Maximal Orders and Arithmetic Fuchsian Groups

Edson D. Carvalho
Dep. de Matemática, FEIS, UNESP
15385-000, Ilha Solteira, SP
edson@mat.feis.unesp.br

Antônio A. Andrade
Dep. de Matemática, IBILCE, UNESP
15054-000, S.J.Rio Preto, SP
andrade@ibilce.unesp.br

Jaime E. Apaza Rodriguez
Dep. de Matemática, FEIS, UNESP,
15385-000, Ilha Solteira, SP
jaime@mat.feis.unesp.br.

Abstract: *In this work we identifying arithmetic fuchsian groups by quaternion order over real quadratic extension, whose elements are isometries that action on hyperbolic plane by Möbius transformations and preserving orientation. We show these quaternion order are not maximal in quaternion algebra over real quadratic extension. However, we identifying the maximal order that contains these orders. This procedure anable us to construction lattices in hyperbolic plane which are associated to signal constellation.*

Keywords: *Quaternion order, Maximal order, Arithmetic fuchsian groups, Hyperbolic plane, Information theory*

1 Introduction

Information theory is at the intersection of mathematics, statistics, computer science, physics, and electrical engineering. Its impact has been crucial to the success of the Voyager missions to space, the invention of the compact disc, the feasibility of mobile phones, the development of the Internet.

Historically, information theory was developed by Claude E. Shannon. In [1], Shannon to find fundamental limits on compressing and reliably storing and communicating data. Important subfields of information theory are algorithmic complexity theory, algorithmic information theory, measures of information, source coding and channel coding.

In particular, this work is inside of the context of channel coding. We know a great number of discrete memoryless channels of practical interest are embedded on compact surfaces with genus $g = 0, 1, 2, 3$ [2], and addition to this, the design of geometrically signals sets and codes were extensively considered only for the cases $g = 0$ and $g = 1$.

In [3] it is shown that the error probability depends on the curvature, $K^{'}$ or equivalently, on the genus of a surface, and that the best performance is achieved when considering surfaces with constant negative curvature among the possible values taking on by $K^{'}, (K^{'} < 0, K^{'} > 0,$ and $K^{'} = 0)$.

However, we know the compact surfaces with genus $g \geq 2$ are modeled on hyperbolic plane [6]. Remember, the hyperbolic plane has negative curvature. Within the context of designing digital communications system in hyperbolic spaces, it is necessary to establish a systematic procedure for the construction of lattices (quaternion order of quaternion algebra). Because, the choice of signal constellation (quotient of an order by a nontrivial ideal) to be used plays a fundamental role, and the performance of the system is dependent on such signals constellations [5]. It is by this procedure that we identify the algebraic and geometric structures in order

to construct geometrically uniform codes in hyperbolic spaces (see also, [4] for the Euclidean spaces), and consequently to achieve the desired efficiency.

A Fuchsian group Γ is a discrete subgroup of $PSL(2,\mathbb{R}) = SL(2,\mathbb{R})/\{\pm \mathrm{I}\}$, (I is the identity matrix), that is, Γ consists of isometries on $\mathbb{H}^2 = \{z = x + iy \in \mathbb{C} : y > 0\}$ (upper half-plane Euclidean model for the hyperbolic plane, endowed with the Riemannian metric $ds^2 = dx^2 + dy^2)/y^2$, that preserving orientation and action on $\mathbb{H}^2$ by homomorphism [6], 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 Poincaré disc model (another Euclidean model for hyperbolic plane), $\mathbb{D}^2 = \{z \in \mathbb{C} \,|\, |z| < 1\}$, with the Riemmanian metric $ds^2 = dz/|z|$, whose Möbius transformations is given by $T_A(z) = \frac{az+c}{\overline{c}z+\overline{a}}$, with $a, c \in \mathbb{C}$ and $|a|^2 - |c|^2 = 1$. Morever, the mapping $f(z) = (zi+1)/(z+i)$, is an isometry between $\mathbb{H}^2$ and $\mathbb{D}^2$.

