Hyperbolic lattices: a new propose for space time coding theory

Edson Donizete de Carvalho, Antonio Aparecido de Andrade

***Abstract*— In the context of space-time block codes (STBCs), the theory of hyperbolic lattices over totally real number field is presented, as well as theoretic criteria to check if such algebras are division algebras from arithmetic Fuchsian groups. These can be used to obtain families of 2×2 STBCs that satisfies the properties of linear dispersion, full rate and full diversity.**

I. INTRODUCTION

The large capacity of multiple-antenna systems and the willingness to transmit at higher data rates with better performance over wireless channels have motivated much research on signal processing over multiple transmit-receive antennas. A higher data rate can be achieved by transmitting symbols simultaneously from M transmit antennas. Full rate and full diversity codes for the 2×2 coherent multiple-input multiple-output (MIMO) systems, were first constructed by Damen et al. [1], using algebraic number theory. Tarokh et al. [2] showed that the main code design criterion for the space-time block codes (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. Hassibi [3] introduced linear dispersion space-time block codes (LD-STBCs), i.e, if two codeword matrices X_1, X_2 belong to the code $\mathcal{C}$ then $X_1 \pm X_2 \in \mathcal{C}$ and $X_1 X_2 \in \mathcal{C}$. The idea of LD-STBCs is to spread the information symbols over space and time. Oggier [4] reformulated the rank criterion for LD-STBCs, when the codeword matrices are square, establishing that the STBC is fully diverse if

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

By linearity we have $| \det(X) |^2 \neq 0$ for all nonzero codeword $X \in \mathcal{C}$.

Also, division algebras have been proposed ([5], [6], [4], [7] and [8]) as a new tool for the construction of STBCs, since these algebras are non-commutative naturally yielding linear fully diverse codes. However, determining precisely these division algebras may be a nontrivial problem.

Katok [9] characterized some particular classes of 2×2 matrix spaces $M_2(\mathbb{R})$ isomorphic to quaternion algebra (division algebra). The construction of these matrix spaces is based on the existence of arithmetic Fuchsian group, i.e, a discrete subgroup of $PSL(2, \mathbb{R})$ obtained by some arithmetic construction in the hyperbolic plane.

The author is with the Department of Mathematics, Feis - Unesp, CEP 15385-000, Ilha Solteira - SP, Brazil, email: edson@mat.feis.unesp.br

The author is with the Department of Mathematics, Ibilce - Unesp, CEP 15054-000, São José do Rio Preto - SP, Brazil. email: andrade@ibilce.unesp.br

Carvalho [10], [11], proposed an arithmetic procedure for the identification of the elements of the arithmetic Fuchsian group Γ_{4g} by elements of an order $\mathcal{O}$ from the quaternion algebra $\mathcal{A}$ over the integer ring $\mathcal{O}_K$ of a quadratic extension K of $\mathbb{Q}$, obtained from hyperbolic tessellation $\{4g, 4g\}$, where $g = 2, 3$ denotes the genus of compact surface which is modulated in the hyperbolic plane, when $[K : \mathbb{Q}] = 2$. The generators of Γ_{4g} are given by

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

with $a, b, c, d \in \mathbb{Z}[\theta]$, where $\mathbb{Z}[\theta]$ is the integer ring of $\mathbb{Q}(\sqrt{m})$, $m > 0$, $r_1 = -r_2 \in \mathbb{Z}$, $t \in \mathbb{Z}[\theta]$ and $\sqrt{t} \notin \mathbb{Z}[\theta]$. In the Sections II and III, we caracterize the quaternion orders found in [8], [11] in terms of lattices, we will call these lattices of hyperbolic lattices.

Carvalho et al. [11] proposed an arithmetic procedure for construction a class of STBCs satisfying the properties of full-diversity, linear dispersion and full-rate.

On the other hand, also in the hyperbolic context, Luzzi et.al [12] proposed a new method called *algebraic reduction* for 2×2 STBCs based on quaternion algebra $\mathcal{O}$ (whose elements are units of $\mathcal{O}$ identified by the elements of symmetric group associated to fundamental region in the hyperbolic space) which directly exploits the multiplicative structure of the STBCs in additional to the lattices structure and consists in absorbing a part of the channel into the code.

So the study and developing the theory of the hyperbolic lattices in this work is clearly motivated by an analogy from the error-correcting codes found in [8] and [12]: why we caracterize the terms of fundamental region, Gram matrix, generator matrix and the index associated to quotient of the lattices by sublattices as in the Euclidean case, fact that not fully been exploited yet in terms of coding theory literature.

