International Scholarly Research Network
ISRN Algebra
Volume 2012, Article ID 956017, 14 pages
doi:10.5402/2012/956017

*Research Article*

# Codes over Graphs Derived from Quotient Rings of the Quaternion Orders

**Cátia R. de O. Quilles Queiroz[1] and Reginaldo Palazzo Júnior[2]**

[1] *Departamento de Matemática, ICEx, UNIFAL, R. Gabriel Monteiro da Silva, 700 Centro, 37130-000 Alfenas, MG, Brazil*
[2] *Departamento de Telemática, FEEC, UNICAMP, Avenida Albert Einstein 400, Cidade Universtaria Zeferino Vaz, 13083-852 Campinas, SP, Brazil*

Correspondence should be addressed to Cátia R. de O. Quilles Queiroz, catia_quilles@hotmail.com

Received 13 February 2012; Accepted 6 March 2012

Academic Editors: H. Airault, A. Milas, and H. You



We propose the construction of signal space codes over the quaternion orders from a graph associated with the arithmetic Fuchsian group $\Gamma_8$. This Fuchsian group consists of the edge-pairing isometries of the regular hyperbolic polygon (fundamental region) $P_8$, which tessellates the hyperbolic plane $\mathbb{D}^2$. Knowing the generators of the quaternion orders which realize the edge pairings of the polygon, the signal points of the signal constellation (geometrically uniform code) derived from the graph associated with the quotient ring of the quaternion order are determined.

## 1. Introduction

In the study of two-dimensional lattice codes, it is known that the lattice $\mathbb{Z}^2$ is associated with a type of digital modulation known as quadrature amplitude modulation, QAM modulation, denoted by $x_i(t) = \alpha_i \cos w_0 t + \beta_i \sin w_0 t$, where $\alpha_i$ and $\beta_i$ take values on a finite integer set, whose performance under the (bit) error probability criterion is better than that of the phase-shift keying modulation, PSK modulation, denoted by $y_i(t) = A\cos(w_0 t + \phi_i)$, where $\phi_i$ takes values on a finite set, for the same average energy. The PSK modulation is associated with the $n$th roots of unity. The question that emerges is why a QAM signal constellation achieves better performance in terms of the error probability? Topologically, the fundamental region of the PSK signal constellation is a polygon with two edges oriented in the same direction, whereas the fundamental region of the QAM signal constellation is a square with opposite edges oriented in the same direction. The edge pairing of each one of these fundamental regions leads to oriented compact surfaces with genus $g = 0$ (sphere) and $g = 1$ (torus), respectively. We infer that the topological invariant associated with the performance of the signal constellation is the genus of the surface which is obtained by pairing the edges of the

fundamental region associated with the signal code. In the quest for the signal code with the best performance, we construct signal codes associated with surfaces with genus $g \geq 2$. Such surfaces may be obtained by the quotient of Fuchsian groups of the first kind, [1]. Here, we consider only the case $g = 2$.

The concept of geometrically uniform codes (GU codes) was proposed in [2] and generalized in [3]. In [4], these GU codes are summarized for any specific metric space, and in [5], new metrics are derived from graphs associated with quotient rings. Such codes have highly desirable symmetry properties, such as the following: every Voronoi region is congruent; the distance profile is the same for any codeword; the codewords have the same error probability; the generator group is isomorphic to a permutation group acting transitively on the codewords. In [6, 7], geometrically uniform codes are constructed in $\mathbb{R}^2$ from graphs associated with Gaussian and Eisenstein-Jacobi integer rings. For the Gaussian integer rings, the Voronoi regions of the signal constellation are squares and may be represented by the lattice $\mathbb{Z}^2$, whereas for the Eisenstein-Jacobi integer ring the Voronoi regions of the signal constellation are hexagons and may be represented by the lattice $A_2$.

In this paper, we propose the construction of signal space codes over the quaternion orders from graphs associated with the arithmetic Fuchsian group $\Gamma_8$. This Fuchsian group consists of the edge-pairing isometries of the regular hyperbolic polygon (fundamental region) $P_8$ (8 edges) which tessellates the hyperbolic plane $\mathbb{D}^2$. The tessellation is the self-dual tessellation $\{8, 8\}$, [8], where the first number denotes the number of edges of the regular hyperbolic polygon, and the second one denotes the number of such polygons which cover each vertex.

This paper is organized as follows. In Section 2, basic concepts on quaternion orders and arithmetic Fuchsian groups are presented. In Section 3, the identification of the arithmetic Fuchsian group derived from the octagon is realized by the associated quaternion order. In Section 4, quotient ring of the quaternion order is constructed, and we show that the cardinality of this quotient ring is given by the norm to the fourth power. In Section 5, some concepts related to graphs and codes over graphs are presented. Finally, in Section 6, an example of a GU code derived from a graph over the quotient ring of the quaternion order is established.

## 2. Preliminary Results

In this section, some basic and important concepts regarding quaternion algebras, quaternion orders, and arithmetic Fuchsian groups with respect to the development of this paper are presented. For a detailed description of these concepts, we refer the reader to [9–13].

### 2.1. Quaternion Algebras

Let $\mathbb{K}$ be a field. A quaternion algebra $\mathcal{A}$ over $\mathbb{K}$ is a $\mathbb{K}$-vector space of dimension 4 with a $\mathbb{K}$-base $\mathfrak{B} = \{1, i, j, k\}$, where $i^2 = a$, $j^2 = b$, $ij = -ji = k$, $a, b \in \mathbb{K} - \{0\}$, and denoted by $\mathcal{A} = (a, b)_{\mathbb{K}}$.

Let $\alpha \in \mathcal{A}$ be given by $\alpha = a_0 + a_1 i + a_2 j + a_3 ij$, where $a_0, a_1, a_2, a_3 \in \mathbb{K}$. The conjugate of $\alpha$, denoted by $\bar{\alpha}$, is defined by $\bar{\alpha} = a_0 - a_1 i - a_2 j - a_3 ij$. Thus, the reduced norm of $\alpha \in \mathcal{A}$, denoted by $\mathrm{Nrd}_{\mathcal{A}}(\alpha)$, or simply $\mathrm{Nrd}(\alpha)$ when there is no confusion, is defined by

$$\mathrm{Nrd}(\alpha) = \alpha \cdot \bar{\alpha} = a_0^2 - a a_1^2 - b a_2^2 + ab a_3^2, \tag{2.1}$$

and the reduced trace of $\alpha$ by

$$\mathrm{Trd}(\alpha) = \alpha + \bar{\alpha} = 2a_0. \tag{2.2}$$

Notice that the reduced norm is a quadratic form such that

$$\begin{aligned} \mathrm{Nrd} : \mathcal{A} &\longrightarrow \mathbb{K}, \\ \alpha &\longmapsto a_0^2 - aa_1^2 - ba_2^2 + aba_3^2, \end{aligned} \tag{2.3}$$

which may also be denoted by its normal form $\langle 1, -a, -b, ab\rangle$.

Let $\mathcal{A} = (a,b)_{\mathbb{K}}$ be a quaternion algebra over a field $\mathbb{K}$ and $\varphi : \mathbb{K} \to \mathbb{F}$ a field homomorphism. Define

$$\mathcal{A}^{\varphi} = \big(\varphi(a), \varphi(b)\big)_{\varphi(\mathbb{K})}, \qquad \mathcal{A}^{\varphi} \otimes \mathbb{F} = \big(\varphi(a), \varphi(b)\big)_{\mathbb{F}}, \tag{2.4}$$

where $\mathcal{A}^{\varphi} \otimes \mathbb{F}$ denotes the tensor product of the algebra $\mathcal{A}^{\varphi}$ by the field $\mathbb{F}$, [9]. Each homomorphism $\varphi$ in the algebra $\mathcal{A}^{\varphi} = (\varphi(a), \varphi(b))_{\varphi(\mathbb{K})}$ is called *place* of the quaternion algebra $\mathcal{A}$.

