Blanco-Chacon, I.; Hollanti, C.; Alsina, M.; Remón, Dionis

Fuchsian codes with arbitrarily high code rates

Published in:
Journal of Pure and Applied Algebra

DOI:
10.1016/j.jpaa.2015.06.005

Published: 01/01/2016

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

FUCHSIAN CODES WITH ARBITRARILY HIGH CODE RATES

IVÁN BLANCO-CHACÓN, CAMILLA HOLLANTI, MONTSERRAT ALSINA,
AND DIONÍS REMÓN

Abstract. Recently, so-called Fuchsian codes have been proposed in [I. Blanco-Chacón et al., "Nonuniform Fuchsian codes for noisy channels", J. of the Franklin Institute 2014] for communication over channels subject to additive white Gaussian noise (AWGN). The two main advantages of Fuchsian codes are their ability to compress information, i.e., high code rate, and their logarithmic decoding complexity. In this paper, we improve the first property further by constructing Fuchsian codes with arbitrarily high code rates while maintaining logarithmic decoding complexity. Namely, in the case of Fuchsian groups derived from quaternion algebras over totally real fields we obtain a code rate that is proportional to the degree of the base field. In particular, we consider arithmetic Fuchsian groups of signature $(1; e)$ to construct explicit codes having code rate six, meaning that we can transmit six independent integers during one channel use.

1. Introduction

Nonuniform codes are known to be good in terms of approaching the capacity of a channel affected by additive white Gaussian noise (AWGN). They have been used already in early-state signal transmission, *e.g.*, in the so-called *codec* transmission, and are present more recently in the Digital Video Broadcasting Next Generation Handheld (DVB-NGH) standard [5]. Unfortunately, nonuniform codes are in general subject to brute-force maximum-likelihood (ML) decoding methods, resulting in a linear decoding complexity in the codebook size. Recently, in [2] and [4], a family of nonlinear and nonuniform *Fuchsian codes* were constructed based on Fuchsian groups of the first kind defined from quaternion algebras over $\mathbb{Q}$. The decoding procedure of these codes is based on a modified point reduction algorithm having logarithmic complexity in the codebook size, which was shown to imply logarithmic decoding complexity for the Fuchsian codes [2], [3].

In this paper, we will study one of the key features of a *code*, namely its ability to carry information. In other words, how many bits per channel use we will be

able to send when using a given code. Here, we will do this in conjunction with Fuchsian codes. To this end, let us start with the following intuitive definition, which will be formalized later (cf. Def. 3.4).

Definition 1.1. Let $C \subset \mathbb{C}$ denote a codebook of size $|C| < \infty$, and let k denote the number of independent integers embedded in each codeword. The *code rate* is

$$R = k$$

(independent integer) symbols per channel use (spcu).

The *data rate* is

$$R_d = \log_2 |C|$$

bits per channel use (bpcu).

The code rate can be thought of as the ability of the code to compress information, and the data rate as the transmission speed enabled by the code.

Remark 1.2. When encoding over multiple channel uses, as is the case for lattice codes and space–time codes [12], the suitable definition for code rate is $R = k/T$, where T is the number of channel uses. With $T = 1$, this coincides with the definition above.

Apart from the sub-linear decoding complexity, another advantage of the Fuchsian codes in [2] is that they allow, in the sense of the above definition, to compress information. Namely, they enable us to embed three independent integers in one complex number to be transmitted, having thus code rate $R = 3$. In comparison to the usual way of transmitting a complex signal, *e.g.*, by using the quadrature amplitude modulation (QAM) consisting of a finite subset of Gaussian integers

$$\mathbb{Z}[i] = \{c = a + bi \,|\, a, b \in \mathbb{Z}\}$$

embedding only two independent integers, the rate of a Fuchsian code [2] is 50% higher. The algebraic reason for the higher rate will become evident in Section 3.

In what follows, we will consider quaternion algebras defined over totally real field extensions of $\mathbb{Q}$ of degree bigger than 1. As we will see, this implies that we can increase the code rate even further. Since the point reduction algorithm works in general for arithmetic Fuchsian groups, we have adapted it to some explicit groups derived from the arithmetic Fuchsian groups of signature $(1; e)$. These groups allow us to construct Fuchsian codes with higher rates. We will show explicit examples of a rate six code, and our method can indeed produce fully explicit codes of rate up to 18.

The motivation for increasing the code rate initially came for lattice coding [12]. For lattice codes, higher code rate typically implies higher data rates (or equivalently, bigger codebook, cf. Def. 1.1.) without having to increase the transmission power or to compromise the minimum distance. As the transmission power is determined by the Euclidean norm of the transmitted codeword, this results from the fact that a higher rank lattice with a unit volume has more points within a Euclidean hypercube of a given edge length than a lower rank lattice with a unit volume. To get an intuition, one can think of how many integer points are there in the real line between, say, 0 and 10, versus how many integral points are there in a $10 \times 10 \times 10$ cube in $\mathbb{R}^3$. The same is naturally valid for Euclidean hyperspheres. Therefore, it is desirable to maximize the code rate. For the proposed higher rate Fuchsian codes there is a caveat: due to the nonlinear and nonuniform structure, there is no *a priori* reason why higher rate should imply a bigger codebook. It seems difficult to give a rigorous proof for this, so we have settled with numerical experiments to see how the rate affects the codebook size. In our example cases, higher rate seems to indeed imply a bigger codebook, given the minimum distance and the hypersphere radius.

Our interest in Fuchsian groups as a basis for code construction stems from a series of recent papers by Palazzo *et al.* In [20, 6, 16, 17], among others, various interesting connections between Fuchsian groups and signal constellation design are presented. In [20], the authors construct Fuchsian groups suitable for signal constellation design. In [16], the authors consider the unit disk model of the hyperbolic plane as the signal space, and the noise is modeled as a hyperbolic Gaussian random variable. By using some results of hyperbolic geometry they construct a hyperbolic equivalent to QAM and PSK constellations and point out that, when the channel model is hyperbolic (this is the case *e.g.* in power transmission line communications [7]), the proposed hyperbolic constellations provide higher coding gains than the classical Euclidean variants. Building on this work, in [17] the authors construct dense tessellations and count Dirichlet domains attached to certain families of these tessellations. In [6] the authors use units of quaternion orders to construct space-time matrices with the potential use case being wireless multi-antenna (MIMO) communications. We refer the reader to [13, 8] as the early references to the use of division algebras and maximal orders in MIMO.

Although codes related to Fuchsian groups had been considered before, our approach in [2] was original in that it described a complete construction and decoding process, whereas earlier work had largely concentrated on the constellation design while giving little attention to the decoding and performance aspects. Another key difference to the aforementioned works was, as is the case of the present paper, that we are studying codes on the *complex plane* arising from quaternion algebras and Fuchsian groups, and our aim is to apply the codes to the classical (Euclidean) channel models such as the aforementioned AWGN channel, with

possible future extension to fading channels. We do not use hyperbolic metric as our design metric, but use the Fuchsian group as a starting point to the code generation. Nevertheless, our decoder will rely on hyperbolic geometry as opposed to the classical decoders based on Euclidean geometry.