In this work, associated with the Fuchsian group Γ, we show there is a fundamental region $\mathcal{P}$ (polygonal shape containing $4g$ edges). The pairing of the $4g$ edges of a hyperbolic polygon $\mathcal{P}_{4g}$ to be considered in Section 3, leads to an oriented compact surface $\mathbb{H}^2/\Gamma_{4g}$, 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 $\mu(\mathcal{P}_{4g}) = \mu(\mathbb{H}^2/\Gamma_{4g})$, is finite.

Thus, in this work the signals constellations are considered as the barycenters of the regular hyperbolic polygons with $4g$ edges, denoted by $\mathcal{P}_{4g}$. Each barycenter, or equivalently, each signal u in the signal constellation is the image of another signal v in the constellation, by the application of a hyperbolic isometric $T \in \Gamma_{4g}$, that is, $T(u) = v$.

Note that, if the corresponding group acts transitively on the signals constellation then the resulting signal constellation is said to be geometrically uniform, [4].

2 Quaternion Order and Arithmetic Fuchsian Groups

Let $\mathcal{A} = (t,s)_{\mathbb{F}}$ be a quaternion algebra over a number field $\mathbb{F}$ with basis $\{1, i, j, ij\}$, satisfying $i^2 = t, j^2 = s, ij = -ji$, and $(ij)^2 = -ts$, where $t, s \in \mathbb{F}^* = \mathbb{F} - \{0\}$. If $x \in \mathcal{A}$, then $x = x_0 + x_1 i + x_2 j + x_3 ij$ with $x_0, x_1, x_2, x_3 \in \mathbb{F}$, and $\overline{x} = x_0 - x_1 i - x_2 j - x_3 ij$ is called 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 $\tau : \mathcal{A} \to M\left(2, \mathbb{F}\left(\sqrt{t}\right)\right)$ that associate to the base elements $1, i, j, ij$ the matrices $M_0, M_1, M_2, M_3 \in M\left(2, \mathbb{F}\left(\sqrt{t}\right)\right)$ respectively, with

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad M_1 = \begin{bmatrix} \sqrt{t} & 0 \\ 0 & -\sqrt{t} \end{bmatrix}, \qquad M_2 = \begin{bmatrix} 0 & r_1 \\ r_2 & 0 \end{bmatrix}, \qquad M_3 = \begin{bmatrix} 0 & r_1\sqrt{t} \\ -r_2\sqrt{t} & 0 \end{bmatrix}$$

where $s = r_1 r_2$, and τ is an embedding of $\mathcal{A}$ in $M(2, \mathbb{F}(\sqrt{t}))$. Thus

$$\tau(x_0 + x_1 i + x_2 j + x_3 ij) = x_0 M_0 + x_1 M_1 + x_2 M_2 + x_3 M_3 = \begin{bmatrix} x_0 + x_1\sqrt{t} & r_1(x_2 + x_3\sqrt{t}) \\ r_2(x_2 - x_3)\sqrt{t} & x_0 - x_1\sqrt{t} \end{bmatrix},$$

when $x = x_0 + x_1 i + x_2 j + x_3 ij$.

Morever, 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. It is a simple matter to show that τ is onto in $M(2, \mathbb{F})$ if and only if $t = k^2$, for some $k \in \mathbb{F}^* = \mathbb{F} \setminus \{0\}$.

This shows that there are two possibilities for a quaternion algebra $\mathcal{A}$ over $\mathbb{F}$. Either it is isomorphic to the matrix algebra $M(2, \mathbb{F})$ (in this case we say that $\mathcal{A}$ is *non-ramified*), or to a

sub-algebra of $M(2,\mathbb{F}(\sqrt{t}))$, with $\sqrt{t}\notin\mathbb{F}$, having the structure of a division ring, denoted by $\mathbb{H}$. In this case we say that $\mathcal{A}$ is *ramified* for some $t\in\mathbb{F}$.

If $\mathcal{A}\simeq(t,s)_{\mathbb{F}}$ quaternion algebras over number field $\mathbb{F}$, and $\sigma:\mathbb{F}\to\mathbb{K}$ is any homomorphism of $\mathbb{F}$ into another field $\mathbb{K}$, we define $\mathcal{A}^{\sigma}=(\sigma(t),\sigma(s))_{\sigma(\mathbb{F})}$, and $\mathcal{A}^{\sigma}\otimes\mathbb{K}=(\sigma(t),\sigma(s))_{\mathbb{K}}$.