Hence, the problem is faced with the hyperbolic lattices $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]} \simeq (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ and $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]} \simeq (3 + 2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$ obtained from identification to arithmetic Fuchsian groups Γ_8 and Γ_{12} [8], [11]. Thus of goal of this paper is obtain a systematic procedure for the construction of sublattices from lattices $\Gamma = \mathcal{O}_{\mathbb{Z}[\sqrt{2}]}, \mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$, such that the index are given by $|\Gamma/\Gamma_n| = 2^n$. These sublattices can be used to construct a family of 2×2 STBCs that satisfies the property of the linear dispersion, full rate and full diversity.

This paper is organized as follows. In Section II, we present the concepts of arithmetic Fuchsian group and quaternion order. In Section III, we present concepts of hyperbolic lattices. In Section IV, we construct sublattices from hyperbolic

lattices. In Section V, we present a new family of space-time block codes via hyperbolic lattices.

II. Arithmetic Fuchsian Groups and Quaternion Order

We consider $\mathbb{H}^2 = \{z = x + iy \in \mathbb{C} : y > 0\}$ be the complex upper half-plane model for the hyperbolic plane equipped with the hyperbolic metric $ds^2 = (dx^2 + dy^2)/y^2$.

The group $PSL(2,\mathbb{R}) = SL(2,\mathbb{R})/\{\pm \mathrm{I}\}$, where I is the identity matrix, acting on $\mathbb{H}^2$ by Möbius transformation. The matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{R})$, determines a transformation $T_A : \mathbb{H}^2 \to \mathbb{H}^2$ defined as $T_A(z) = \dfrac{az+b}{cz+d}$, where $a, b, c, d \in \mathbb{R}$ and $det(T_A) = ad - bc = 1$.

We will consider $\mathbb{D}^2 := \{z \in \mathbb{C} | \, |z| < 1\}$ the Poincaré disc, which is another model for the hyperbolic plane equipped with the hyperbolic metric $ds^2 = dz/|z|$.

The isometry $f(z) = \dfrac{zi+1}{z+i}$, whose matrix associated is given by

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

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

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

The group $PSU(1,1)$ consists of orientation preserving isometries $T : \mathbb{D}^2 \to \mathbb{D}^2$, acting on $\mathbb{D}^2$ by homeomorphisms. 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 one of these transformations the following pair of matrices are associated

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

A Fuchsian group G is defined as a discrete subgroup of $PSL(2,\mathbb{R})$ and can be give as the quotient space $G/\mathbb{H}^2$ equipped with the structure of Riemman surface.

For our proposes, we restrict the followings cases:

- when the surface $G/\mathbb{H}^2$ is compact, and
- when the hyperbolic volume $vol(\mathcal{F}_G)$, that is, the measure of a fundamental region, is finite.

The genus associated of the compact surface $G/\mathbb{H}^2$ is given by [13]

$$g = g(G) = \frac{1}{4\pi} vol(\mathcal{F}_G) + 1 - \sum_{m \geq 2} e(m,G) \frac{m-1}{2m}, \tag{3}$$

where $e(m,G)$ denote the number of elliptic points of order m associated to surface $G/\mathbb{H}^2$.

In this work, we only consider the case where $e(m,G) = 0$ and G is arithmetic. Let G_g be a Fuchsian group associated to a surface with genus g. For example, if $g = 2$ and $g = 3$, by Equation (3) we have that $vol(\mathcal{F}_{G_2}) = 4\pi$ and $vol(\mathcal{F}_{G_3}) = 8\pi$, respectively.

We have that $\Gamma_2 \subseteq \Gamma_1$ are two Fuchsian groups with finite index $[\Gamma_2 : \Gamma_1]$ and

$$[\Gamma_1 : \Gamma_2] = \frac{vol(\Gamma_1)}{vol(\Gamma_2)}. \tag{4}$$

If $\Gamma_1 = G_g$ we have the following question:

(I) Which is the index $[\Gamma_1 : \Gamma_i]$ associated to quotient of the group G_g by a subgroup Γ_i?

For the answer we need to known the volumes $vol(\Gamma_1)$ and $vol(\Gamma_i)$. The $vol(\Gamma_1)$ is easy to determine by Equation (3), but the volume $vol(\Gamma_i)$ is not immediate. However, we will see in the next subsection that when the Fuchsian group is arithmetic it is possible related these groups by orders in the quaternion algebras. Furthermore, we will see that the answer of question (I) is very easy with this identification.