The paper is organized as follows: in Section 2 we give some background and notation on Fuchsian groups acting on the complex upper half-plane, specially those coming from quaternion algebras over a number field F, in a more general setting than [4] and [2]. In Section 3, we generalize the construction of Fuchsian codes in order to obtain codes of arbitrarily high rates. In particular, by using quaternion algebras over totally real extensions $F/\mathbb{Q}$, we prove that the code rate is at least $3n$, where $n = [F : \mathbb{Q}]$ is the degree of the base field. In Section 4, we explore such Fuchsian codes for a number of Fuchsian groups derived from those of signature $(1; e)$, classified by Takeuchi [19]. This task has required to explicitly construct suitable fundamental domains for these groups and to adapt the point reduction algorithm [3] to our case. We also provide some numerical evidence to justify the study of higher rate Fuchsian codes by showing that increasing the rate may indeed increase the codebook size and hence the data rate. In the last section, we expose the conclusions and discuss directions for future research.

2. Action of arithmetic Fuchsian groups on the hyperbolic plane

Next we review some algebraic concepts and results related to Fuchsian groups acting on the complex upper half-plane, in particular those arising from quaternion algebras over a number field F, thus extending our work in [2].

2.1. **Tessellations on the complex plane.**

Let us denote by $\mathrm{SL}(2,\mathbb{R})$ the special linear group of 2×2-matrices with entries in $\mathbb{R}$ and determinant equal to 1. There is a group action on the Riemann sphere $\mathbb{C} \cup \{\infty\}$ defined by:

(2.1)
$$\gamma(z) = \frac{az+b}{cz+d}, \quad \gamma(\infty) = \frac{a}{c} = \lim_{z\to\infty} \gamma(z), \quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}),\ z \in \mathbb{C}.$$

These maps $z \mapsto \gamma(z)$ are called *fractional linear transformations* or *Möbius transformations* of the Riemann sphere. The unique matrices fixing all the points are Id and $-\mathrm{Id}$. Thus, $\mathrm{SL}(2,\mathbb{R})/\{\pm \mathrm{Id}\}$ acts faithfully on $\mathbb{C}$, that is to say, each element other than the identity acts nontrivially. The complex upper half-plane

$$\mathcal{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$$

is stable under this action. In fact the Möbius transformations are the group of isometries of $\mathcal{H}$ with respect to the hyperbolic geometry.

We will consider discrete subgroups of $\mathrm{SL}(2,\mathbb{R})$ with a proper and discontinuous action on $\mathcal{H}$ such that the hyperbolic volume of the quotient of $\mathcal{H}$ by that action is finite. These groups are called Fuchsian groups of the first kind, Fuchsian groups in short. By abuse of notation, we will use the same notation for the groups in $\mathrm{SL}(2,\mathbb{R})$ and $\mathrm{SL}(2,\mathbb{R})/\{\pm \mathrm{Id}\}$. Let us also recall that whenever a group acts on a set, it divides the set into equivalence classes.

Definition 2.1. For a Fuchsian group Γ, a fundamental domain is a closed hyperbolic polygon $\mathcal{F}$ in $\mathcal{H}$ satisfying:

a) For any z, z' in the interior of $\mathcal{F}$, if there exists $\gamma \in \Gamma$ such that $\gamma(z) = z'$, then $z = z'$ and $\gamma = Id$.
b) For any $z \in \mathcal{H}$, there exists $z_0 \in \mathcal{F}$ and $\gamma \in \Gamma$ such that $\gamma(z) = z_0$.

Each election of a fundamental domain for the action of a Fuchsian group Γ leads to a regular tessellation of the upper half-plane by hyperbolic polygons, which will be useful for the code construction. In fact the unlimited number of tessellations is one of the advantages of the hyperbolic plane compared to the Euclidean one.

Given a fundamental domain of Γ and $z \in \mathcal{H}$, the problem of finding $z_0 \in \mathcal{F}$ and $\gamma \in \Gamma$ such that $\gamma(z) = z_0$ is known as the *point reduction problem* and requires an algorithmic solution referred to as the point reduction algorithm. Here, we will consider tessellations obtained from Fuchsian groups arising from quaternion algebras.

2.2. **Quaternion algebras, orders and arithmetic Fuchsian groups.** Let F be an arbitrary field with $\mathrm{char}\, F \neq 2$. The quaternion algebra H denoted by $\left(\frac{a,b}{F}\right)$, $a, b \in F \setminus \{0\}$, is the F-algebra with F-basis $\{1, I, J, K\}$ subject to the multiplication rules $I^2 = a, J^2 = b, K = IJ = -JI$. For more details on quaternion algebras, cf. [21] and [1].

In a quaternion algebra, there is a natural conjugation such that for $\omega = x + yI + zJ + tK \in H$ the conjugate is $\overline{\omega} = x - yI - zJ - tK$. Then the reduced trace and the reduced norm are defined by

$$\mathrm{Tr}(\omega) = \omega + \overline{\omega} = 2x, \qquad \mathrm{N}(\omega) = \omega\overline{\omega} = x^2 - ay^2 - bz^2 + abt^2.$$

It is well known that a quaternion F-algebra H is a central simple algebra of dimension 4 over F, and by Wedderburn's structure theorem H is isomorphic to either $\mathrm{M}(2, F)$ or to a skew field, also called a division F-algebra. If $F = \mathbb{C}$, or more generally F is algebraically closed, only matrix algebras are obtained. If $F = \mathbb{R}$, or in general a local field different from $\mathbb{C}$, there exists a unique division F-algebra up to isomorphism. In the real case, the unique quaternion division

algebra is the Hamilton quaternion $\mathbb{R}$-algebra, $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$. Of course, for any field F, $\left(\frac{1,1}{F}\right) \cong \mathrm{M}(2,F)$.

Given F a number field, for each place ν of F, that is an archimedean or non-archimedean absolute value of F, consider the local field F_ν. Then $H_\nu := H \otimes F_\nu$ is a quaternion algebra over the local field. We say that H is *ramified* at ν if H_ν is a division algebra; otherwise, H is said to *split* at ν. The set of places where H is ramified is a finite set of even cardinality and it characterizes the quaternion algebra up to isomorphism.

From now on, consider F a totally real algebraic number field with ring of integers R and $[F:\mathbb{Q}] = n$. We will assume that H is a division algebra, that is $H \ncong \mathrm{M}(2,F)$, and that H ramifies precisely at $n-1$ out of the n completions of F with respect to the Galois embeddings of $F/\mathbb{Q}$ into $\mathbb{R}$, the archimedean places. Namely, H satisfies the following condition

$$H \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}(2,\mathbb{R}) \times \mathbb{H}^{n-1}. \tag{2.2}$$

In the case of quaternion $\mathbb{Q}$-algebras, this means that H is an indefinite quaternion algebra. Such algebras were used to consider Fuchsian groups and to define associated Fuchsian codes in [2].

Lemma 2.2. *The following map ϕ is a monomorphism of F-algebras, giving a left regular representation of the quaternion algebra in a matrix algebra:*

$$\begin{aligned} \phi : \left(\frac{a,\, b}{F}\right) \quad &\to \quad \mathrm{M}(2,(F(\sqrt{a}))) \\ x + yI + zJ + tK &\mapsto \begin{pmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{pmatrix}. \end{aligned}$$

Remark 2.3. Notice that for any $\omega \in H$, $\mathrm{N}(\omega) = \det(\phi(\omega))$, and $\mathrm{Tr}(\omega) = \mathrm{Tr}(\phi(\omega))$. If $\sqrt{a} \in \mathbb{R}$, then $\mathrm{M}(2,(F(\sqrt{a}))) \subseteq \mathrm{M}(2,\mathbb{R})$. In particular, if we restrict to quaternion elements in H with reduced norm equal to 1, then the image under ϕ is contained in $\mathrm{SL}(2,\mathbb{R})$.