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

$$\rho_1:\mathcal{A}^{\varphi_1}\otimes\mathbb{R}\to M(2,\mathbb{R}),\qquad \rho_i:\mathcal{A}^{\varphi_i}\otimes\mathbb{R}\to\mathbb{H}. \tag{1}$$

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 $Nrd_{\mathbb{H}}(x)=det(\rho_1(x))$, $Trd_{\mathbb{H}}(x)=tr(\rho_1(x))$, $\varphi_i(Nrd_{\mathbb{H}}(x))=Nrd_{\mathbb{H}}(\rho_i(x))$ and $\varphi_i(Trd_{\mathbb{H}}(x))=Trd_{\mathbb{H}}(\rho_i(x))$.

Let $\mathcal{O}_{\mathbb{F}}$ be the ring of integers of $\mathbb{F}$. An *order $\mathcal{O}$ in $\mathcal{A}$ over $\mathbb{F}$* is free $\mathcal{O}_{\mathbb{F}}$-module containing 1 with rank equal $4n$. Let $\mathcal{P}$ be the prime ideal in $\mathcal{O}_{\mathbb{F}}$ and let be the Hilbert symbol, denoted by $(\frac{-,-}{\mathcal{P}})$, given by function from $\mathbb{F}^*\times\mathbb{F}^*$ to $\{-1,1\}$ defined by

$$(a,b)=\begin{cases}1, & if\ z^2=ax^2+by^2\ \ (mod\,\mathcal{P})\ has\ nonzero\ solution\ (x,y,z)\in\mathbb{F}^3\\ \\ -1, & if\ not.\end{cases}$$

The quaternion algebra $(t,s)_{\mathbb{F}}$ is called ramified at $\mathcal{P}$ iff $(\frac{t,s}{\mathcal{P}})=-1$. Also, the discriminant $d(\mathcal{A})$ of $\mathcal{A}$ s defined as the product of the prime ideals at which $\mathcal{A}$ is ramified. Let $\mathcal{O}$ be an order in A. The discriminant $d(\mathcal{O})$ of $\mathcal{O}$ is defined as the square root of the $\mathcal{O}_{\mathbb{F}}$-ideal generated by $det(Tr(x_i.\bar{x_j}))$, where $\{x_1,x_2,x_3,x_4\}$ is an $\mathcal{O}_{\mathbb{F}}$-basis of the quaternion order $\mathcal{O}$. If $\mathcal{M}$ is a maximal order in $\mathcal{A}$ containing $\mathcal{O}$, then the discriminant satisfies $d(\mathcal{O})=d(\mathcal{M})[\mathcal{M}:\mathcal{O}]$ and $d(\mathcal{M})=d(A)$.

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 $\Gamma\,(\mathcal{A},\mathcal{O}):=\rho_1\left(\mathcal{O}^1\right)/\{\pm\mathrm{Id}\}$. It is known (and proved by Takeushi in 1975, [7]) 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 it is possible to characterize the Fuchsian groups that are derived from a quaternion algebra.

Theorem 2.1 *[6] Let Γ be 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 $\mathbb{F}$ if and only if Γ satisfies the following conditions.*

i) *If $\mathbb{F}=\{\mathbb{Q}(tr(T):T\in\Gamma)\}$, then, $\mathbb{F}$ is a number field of finite degree and $tr(\Gamma)$ is in $\mathcal{O}_{\mathbb{F}}$.*

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

3 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 $S_g=\langle a_1,b_1,a_2,b_2,...,a_g,b_g|\prod_{i=1}^{g}[a_i,b_i]=\mathrm{Id}\rangle$ with $[a_i,b_i]=a_ib_ia_i^{-1}b_i^{-1}$. Let us consider a regular polygon $\mathcal{P}_g$ with $4g$ edges and angles with measure equal to $2\pi/4g$. Hence, the corresponding a fundamental region of self-dual tessellations of the hyperbolic plane is denoted by $\{4g,4g\}$, we and denote its edges, in some cyclic fixed order, as $u_1,v_1,u_1^{'},v_1^{'},...,u_g,v_g,u_g^{'},v_g^{'}$

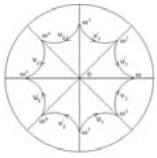

Figura 1: Octagon

The Fig. 1 illustrates the fundamental region, octagon $\mathcal{P}_8$, of the self-dual tessellation $\{8,8\}$ with its sides labelled by u_1, u_1', v_1, v_1', u_2, u_2', v_2, v_2'.