A. Quaternion Order

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

The *quaternion algebra* $\mathcal{A} = (t,s)_F$ is defined as a 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 $t, s \in \dot{F} = F - \{0\}$. There is a linear map $\tau : \mathcal{A} \to \mathcal{M}_2(F(\sqrt{t}))$, [10]-[11], that associates the basis elements $1, i, j, ij$ to the matrices $M_0, M_1, M_2, M_3 \in \mathcal{M}_2(F(\sqrt{t}))$, respectively, where

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

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

$s = r_1 r_2$ and τ is an embedding of $\mathcal{A}$ in $\mathcal{M}_2(F(\sqrt{t}))$. Thus

$$\tau(x_0 + x_1 i + x_2 j + x_3 ij) = \frac{1}{2} \begin{pmatrix} x_0 + x_1\sqrt{t} & r_1(x_2 + x_3\sqrt{t}) \\ r_2(x_2 - x_3\sqrt{t}) & x_0 - x_1\sqrt{t} \end{pmatrix}, \tag{5}$$

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 to $\mathcal{M}_2(F)$ if and only if $t = k^2$, for some $k \in F^*$.

There exists $\mathbb{R}$-isomorphisms ρ_i, given by

$$\rho_1 : A^{\sigma_1} \otimes \mathbb{R} \to M(2,\mathbb{R}), \qquad \rho_i : A^{\sigma_i} \otimes \mathbb{R} \to \mathbb{H}. \tag{6}$$

with $2 \leq i \leq n$, where $\mathcal{A}$ is *non-ramified* in ρ_1 and *ramified* in the remaining ρ_i's, and $\mathbb{H}$ denotes the Hamilton quaternion, $\mathbb{H} = (-1,-1)_{\mathbb{R}}$.

An 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 $\mathrm{Nrd}(x\overline{x}) = x_0^2 - tx_1^2 - sx_2^2 + tsx_3^2$.

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 $F\mathcal{O} = \mathcal{A}$. For each order $\mathcal{O}$ in $\mathcal{A}$, consider $\mathcal{O}^1$ as the set

$$\mathcal{O}^1 = \{x \in \mathcal{O} : \mathrm{Nrd}(x) = 1\}.$$

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 Equation (6) in $\mathcal{O}^1$. In fact, if $x \in \mathcal{O}^1$, then $\mathrm{Nrd}(x) = \det(\rho_1(x)) = 1$. From this, it follows that $\rho_1(\mathcal{O}^1)$ is a subgroup of $SL(2,\mathbb{R})$. Therefore, the derived group from the quaternion algebra $\mathcal{A} = (t,s)_F$ whose order is $\mathcal{O}$, and denoted by $\Gamma(\mathcal{A},\mathcal{O})$, is given by

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

The group $\Gamma(\mathcal{A},\mathcal{O})$ is a Fuchsian group [9].

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*.

III. Hyperbolic Lattices

Let $\mathcal{A} = (t,s)_F$ be a quaternion algebra over F and R be a ring of F. An *R-order* $\mathcal{O}$ in $\mathcal{A}$ is a subring of $\mathcal{A}$ containing 1, equivalently, it is a finitely generated R-module such that $\mathcal{A} = F\mathcal{O}$. We also call an *$R$-order* $\mathcal{O}$ as a hyperbolic lattice given by identification with an arithmetic Fuchsian group. If Γ is an hyperbolic lattices given by an R-order $\mathcal{O}_\Gamma$ in $\mathcal{A}$, then there exists a basis $\{e_1,e_2,e_3,e_4\}$ of $\mathcal{A}$ and an R-ideal $\mathcal{A}$ such that

$$\mathcal{O}_\Gamma = \mathcal{A}e_1 \oplus Re_2 \oplus Re_3 \oplus Re_4,$$

where $\oplus$ denotes the direct sum. We have that $x \cdot y \in \mathcal{O}_\Gamma$ for all $x, y \in \mathcal{O}_\Gamma$. Furthermore, since every $x \in \mathcal{O}_\Gamma$ is integral over R [14], it follows that $Nrd(x), Trd(x) \in R$, [13].