An R-order $\mathcal{O}$ in H is a finitely generated R-submodule, *i.e.*, a subring such that $\mathcal{O} \otimes F \simeq H$. The elements in $\mathcal{O}$ are integral, namely for any $\omega \in \mathcal{O}$, its characteristic polynomial $x^2 - \mathrm{Tr}(\omega)x + \mathrm{N}(\omega)$ has coefficients in R.

For an order $\mathcal{O}$, a Fuchsian group Γ is obtained by using the map ϕ:

$$\Gamma = \phi(\mathcal{O}_+^*), \qquad \text{where } \mathcal{O}_+^* = \{\omega \in \mathcal{O} \mid \omega \text{ invertible}, \mathrm{N}(\omega) > 0\}.$$

In the case of the base field being $\mathbb{Q}$, it is interesting to consider Eichler orders $\mathcal{O}$. Eichler orders are intersections of two maximal orders. When H is indefinite,

the discriminant of the quaternion algebra $D \in \mathbb{Z}$ is defined as the product of all finite primes where H is ramified. The discriminant is an invariant of the quaternion algebra. The group $\phi(\mathcal{O}_+^*)$ is denoted by $\Gamma(D,N)$, where $N \in \mathbb{N}$ is the level of the Eichler order, and $N = 1$ for a maximal order. The group $\Gamma(D,N)$ is well-defined up to conjugation.

Remark 2.4. After Weil's results on the classification of classical groups, the list of all arithmetic subgroups of $\mathrm{SL}(2,\mathbb{R})$ is exhausted up to commensurability by Fuchsian groups coming from quaternion algebras over totally real number fields, cf. [10], where two groups G_1 and G_2 are said to be commensurable if $G_1 \cap G_2$ has finite index both in G_1 and in G_2. Thus the Fuchsian groups derived from quaternion algebras are in the main focus when studying tessellations.

Fuchsian groups derived from quaternion algebras and their quotients $\Gamma\backslash\mathcal{H}$ also led to the theory of Shimura curves in the sixties [14]. The case of matrix algebras corresponds to classical modular curves. Since we assumed that H is a division algebra, the quotient is already compact and there are no cusps. Thus the classical problems of finding fundamental domains and reducing points to a given fundamental domain call for algorithmic solutions different from those available for the modular case. For more results on fundamental domains, see [1], [9], [22].

As already mentioned, a general algorithm for the point reduction problem was recently proposed in [3]. Some specific examples can be found in [2].

2.3. **The point reduction algorithm (PRA).** As the decoding of Fuchsian codes is based on the point reduction algorithm, let us summarize here its main features. See [3] for validity and complexity proofs.

First, let us recall that the construction of a fundamental domain for Γ following Fords's method (cf. [10]) is based on the use of *isometric circles* $I(\gamma)$, *i.e.*, hyperbolic lines in the upper half-plane associated to the matrices $\gamma \in \Gamma$:

$$I(\gamma) = \{z \in \mathcal{H} \mid |cz + d| = 1\}, \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, c \neq 0.$$

Notation 2.5. For any Fuchsian group Γ and any fixed fundamental domain $\mathcal{F}(\Gamma)$, let us denote by G the minimal subset of Γ such that the edges of $\mathcal{F}(\Gamma)$ are included in the set of isometric circles defined by the elements of G. As a presentation of the group Γ arises from the pairing of the edges, we can assume that the generators of Γ are included in G. The set G splits into two subsets denoted by G^{int} and G^{ext} according to whether the fixed fundamental domain is located in the interior or in the exterior of each isometric circle, respectively. Hence, if

$\mathrm{ext}(I(\gamma))$ and $\mathrm{int}(I(\gamma))$ denote the exterior and the interior of the isometric circle $I(\gamma)$, the fundamental domain $\mathcal{F}(\Gamma)$ is the closure of

$$\bigcap_{\gamma\in G^{\mathrm{ext}}} \mathrm{ext}(I(\gamma)) \cap \bigcap_{\gamma\in G^{\mathrm{int}}} \mathrm{int}(I(\gamma)).$$

Now we are ready to introduce the point reduction algorithm (PRA). It gives a solution to the reduction point problem; namely, it reduces a given point $z \in \mathcal{H}$ to a point $z_0 \in \mathcal{F}$, and yields a transformation $\gamma \in \Gamma$ such that $\gamma(z) = z_0$.

PRA (Point Reduction Algorithm)

Step 1 Initialize: $z_0 = z$ and $\gamma = \mathrm{Id}$.
Step 2 Check if $z_0 \in \mathcal{F}$.
If $z_0 \in \mathcal{F}$, return z_0 and γ. Quit.
If $z_0 \notin \mathcal{F}$, return $g \in G$ such that:
$z_0 \in \mathrm{int}(\mathrm{I}(g))$, if $g \in G^{\mathrm{ext}}$,
$z_0 \in \mathrm{ext}(\mathrm{I}(g))$ if $g \in G^{\mathrm{int}}$.
Step 3 Compute $z_0 = g(z_0)$ and $\gamma = g \cdot \gamma$. Go to Step 2.

The PRA will be used for the decoding of Fuchsian codes in the sequel. In order to study the complexity of the algorithm when applied to Fuchsian codes, we state the following remark and definition.

Remark 2.6. Consider $z, z' \in \gamma(\mathcal{F})$, $\gamma \in \Gamma$, $z \neq z'$. By construction, to run the PRA with input z or z' will output different points z_0 or z_0', respectively, but the same matrix $g = \gamma$, in the same number of steps.

Definition 2.7. Given a matrix $\gamma \in \Gamma$, the *depth* of γ, denoted by $\ell(\gamma)$, is the minimal number of iterations of the PRA to reduce $\gamma(\tau)$ to the fundamental domain for any $\tau \in \mathcal{F}$.

3. General construction of Fuchsian codes

In [2], we described in detail how to construct and decode Fuchsian codes in an AWGN channel. In order to make this paper self-contained, we shortly restate the process in this more general setting, focusing on some essential properties.

3.1. General construction.

Let Γ be a Fuchsian group as in Section 2.1.

The first step in the construction of the code is to fix a fundamental domain $\mathcal{F} = \mathcal{F}(\Gamma)$, which determines a tessellation of the complex upper half-plane $\mathcal{H}$, and a set $G \subset \Gamma$ whose corresponding isometry circles are the edges of the fundamental domain, following the notation in Section 2.

The main step in the process is to choose a set of N different elements in Γ, $S_\Gamma = \{\gamma_1, \dots \gamma_N\}$, what is equivalent to choosing N different tiles in the tessellation. Moreover, we choose τ to be an interior point of $\mathcal{F}$; this condition ensures that $\gamma(\tau) \neq \tau$ for all $\gamma \in \Gamma \setminus \{\pm \mathrm{Id}\}$.

Finally, considering the action of the group Γ in the complex upper half-plane $\mathcal{H}$, we obtain the codewords $\gamma_1(\tau), \dots \gamma_N(\tau)$ in $\mathcal{H}$. The condition on τ ensures $\gamma_i(\tau) \neq \gamma_j(\tau)$. We can double the number of points by expanding to the lower half-plane in a natural way by including the opposites $-\gamma_i(\tau)$. Thus, the codebook consists of the $2N$ complex points constructed by using τ and S_Γ, and the symmetry with respect to the origin. Based on the outlined process, we give a formal definition of a Fuchsian code below, and summarize the construction process in Table 1.