Let $\mathbb{K}$ be a totally real algebraic number field of degree $n$. This means that the $n$ monomorphisms $\varphi_i$, $i = 1, \ldots, n$ are all real, that is, $\varphi_i(\mathbb{K}) \subset \mathbb{R}$. Therefore, the $n$ distinct places are defined by $\mathbb{R}$-isomorphisms

$$\rho_1 : \mathcal{A}^{\varphi_1} \otimes \mathbb{R} \longrightarrow M_2(\mathbb{R}), \qquad \rho_i : \mathcal{A}^{\varphi_i} \otimes \mathbb{R} \longrightarrow \mathcal{H}, \tag{2.5}$$

where $\varphi_1$ is the identity, $\varphi_i$ is an embedding of $\mathbb{K}$ on $\mathbb{R}$, for $i = 1, \ldots, n$, and $\mathcal{H}$ is a division subalgebra of $M_2(\mathbb{K}(\sqrt{a}))$. Hence, $\mathcal{A}$ is not ramified at the place $\varphi_1$ and ramified at the places $\varphi_i$, for $2 \le i \le n$.

Let $\mathrm{Nrd}_{\mathcal{H}}$ and $\mathrm{Trd}_{\mathcal{H}}$ be the reduced norm and the reduced trace in $\mathcal{H}$, respectively. Given $\alpha \in \mathcal{A}$, it is easy to verify that

$$\mathrm{Nrd}_{\mathcal{H}}(\alpha) = \det\big(\rho_1(\alpha)\big), \qquad \mathrm{Trd}_{\mathcal{H}}(\alpha) = \mathrm{tr}\big(\rho_1(\alpha)\big). \tag{2.6}$$

Now, from the identification of $\alpha_i$ with $\varphi_i(\alpha_i)$, for $i = 0, 1, 2, 3$, it follows that for every $2 \le i \le n$,

$$\varphi_i(\mathrm{Nrd}_{\mathcal{H}}(\alpha)) = \mathrm{Nrd}_{\mathcal{H}}\big(\rho_i(\alpha)\big), \qquad \varphi_i(\mathrm{Trd}_{\mathcal{H}}(\alpha)) = \mathrm{Trd}_{\mathcal{H}}\big(\rho_i(\alpha)\big). \tag{2.7}$$

Furthermore, as the reduced norm of an element is given by the determinant of the isomorphism $\rho_1$, one may verify that

$$\mathrm{Nrd}_{\mathcal{H}}\big(\alpha \cdot \beta\big) = \mathrm{Nrd}(\alpha)_{\mathcal{H}} \cdot \mathrm{Nrd}_{\mathcal{H}}\big(\beta\big), \tag{2.8}$$

for any $\alpha, \beta \in \mathcal{A}$.

**Proposition 2.1** (see [13]). *Let $\mathcal{A} = (a,b)_{\mathbb{K}}$ be a quaternion algebra with a basis $\{1,i,j,k\}$, $r \in \mathbb{N}^*$, with $r$ fixed, and let $R$ be the set*

$$R = \left\{ \frac{\alpha}{r^m} : \alpha \in I_{\mathbb{K}} \text{ and } m \in \mathbb{N} \right\}, \tag{2.9}$$

*where $I_{\mathbb{K}}$ is the ring of integers of $\mathbb{K}$. Then $\mathcal{O} = \{x = x_0 + x_1 i + x_2 j + x_3 k : x_0, x_1, x_2, x_3 \in R\}$ is an order in $\mathcal{A}$.*

*Proof.* We have that $R$ is a subring of $\mathbb{K}$ containing $I_{\mathbb{K}}$ and that $\mathcal{O}$ is an $R$-module. On the other hand, if $\beta \in \mathbb{K}$, then there exists $c \in \mathbb{Z} - \{0\}$ such that $c \in I_{\mathbb{K}}$. Therefore, for any $x_0, x_1, x_2, x_3 \in \mathbb{K}$, there exists $c_l \in \mathbb{Z} - \{0\}$ such that $c_l x_l = \alpha l \in I_{\mathbb{K}}$, $l = 0,1,2,3$. Thus, given $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{A}$, there exists $\gamma \in \mathbb{K}$ such that $x = \gamma x'$, with $x' \in \mathcal{O}$. Therefore, $\mathcal{A} = \mathbb{K}\mathcal{O}$, which shows that $\mathcal{O}$ is an order in $\mathcal{A}$. □

*Example 2.2.* Let $\mathcal{H} = (-1,-1)_{\mathbb{R}}$ be the Hamilton quaternion algebra and $\mathcal{H}^1 = \{\alpha \in \mathcal{H} : \mathrm{Nrd}_{\mathbb{R}}(\alpha) = 1\}$. Hence, given $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{H}^1$, from (2.1), we have $\mathrm{Nrd}_{\mathbb{R}}(\alpha) = a_0^2 - a a_1^2 - b a_2^2 + ab a_3^2 k = a_0^2 + a_1^2 + a_2^2 + a_3^2 = 1$, which implies that $a_0^2 = 1 - a_1^2 - a_2^2 - a_3^2$ and so $|a_0| \leq 1$. Now, from (2.2), it follows that $\mathrm{Trd}_{\mathbb{R}}(\alpha) = 2a_0$, and so $\mathrm{Trd}_{\mathbb{R}}(\alpha) = 2a_0 \in [-2,2]$. Therefore, $\mathrm{Trd}_{\mathbb{R}}(\mathcal{H}^1) = [-2,2]$.

Given $\mathcal{A}$, a quaternion algebra over $\mathbb{K}$, and $R$, a ring of $\mathbb{K}$, an $R$-order $\mathcal{O}$ in $\mathcal{A}$ is a subring with unity of $\mathcal{A}$ which is a finitely generated $R$-module such that $\mathcal{A} = \mathbb{K}\mathcal{O}$. Hence, if $\mathcal{A} = (a,b)_{\mathbb{K}}$ and $I_{\mathbb{K}}$, the integer ring of $\mathbb{K}$, where $a, b \in I_{\mathbb{K}} - \{0\}$, then $\mathcal{O} = \{a_0 + a_1 i + a_2 j + a_3 ij : a_0, a_1, a_2, a_3 \in I_{\mathbb{K}}\}$ is an order in $\mathcal{A}$ denoted by $\mathcal{O} = (a,b)_{I_{\mathbb{K}}}$.

*Example 2.3.* Given $\mathcal{H} = (-1,-1)_{\mathbb{R}}$ the Hamilton quaternion algebra, the integer ring of $\mathbb{R}$ is $\mathbb{Z}$, and the quaternion order $\mathcal{H}[\mathbb{Z}] = \{a_0 + a_1 i + a_2 j + a_3 ij : a_0, a_1, a_2, a_3 \in \mathbb{Z}\}$ is called the ring of integral Hamiltonian quaternions, or the Lipschitz integers.

## 2.2. Hyperbolic Lattices

Let $\mathcal{A} = (a,b)_{\mathbb{K}}$ be a quaternion algebra over $\mathbb{K}$, let $R$ be a ring of $\mathbb{K}$, and let be $\mathcal{O}$ an $R$-order in $\mathcal{A}$. We also call $\mathcal{O}$ a hyperbolic lattice due to its identification with an arithmetic Fuchsian group.