Definition 1: Let M the the matrix

$$M = \begin{pmatrix} x_0 + x_1\sqrt{t} & r_1(x_2 + x_3\sqrt{t}) \\ r_2(x_2 - x_3\sqrt{t}) & x_0 - x_1\sqrt{t} \end{pmatrix},$$

which is a matrix identified by element $x = x_0 + x_1 i + x_2 j + x_3 ij \in \mathcal{O}$. The matrix M is called of *generator matrix* for the hyperbolic lattice and the *Gram matrix* is given by $G = MM^t$, where M^t is obtained of the element $\overline{x} = x_0 - x_1 i - x_2 j - x_3 ij \in \mathcal{O}$.

A difference between Euclidean lattices and hyperbolic lattices is related to fact that the hyperbolic distance between two points $x, y \in \mathbb{H}^2$ is not an inner product. Also, we have that $\mathbb{H}^2$ not admit structure of the vector spaces as well as in the Euclidean spaces. Therefore, it does not make sensible to consider points lattices as well in the Euclidean lattices. Consequently, by the same argument it does not sensible to consider the volume these lattices given by square root of the determinant associated to matrix generator. However, we have following definition.

Definition 2: The volume of an hyperbolic lattice, denoted by $vol(\Gamma)$, is given by $vol(\mathcal{F}_\Gamma)$, where $\mathcal{F}_\Gamma$ is a fundamental region associated to group Γ.

Definition 3: Let $\mathcal{O}$ be an order over the integer ring $\mathcal{O}_F$. The discriminant $d(\mathcal{O})$ of $\mathcal{O}$ is defined as the square root of the $\mathcal{O}_F$-ideal generated by $det(Tr(x_i\bar{x_j}))_{i,j}^4$, where $\{x_1,x_2,x_3,x_4\}$ is an $\mathcal{O}_F$-basis of the quaternion order $\mathcal{O}$.

Notice this invariant not depend on the choice of the lattices basis.

Proposition 1: If $\mathcal{A} = (t,s)_F$ and $\mathcal{O}_F$ is the integer ring of F, where $t, s \in \mathcal{O}_F$, then $\mathcal{O} = (t,s)_{\mathcal{O}_F} = \{x_0 + x_1 i + x_2 j + x_3 k : x_0,\ x_1,\ x_2,\ x_3 \in \mathcal{O}_F\}$, is an order in $\mathcal{A}$ with an $\mathcal{O}_F$-basis given by $\{x_0,x_1,x_2,x_3\} = \{1,i,j,k\}$ and the discriminant $d(t,s)_{\mathcal{O}_F}$ is given by $d(t,s)_{\mathcal{O}_F} = 4ts$.

Proof. Let $\mathcal{O}$ be an order in $\mathcal{A} \simeq (t,s)_F$ with a basis $\{x_1,x_2,x_3,x_4\}$, satisfying the conditions $x_1 = 1$, $x_2^2 = t$, $x_3^2 = s$, $x_2x_3 = ts$ and $x_2x_3 = -x_3x_2$, where $t, s \in F^*$. Thus the discriminant $d(\mathcal{O})$ is given by the square root of the $\mathcal{O}_F$-ideal generated by $det(Tr(x_i\bar{x_j}))_{i,j=1}^4$. Since $Tr(x_i\bar{x_j}) = 0$ if $i \neq j$, it follows that the matrix $(Tr(x_i\bar{x_j}))$ is given by

$$(Tr(x_i\bar{x_j})) = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2t & 0 & 0 \\ 0 & 0 & 2s & 0 \\ 0 & 0 & 0 & 2ts \end{pmatrix}.$$

Therefore, $det(Tr(x_i\bar{x_j})) = 16(ts)^2$ and thus $d(\mathcal{O}) = (det(Tr(x_i\bar{x_j})))^{\frac{1}{2}} = 4st$.

Example 1: Let $\mathcal{A}_1 = (\sqrt{2},-1)_{\mathbb{Q}(\sqrt{2})}$ be an algebra with basis $\{1,i,j,k\}$ satisfying $i = \sqrt[4]{2}$, $j = Im$, and $k = \sqrt[4]{2}Im$, where Im denotes an imaginary unit. Let us also consider the following order $\mathcal{O}_1 = (\sqrt{2},-1)_{\mathbb{Z}[\sqrt{2}]}$, where $\mathbb{Z}[\sqrt{2}]$ is the integer ring of the number field $\mathbb{Q}(\sqrt{2})$. By Proposition (1) we have that $d(\mathcal{O}_1) = -4\sqrt{2} = -(\sqrt{2})^5$.