Definition 3.1. Let Γ be a Fuchsian group. Given a fundamental domain $\mathcal{F}(\Gamma)$, a set $S_\Gamma = \{\gamma_1, \dots \gamma_N\} \subset \Gamma$, and a point τ in the interior of $\mathcal{F}(\Gamma)$, we define the associated *Fuchsian code* as $\mathcal{C} = \{\pm\gamma(\tau) \mid \gamma \in S_\Gamma\} \subseteq \mathbb{C}$. The set of codewords is also referred as a *q-nonuniform Fuchsian constellation*, q-NUF in short, where $q = |\mathcal{C}| = 2N$ is the size of the code. The point τ will be called the *center* of the code.

TABLE 1. Sketch of the code construction process.

FIX:	→	CHOOSE:	→	SET CODEBOOK $\mathcal{C}$:
Fuchsian group Γ Fund. domain $\mathcal{F}(\Gamma)$		$S_\Gamma = \{\gamma_1, \dots \gamma_N\} \subset \Gamma$ τ in the interior of $\mathcal{F}(\Gamma)$		$\{\pm\gamma_1(\tau), \dots \pm\gamma_N(\tau)\}$ $\lvert\mathcal{C}\rvert = 2N$

This construction was stated in [2] in the case of groups $\Gamma(D, 1)$ derived from quaternion algebras over $\mathbb{Q}$. We refer the interested reader there for explicit examples, including details about representations of the groups, fundamental domains, centers of the codes, lists of codewords, as well as some experimental results.

The general construction stated above now allows us to construct more general codes, as long as we are able to determine the respective fundamental domains. In particular, it can be applied to groups derived from quaternion algebras over a totally real field. The behavior and performance of Fuchsian codes will essentially depend on the choices in the intermediate step. An algebraic and geometric study of Fuchsian groups and their fundamental domains will therefore be useful for developing a general understanding of various code parameters, such as the minimum distance and average transmission power. We refer again to [2] for a more detailed exposition.

3.2. **Decoding of Fuchsian codes.** Let $\mathcal{C} \subseteq \mathbb{C}$ be a q-NUF constellation with center τ, associated to a fixed Fuchsian group Γ with a fixed fundamental domain $\mathcal{F}$. It is clear that given $x \in \mathcal{C}$, $\Im(x) > 0$, the PRA described in Section 2.3 computes $\gamma \in \Gamma$ such that $x = \gamma(\tau)$, which is equivalent to finding the tile containing x in the tessellation of $\mathcal{H}$ induced by the fundamental domain $\mathcal{F}$. If $\Im(x) < 0$, it is enough to consider $-x$ and then apply the PRA.

In the context of AWGN channels, let $x = \gamma(\tau) \in \mathcal{C} \subset \mathbb{C}$ be the transmitted codeword and y the received signal, $y = x + \varepsilon = \gamma(\tau) + \varepsilon \in \mathbb{C}$, where ε is the Gaussian noise. The basic idea underlying our decoding technique is that, provided that the channel is of sufficiently good quality, the received signal y will belong to the tile $\gamma(\mathcal{F})$ determined by x. In other words, when we apply the PRA to y, it will return γ and the transmitted codeword $x = \gamma(\tau)$ can be recovered. In order to measure the decoding complexity when employing the PRA, we define (also cf. Def. 2.7):

Definition 3.2. The *depth* of the code is $\ell(\mathcal{C}) := \max\{\ell(\gamma) \mid \gamma \in S_\Gamma\}$.

Next, we describe the encoding and decoding process of Fuchsian codes in detail. In order to remain in the upper half-plane whilst decoding, we initialize the algorithm with $z_0 = y$ if $\Im(y) > 0$, and with $z_0 = -y$ if $\Im(y) < 0$. Since $\mathbb{R}$ has measure zero in $\mathbb{C}$, the case $\Im(y) = 0$ occurs with probability zero.

Encoding and decoding of Fuchsian codes

Step 1 Assign a matrix $\gamma \in \mathbb{C}$.
Step 2 Compute the codeword $x = \gamma(\tau)$.
Step 3 Transmit x using the AWGN channel.
The receiver obtains $y = x + \varepsilon$, where ε is the Gaussian noise.
Step 4 Decode the signal y:
If $\Im(y) > 0$, apply PRA to y, obtain γ.
If $\Im(y) < 0$, save the sign information, $y \leftarrow -y$,
apply PRA to y, obtain γ.
Step 5 $\gamma \leftarrow$ (sign information) $\times \gamma$.

The following theorem proves the existence of Fuchsian codes with logarithmic decoding complexity.

Theorem 3.3. *Let Γ be a Fuchsian group containing a non-abelian free subgroup. There exist Fuchsian codes $\mathcal{C}$ associated to Γ such that the decoding algorithm for $\mathcal{C}$ has logarithmic complexity in $|\mathcal{C}|$, namely, the number $r_\mathcal{C}$ of arithmetic operations satisfies*

$$r_\mathcal{C} = O(\log(|\mathcal{C}|).$$

The proof is analogous to the corresponding results in [2], so we only provide a sketch of the proof. The first part of the proof is to count the maximal number of arithmetic operations when running the PRA. In each iteration, we got that the number of operations only depends on the fundamental domain, and not on the code size. As the number of iteration is bounded by the depth $\ell(\mathcal{C})$, $r_{\mathcal{C}} = O(\ell(\mathcal{C}))$. Secondly, by using the technical condition given by the existence of a non-abelian free subgroup, a Fuchsian code $\mathcal{C}$ can be constructed in such a way that $\ell(\mathcal{C}) = O(\log(|\mathcal{C}|)$. The key point is to choose S_Γ as large as possible while controlling the depth of their elements.

Combining these two parts, we deduce the existence of Fuchsian codes with logarithmic complexity.

Actually, for a fixed Fuchsian group Γ the complexity of the decoding algorithm depends only on the selection of the subset S_Γ. The choice of the center of the code τ will influence the performance of the code, being related to the minimum border distance, as stated in [2] (see the code design criterion therein).

3.3. **The rate.** Let us reduce to the case of Fuchsian groups derived from quaternion algebras H over F, as in Section 2.2. To this end, let F be a totally real number field with ring of integers R and $[F : \mathbb{Q}] = n$. Now H is a division algebra satisfying condition 2.2, and $\Gamma = \phi(\mathcal{O}^*_+)$ for an order $\mathcal{O}$ in H, and ϕ the regular representation of H in $\mathrm{M}(2, \mathbb{R})$ (cf. Lemma 2.2). Consider a code $\mathcal{C} = \{\pm\gamma(\tau) \mid \gamma \in S_\Gamma\} \subseteq \mathbb{C}$.

In the case $F = \mathbb{Q}$, when we restrict to the natural order $\mathbb{Z}[1, I, J, K]$, a complex number $\gamma(\tau)$ to be transmitted is identified with the matrix $\gamma \in S_\Gamma \subset \phi(\mathcal{O}^*_+)$ (recall that we take τ an interior point of the fundamental domain). Writing $\gamma = \begin{pmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{pmatrix}$ with $x, y, z, t \in \mathbb{Z}$, we can identify γ with the 4-tuple $(x, y, z, t) \in \mathbb{Z}^4$, which is subject to the normic equation

$$x^2 - ay^2 - bz^2 + abt^2 = 1, \quad a > 0 \tag{3.1}$$

Thus, the 4-tuple consists of 3 algebraically independent integers. This is equivalent to say that the set of 4-tuples satisfying the normic equation has 3 algebraic degrees of freedom. Notice that this is precisely the dimension of the algebraic set defined by the normic equation (which is not empty, since it contains all the infinite 4-tuples attached to the Fuchsian group). The concept of algebraic code rate, denoted R, will be hence defined so that for this code we have $R = 3$ symbols per channel use (spcu). We can easily generalize this notion of code rate for Fuchsian codes over totally real number fields.