Now, we determine of generators of Fuchsian Groups Γ_{4g} whose 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 given by $tr(T_i) > 2$) , where g is the genus of compact surface $\mathbb{H}^2/\Gamma$, and whose hyperbolic area is $\mu(\mathbb{H}^2/\Gamma_{4g}) = 4\pi(g-1)$.

If we consider T_{A_i}, T_{B_i}, when $i = 1, ..., g$, to be 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}, when $i = 1, ..., g$ is canonically isomorphic to S_{4g} (see [6], pp 94). Considering the Poincare model $\mathbb{D}^2$, and assuming that $0 \in \mathbb{D}^2$ is the barycenter of $\mathcal{P}_g$, we can find explicit formula for the matrices A_i and B_i that generates the transformations T_{A_i} and T_{B_i}, for $i = 1, ..., g$. Following exactly the same kind of procedures done by Katok for the case $g = 2$ (see [6, Example C, pp 95]), we have the following result.

Proposition 3.1 *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 another matrices generators are given by $A_i = C^{4i} A_1 C^{-4i}$ and $B_i = C^{4i+1} A_1 C^{4i+1}$ for every $i = 1, ..., g$, where C is 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 generators transformations $T_{A_1} \in \Gamma_8$ is give, 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 another 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*

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

and the another matrices A_2, A_3, B_1, B_2 and B_3 are given by conjugation.

Now, taking the correspondents real matrices of $PSL(2,\mathbb{R})$ by isometries $f:\mathbb{H}^2 \longrightarrow \mathbb{D}^2$ give by $f(z)=\frac{zi+1}{z+i}$, we have, $\Gamma = f^{-1}\Gamma_{4g}f$ is a subgroup of $PSL(2,\mathbb{R})$,where $g=2,3$, and whose generators matrices are given by $f^{-1}A_if = D_i$ and $f^{-1}B_if = E_i$. In particular, we have for $A_1 \in \Gamma_8$ is given by

$$f^{-1}A_1f = D_1 = \begin{bmatrix} \frac{(2+\sqrt{2})+(-2-\sqrt{2})\sqrt[4]{2}}{2} & \frac{(2+\sqrt{2})-(\sqrt{2})(\sqrt[4]{2})}{2} \\ \frac{(-2-\sqrt{2})+(\sqrt{2})(\sqrt[4]{2})}{2} & \frac{(2+\sqrt{2})+(2+\sqrt{2})\sqrt[4]{2}}{2} \end{bmatrix},$$

and $A_1 \in \Gamma_{12}$ is given by

$$f^{-1}A_1f = D_1 = \begin{bmatrix} \frac{(2+\sqrt{3})+\sqrt{3+2\sqrt{3}}(1+\sqrt{3})}{2} & \frac{(3+2\sqrt{3})+\sqrt{3+2\sqrt{3}}(-1+\sqrt{3})}{2} \\ \frac{-(3+2\sqrt{3})+\sqrt{3+2\sqrt{3}}(-1+\sqrt{3})}{2} & \frac{(2+\sqrt{3})-(\sqrt{3+2\sqrt{3}})(1+\sqrt{3})}{2} \end{bmatrix}.$$

Remark 3.1 *If we compute all the generators matrices $M = D_i$ or $M = E_i$ for $i = 1,\ldots,g$, of Γ_{4g} it is easy to check the matrices are given by:*

(i) If $g = 2$,

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

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

(i) If $g = 3$,

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

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.

