt{2}$ if $M \in \mathcal{A}_8(2)$ and $\theta = 3 + 2\sqrt{3}$ if $M \in \mathcal{A}_{12}(2)$. As consequence of Equation (4), it follows that $\det(H) = \det(f^{-1}(H)) \in \mathcal{A}_{4g}(2)$. Thus, $\det(H) \neq 0$ and therefore C is fully diversity.

6 Conclusion

In this work, we constructed a new class of STBCs from symmetric groups (in this case arithmetic Fuchsian groups) associated with the regular polygon octogon and dodecagon of self-dual tessellation $\{8, 8\}$ and $\{12, 12\}$, respectively.

However, we known there are infinitely possibilities of tessellations of hyperbolic plane by regular polygons. This fact suggest another possibilities of identifications of arithmetic Fuchsian groups by quaterion orders. Therefore, its open another possibilities to constructions STBCs that using this theory.

REFERENCES

[1] S.M. Alamouti, *A simple transmit diversity technique for wireless communications*, IEEE Journal on Selected Areas in Communications **16**(8), (1998), 1451–1458.

[2] V. Tarokh, N. Seshadri and A.R. Calderbank, *Space-time codes for high data rate wireless communications: performance criterion and code construction*. IEEE Trans. Inform. Theory, **44** (1998), 744–765.

[3] M.O. Damen, A. Tewfik and J.-C. Belfiore, *A construction of a space-time code based on the theory numbers*. IEEE Trans. Inform. Theory, **48**(3) (2002), 753–760.

[4] B. Hassibi and B.M. Hochwald, *High-rate codes that are linear in space and time*. IEEE Trans. Inform. Theory, **48** (2002), 1804–1824.

[5] F. Oggier, G. Rekaya, J-C. Belfiore and E. Viterbo, *Perfect space-time block codes*. IEEE Trans. Inform Theory, **52**(9) (2006), 3885–3902.

[6] B.A. Sethuraman and B.S. Rajan, *Full-diversity, hight-rate space-time block codes from division algebras*. IEEE Trans. Inform. Theory, **9**(10) (2003), 2596–2616.

[7] J.C. Belfiore, G. Rekaya and E. Viterbo, *The golden code: a* 2×2 *full rate space time code with non vanishing determinants*. IEEE Trans. Inform. Theory, **51**(4) (2005), 1432–1436.

[8] R. Vehkalahti, C. Hollanti, J. Lahtonen and K. Ranto, *On the densest MIMO lattices from cyclic division algebras*. IEEE Trans. Inform. Theory, **55**(8) (2009), 3751–3779.

[9] S. Katok. *Fuchsian groups*. The University of Chicago Press (1992).

[10] K. Takeuchi, *A characterization of arithmetic Fuchsian groups*. J. Math. Soc. Japan, **27**(4) (1975), 600–612.

[11] O.T. O'Meara, *Maximal orders*, Academic Press, London (1975).

[12] A. Beardon, *The geometry of discret groups*. Springer-Verlag, New York (1983).

[13] M.L. Macasieb, *Derived arithmetic Fuchsian groups of genus two*. Experimental Mathematics, **17**(3) (2008), 347–369.