Let F be a totally real number field of degree n with ring of integers R, let B be a quaternion F-algebra satisfying condition 2.2 and $\Gamma = \phi\left(\mathcal{O}^*_+\right)$, with $\mathcal{O}$ a

maximal R-order. Each matrix $\gamma \in \Gamma$ has the form $\gamma = \begin{pmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{pmatrix}$ with $(x, y, z, t) \in R^4$. Fixing a $\mathbb{Z}$-basis of R, we can identify x with an n-tuple $(x_1, ..., x_n) \in \mathbb{Z}^n$ and analogously with y, z, and t. Hence, we can identify the matrix γ with a $4n$-tuple $(x_1, ..., x_n, y_1, ...y_n, z_1...z_n, t_1, ..., t_n) \in \mathbb{Z}^4$.

The fact that the 4-tuple $(x, y, z, t) \in R^4$ satisfies the normic equation (defined over R) is equivalent to the fact that the corresponding $4n$-tuple satisfies a certain system of polynomial equations (defined over $\mathbb{Z}$). This system of polynomial equations defines an algebraic set which we denote by $A(\Gamma)$. Notice that this algebraic set has infinitely many elements, hence, its algebraic dimension is well defined.

Definition 3.4. The algebraic code rate in symbols per channel use (spcu), or code rate from now on, of the Fuchsian code attached to a Fuchsian group $\Gamma = \phi(\mathcal{O}_+^*)$ satisfying condition 2.2 is the algebraic dimension of the algebraic set $A(\Gamma)$.

Remark 3.5. The code rate defined this way, measures how many degrees of freedoms are there in the set of $4n$-tuples attached to the Fuchsian group. We can think of the code rate, hence, as the number of algebraically independent (non-redundant) symbols in each $4n$-tuple, or as we said in the introduction, the maximal number of independent symbols embedded in each codeword $\gamma(\tau)$, with $\gamma \in \Gamma$.

Notice that if an undetermined system of t polynomial equations in n variables has solutions, then the set of all complex solutions is an algebraic set of dimension at least $n - t$. In particular, the code rate of a Fuchsian code will be at least $4n - t$, being t the number of equations defined over $\mathbb{Z}$ which are equivalent to the normic equation, which is defined over R.

The main result on the existence of Fuchsian codes of arbitrarily high rates is the following theorem. The proof consists on proving the two propositions stated after the theorem.

Theorem 3.6 (Main Theorem)**.** *Let F be a totally real number field of degree n. There exist infinitely many Fuchsian codes with rate at least $3n$ attached to F.*

In order to prove our main theorem we first prove that, for a fixed quaternion algebra satisfying 2.2, there are Fuchsian codes of rate at least $3n$. This is Proposition 3.7. Second, we prove the existence of such quaternion algebras in Proposition 3.8.

Proposition 3.7. *Let $F/\mathbb{Q}$ be a totally real number field of degree n, with ring of integers R, and H a quaternion F-algebra satisfying condition 2.2. Then, a Fuchsian code associated to the natural order $R[1, I, J, K]$ has code rate at least $3n$.*

Proof. Consider the natural order $R[1, I, J, K]$ of the quaternion algebra $H = \left(\frac{a,b}{F}\right)$. Then Γ is determined by 4-tuples $(x, y, z, t) \in R^4$ satisfying $x^2 - ay^2 - bz^2 + abt^2 = 1$.

Let $\{\theta_1, ..., \theta_n\}$ be a $\mathbb{Z}$-basis of R with $\theta_1 = 1$. Writing $x = \sum_{k=1}^{n} x_k\theta_k$, $y = \sum_{k=1}^{n} y_k\theta_k$, $z = \sum_{k=1}^{n} z_k\theta_k$, $t = \sum_{k=1}^{n} t_k\theta_k$, each of these algebraic integers can be identified with its coordinates in the integral basis. Thus any 4-tuple $(x, y, z, t) \in R^4$ can be identified as a $4n$-tuple of rational integers.

Let us expand the normic equation $x^2 - ay^2 - bz^2 + abt^2 = 1$ such that it corresponds to a system of polynomial equations defined over $\mathbb{Z}$. We set $x^2 = \sum_{k=1}^{n} f_{x,k}(x_1, ..., x_n)\theta_k$, with $f_{x,k} \in \mathbb{Z}[x_1, ..., x_n]$ a quadratic homogeneous polynomial, and analogously for y, z, t, and obtain

$$x^2 - ay^2 - bz^2 + abt^2 = \sum_{k=0}^{n-1}(f_{x,k} - af_{y,k} - bf_{z,k} + abf_{t,k})\theta_k.$$

Since $a, b \in R$, the equation can be rewritten as

$$x^2 - ay^2 - bz^2 + abt^2 = \sum_{k=1}^{n} g_k\theta_k,$$

with $g_k \in \mathbb{Z}[x_1, ..., x_n, ..., t_1, ..., t_n]$ quadratic homogeneous polynomials. The condition $x^2 - ay^2 - bz^2 + abt^2 = 1$ now becomes equivalent to

$$\begin{aligned} &g_1(x_1, ..., x_n, ..., t_1, ..., t_n) = 1, \\ &g_k(x_1, ..., x_n, ..., t_1, ..., t_n) = 0, \quad \text{for } 2 \leq k \leq n. \end{aligned}$$

This system defines the algebraic set $A(\Gamma)$. Since a $4n$-tuple corresponding to an element of the Fuchsian group bears n restrictions, and the algebraic set $A(\Gamma)$ contains infinitely many solutions, we see that the algebraic dimension of $A(\Gamma)$, or equivalently, the code rate of the Fuchsian code attached to Γ is at least $3n$ spcu, proving the proposition. □

The following proposition addresses the question whether there exist quaternion algebras to which the above proposition can be applied.

Proposition 3.8. *Let F be a totally real number field of degree n. There exist infinitely many quaternion algebras H over F satisfying the condition 2.2.*

Proof. If $n \geq 3$ is odd, define Σ to be the set of all but one archimedean absolute values of F. Otherwise, define Σ as the set of all but one archimedean absolute places and add a non-archimedean absolute value $\nu_{\mathfrak{p}}$ attached to a prime ideal $\mathfrak{p}$ of F. Thus, Σ is of even cardinality and, by the well-known classification theorem of quaternion algebras, there exists a unique quaternion algebra H up to isomorphism such that H ramifies exactly for each $\nu \in \Sigma$. This is equivalent to say $H_\nu = H \otimes_{\mathbb{Q}} F_\nu = \mathrm{M}(2, F_\nu)$ for all $\nu \notin \Sigma$. Therefore H splits only at one archimedean absolute value satisfying the condition 2.2.

The corresponding result holds for Σ' constructed from Σ by adding an even number of non-archimedean absolute values as before. Therefore, there exists infinitely many quaternion algebras satisfying the desired condition. □

3.4. **Cyclotomic Fuchsian codes.** Let p be an odd prime, $\zeta_p \neq 1$ a primitive p-th root of unity, and consider the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$. Then, fix the number field $F = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, which is the maximal totally real subfield of $\mathbb{Q}(\zeta_p)$. We have that $[F : \mathbb{Q}] = (p-1)/2$. This will allow us to construct infinitely many Fuchsian codes of rate at least $3(p-1)/2$ provided that we can find quaternion algebras H over F satisfying the required condition, namely $H \otimes_{\mathbb{Q}} \mathbb{R} = \mathrm{M}(2, \mathbb{R}) \times \mathbb{H}^{(p-3)/2}$. Let us denote by Ω_F the set of all possible absolute values attached to F, archimedean or not.