Lemma 3.1 *[6] If $\mathbb{H} \simeq (-1,-1)_{\mathbb{R}}$ and $\mathbb{H}^1 = \{x \in \mathbb{H} : Nrd_{\mathbb{H}}(x) = 1\}$ is the set of quaternion algebra of reduced norm 1, then $Trd_{\mathbb{H}}(\mathbb{H}^1)$ is bound in $\mathbb{C}$.*

Theorem 3.1 *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 [6, Example C, pp 95]). Thus, first we shown the conditions (i) and (ii) of Theorem 2.1 are satisfied for elements of Γ_8. By, Remark 3.1, 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 $\mathbb{Q}(tr(\Gamma_8)) = \mathbb{Q}(a_1 + a_2\sqrt{2}) = \mathbb{Q}(\sqrt{2})$, and $tr(M) \in \mathbb{Z}[\sqrt{2}]$. Since $\mathbb{Q}(\sqrt{2})$ is a totally real quadratic extension of $\mathbb{Q}$, its follow the condition (i) of Theorem 2.1 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 3.1, generators of Γ_8 and therefore all elements of Γ_8 are embedded into $M(2,\mathbb{K})$, where $\mathbb{K} = \mathbb{Q}(\sqrt{2})(\sqrt{\sqrt{2}})$. Thus, φ_2 extends to an isomorphism $\Psi_2 : \mathbb{K} \longrightarrow \mathbb{C}$, 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

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

where we denote this set by $\mathcal{A}^{\Psi_2} \otimes \mathbb{R} \approx \mathbb{H}$(see [6, Example C, pp 149]). Now, if $T \in \Gamma$, then $tr(T) = a + \overline{a}$ and by Lemma 3.1, where $\Psi_2(a) + \Psi_2(\overline{a}) \in [-2, 2]$. 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 $\varphi_2(tr(\Gamma))$ is bound in $\mathbb{C}$.

Theorem 3.2 *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 3.3 *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 $a, b, c, d \in \mathcal{O}_{\mathbb{F}}$, with $\sqrt{t} \notin \mathcal{O}_{\mathbb{F}}, r_1 = 1$ and $r_2 = -1$, then, Γ is identified by quaternion order $\mathcal{O} \simeq (t, s)_{\mathcal{O}_{\mathbb{F}}}$ of quaternion algebra $A \simeq (t, s)_{\mathbb{F}}$, where $s = r_1 r_2$.

It easy to show the product of two matrices of Theorem 3.3 assumes the same form M. In practice, we have that all the elements of Γ may be obtained by directly relations of product the matrices generators and this fact guaranteed that all the elements of Γ assumes the same form M.

Remark 3.2 *By Theorem 3.3 and Remark 3.1, we have, $\Gamma_8 \simeq (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ and $\Gamma_{12} \simeq (3 + 2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$.*

The next step is to show that the quaternions orders $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]} \simeq (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ and $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]} \simeq (3+2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$ are not maximal in quaternion algebras $A_{\mathbb{Q}(\sqrt{2})} \simeq (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})}$ and $A_{\mathbb{Q}(\sqrt{3})} \simeq (3 + 2\sqrt{3}, -1)_{\mathbb{Q}(\sqrt{3})}$, respectively.

Proposition 3.2 *Let $\mathcal{O} = \mathcal{O}_{\mathbb{F}} + i\mathcal{O}_{\mathbb{F}} + \mathcal{O}_{\mathbb{F}}j + \mathcal{O}_{\mathbb{F}}ij$ to be on quaternion order $(t, s)_{\mathcal{O}_{\mathbb{F}}}$ of quaternion algebra $\mathcal{A} \simeq (t, s)_{\mathbb{F}}$ over number field $\mathbb{F}$, where $\mathcal{O}_{\mathbb{F}}$ is integer ring of number field $\mathbb{F}$. Then the discrimant $d(t, s)_{\mathcal{O}_{\mathbb{F}}}$ is given by $d(t, s)_{\mathcal{O}_{\mathbb{F}}} = 4ts$.*

Example 3.3 **(i)** *If the quaternion order is given by $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]} \simeq (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ then $d(\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}) = -4\sqrt{2} = -(\sqrt{2})^5$.*

(ii) *If the quaternion order is given by $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]} \simeq (3 + 2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$ then $d(\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}) = -4(3 + 2\sqrt{3})$.*

Proposition 3.3 *The quaternion order $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]} \simeq (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ is not maximal order in $A_{\mathbb{Q}(\sqrt{2})} \simeq (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})}$.*

Proof.