The lattices $\mathcal{O}$ are used as the basic entity in generating the signals of a signal constellation in the hyperbolic plane. Since $\mathcal{O}$ is an order in $\mathcal{A}$, then there exists a basis $\{e_1, e_2, e_3, e_4\}$ of $\mathcal{A}$ and $R$-ideal $\mathfrak{a}$ such that $\mathcal{O} = \mathfrak{a}e_1 \oplus Re_2 \oplus Re_3 \oplus Re_4$, where $\oplus$ denotes direct sum. Note that by definition, given $x, y \in \mathcal{O}$, we have $x \cdot y \in \mathcal{O}$. Furthermore, since every $x \in \mathcal{O}$ is integral over $R$, [14], it follows that $\mathrm{Nrd}(x), \mathrm{Trd}(x) \in R$, [15].

An invariant of an order $\mathcal{O}$ is its discriminant, $d(\mathcal{O})$. For that, let $\{x_0, x_1, x_2, x_3\}$ be a set consisting of the generators of $\mathcal{O}$ over $R$. The discriminant of $\mathcal{O}$ is defined as the square root of the $R$-ideal generated by the set $\{\det(\mathrm{Tr}(x_i, \bar{x}_j)) : 0 \leq i, j \leq 3\}$.

*Example 2.4.* Let $\mathcal{A} = (a,b)_{\mathbb{K}}$, and let $I_{\mathbb{K}}$ be the ring of integers of $\mathbb{K}$, where $a, b \in I_{\mathbb{K}}^* = I_{\mathbb{K}} - \{0\}$. Then, [16], $\mathcal{O} = \{x_0 + x_1 i + x_2 j + x_3 k : x_0, x_1, x_2, x_3 \in I_{\mathbb{K}}\}$ is an order in $\mathcal{A}$ denoted by $\mathcal{O} = (a,b)_{I_{\mathbb{K}}}$. The discriminant of $\mathcal{O}$ is the principal ideal $R \cdot \det(Tr(x_i, \bar{x}_j))$, where $\{x_0, x_1, x_2, x_3\} = \{1, i, j, k\}$, [14]. On the other hand, it is not difficult to see that $\mathrm{Tr}(x_i\ \bar{x}_j)$ is the following

diagonal matrix:

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -2a & 0 & 0 \\ 0 & 0 & -2b & 0 \\ 0 & 0 & 0 & 2ab \end{pmatrix}. \tag{2.10}$$

Therefore,

$$d(\mathcal{O}) = 4ab. \tag{2.11}$$

One of the main objectives of this paper is to identify the arithmetic Fuchsian group in a quaternion order. Once this identification is realized, then the next step is to show the codewords of a code over graphs or the signals of a signal constellation (quotient of an order by a proper ideal). However, for the algebraic labeling to be complete, it is necessary that the corresponding order be *maximal*. An order $\mathcal{M}$ in a quaternion algebra $\mathcal{A}$ is called *maximal* if $\mathcal{M}$ is not contained in any other order in $\mathcal{A}$, [14].

If $\mathcal{M}$ is a maximal order in $\mathcal{A}$ containing another order $\mathcal{O}$, then the discriminant satisfies, [15], $d(\mathcal{O}) = d(\mathcal{M}) \cdot [\mathcal{M} : \mathcal{O}]$, $d(\mathcal{M}) = d(\mathcal{A})$. Conversely, if $d(\mathcal{O}) = d(\mathcal{A})$, then $\mathcal{O}$ is a maximal order in $\mathcal{A}$.

*Example 2.5.* Let $\mathcal{A}$ be an algebra $\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})}$ with a basis $\{1, i, j, k\}$ satisfying $i = \sqrt[4]{2}$, $j =$ Im, and $k = \sqrt[4]{2}\,\mathrm{Im}$ where Im denotes an imaginary unit, $\mathrm{Im}^2 = -1$. Let us also consider the following order (Proposition 2.1 considers a more general case for $\mathcal{O}$) in $\mathcal{A}$, $\mathcal{O} = \{x = x_0 + x_1 i + x_2 j + x_3 k : x_0, x_1, x_2, x_3 \in R\}$, that is, $\mathcal{O} = (\sqrt{2}, -1)_R$, where $R = \{x/2^n : x \in \mathbb{Z}[\sqrt{2}] \text{ and } n \in \mathbb{N}\}$. Thus, by (2.11), $d(\mathcal{O}) = -\sqrt{2}$. Furthermore, $d(\mathcal{A}) = -\sqrt{2}$, [15]. Hence, $\mathcal{O}$ is a maximal order in $\mathcal{A}$.

### 2.3. Arithmetic Fuchsian Groups

Consider the upper-half plane $\mathbb{H}^2 = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ endowed with the Riemannian metric

$$ds = \frac{\sqrt{dx^2 + dy^2}}{y}, \tag{2.12}$$

where $z = x + y\,\mathrm{Im}$. With this metric $\mathbb{H}^2$ is the model of the hyperbolic plane or the Lobachevski plane. Let $\mathrm{PSL}(2, \mathbb{R})$ be the set of all the Möbius transformations of $\mathbb{C}$ over itself as

$$\left\{ z \longrightarrow \frac{az + b}{cz + d} : a, b, c, d \in \mathbb{R},\ ad - bc = 1 \right\}. \tag{2.13}$$

Consider the group of real matrices $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $\det(g) = ad - bc = 1$, and $\mathrm{Tr}(g) = a + d$ is the trace of the matrix $g$. This group is called unimodular, and it is denoted by $\mathrm{SL}(2, \mathbb{R})$.

The set of linear fractional Möbius transformations of $\mathbb{C}$ over itself as in (2.13) is a group such that the product of two transformations corresponds to the product of the corresponding matrices, and the inverse transformation corresponds to the inverse matrix. Each transformation $T$ is represented by a pair of matrices $\pm g \in \mathrm{SL}(2,\mathbb{R})$. Thus, the group of all transformations (2.13), called $\mathrm{PSL}(2,\mathbb{R})$, is isomorphic to $\mathrm{SL}(2,\mathbb{R})/\{\pm I_2\}$, where $I_2$ is the $2 \times 2$ identity matrix, that is,

$$\mathrm{PSL}(2,\mathbb{R}) \approx \frac{\mathrm{SL}(2,\mathbb{R})}{\{\pm I_2\}}. \tag{2.14}$$

A Fuchsian group $\Gamma$ is a discrete subgroup of $\mathrm{PSL}(2,\mathbb{R})$, that is, $\Gamma$ consists of the orientation-preserving isometries $T : \mathbb{H}^2 \to \mathbb{H}^2$, acting on $\mathbb{H}^2$ by homeomorphisms.