The following technical lemma will be used in order to make easier the construction of quaternion algebras over the field $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ satisfying the condition 2.2 and to be more explicit in the description of such quaternion F-algebras over which we can construct Fuchsian codes.

Lemma 3.9 ([11], 6.13)**.** *Let F be a number field, $b \in F^*$ and $\Sigma \subseteq \Omega_F$ a finite subset of even cardinality. Suppose that b is a non-square element in F_ν for any $\nu \in \Sigma$. Then, there exists an element $a \in K^*$ such that the quaternion algebra $\left(\frac{a,b}{F}\right)$ splits precisely at the absolute values $\nu \notin \Sigma$.*

Proposition 3.10. *For every prime $p \geq 5$, there exists $a \in F = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ such that*

$$\left(\frac{a,-1}{F}\right) \cong \mathrm{M}(2,\mathbb{R}) \times \mathbb{H}^{\frac{p-3}{2}}.$$

Proof. Let us define a set Σ of absolute values of places F in the following way:

- If $p \equiv 3 \pmod 4$, take Σ to be the set of all archimedean absolute values minus one.
- If $p \equiv 1 \pmod 4$, take Σ to be the set of all archimedean absolute values minus one, adjoining a finite place, $\nu_{\mathfrak{q}}$, attached to a prime ideal $\mathfrak{q}$ of F over a rational prime q such that
  $q \equiv 1 \pmod p$,
  $q \equiv 3 \pmod 4$.
  Notice that such a prime always exists, due to the Chinese remainder theorem. Indeed there are infinitely many, due to the theorem by Dirichlet on primes in arithmetic progressions.

In the first case, Σ contains only archimedean absolute values. Since for any $\nu \in \Sigma$, $\nu(F) \subseteq \mathbb{R}$, it turns out that -1 is not a square in F_ν, and by applying lemma 3.9, we have that there exists $a \in F$ such that $\left(\frac{a,-1}{F}\right) \cong \mathrm{M}(2,\mathbb{R}) \times \mathbb{H}^{\frac{p-3}{2}}$.

In the second case, likewise, for all the archimedean places $\nu \in \Sigma$, -1 is not a square in F_ν. The same hold for the the non-archimedean absolute value $\nu_{\mathfrak{q}}$:

First, by a well known result on cyclotomic fields (cf. [23] 2.13), q factors in $p-1$ distinct prime ideals in $\mathbb{Q}(\zeta_p)$. Hence, q will factor in $(p-1)/2$ distinct prime ideals in F, i.e, is totally split. Hence, denoting by $\mathcal{O}_{F_{\nu_{\mathfrak{q}}}}$ the ring of integers of $F_{\nu_{\mathfrak{q}}}$, and (abusing notation), by $\mathfrak{q}$ the unique maximal ideal of $\mathcal{O}_{F_{\nu_{\mathfrak{q}}}}$, we have that $\mathcal{O}_{F_{\nu_{\mathfrak{q}}}}/\mathfrak{q} \cong \mathbb{F}_q$. Hence, if -1 were a square in $F_{\nu_{\mathfrak{q}}}$ (hence in $\mathcal{O}_{F_{\nu_{\mathfrak{q}}}}$), by reducing modulo $\mathfrak{q}$, we would have that $\left(\frac{-1}{q}\right) = 1$, a contradiction with the fact that $q \equiv 3 \pmod 4$.

This way, -1 is a non-square for each absolute value $\nu \in \Sigma$, and applying lemma 3.9 again, the result holds. □

Applying Theorem 3.6 and this proposition, we deduce the following corollary.

Corollary 3.11. *For any p odd prime, such that $p \equiv 1 \pmod 4$, there exist infinitely many Fuchsian codes with rate at least $3(p-1)/2$, related to $F = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. The corresponding quaternion algebras can be taken of the form $\left(\frac{a,-1}{F}\right)$, for an infinite family of elements $a \in F^*$.*

Proof. In the proof of proposition 3.10, we have freedom to choose among infinitely many primes q satisfying the two conditions

$$q \equiv 1 \pmod{p},$$
$$q \equiv 3 \pmod{4}.$$

For each of these primes q, we choose a prime ideal $\mathfrak{q}$ above q, yielding a quaternion algebra $\left(\frac{a_q,-1}{F}\right)$, ramifying at $\mathfrak{q}$ and at some archimedean primes. Since, due to the classification theorem, quaternion algebras ramifying at the same places are isomorphic, the elements a_q have to be distinct all of them.

Now, since the ring of integers of F is $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$, the Fuchsian code attached to each of the quaternion F-algebras $\left(\frac{a_q,-1}{F}\right)$ is defined to be image under the left regular representation of the natural order $\mathbb{Z}[\zeta_p + \zeta_p^{-1}][1, I, J, K]$, where $I^2 = a_q$. □

Remark 3.12. For a fixed $F = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, the previous proposition provides a method for choosing quaternion algebras over F in order to construct Fuchsian codes with rate $3(p-1)/2$. However, there are also other means to construct Fuchsian codes. For instance, for $p = 7$, by using Magma, we see that the quaternion algebra over F given by $a = b = \zeta_7 + \zeta_7^{-1}$ also satisfies the conditions and leads to Fuchsian codes of rate at least 9.

4. Arithmetic Fuchsian groups of signature $(1; e)$

In this section, we give an explicit construction for a particular family of Fuchsian groups derived from the so called arithmetic Fuchsian groups of signature $(1; e)$. Some of these Fuchsian groups were also considered in [4]. Here, we will deal with some Fuchsian groups derived from the arithmetic Fuchsian groups of signature $(1; e)$ defined over totally real fields. In the first subsection, we explicitly construct the Fuchsian codes attached to the arithmetic Fuchsian codes of signature $(1; e)$, while in the second subsection we provide numerical data to demonstrate that, at least in some example cases, higher code rate allows us to increase the codebook size (equivalently, data rate) for a fixed minimum distance and maximum transmission power (cf. Section 1). Future work consists of giving a rigorous proof for this fact.

4.1. **Explicit construction.**

Arithmetic Fuchsian groups were characterized in [18] by Takeuchi, who moreover classified and gave a complete list of them in the case of signature $(1; e)$ in [19], determining the associated quaternion algebra up

to isomorphism. We summarize below the main properties useful for this paper. We refer to the same references for algebraic details and proofs.

Proposition 4.1. *Let T be an arithmetic Fuchsian group of signature $(1;e)$ associated to a division quaternion algebra H. We can assume $-\mathrm{Id} \in T$. Then,*

i) The genus of the compact Riemmann surface $\mathcal{H}/T$ is 1.

ii) There exist $\alpha, \beta, \gamma \in T$ satisfying $\mathrm{Tr}(\alpha), \mathrm{Tr}(\beta) > 2$ and $\mathrm{Tr}(\gamma) = 2\cos\left(\frac{\pi}{e}\right)$, such that the group T admits a presentation of the form

$$T = \left\langle \alpha, \beta, \gamma \mid \alpha\beta\alpha^{-1}\beta^{-1}\gamma = -\mathrm{Id},\ \gamma^e = -\mathrm{Id} \right\rangle.$$

iii) A fundamental triple (α, β, γ) of generators of T is uniquely determined by $(x, y, z) = (\mathrm{Tr}(\alpha), \mathrm{Tr}(\beta), \mathrm{Tr}(\gamma))$, up to $\mathrm{GL}(2, \mathbb{R})$-conjugation.