Example 2: Let $\mathcal{A}_2 = (3+2\sqrt{3},-1)_{\mathbb{Q}(\sqrt{3})}$ be an algebra with basis $\{1,i,j,k\}$ satisfying $i = \sqrt{3+2\sqrt{2}}$, $j = Im$, and $k = \sqrt{3+2\sqrt{2}}Im$, where Im denotes an imaginary unit. Let us also consider the following order $\mathcal{O}_2 = (3+2\sqrt{3},-1)_{\mathbb{Z}[\sqrt{3}]}$, where $\mathbb{Z}[\sqrt{3}]$ is the integer ring of the number field $\mathbb{Q}(\sqrt{3})$. Then, by Proposition (1), $d(\mathcal{O}_2) = -4(3+2\sqrt{3})$.

Remark 1: Let Λ_1 and Λ_2 be two hyperbolic sublattices of hyperbolic lattices Γ such that $\Lambda_2 \subseteq \Lambda_1$. We have that $d(\Gamma_1)$ is a factor of $d(\Gamma_2)$.

Then the index $[\Gamma : \Lambda]$ is related with the discriminants by the following proposition.

Proposition 2 ([14], p.66):

$$[R : d(\Lambda)] = [\Gamma : \Lambda]^2 [R : d(\Gamma)].$$

IV. Families of hyperbolic sublattices from hyperbolic lattices

In this section, we propose one procedure to construction of families of hyperbolic sublattices from hyperbolic lattices $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}(\sqrt{2},-1)$ and $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}(3+2\sqrt{3},-1)$, respectively. Also we show the index partitioning of sublattices in these hyperbolic lattices are given by 2^n.

Let $\mathbb{Z}[\sqrt{m}]$ for $m = 2,3$. We have that $\mathbb{Z}[\sqrt{m}]$ is an Euclidean domain and also is the integer ring from number field $\mathbb{Q}(\sqrt{m})$. The relative norm associated to the element $z = a+b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ is given by $\mathcal{N}(a+b\sqrt{m}) = a^2 - mb^2$.

Proposition 3: If Λ and Γ are two $\mathbb{Z}[\sqrt{m}]$-orders for $m = 2,3$ such that the discriminants associated are given by

$d(\Lambda) =< a + b\sqrt{m} >$ and $d(\Gamma) =< 2^n(a + b\sqrt{m}) >$, respectively, then the index associated to quotient of hyperbolic lattice Λ by the hyperbolic sublattice is given by $[\Gamma : \Lambda] = 2^n$, for $n \geq 1$.

Proof. We have that discriminants are ideals from the integer ring $\mathbb{Z}[\sqrt{m}]$, and the relative norms are given by $\mathcal{N}(2^n(a + b\sqrt{m})) = \mathcal{N}(2^n)\mathcal{N}(a + b\sqrt{m}) = (2^n)^2\mathcal{N}(a + b\sqrt{m})$ and $\mathcal{N}(a + b\sqrt{m})$, respectively. By Proposition 2, we have that $[\Gamma : \Lambda]^2 = \frac{\mathbb{Z}[\sqrt{m}] : d(\Lambda)\mathbb{Z}[\sqrt{m}]}{\mathbb{Z}[\sqrt{m}] : d(\Gamma)\mathbb{Z}[\sqrt{m}]} = \frac{\mathcal{N}(2^n(a + b\sqrt{m}))}{\mathcal{N}(a + b\sqrt{m})} = \frac{\mathcal{N}(2^n)\mathcal{N}(a + b\sqrt{m})}{\mathcal{N}(a + b\sqrt{m})} = \mathcal{N}(2^n) = (2^n)^2$. Therefore,

$$[\Gamma : \Lambda] = 2^n, \tag{7}$$

which concludes the proof.

Proposition 4: If $\mathcal{P}_n$ is an ideal of the integer ring $\mathbb{Z}[\sqrt{2}]$, generate by $\mathcal{P}_n =< 2^n\sqrt{2} >$, then there is $\mathbb{Z}[\sqrt{2}]$-order $\Lambda_n \simeq (2^n\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ such that $d(\Lambda_n) = 2^n\sqrt{2}$.