Another Euclidean model of the hyperbolic plane is given by the Poincaré disc $\mathbb{D}^2 = \{z \in \mathbb{C} : |z| < 1\}$ endowed with the Riemannian metric

$$ds^2 = \frac{4\left(dx^2 + dy^2\right)}{\left[1 - \left(x^2 + y^2\right)\right]^2}, \tag{2.15}$$

where $z = x + y\,\mathrm{Im}$. Analogously, the discrete group $\Gamma_p$ of orientation-preserving isometries $T : \mathbb{D}^2 \to \mathbb{D}^2$ is also a Fuchsian group, given by the transformations $T_p \in \Gamma_p < \mathrm{PSL}(2,\mathbb{C})$ such that

$$T_p(z) = \frac{az + c}{\bar{c}\, z + \bar{a}}, \qquad a, b \in \mathbb{C},\ |a|^2 - |c|^2 = 1. \tag{2.16}$$

Furthermore, we may write $T_p = f \circ T \circ f^{-1}$, where $T \in \mathrm{PSL}(2,\mathbb{R})$, and $f : \mathbb{H}^2 \to \mathbb{D}^2$ is an isometry given by

$$f(z) = \frac{z\,\mathrm{Im} + 1}{z + \mathrm{Im}}. \tag{2.17}$$

Therefore, the Euclidean models of the hyperbolic plane such as the Poincaré disc and the upper-half plane are isomorphic, and they will be used according to the need. Notice that the Poincaré disc model is useful for the visualization, whereas the upper-half plane is useful for the algebraic manipulations.

For each order $\mathcal{O}$ in $\mathcal{A}$, consider $\mathcal{O}^1$ as the set $\mathcal{O}^1 = \{\alpha \in \mathcal{O} : \mathrm{Nrd}_{\mathcal{A}}(\alpha) = 1\}$. Note that $\mathcal{O}^1$ is a multiplicative group.

Now, note that the Fuchsian groups may be obtained by the isomorphism $\rho_1$ in (2.5). In fact, from (2.6), we have $\mathrm{Nrd}_{\mathcal{A}}(\alpha) = \det(\rho_1(\alpha))$. Furthermore, we know that $\mathcal{O}^1$ is a multiplicative group, and so $\rho_1(\mathcal{O}^1)$ is a subgroup of $\mathrm{SL}(2,\mathbb{R})$, that is, $\rho_1(\mathcal{O}^1) < \mathrm{SL}(2,\mathbb{R})$. Therefore, the group derived from a quaternion algebra $\mathcal{A} = (a,b)_{\mathbb{K}}$ and whose order is $\mathcal{O}$,

denoted by $\Gamma(\mathcal{A},\mathcal{O})$, is given by

$$\Gamma(\mathcal{A},\mathcal{O}) = \frac{\rho_1(\mathcal{O}^1)}{\{\pm Id_2\}} < \frac{\mathrm{SL}(2,\mathbb{R})}{\{\pm Id_2\}} \cong \mathrm{PSL}(2,\mathbb{R}). \tag{2.18}$$

As a consequence, consider the following.

**Theorem 2.6** (see [11]). *$\Gamma(\mathcal{A},\mathcal{O})$ is a Fuchsian group.*

These previous concepts and results lead to the concept of arithmetic Fuchsian groups. Since every Fuchsian group may be obtained in this way, we say that a Fuchsian group is derived from a quaternion algebra if there exists a quaternion algebra $\mathcal{A}$ and an order $\mathcal{O} \subset \mathcal{A}$ such that $\Gamma$ has finite index in $\Gamma(\mathcal{A},\mathcal{O})$. The group $\Gamma$ is called an *arithmetic Fuchsian group*.

Theorem 2.7 establishes the necessary and sufficient conditions for arithmetic of Fuchsian groups, and its characterization makes use of the set consisting of the traces of its elements, that is, $\mathrm{Tr}(\Gamma) = \{\pm \mathrm{T}r(T) : T \in \Gamma\}$.

**Theorem 2.7** (see [11, 16]). *Let $\Gamma$ be a Fuchsian group where the fundamental region has finite area, that is, $\mu(\mathbb{H}^2/\Gamma) < \infty$. Then $\Gamma$ is derived from a quaternion algebra $\mathcal{A}$ over a totally real number field $\mathbb{K}$ if and only if the following conditions are satisfied by $\Gamma$:*

(1) *if $\mathbb{K}_1 = \mathbb{Q}(\mathrm{Tr}(T) : T \in \Gamma)$, then $\mathbb{K}_1$ is an algebraic number field of finite degree, and $\mathrm{Tr}(\Gamma)$ is contained in $I_{\mathbb{K}_1}$, the ring of integers of $\mathbb{K}_1$;*

(2) *if $\varphi$ is an embedding of $\mathbb{K}_1$ in $\mathbb{C}$ such that $\varphi \neq Id$, then $\varphi(\mathrm{Tr}(\Gamma))$ is bounded in $\mathbb{C}$.*

## 3. Identification of $\Gamma_8$ in $\Gamma(\mathcal{A},\mathcal{O}), \mathcal{O} \subset \mathcal{A}$

In this section, we identify the arithmetic Fuchsian group $\Gamma_8$ derived from a quaternion algebra $\mathcal{A}$ over a number field $\mathbb{K}$, for $[\mathbb{K} : \mathbb{Q}] = 2$, where $[\mathbb{K} : \mathbb{Q}]$ denotes the degree of the field extension, and $g = 2$ denotes the genus of the surface $\mathbb{D}^2/\Gamma_8$ in a quaternion order.

From [17], if $g = 2$, the arithmetic Fuchsian group $\Gamma_8$ is derived from a quaternion algebra $\mathcal{A}$ over a totally real number field $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. The elements of the Fuchsian group $\Gamma_8$ are identified, by an isomorphism, with the elements of the order $\mathcal{O} = (\sqrt{2},-1)_{I_{\mathbb{K}}}$, where $I_{\mathbb{K}}$ denotes the integer ring of $\mathbb{K}$.

To verify if a Fuchsian group associated with an order as specified in the previous paragraph is in fact arithmetic, it suffices to show that the quaternion algebra is not ramified at $\varphi_1$, and it is ramified at the remaining places.

Consider the Fuchsian group $\Gamma_8$, given a quaternion algebra $\mathcal{A} = (\sqrt{2},-1)_{\mathbb{K}}$, and the elements of $T \in \Gamma$ are given by

$$T = \frac{1}{2^s}\begin{pmatrix} x_l + y_l\sqrt{2} & z_l + w_l\sqrt{2} \\ -z_l + w_l\sqrt{2} & x_l - y_l\sqrt{2} \end{pmatrix}, \tag{3.1}$$

where $s \in \mathbb{N}$, $x_l, y_l, z_l, w_l \in \mathbb{Z}[\sqrt{2}]$. Since $\varphi_1$ is the identity, it follows that $\mathcal{A} \simeq M_2(\mathbb{K})$ is not ramified at $\varphi_1$. Now, observe that $\sqrt{2}$ is square-free for $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, that is, there is no $t \in \mathbb{K} - \{0\}$ such that $t^2 = \sqrt{2}$. Therefore, $\mathcal{A}$ is ramified at all places $\varphi_i$, except at $\varphi_1$.

On the other hand, the order $\mathcal{O} = (\sqrt{2}, -1)_{I_{\mathbb{K}}}$ is not a maximal order in the quaternion algebra $\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{K}}$ for the discriminant is not $4\sqrt{2}$. Since we are interested in realizing a complete algebraic labeling, we have to find an order that contains the order $\mathcal{O}$ in $\mathcal{A}$ and that it is maximal. From [13], we have that $\mathcal{O} = (\sqrt{2}, -1)_R$, where $R = \{\alpha/2^m : \alpha \in \mathrm{I}_{\mathbb{K}}, \mathrm{m} \in \mathbb{N}\}$ is a maximal order that contains $\mathcal{O} = (\sqrt{2}, -1)_{I_{\mathbb{K}}}$. Therefore, this is the order we are taking into consideration in the case of interest.