Proposition 4.2. *Consider a group T as above, determined by the generators α, β, γ and (x, y, z) as above. Denote by $T^{(2)}$ the subgroup of T generated by $\{\gamma^2 \mid \gamma \in T\}$. Then,*

i) $T^{(2)}$ is a normal subgroup of T, and $[T : \{\pm Id\}T^{(2)}] = 4$.

ii) $T^{(2)} = \langle \alpha^2, \beta^2, \gamma, \alpha\gamma\alpha^{-1}, \beta\gamma\beta^{-1}, \alpha\beta\gamma\beta^{-1}\alpha^{-1} \rangle$.

iii) $T^{(2)}$ is a Fuchsian group derived from a quaternion algebra $\left(\frac{a,b}{F}\right)$, where $F = \mathbb{Q}(x^2, y^2, xyz)$, $a = x^2(x^2 - 4)$ and $b = -(2 + 2\cos(\pi/e)x^2y^2)$. In particular, $T^{(2)}$ is contained in the image by the regular representation of the group of units of reduced norm 1 of a maximal order of $\left(\frac{a,b}{F}\right)$.

The generators for the groups $T^{(2)}$ will be made explicit by using the following result on the groups T, proved by Sijsling, cf. [15].

Proposition 4.3. *Let T be an arithmetic Fuchsian group of signature $(1;e)$ generated by α and β. Then, after a change of variables, we can suppose that $\alpha = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ with λ an algebraic integer and $\beta = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$.*

We are interested in the explicit construction of codes attached to $\Gamma = T^{(2)}$ for several groups T in the list given by Takeuchi. Table 2 gives the parameters of the sample groups we will consider, using the same notation as in the previous propositions.

For each group $\Gamma = T_i^{(2)}$, the code construction process can be made explicit.

TABLE 2. Parameters of our sample groups

Group	(x, y, z)	e	F	a	b
T_1	$(\sqrt{5}, 2\sqrt{3}, \sqrt{15})$	2	$\mathbb{Q}$	5	-30
T_2	$\left(\sqrt{3+\sqrt{5}}, \sqrt{9+3\sqrt{5}}, \sqrt{6+\frac{9}{2}\sqrt{5}}\right)$	5	$\mathbb{Q}(\sqrt{5})$	$2+2\sqrt{5}$	$-6(25+11\sqrt{5})$
T_3	$\left(\sqrt{3+\sqrt{3}}, \sqrt{8+4\sqrt{3}}, \sqrt{9+5\sqrt{3}}\right)$	2	$\mathbb{Q}(\sqrt{3})$	$2\sqrt{3}$	$-3-2\sqrt{3}$
T_4	$\left(\sqrt{3+\sqrt{5}}, \sqrt{6+2\sqrt{5}}, \sqrt{7+3\sqrt{5}}\right)$	2	$\mathbb{Q}(\sqrt{5})$	$2+2\sqrt{5}$	$-14-6\sqrt{5}$
T_5	$\left(\sqrt{2+(1+\sqrt{13})/2}, \sqrt{16+4\sqrt{13}}, \sqrt{12+\frac{9}{2}(1+\sqrt{13})}\right)$	2	$\mathbb{Q}(\sqrt{13})$	$(-1+\sqrt{13})/2$	$-3(11+3\sqrt{13})$
T_6	$\left(\sqrt{3+\frac{1}{2}(1+\sqrt{5})}, \sqrt{14+6\sqrt{5}}, \sqrt{16+7\sqrt{5}}\right)$	5	$\mathbb{Q}(\sqrt{5})$	$(-1+3\sqrt{5})$	$-2(115+51\sqrt{5})$
T_7	$\left(\sqrt{3+\sqrt{3}}, \sqrt{14+6\sqrt{3}}, \sqrt{15+8\sqrt{3}}\right)$	6	$\mathbb{Q}(\sqrt{3})$	$6(4+\sqrt{3})$	$-3(31+18\sqrt{3})$

First, we can easily find the generators of $T_i^{(2)}$, by applying Proposition 4.3 to compute the explicit matrices α and β. Namely, given the trace triple (x, y, z), the equation $\mathrm{Tr}(\alpha) = \lambda + \lambda^{-1} = x$ will determine α; then, we obtain a by solving $\mathrm{Tr}(\beta) = 2a = y$; and finally, $\mathrm{Tr}(\alpha\beta) = z$ will give b, determining β. Thus, we have an explicit presentation of each group $\Gamma = T_i^{(2)}$.

The next step to construct our codes is to determine a fundamental domain for Γ in each case. Fundamental domains for several arithmetic Fuchsian groups over $\mathbb{Q}$ can be found in [1]. For the general totally real case, it is more complicated. In the present work, we have effectively computed them with the aid of *Mathematica* by using the explicit generators of the groups computed above.

Example 4.4. Let us consider $\Gamma = T_2^{(2)}$. The generators of the group, given in Proposition 4.2, are obtained from:

$$\alpha = \tfrac{1}{2}\begin{pmatrix} \sqrt{3+\sqrt{5}} - \sqrt{-1+\sqrt{5}} & 0 \\ 0 & \sqrt{3+\sqrt{5}} + \sqrt{-1+\sqrt{5}} \end{pmatrix};$$

$$\beta = \tfrac{1}{2}\begin{pmatrix} \sqrt{3(3+\sqrt{5})} & -\sqrt{5+3\sqrt{5}} \\ -\sqrt{5+3\sqrt{5}} & \sqrt{3(3+\sqrt{5})} \end{pmatrix}.$$

A fundamental domain for $\Gamma = T_2^{(2)}$ is displayed in Figure 1. Its edges are given by the isometric circles of the following transformations:

$$\alpha^2, \alpha^{-2}, \beta^2, \beta^{-2}, \gamma, \gamma^{-1}, \alpha^{-1}\beta\alpha\beta^{-1}, \left(\alpha^{-1}\beta\alpha\beta^{-1}\right)^{-1},$$
$$\alpha\beta^{-1}\alpha^{-1}\beta, \left(\alpha\beta^{-1}\alpha^{-1}\beta\right)^{-1}, \alpha^{-1}\beta^{-1}\alpha\beta, \left(\alpha^{-1}\beta^{-1}\alpha\beta\right)^{-1}.$$

Now we turn the attention to the design of the codes. We fix $\tau = i$ as the center of the code, and for each code size $q = 2N$, we have chosen a set of matrices $S_\Gamma = \{\gamma_1, ..., \gamma_N\}$ with the aim of minimizing the average energy $\frac{1}{N}\sum_{i=1}^{N} |\gamma_i(\tau)|^2$.

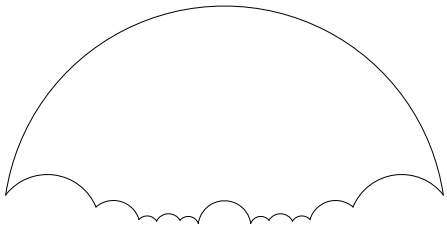

FIGURE 1. Fundamental domain for group $T_2^{(2)}$

We display in tables 3 and 4 the choices for the set of elements S_Γ for the sample groups $\Gamma = T_i^{(2)}$, giving 4-NUF and 16-NUF constellations.