By Example 3.3 $d(\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}) = -(\sqrt{2})^5$. Now if $\mathcal{P}$ is a prime ideal in $\mathbb{Z}[\sqrt{2}]$ generated by $\sqrt{2}$ (remember $\mathbb{Z}[\sqrt{2}]$ is principal ring), then $d(\mathcal{A})/d(\mathcal{O}) = \mathcal{P}^5$ and $d(\mathcal{A})$ is given by the product of the prime ideals at $\mathcal{A}$ is ramified. Thus, $\mathcal{P}$ is the only prime ideal, that we need to check if $\mathcal{A}$ is ramified in $\mathbb{Z}[\sqrt{2}]$ for this case. For this, we compute the Hilbert symbol $(\frac{\sqrt{2},-1}{\mathcal{P}})$. We assume $(\frac{\sqrt{2},-1}{\mathcal{P}}) = 1$, that is, the equation $z^2 = \sqrt{2}x^2 - 1y^2 (mod\, \mathcal{P})$ has non-zero solution $(x, y, z) \in \mathbb{Q}(\sqrt{2})^3$.
If $x = x_1 + x_2\sqrt{2}, y = y_1 + y_2\sqrt{2}$ and $z = z_1 + z_2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, then $\sqrt{2}$ divides $(z_1^2 + 2z_2^2) + 2\sqrt{2}z_1z_2 - \sqrt{2}[(x_1^2 + 2x_2^2) + 2\sqrt{2}x_1x_2] + (y_1^2 + 2y_2^2) + 2\sqrt{2}y_1y_2$. Since $\sqrt{2}$ is a factor of $2\sqrt{2}z_1z_2$, $\sqrt{2}[(x_1^2+2x_2^2)+2\sqrt{2}x_1x_2]$ and $2\sqrt{2}y_1y_2$ we have that $\sqrt{2}$ divides $(z_1^2+2z_2^2)+(y_1^2+2y_2^2) = (z_1^2+y_1^2)+2(z_2^2+y_2^2)$ and $\sqrt{2}$ divides $(z_1^2+y_1^2)$. In this way, we obtain $q_1+q_2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ such that

$z_1^2+y_1^2=\sqrt{2}(q_1+q_2\sqrt{2})=\sqrt{2}q_1+2q_2$, or as, $z_1^2+y_1^2=2q_2$ and $q_1=0$ thus $z_1^2+y_1^2\equiv 0\ (mod\, 2)$. Therefore $y_1=0, z_1=2^k$ or $y_1=2^k, z_1=0$ for some integer k, are only possibly solutions for this equation.

Case I) If $y_1=0$ and $z_1=2^k$, then $(2^k+z_2\sqrt{2})^2=\sqrt{2}[(x_1^2+2x_2^2)+2\sqrt{2}x_1x_2]-2y_2^2$ and $(2^{2k}+2.2^k z_2\sqrt{2}+2z_2^2)=\sqrt{2}[(x_1^2+2x_2^2+2\sqrt{2}x_1x_2]-2y_2^2$. and as consequence $\sqrt{2}$ divides x_1^2. Thus we have that $t_1+t_2\sqrt{2}\in\mathbb{Q}(\sqrt{2})$ where $x_1^2=\sqrt{2}(t_1+t_2\sqrt{2})=2t_2+t_1\sqrt{2}$ and $x_1^4=(4t_2^2+4\sqrt{2}t_1t_2+2t_1^2)$. Note $t_1=0$, by consequence $x_1^4=4t_2^2$ then $x=\pm\sqrt{2}\sqrt{t}\notin\mathbb{Q}$.

Case II) If $y_1=2^k$ and $z_1=0$, then $(z_2\sqrt{2})^2=\sqrt{2}[(x_1^2+2x_2^2)+2\sqrt{2}x_1x_2]-(2^k+y_2\sqrt{2})^2$ and $(2z_2^2)=\sqrt{2}[(x_1^2+2x_2^2+2\sqrt{2}x_1x_2]-(2^{2k}+2.2^k y_2\sqrt{2}+2y_2^2)$. Therefore $\sqrt{2}$ divides x_1^2. Similary to case I, we obtain the same contradiction.

Thus, we conclude that if $\mathcal{A}$ is ramified in only prime ideal $\mathcal{P}$ then $d(\mathcal{A})=\sqrt{2}$. Since $d(\mathcal{A})\neq d(\mathcal{O})$, it follows that $\mathcal{O}$ is not a maximal order in $\mathcal{A}$.