## 4. 4. Quotient Rings of the Quaternion Order $\mathcal{O} = (\sqrt{2}, -1)_R$ Where $R = \{\alpha/2^m : \alpha \in I_{\mathbb{K}}, m \in \mathbb{N}\}$

Consider the self-dual tessellation $\{8, 8\}$ having an octagon as the fundamental region. We know from the previous sections that the arithmetic Fuchsian group $\Gamma_8$ is derived from a quaternion algebra over $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, with the identification of the generators by the order $\mathcal{O} = (\sqrt{2}, -1)_{I_{\mathbb{K}}}$. Thus, let $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ and $\{1, i, j, k\} = \{1, \sqrt{\sqrt{2}}, \mathrm{Im}, \sqrt{\sqrt{2}}\,\mathrm{Im}\}$ be a basis of the quaternion algebra $\mathcal{A} = (\sqrt{2}, -1)_{I_{\mathbb{K}}}$, where $i^2 = \sqrt{2}$, $j^2 = -1$, $k = ij = \sqrt{\sqrt{2}}\,\mathrm{Im}$.

The ring of integers of $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$; hence, $\mathcal{O} = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in \mathbb{Z}[\sqrt{2}]\}$ is in fact an order in $\mathcal{A}$. Due to the simplicity of this order, we start with it and gradually extend it to the order $\mathcal{O}= (\sqrt{2}, -1)_R$, where $R = \{\alpha/2^m : \alpha \in \mathbb{Z}[\sqrt{2}],\ m \in \mathbb{N}\}$ which realizes the complete labeling.

Observe that $\mathcal{O} = \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in \mathbb{Z}[\sqrt{2}]\}$ is an extension of $\mathbb{Z}[\sqrt{2}]$ of dimension 4, for it has $\{1, i, j, k\}$ as its basis, and we have that $\mathcal{O}$ is a subring of $\mathcal{A}$ containing 1 and which is a finitely generated $\mathbb{Z}[\sqrt{2}]$-module. Now, if we look at the order $\mathcal{O}$ as an extension of $\mathbb{Z}$, the dimension increases to 8, and the basis of $\mathcal{O}$ over $\mathbb{Z}$ is given by $\{1, \sqrt{\sqrt{2}}, i, \sqrt{2}i, j, \sqrt{\sqrt{2}}j, k, \sqrt{\sqrt{2}}k\}$. In this case, the order will be denoted by $\mathcal{O}_{\mathbb{Z}}$. We may still verify that according to the definition of order, $\mathcal{O}_{\mathbb{Z}}$ is a free $\mathbb{Z}$-module with rank $4n = 8$, where $n = [\mathbb{K} : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and in this way, we are not working with the quaternions anymore, but with the octonions, a set which besides being noncommutative is also nonassociative.

### 4.1. Case $g = 2$

Given the genus $g = 2$, the arithmetic Fuchsian group $\Gamma_8$ is derived from a quaternion algebra $\mathcal{A}$ over a totally real number field $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, and the elements of $\Gamma_8$ are identified, via an isomorphism, with the elements of $\mathcal{O}= (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$. Hence, given $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ and $\mathcal{O}= (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ such that $\mathcal{O} = \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in \mathbb{Z}[\sqrt{2}], i^2 = \sqrt{2}, j^2 = -1, k^2 = -\sqrt{2}\}$, the reduced norm of an element $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{O}$ is given by

$$\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) = \alpha\,\bar{\alpha}= a_0^2 - \sqrt{2}a_1^2 + a_2^2 - \sqrt{2}a_3^2 \in \mathbb{Z}\left[\sqrt{2}\right], \tag{4.1}$$

and it satisfies $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) \in I_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$. Next, we verify in which cases this norm is an element belonging to $\mathbb{Z}$.

**Proposition 4.1.** *Given $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{O}$, where $a_i = x_i + y_i\sqrt{2}$, where $x_i, y_i \in \mathbb{Z}$, then $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) \in \mathbb{Z}$ if and only if $2x_0y_0 - x_1^2 - 2y_1^2 + 2x_2y_2 - x_3^2 - 2y_3^2 = 0$. In this case, the norm is given by $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) = x_0^2 + 2y_0^2 - 4x_1y_1 + x_2^2 + 2y_2^2 - 4x_3y_3$.*

*Proof.* From (4.1), we have $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) = \alpha\,\bar{\alpha} = a_0^2 - \sqrt{2}a_1^2 + a_2^2 - \sqrt{2}a_3^2$. Since $a_i \in \mathbb{Z}[\sqrt{2}]$, it may be written as $a_i = x_i + y_i\sqrt{2}$, where $x_i, y_i \in \mathbb{Z}$. Thus, $a_i^2 = x_i^2 + 2y_i^2 + 2\sqrt{2}x_iy_i$, and from this, it follows that

$$\begin{aligned}\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) = a_0^2 - \sqrt{2}a_1^2 + a_2^2 - \sqrt{2}a_3^2 &= x_0^2 + 2y_0^2 + 2\sqrt{2}x_0y_0 - \sqrt{2}\left(x_1^2 + 2y_1^2 + 2\sqrt{2}x_1y_1\right)\\ &+ x_2^2 + 2y_2^2 + 2\sqrt{2}x_2y_2 - \sqrt{2}\left(x_3^2 + 2y_3^2 + 2\sqrt{2}x_3y_3\right) = x_0^2 + 2y_0^2 - 4x_1y_1 + x_2^2\\ &+ 2y_2^2 - 4x_3y_3 + \sqrt{2}\left(2x_0y_0 - x_1^2 - 2y_1^2 + 2x_2y_2 - x_3^2 - 2y_3^2\right).\end{aligned} \tag{4.2}$$

Hence, $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) \in \mathbb{Z}$ if and only if $2x_0y_0 - x_1^2 - 2y_1^2 + 2x_2y_2 - x_3^2 - 2y_3^2 = 0$, from which it follows that

$$\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) = x_0^2 + 2y_0^2 - 4x_1y_1 + x_2^2 + 2y_2^2 - 4x_3y_3 \in \mathbb{Z}. \tag{4.3}$$

□

Now, considering the order $\mathcal{O}$ as an extension of $\mathbb{Z}$, denoted by $\mathcal{O}_{\mathbb{Z}}$, the reduced norm of an element $\alpha = a_0 + a_1i + a_2j + a_3k \in \mathcal{O}_{\mathbb{Z}}$ is given by

$$\mathrm{Nrd}_{\mathbb{Z}}(\alpha) = \alpha\,\bar{\alpha} = a_0\,\bar{a_0} - \sqrt{2}a_1\,\bar{a_1} + a_2\,\bar{a_2} - \sqrt{2}a_3\,\bar{a_3} \in Z\left[\sqrt{2}\right], \tag{4.4}$$

where $\bar{a_i}$ denotes the conjugate of $a_i$.

Since the proof of the next result is similar to the proof of Proposition 4.1, we omit it.

**Proposition 4.2.** *Given $\alpha = a_0 + a_1i + a_2j + a_3k \in \mathcal{O}_{\mathbb{Z}}$, where $a_i = x_i + y_i\sqrt{2}$, where $x_i, y_i \in \mathbb{Z}$, then $\mathrm{Nrd}_{\mathbb{Z}}(\alpha) \in \mathbb{Z}$ if and only if $x_1^2 + x_3^2 - 2(y_1^2 + y_3^2) = 0$. In this case, the norm is given by $\mathrm{Nrd}_{\mathbb{Z}}(\alpha) = x_0^2 - 2y_0^2 + x_2^2 - 2y_2^2 \in \mathbb{Z}$.*

*Remark 4.3.* When there is no confusion in the notation being used, we will denote for simplicity the reduced norm of $\alpha$ by $\mathrm{Nrd}(\alpha)$.