Proof. Let $\{x_0, x_1, x_2, x_3\}$ be a $\mathbb{Z}[\sqrt{2}]$-basis where $x_0 = 1, x_1^2 = 2^n\sqrt{2}, x_2^2 = -1$. Thus $t = x_1^2 = 2^n\sqrt{2}$ and $s = -1$. By Equation (5) we obtain the correspondent $\mathbb{Z}[\sqrt{2}]$-order $\Lambda_n \simeq (2^n\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ and, by Proposition 1, we have that $d(\Lambda_n) = 2^n\sqrt{2} = \mathcal{P}_n$.

The combination of Proposition 5 and Equation (7) given us a general procedure to the construction of $\mathbb{Z}[\sqrt{2}]$-orders such that

$$\ldots \subset \Lambda_{n+1} \subset \Lambda_n \subset \Lambda_{n-1} \subset \ldots \Lambda_2 \subset \Lambda_1 \subset \Lambda_0, \tag{8}$$

and $|\frac{\Lambda_{n+1}}{\Lambda_n}| = 2$, for all $n \geq 0$.

Proposition 5: If $\mathcal{P}_n$ is an ideal of the integer ring $\mathbb{Z}[\sqrt{3}]$, generated by $\mathcal{P}_n =< 2^n(3 + 2\sqrt{3}) >$, then there is an $\mathbb{Z}[\sqrt{3}]$-order Λ_n such that $d(\Lambda_n) = 2^n\sqrt{3}$.

Proof. Let $\{x_0, x_1, x_2, x_3\}$ be a $\mathbb{Z}[\sqrt{3}]$-basis such that $x_0 = 1, x_1^2 = 2^n(3 + 2\sqrt{3}), x_2^2 = -1$. Thus $t = x_1^2 = 2^i(3 + 2\sqrt{3})$ and $s = -1$. By Equation (5) we obtain the correspondent $\mathbb{Z}[\sqrt{3}]$-order $\Lambda_n \simeq (2^n(3+2\sqrt{3}), -1)_{\mathbb{Z}[\sqrt{3}]}$ and, by Proposition 1, we have that $d(\Lambda_n) = 2^n(3 + 2\sqrt{3}) = \mathcal{P}_n$.

The combination of Proposition 5 and Equation (7) given us a general procedure to construction $\mathbb{Z}[\sqrt{3}]$-orders such that

$$\ldots \subset \Lambda_{n+1} \subset \Lambda_n \subset \Lambda_{n-1} \subset \ldots \Lambda_2 \subset \Lambda_1 \subset \Lambda_0, \tag{9}$$

and $|\frac{\Lambda_{n+1}}{\Lambda_n}| = 2$, for all $n \geq 0$.

V. Families of Space-Time Block Codes from Hyperbolic Sublattices

we denote by $\mathcal{A}_{4g}$ with $g = 2, 3$ the quaternion order $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]} \simeq (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ and $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]} \simeq (3 + 2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$, respectively. These quaternion orders satisfies the property of division algebra [10], [8]. Also we denote by $M_{\mathcal{A}_{4g}}(2) \simeq P^{-1}\mathcal{A}_{4g}P$, where $g = 2, 3$ and P is the invertible matrix given by the matrix in the Equation (1). Consequently, $M_{\mathcal{A}_{4g}}(2)$ is a division algebra (see [8]). Similarity, we denote by $\mathcal{A}_{4g,2^n}(2)$ the sublattices from the lattices $\mathcal{A}_{4g}$ and $M_{\mathcal{A}_{4g,2^n}}(2) \simeq P^{-1}\mathcal{A}_{4g,2^n}P$. In this context we goal are to show the matrix spaces $M_{\mathcal{A}_{4g,2^n}}(2)$ satisfies the property of division ring.

Remark 2: Let $M \in \mathcal{A}_{4g}(2)$, where

$$M = \frac{1}{2}\begin{pmatrix} x + y\theta' & z + w\theta' \\ -(z - w\theta') & x - y\theta' \end{pmatrix}, \tag{10}$$

with $x = a_1 + a_2\theta, y = b_1 + b_2\theta, w = c_1 + c_2\theta, z = d_1 + d_2\theta \in \mathbb{Z}[\theta]$. If $g = 2$ we have that $\theta = \sqrt{2}$, and $\theta' = \sqrt{2^n\sqrt{2}}$, and if $g = 3$ we have that $\theta = \sqrt{3}$ and $\theta' = \sqrt{3 + 2\sqrt{3}}$. We can see that the elements $x + y\theta', x - y\theta', z + w\theta$ and $-(z - w\theta')$ as elements of the number field $L = F(\theta') = \{a + b\theta'; a, b \in F\}$ with Galois group $G(L/F) = \{id, \sigma\}$, where id is the identity and σ is homomorphism given by $\sigma(a + b\theta') = a - b\theta'$ for all $a, b \in F$. Let $x_0 = x + y\theta'$ and $x_1 = z + w\theta'$. Therefore, we have that the matrix $M \in \mathcal{A}_{4g}(2)$ is given by

$$M = \begin{pmatrix} x_0 & x_1 \\ -\sigma(x_1) & \sigma(x_0) \end{pmatrix}. \tag{11}$$