Proposition 3.4 *The quaternion order $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}\simeq(3+2\sqrt{3},-1)_{\mathbb{Z}[\sqrt{3}]}$ is not maximal order in $\mathcal{A}_{\mathbb{Q}(\sqrt{3})}\simeq(3+2\sqrt{3},-1)_{\mathbb{Q}(\sqrt{3})}$.*

If $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}\simeq(\sqrt{2},-1)_{\mathbb{Z}[\sqrt{2}]}$, then a $\mathbb{Z}[\sqrt{2}]$-basis for $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ is given by $1, i=\sqrt[4]{2}, j=l$ and $ij=\sqrt[4]{2}.l$ where $l^2=-1$ and $ij=-ji$. But is not maximal order. However, if $1, \frac{i}{2}=\frac{\sqrt[4]{2}}{2}, j=l$ is another $\mathbb{Z}[\sqrt{2}]$ basis, where $\frac{i}{2}.j=-j\frac{i}{2}$, then it is possibly build a new quaternion order $\mathcal{M}_{\mathbb{Z}[\sqrt{2}]}\simeq(\frac{\sqrt{2}}{4},-1)_{\mathbb{Z}[\sqrt{2}]}$ containing $(\sqrt{2},-1)_{\mathbb{Z}[\sqrt{2}]}$, where $d(\mathcal{M}_{\mathbb{Z}[\sqrt{2}]})=\sqrt{2}$ (Proposition 3.2). Therefore, we conclude $d(\mathcal{M})=d(A)$ and $\mathcal{M}_{\mathbb{Z}[\sqrt{2}]}$ is a maximal order in $A_{\mathbb{Z}[\sqrt{2}]}$.

Similary, if $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}\simeq(3+2\sqrt{3},-1)_{\mathbb{Z}[\sqrt{3}]}$, then a $\mathbb{Z}[\sqrt{3}]$-basis for $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$ is given by $1, i=\sqrt{2+3\sqrt{3}}, j=l$ and $ij=\sqrt{3+2\sqrt{3}}.l$ where $l^2=-1$ and $ij=-ji$. But is not a maximal order. However, if $1, \frac{i}{2}=\frac{\sqrt{3+2\sqrt{3}}}{2}, j=l$ where $\frac{i}{2}j=-j\frac{i}{2}$, then it is possibly build a new quaternion order $\mathcal{M}_{\mathbb{Z}[\sqrt{3}]}\simeq(\frac{3+2\sqrt{3}}{4},-1)_{\mathbb{Z}[\sqrt{3}]}$ containing $(3+2\sqrt{3},-1)_{\mathbb{Z}[\sqrt{3}]}$, when $d(\mathcal{M}_{\mathbb{Z}[\sqrt{3}]})=\sqrt{3}$. Therefore we conclude $d(\mathcal{M})=d(A)$ and $\mathcal{M}_{\mathbb{Z}[\sqrt{3}]}$ is a maximal order in $A_{\mathbb{Z}[\sqrt{3}]}$.

Referências

[1] C.E. Shannon, The mathematical theory of communication, in The Bell System Technical Journal, Vol. 27, pp. 623-656, October 1948.

[2] R.G. Cavalcante, H. Lazari, J.D. Lima and R. Palazzo Jr., A new approuch to the design of digital communication systems, in Discrete Mathematics and Theoretical Computer Science -DIMACS Series, America Mathematica Society, vol.68, pp. 145-177, August 2005.

[3] R.G. Cavalcante, and R. Palazzo Jr., Performance analysis of MPSK signal constellations in Riemannian varieties, Lecture Notes in Computer Science, Springer-Verlag, 2003.

[4] G.D. Forney, Geometric uniform codes, in IEEE Trans. Inform. Theory, vol. 37, pp. 1241-1260, September 1991.

[5] E.B. Silva, M. Firer, S.R. Costa and R. Palazzo Jr., Signal constellations in the hyperbolic plane: A proposal for new communication systems, in Journal of the Franklin Institute, vol.343, pp. 69-82, 2006.

[6] S. Katok, Fuchsian Groups, University of Chicago Press, Chicago and London, 1992.

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