**Theorem 4.4.** *Let $0 \neq \alpha \in \mathcal{O}$. If $\mathrm{Nrd}(\alpha) \in \mathbb{Z}$, then $\mathcal{O}/\langle\alpha\rangle$ has $\mathrm{Nrd}(\alpha)^4$ elements.*

*Proof.* Let $0 \neq \alpha \in \mathcal{O}$ and $\mathrm{Nrd}(\alpha) = N \in \mathbb{Z}$. First, we show that $\mathcal{O}/\langle N\rangle$ has $N^8$ elements. As $N \in \mathbb{Z}$, let us consider $\mathcal{O}$ over $\mathbb{Z}$. However, $[\mathcal{O} : \mathbb{Z}] = 8$, and the basis of $\mathcal{O}$ over $\mathbb{Z}$ is $\{1, \sqrt{2}, i, i\sqrt{2}, j, j\sqrt{2}, k, k\sqrt{2}\}$. Thus, $\alpha \in \mathcal{O}$ is of the form $\alpha = a_0 + a_1\sqrt{2} + a_2i + a_3i\sqrt{2} + a_4j + a_5\sqrt{2}j + a_6k + a_7k\sqrt{2}$.

Now, given two elements $\beta, \beta' \in \mathcal{O}$,

$$\begin{aligned}\beta &= b_0 + b_1\sqrt{2} + b_2i + b_3i\sqrt{2} + b_4j + b_5\sqrt{2}j + b_6k + b_7k\sqrt{2}, \quad b_i \in \mathbb{Z},\\ \beta' &= b_0' + b_1'\sqrt{2} + b_2'i + b_3'i\sqrt{2} + b_4'j + b_5'\sqrt{2}j + b_6'k + b_7'k\sqrt{2}, \quad b_i' \in \mathbb{Z},\end{aligned} \tag{4.5}$$

we say that $\beta$ and $\beta'$ are congruent modulo $N$ if there exists

$$\beta'' = b_0'' + b_1''\sqrt{2} + b_2''i + b_3''i\sqrt{2} + b_4''j + b_5''\sqrt{2}j + b_6''k + b_7''k\sqrt{2}, \qquad b_i'' \in \mathbb{Z}, \tag{4.6}$$

such that $\beta - \beta' = \beta'' N$. Thus, $b_i - b_i' = b_i'' N$, for $i = 0, 1, \ldots, 7$, that is, $b_i \equiv b_i' (\mathrm{mod} N)$ which implies that there exist $N$ possibilities for each $b_i$, and thus, $N^8$ different equivalence classes modulo $N$.

Now, since $\mathrm{Nrd}(\alpha) = \alpha\ \bar{\alpha}$, we have the following chain of ideals: $\langle \mathrm{Nrd}(\alpha) \rangle = \langle \bar{\alpha}\ \alpha \rangle \subseteq \langle \alpha \rangle$. From the third isomorphism theorem for $A$-modules, [10], we have the following sequence of left $A$-module:

$$0 \longrightarrow \frac{\langle \alpha \rangle}{\langle \alpha\ \bar{\alpha} \rangle} \longrightarrow \frac{A}{\langle \alpha\ \bar{\alpha} \rangle} \longrightarrow \frac{A}{\langle \alpha \rangle} \longrightarrow 0. \tag{4.7}$$

We denote the number of elements of $A/\langle \alpha \rangle$ by $n$ and the number of elements of $\langle \alpha \rangle / \langle \alpha\ \bar{\alpha} \rangle$ by $m$. Then, as a consequence of the Lagrange theorem, [10], we may consider the previous exact sequence as a sequence of Abelian groups, thus leading to $\mathrm{Nrd}(\alpha)^8 = nm$. If we prove that $n = m$, we may finally conclude that $n = \mathrm{Nrd}(\alpha)^4$. Now, observe that the function

$$f : \frac{A}{\langle \bar{\alpha} \rangle} \longrightarrow \frac{\langle \alpha \rangle}{\langle \alpha\ \bar{\alpha} \rangle}, \tag{4.8}$$

defined by $f(\beta + \langle \bar{\alpha} \rangle) = \beta\alpha + \langle \alpha\ \bar{\alpha} \rangle$, is well defined, and it is an isomorphism of the left $A$-module. Therefore, $m$ is exactly the number of elements of $A/\langle \bar{\alpha} \rangle$.

Finally, the quaternion conjugation is an antiautomorphism, which implies that $A/\langle \bar{\alpha} \rangle$ and $A/\langle \alpha \rangle$ have the same cardinality, that is, $n = m$. □

*Example 4.5.* Let $\alpha = 1 + j \in \mathcal{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$, then $\mathrm{Nrd}(\alpha) = 2$. From Theorem 4.4, $\mathcal{O}/\langle \alpha \rangle$ has 16 elements, obtained by the quotient of the order $\mathcal{O}$ and the ideal $\langle 1 + j \rangle$, that is, we take the elements of $\mathcal{O}$ and reduce them modulo $(1 + j)$, obtaining

$$\begin{aligned} \frac{\mathcal{O}}{\langle 1 + j \rangle} = \Big\{ & 0,\ 1,\ \sqrt{2,1} + \sqrt{2},\ i,\ 1 + i,\ \sqrt{2} + i,\ \sqrt{2}i,\ \left(1 + \sqrt{2} + i\right),\ 1 + \sqrt{2}i,\ \sqrt{2} + \sqrt{2}i,\ \left(1 + \sqrt{2}\right) \\ & + \sqrt{2}i,\ \left(1 + \sqrt{2}\right)i,\ 1 + \left(1 + \sqrt{2}\right)i,\ \sqrt{2} + \left(1 + \sqrt{2}\right)i,\ \left(1 + \sqrt{2}\right) + \left(1 + \sqrt{2}\right)i \Big\}. \end{aligned} \tag{4.9}$$

*Example 4.6.* Given $\alpha = 2 + \sqrt{2} \in \mathcal{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$, from Proposition 4.1, we have $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) = 6 + 4\sqrt{2} \notin \mathbb{Z}$. However, taking the order as an extension of $\mathbb{Z}$, that is,

$\mathcal{O}_{\mathbb{Z}} = (\sqrt{2}, -1)_{\mathbb{Z}}$ from Proposition 4.2, we have $\mathrm{Nrd}_{\mathbb{Z}}(\alpha) = 2$, and $\mathcal{O}/\langle\alpha\rangle$ has 16 elements, given by

$$\frac{\mathcal{O}}{\left\langle 2+\sqrt{2}\right\rangle} = \{0, 1, i, j, k, 1+i, 1+j, 1+k, i+j, i+k, j+k, 1+i+j, 1+i + k, 1+j+k, i+j+k, 1+i+j+k\}. \tag{4.10}$$

*Remark 4.7.* We are not interested in orders such as $\mathcal{O}_{\mathbb{Z}}$, for when the order $\mathcal{O}$ is extended to the order $\mathcal{O}_{\mathbb{Z}}$, it implies working with octonions; hence, some important properties are lost. Therefore, we consider such an extension when there is no other alternative, that is, when the norm over $I_{\mathbb{K}}$ is not an element in $\mathbb{Z}$.