Proposition 6: If $det(M) = 0$ then $-1 = N_{L/F}(x)$ for any $x \in L$, where $N_{L/F}$ denotes the relative norm associated to field extension L/F.

Proof: We have that $x_0, x_1, \sigma(x_0), \sigma(x_1)$ and $-1 \in \mathcal{O}_L$. Thus $det(M) = x_0\sigma x_0 + 1x_1\sigma(x_1)$. If $det(M) = 0$ then $-1 \in N_{L/F}(\frac{x_0}{x_1})$.

Corollary 1: If $\mathcal{A}_{4g}(2)$ is a division algebra then $-1 \neq N_{L/F}(x)$ for all $x \in L$.

Proof: It is directly consequence of the Proposition 6.

Proposition 7: If $M \in \mathcal{A}_{4g}(2)$ is given by

$$M = \frac{1}{2}\begin{pmatrix} x + y\theta' & z + w\theta' \\ -(z - w\theta') & x - y\theta' \end{pmatrix}, \tag{12}$$

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 $\theta = \sqrt{2}, \theta' = \sqrt{2^n\sqrt{2}}$ if $M \in \mathcal{A}_{8,2^n}(2)$ and $\theta = \sqrt{3}, \theta' = \sqrt{3 + 2\sqrt{3}}$ if $M \in \mathcal{A}_{12,2^n}(2)$, then $N = P^{-1}MP$ is given by

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

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

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

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

which concludes the proof.

Example 3: If $M \in \mathcal{A}_{8,2^n}(2)$, where

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

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

$$N = P^{-1}MP = \begin{pmatrix} m_1 & \sqrt{2^n\sqrt{2}}m_2 \\ \sqrt{2^n\sqrt{2}}m_3 & m_4 \end{pmatrix}, \tag{13}$$

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 4: If $M \in \mathcal{A}_{12,2^n}(2)$, where

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

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

$$N = P^{-1}MP = \begin{pmatrix} m_1 & \sqrt{2^n(3+2\sqrt{3})}m_2 \\ \sqrt{2^n(3+2\sqrt{3})}m_3 & m_4 \end{pmatrix}, \tag{14}$$

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

The alphabet of a space-time code is the complex numbers usually taking from the ring of algebraic integers $\mathbb{Z}[i]$ (*QAM* symbols), and in general from a number field. The next theorem provides a systematic construction of the arithmetic Fuchsian codes $\mathcal{C} \subseteq M_{\mathcal{A}_{4g,2^n}}(2)$ as a subclass of the space-time codes.

Theorem 1: Let $F = \mathbb{Q}(\theta)$ and $L = F(\theta')$, where $\theta' = \sqrt{2^n\sqrt{2}}$ or $\sqrt{2^n(3+2\sqrt{3})}$. If $\mathcal{C} \subseteq \mathcal{M}_{4g}(2)$, then $\mathcal{C}$ is an arithmetic Fuchsian code (space-time code) satisfying the following properties: (1) $\mathcal{C}$ is linear dispersion space-time code, (2) $\mathcal{C}$ is full rate and (3) $\mathcal{C}$ is full diversity.

Proof:

1) If $X, Y \in \mathcal{C}$ then $X \pm Y, XY \in \mathcal{C}$ and therefore $\mathcal{C}$ is a linear dispersion space-time code.
2) For each code matrix $N \in \mathcal{C}$ given by Equation (13), we have the four information symbols belonging to $\mathbb{Z}[i]$ are encoded as $a_1 + ic_1, a_2 + ic_2, d_1 + ib_1, d_2 + ib_2$. As consequence, we have that $\mathcal{C}$ is full rate.
3) If $N \in \mathcal{C} \subseteq \mathcal{M}_{4g,2^n}(2)$, then N is given by

$$N = \frac{1}{2}\begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix}, \tag{15}$$