**Corollary 4.8.** *If $\beta \in \mathcal{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ is a right divisor of $\alpha$ and $\mathrm{Nrd}(\beta) \in \mathbb{Z}$, then the left ideal generated by $\beta$, $\langle\beta\rangle \subseteq \mathcal{O}$ has $\mathrm{Nrd}(\alpha)^4/\mathrm{Nrd}(\beta)^4$ elements.*

Note from Corollary 4.8 that $\langle\beta\rangle$ generates a code with $\mathrm{Nrd}(\alpha)^4/\mathrm{Nrd}(\beta)^4$ codewords, therefore, a subcode of $\mathcal{O}/\langle\alpha\rangle$, whose minimum distance $D_\beta(\eta, \tau) > D_\alpha(\eta, \tau)$.

*Example 4.9.* Given $\alpha = 1 + 2\sqrt{2}j$, from Proposition 4.1, we have $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) = (1)^2 + (2\sqrt{2})^2 = 9$. Now, $\alpha = 1 + 2\sqrt{2}j$ may be written as $1 + 2\sqrt{2}j = (\sqrt{2} + j)^2$; hence, $\beta$ is a right divisor of $\alpha$ and $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\beta) = 3 \in \mathbb{Z}$, then the left ideal generated by $\beta$, $\langle\beta\rangle \subseteq \mathcal{O}$ has $\mathrm{Nrd}(\alpha)^4/\mathrm{Nrd}(\beta)^4 = 9^4/3^4 = 81$ elements.

As can be seen in Example 2.5, for the proof see [13], the order $\mathcal{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ is not a maximal order. Therefore, we have to consider the order over the ring $R = \{\alpha/2^m : \alpha \in \mathbb{Z}[\sqrt{2}], \quad m \in \mathbb{N}\}$, which makes it maximal, hence, given $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ and $\mathcal{O} = (\sqrt{2}, -1)_R$, where $R = \{\alpha/2^m : \alpha \in \mathbb{Z}[\sqrt{2}], \quad m \in \mathbb{N}\}$ such that

$$\mathcal{O} = \left\{a_0 + \frac{a_1}{2}i + \frac{a_2}{2}j + \frac{a_3}{2}k : a_i \in \mathbb{Z}\left[\sqrt{2}\right],\ i^2 = \sqrt{2},\ j^2 = -1,\ k^2 = -\sqrt{2}\right\}, \tag{4.11}$$

we have that the reduced norm of an element $\alpha \in \mathcal{O}$ is given by

$$\mathrm{Nrd}_R(\alpha) = a_0^2 - \frac{1}{2}\sqrt{2}a_1^2 + \frac{1}{2}a_2^2 - \frac{1}{4}\sqrt{2}a_3^2 \in \mathbb{Z}\left[\sqrt{2}\right]. \tag{4.12}$$

Now, for the maximal order, the cardinality of the quotient ring satisfy the following results:

**Theorem 4.10.** *Let $\alpha \in \mathcal{O} = (\sqrt{2}, -1)_R$, where $R = \{\alpha/2^m : \alpha \in \mathbb{Z}[\sqrt{2}],\ m \in \mathbb{N}\}$. If $\mathrm{Nrd}_R(\alpha) = 2^n$, then $\mathcal{O}/\langle\alpha\rangle$ has just one element.*

*Proof.* Let $\gamma \in \mathcal{O}/\langle\alpha\rangle$. We have to show that $\gamma \equiv 0(\mathrm{mod}\alpha)$. To show that $\gamma \equiv 0(\mathrm{mod}\alpha)$ is equivalent to proving that $\gamma = x\alpha$, where $x \in \mathcal{O}$. As $\mathrm{Nrd}_R(\alpha) = 2^n$, we have that $\bar{\alpha}\ \alpha = 2^n$;

hence, $\gamma$ may be written as

$$\gamma = \frac{\gamma}{2^n}\,\bar{\alpha}\,\alpha, \tag{4.13}$$

that is, $\gamma \equiv 0 (\mathrm{mod}\,\alpha)$. In particular, one may verify that $1 \equiv 0(\mathrm{mod}\,\alpha)$, for $1 = (1/2^n)\,\bar{\alpha}\,\alpha$. □

**Theorem 4.11.** *Let* $\alpha \in \mathcal{O} = (\sqrt{2}, -1)_R$, *where* $R = \{\alpha/2^m : \alpha \in \mathbb{Z}[\sqrt{2}], \quad m \in \mathbb{N}\}$. *If* $\mathrm{Nrd}_R(\alpha) \neq 2^n$, *then* $\mathcal{O}/\langle\alpha\rangle$ *has* $\mathrm{Nrd}_R(\alpha)^4$ *elements.*

*Proof.* Let $0 \neq \alpha \in \mathcal{O}$ and $\mathrm{Nrd}_R(\alpha) \neq 2^n$, $\mathrm{Nrd}_R(\alpha) = N \in \mathbb{Z}$. We have to show that the left $\mathcal{O}$-module $\mathcal{O}/\langle N\rangle$ has $N^8$ elements. As $N \in \mathbb{Z}$, let us take $\mathcal{O}$ over $\mathbb{Z}$. However, $[\mathcal{O} : \mathbb{Z}] = 8$ and the basis of $\mathcal{O}$ over $\mathbb{Z}$ is $\{1/2^n, \sqrt{2}/2^n, i/2^n, i\sqrt{2}/2^n, j/2^n, j\sqrt{2}/2^n, k/2^n, k\sqrt{2}/2^n\}$. Hence, the proof is analogous to the proof of Theorem 4.4. □

*Example 4.12.* Let $\alpha = 2 \in \mathcal{O}_R$. Hence, from (4.12), we have that $\mathrm{Nrd}_R(\alpha) = 4$, and by Theorem 4.10, it follows that $\mathcal{O}/\langle\alpha\rangle$ has just one element $\{0\}$.

*Example 4.13.* Let $\alpha = \sqrt{2} + (\sqrt{2}/2)j \in \mathcal{O}_R$. Hence, from (4.12), we have that $\mathrm{Nrd}_R(\alpha) = 3$ and by Theorem 4.11, it follows that $\mathcal{O}/\langle\alpha\rangle$ has 81 elements.

## 5. Codes over Graphs

In this section some concepts of graphs and codes over graphs are considered which will be useful in the next section.

*Definition 5.1.* Let $0 \neq \alpha \in \mathcal{O} = (\theta, -1)_{I_{\mathbb{K}}}$. The distance in $\mathcal{O}$ is the distance induced by the graph $G_\alpha$. Hence, if $\eta,\ \tau \in \mathcal{O}$, then the distance is given by

$$D_\alpha(\eta, \tau) = \min\{|x_1| + |x_2| + 2|x_3| + 2|x_4| - 2|x_2x_3|\}, \tag{5.1}$$

such that $\tau - \eta \equiv x_1 + x_2 i + x_3 j + x_4 k \ (\mathrm{mod}\,\alpha)$.

*Example 5.2.* For $V = \mathcal{O}/\langle\sqrt{2} + j\rangle$. If $\tau = 1$ and $\eta = i$, then $\tau - \eta = 1 - i$. Thus, $D_\alpha(\eta, \tau) = 2$, if $\tau = (\sqrt{2}/2)(1 + i)$ and $\eta = (\sqrt{2}/2)(1 - i)$, then $\tau - \eta = \sqrt{2}i \equiv k(\mathrm{mod}\,\alpha)$. Thus, $D_\alpha(\eta, \tau) = 2$.

Given the distance $D_\alpha$, a graph generated by $\alpha \in \mathcal{O}$ is defined as follows.