where $q_1 = (a_1 + ic_1) + \theta[(a_2 + ic_2)], q_2 = \theta'[(d_1 + ib_1) + (d_2 + ib_2)], q_3 = \theta'[(d_1 - ib_1) + (d_2 - ib_2)]$ and $q_4 = (a_1 - ic_1) + \theta[(a_2 - ic_2)]$, with $a_1 + ic_1, a_2 + ic_2, d_1 + ib_1, d_2 + ib_2 \in \mathbb{Z}[i]$. 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 $f^{-1}(H)$ is given by

$$\begin{pmatrix} Re(n_1) + Im(n_2) & Im(n_1) + Re(n_2) \\ -(Im(n_1) - Re(n_2)) & Re(n_1) - Im(n_2) \end{pmatrix}.$$

Therefore

$$f^{-1}(H) = \frac{1}{2}\begin{pmatrix} x + y\theta' & z + w\theta' \\ -(z - w\theta') & x - y\theta' \end{pmatrix}, \tag{16}$$

with $x, y, z, w \in \mathbb{Z}[\theta]$, where $\theta = \sqrt{2}$ if $M \in \mathcal{A}_{8,2^n}(2)$ and $\theta = 3 + 2\sqrt{3}$ if $M \in \mathcal{A}_{12,2^n}(2)$. We have $det(H) = det(f^{-1}(H)) \in \mathcal{A}_{4g,2^n}(2)$. If $det(H) = 0$ then $det(f^{-1}(H)) = 0$, and by Proposition 6, we have that $-1 = N_{L/F}(x)$ for some $x \in L$, which is a contradiction because $\mathcal{A}_{4g}(2)$ is a division algebra for $g = 2, 3$ and by Corollary 1, we have that $-1 \neq N_{L/F}(x)$ for all $x \in L$. Thus $det(H) \neq 0$ and therefore $\mathcal{C}$ is full diversity.

VI. Conclusion

In this work we give a new method of construction for space time via hyperbolic lattices.

Acknowledgment

The authors would like to thank the FAPESP - 2008/56052-8 by financial support.

References

[1] 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, vol. 48, n. 03, (2002) 753-760.
[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, vol. 44, (1998) 744-765.
[3] B. Hassibi and B.M. Hochwald. *High-rate codes that are linear in space and time*, IEEE Trans. Inform. Theory, vol. 48, (2002) 1804-1824.
[4] F. Oggier, G. Rekaya, J-C. Belfiore and E. Viterbo. *Perfect space-time block codes*, IEEE Trans. Inform Theory, vol. 52, n. 9, (2006).
[5] B.A. Sethuraman and B.S. Rajan. *Full-diversity, hight-rate space-time block codes from division algebras*, IEEE Trans. Inform. Theory, vol. 9, n. (10) (2003), 2596-2616.
[6] J.C. Belfiore, G. Rekaya and and E. Viterbo. *The golden code: A* 2×2 *full rate space-time code with nonvanishing determinants*, IEEE Trans. Inform. Theory, vol. 51, n. 4, (2005) 1432-1436.
[7] A.A. Andrade and E.D. Carvalho. *New family of perfect codes for* 2×2 *MIMO*, International Journal of Applied Mathematics, vol. 23, n. 2, (2010) 191-205.
[8] E. D. Carvalho, A. A. Andrade, J. V. Filho and J.E.A. Rodriguez, *Arithmetic Fuchsian Codes*, Anais do XXVI Simpósio Brasileiro de Telecomunicações 2009 (SBrT), BLUMENAU, SC-Brazil.
[9] S. Katok. *Fuchsian Groups*. The University of Chicago Press, 1992.
[10] E.D. Carvalho, *Construction and Labelling of Geometrically Uniform Signal Constellations in Euclidean and Hyperbolic Spaces*, PhD Dissertation, FECC-UNICAMP, Brazil, 2001 (in Portuguese).
[11] E.D. Carvalho *Identification of Lattices from Genus of Compact*, Proceedings of ITS 2006, 146-151.
[12] L. Luzzi, G. Rekaya-Ben Othman and J.C. Belfiore, *Algebraic reduction for space-time codes based on quaternion algebras*, Pre-Print ArXiv:0809.3365v2 [cs.IT], September 2008.
[13] S. Johansson, Genera of arithmetic Fuchsian groups, in Acta Arith, vol. 86, n. 2, (1998), 171-191.
[14] I. Reiner, Maximal Orders, Academic Press, New York 1975.