*Definition 5.3.* Let $0 \neq \alpha \in \mathcal{O} = (\theta, -1)_{I_{\mathbb{K}}}$. The graph generated by $\alpha$ is defined as $G_\alpha = (V, E)$, where

(1) $V = \mathcal{O}/\langle\alpha\rangle$ denotes the set of vertices;

(2) $E = \{(\eta, \tau) \in V \times V : D_\alpha(\eta, \tau) = 1\}$ denotes the set of edges.

*Example 5.4.* Given $\alpha = \sqrt{2} + j \in \mathcal{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$, from Proposition 4.1, the reduced norm is $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) = 3$. The set of vertices is $V = \mathcal{O}/\langle\sqrt{2} + j\rangle$, and the set of edges satisfies $E$.

*Remark 5.5.* Note that the distance between two signal points $\eta$ and $\tau$ in the graph is the least number of traversed edges connecting the signal point $\eta$ to the signal point $\tau$.

Given a graph $G_\alpha$ with a set of vertices $V$ and distance $D_\alpha$, a code in $G_\alpha$ is a nonempty subset $\mathcal{C}$ of $G_\alpha$. The Voronoi region $V_\eta$ associated with $\eta \in \mathcal{C}$ is the subset consisting of the elements of $V$ for which $\eta$ is the closest signal point in $\mathcal{C}$, that is, $V_\eta = \{\tau \in V; D(\eta,\tau) = D(\eta,\mathcal{C})\}$. The number $t = \max\{D(\eta,\mathcal{C}); \eta \in V\}$ is called *covering radius* of the code. The covering radius is the least number $t$ such that each ball of radius $t$ centered at the signal points of $\mathcal{C}$, given by $B_t(\eta) = \{\tau \in V : D(\eta,\tau) \leq t\}$, covers $V$. The number $\delta = \min\{D(\eta,\tau) : \eta,\tau \in \mathcal{C}, \eta \neq \tau\}$ is the minimum distance of $\mathcal{C}$, and $\delta \leq 2t+1$; the equality holds when each ball of radius $t$ centered at the signal points of $\mathcal{C}$ forms a partition of $V$. A code satisfying this property is called *perfect* and corrects $t$ errors. A code is called *quasiperfect* if the code is capable of correcting every error pattern up to $t$ errors and some patterns with $t+1$ errors and no errors greater than $t+1$. Perfect codes and quasiperfect codes are part of a more general class of codes called *geometrically uniform codes*.

## 6. Example

A code derived from a graph is defined as geometrically uniform if for any two-code sequences, there exists an isometry that takes a code sequence into the other, while it leaves the code invariant. Hence, geometrically uniform codes partition a set of vertices of a graph by the Voronoi regions.

Given an element $\alpha \in \mathcal{O}_R$, we may generate a code over a graph by use of the quotient ring $\mathcal{O}_R/\langle\alpha\rangle$ as the vertices of the graph. Thus, by choosing $\beta$ a divisor of $\alpha$, we obtain a geometrically uniform code, and the vertices of the graph are covered by the action of the isometries on the fundamental region as shown in Section 4.

*Example 6.1.* For $g = 2$, given $\alpha = 1 + 2\sqrt{2}j$, such that $\alpha \in \mathcal{O}_{\mathbb{Z}(\sqrt{2})} = (\sqrt{2},-1)_{\mathbb{Z}(\sqrt{2})}$, the reduced norm is $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha) = 9$. Thus, from Theorem 4.4, the cardinality of the set of vertices $V$ is $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha)^4 = 9^4 = 6561$. Note that $\alpha$ may be written as $1 + 2\sqrt{2}j = (\sqrt{2}+j)^2$, and so $\beta$ is a right divisor of $\alpha$ and $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\beta) = 3 \in \mathbb{Z}$. Therefore, the code generated by $\beta$, $\langle\beta\rangle \subseteq \mathcal{O}$ has $\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\alpha)^4/\mathrm{Nrd}_{\mathbb{Z}[\sqrt{2}]}(\beta)^4 = 9^4/3^4 = 81$ codewords. Note that the Voronoi region associated with each codeword consists of 81 elements. If $\tau = \sqrt{2}+j$ and $\eta = 0$, then $\tau - \eta = \sqrt{2}+j = (1+2\sqrt{2}j)\sqrt{2} - 3j \equiv -3j (\mathrm{mod}\alpha)$. Thus, $D_\alpha(\eta,\tau) = 6$. The minimum distance of this code is $D_\alpha(\eta,\tau) = 6$.

The procedures considered may be extended to surfaces with any genus once the associated quaternion order is known. This allows us to construct new geometrically uniform codes over different signal constellations.

## References


[1] A. F. Beardon, *The Geometry of Discrete Groups*, vol. 91 of *Graduate Texts in Mathematics*, Springer, New York, NY, USA, 1983.

[2] G. D. Forney Jr., "Geometrically uniform codes," *Institute of Electrical and Electronics Engineers*, vol. 37, no. 5, pp. 1241–1260, 1991.

[3] H. Lazari and R. Palazzo Jr., "Geometrically uniform hyperbolic codes," *Computational & Applied Mathematics*, vol. 24, no. 2, pp. 173–192, 2005.

[4] S. I. R. Costa, M. Muniz, E. Agustini, and R. Palazzo Jr., "Graphs, tessellations, and perfect codes on flat tori," *Institute of Electrical and Electronics Engineers*, vol. 50, no. 10, pp. 2363–2377, 2004.

[5] C. Martínez, R. Beivide, and E. M. Gabidulin, "Perfect codes from Cayley graphs over Lipschitz integers," *Institute of Electrical and Electronics Engineers*, vol. 55, no. 8, pp. 3552–3562, 2009.

[6] C. Quilles and R. Palazzo Jr., "Quasi-perfect geometrically uniform codes derived from graphs over gaussian integer rings," in *Proceedings of the IEEE International Symposium on Information Theory*, pp. 1158–1162, Austin, Tex, USA, June 2010.
[7] C. Quilles and R. Palazzo Jr., "Quasi-perfect geometrically uniform codes derived from graphs over integer rings," in *Proceedings of the 3rd International Castle Meeting on Coding Theory and Applications*, pp. 239–244, Barcelona, Spain, September 2011.
[8] P. A. Firby and C. F. Gardiner, *Surface Topology*, Woodhead, 3rd edition, 2001.
[9] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer, New York, NY, USA, 1973.
[10] T. W. Hungerford, *Algebra*, vol. 73 of *Graduate Texts in Mathematics*, Springer, New York, NY, USA, 1980.
[11] K. Takeuchi, "A characterization of arithmetic Fuchsian groups," *Journal of the Mathematical Society of Japan*, vol. 27, no. 4, pp. 600–612, 1975.
[12] I. Stewart and D. Tall, *Algebraic Number Theory*, Chapman and Hall Mathematics Series, Chapman & Hall, London, UK, 2nd edition, 1987.
[13] V. L. Vieira, *Arithmetic fuchsian groups identified over the quaternion orders for the construction of signal constellations [Doctoral Dissertation]*, FEEC-UNICAMP, 2007.
[14] I. Reiner, *Maximal Orders*, vol. 28 of *London Mathematical Society Monographs. New Series*, The Clarendon Press Oxford University Press, Oxford, UK, 2003.
[15] S. Johansson, A description of quaternion algebra, http://www.math.chalmers.se/~sj/forskning.html.
[16] S. Katok, *Fuchsian Groups*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, Ill, USA, 1992.
[17] E. D. Carvalho, *Construction and labeling of geometrically uniform signal constellations in euclidean and hyperbolic spaces [Doctoral Dissertation]*, FEEC-UNICAMP, 2001.