TABLE 3. Choices for the 4-NUF codes

Group T_i	S_Γ, for $\Gamma = T_i^{(2)}$
T_1	$\pm\alpha^2$, $\pm\alpha\gamma\alpha^{-1}$
T_2	$\pm\alpha^2$, $\pm\alpha\gamma\alpha^{-1}$
T_3	$\pm\alpha^2$, $\pm\alpha\gamma\alpha^{-1}$
T_4	$\pm\alpha^2$, $\pm\alpha\gamma\alpha^{-1}$
T_5	$\pm Id$, $\pm\alpha^2$
T_6	$\pm\alpha^2$, $\pm\alpha\gamma\alpha^{-1}$
T_7	$\pm\alpha^2$, $\pm\alpha\gamma\alpha^{-1}$

TABLE 4. Choices for the 16-NUF codes

Group T_i	S_Γ, for $\Gamma = T_i^{(2)}$
T_1	$\pm\alpha^4$, $\pm\alpha^2\gamma$, $\pm\alpha^2\beta^2$, $\pm\alpha\gamma\alpha^{-1}\gamma$, $\alpha^3\gamma\alpha^{-1}$, $\pm\alpha^2\beta\gamma\beta^{-1}$, $\pm\alpha\gamma\beta\gamma\beta^{-1}\alpha^{-1}$, $\pm\alpha^3\beta\gamma\beta^{-1}\alpha^{-1}$
T_2	$\pm\alpha^2$, $\pm\alpha^4$, $\pm\alpha^2\gamma$, $\pm\alpha^2\beta^2$, $\pm\alpha\gamma\alpha^{-1}$, $\pm\alpha\gamma\alpha$, $\pm\alpha\gamma\alpha^{-1}\beta^2$, $\pm\alpha^3\beta\gamma\beta^{-1}\alpha^{-1}$
T_3	$\pm\alpha^2$, $\pm\alpha^4$, $\pm\alpha^2\gamma$, $\pm\alpha^3\gamma\alpha^{-1}$, $\pm\alpha^2\beta\gamma\beta^{-1}$, $\pm\alpha\gamma\alpha^{-1}\beta^2$, $\pm\alpha\gamma\beta\alpha^{-1}\beta^{-1}$, $\pm\alpha^3\beta\gamma\beta^{-1}\alpha^{-1}$
T_4	$\pm\alpha^2$, $\pm\alpha^4$, $\pm\alpha^2\gamma$, $\pm\alpha\gamma\alpha$, $\pm\alpha^3\gamma\alpha^{-1}$, $\pm\gamma\beta\gamma\beta^{-1}$, $\pm\alpha\gamma\alpha^{-1}\beta^2$, $\pm\alpha^3\beta\gamma\beta^{-1}\alpha^{-1}$
T_5	$\pm\alpha^2$, $\pm\alpha^4$, $\pm\alpha^2\gamma$, $\pm\alpha\gamma\alpha^{-1}$, $\pm\alpha^3\gamma\alpha^{-1}$, $\pm\alpha\gamma\alpha^{-1}\beta^2$, $\pm\alpha\gamma\alpha^{-1}\gamma$, $\pm\beta\gamma\beta^{-1}\alpha^2$
T_6	$\pm\alpha^2$, $\pm\alpha^4$, $\pm\alpha^2\gamma$, $\pm\alpha\gamma\alpha^{-1}$, $\pm\alpha^3\gamma\alpha^{-1}$, $\pm\alpha\gamma\alpha^{-1}\gamma$, $\pm\alpha^2\beta\gamma\beta^{-1}$, $\pm\alpha^3\beta\gamma\beta^{-1}\alpha^{-1}$
T_7	$\pm\alpha^2$, $\pm\alpha^4$, $\pm\alpha\gamma\alpha^{-1}$, $\pm\alpha^2\gamma$, $\pm\alpha\gamma\alpha^{-1}\gamma$, $\pm\alpha^3\gamma\alpha^{-1}$, $\pm\alpha^2\beta\gamma\beta^{-1}$, $\pm\alpha^3\beta\gamma\beta^{-1}\alpha^{-1}$

Given the choice of the center τ and S_Γ, the associated Fuchsian code is $\mathcal{C} = \{\pm\gamma(\tau) \mid \gamma \in S_\Gamma\} \subseteq \mathbb{C}$, taking in account the duplication to the lower half-plane. For instance, Figure 2 depicts a 4-NUF constellation for the group $T_2^{(2)}$.

Remark 4.5. In Takeuchi's list, the arithmetic Fuchsian groups of signature $(1; e)$ are defined over number fields of degree $1, 2, 3, 4, 5$ and 6. Hence, in an analogous way Fuchsian codes with data rates $3, 6, 9, 12, 15$ and 18 can be explicitly constructed.

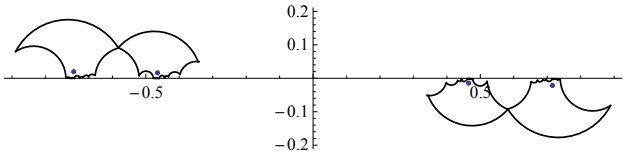

FIGURE 2. 4-NUF constellation and tiles for group $T_2^{(2)}$

4.2. **Numerical data.** Next, we show numerically in the case of Fuchsian codes attached to arithmetic Fuchsian groups of signature $(1; e)$, how a bigger code rate implies a bigger number of codewords with prescribed minimum distance fitting in a Euclidean ball. Hence, in this case, a higher code rate does indeed give us higher data rate without any penalty in the minimum distance or transmission power, along the same lines as for lattice codes, cf. Section 1.

Our approach is as follows: recall that the groups $\Gamma = T_2^{(2)}$ are generated by the elements α^2, β^2, γ, $\alpha\gamma\alpha^{-1}$, $\beta\gamma\beta^{-1}$ and $\alpha\beta\gamma\beta^{-1}\alpha^{-1}$. Using *Mathematica*, we have implemented an algorithm which generates a set of matrices consisting in: first, all the generators of Γ, second, all the possible matrices of the form $\gamma_1\gamma_2$, where γ_1, γ_2 runs over the set of generators, and then, we iterate this procedure until we have a desired number of matrices fixed beforehand. After that, our algorithm deletes the possible repeated matrices of the former stage. This way, we can construct a codebook of each desired size.

Once our codebook is constructed, we count how many codewords are there in the unit ball and in the ball of radius 0.5 for each of the groups T_i. The center of the code has been taken to be i. The minimum distance d (computed up to an accuracy of four decimal digits), in each case, is that of the bigger codebook, i.e., the one fitting inside the unit ball. Notice that, among our choice of codes, the minimum distance corresponds to a code of rate 6.

TABLE 5. Number of codewords inside Euclidean balls of radius $r = 1, 0.5$.

Group	Rate	$r = 1$	$r = 0.5$	d
T_1	3	72	36	0.0001
T_2	6	84	54	0.0005
$T3$	6	80	42	0.0002
$T4$	6	80	40	0.0001
$T5$	6	80	40	0.0003
$T6$	6	84	42	0.0002
$T7$	6	84	42	0.0002

5. Conclusions

In this paper, we have generalized the construction of the Fuchsian codes presented in [4] and [2] to the general case of Fuchsian groups over totally real fields. One of the main features of the codes in [4, 2] is that they have logarithmic decoding complexity. We have shown that by adapting the point reduction algorithm introduced in [3] to the present, more general case, the decoding complexity of the corresponding Fuchsian codes remains logarithmic in the codebook size, provided that we have a fundamental domain and a representation of the Fuchsian group.

In the case of Fuchsian groups Γ associated to quaternion algebras defined over a totally real number field, with an additional hypothesis about their ramification, we have proved that the Fuchsian code attached to Γ has rate at least $3n$, where n is the degree of the base field. This corresponds to at least $3n$-fold (resp. $3n/2$-fold) information compression in terms of the number of independent integers transmitted per codeword compared to the commonly used PAM (resp. QAM) alphabet. Moreover, we have deduced that there exist infinitely many Fuchsian codes of rate $3n$. In particular, by considering subfields of cyclotomic fields, we have made explicit the existence of infinitely many Fuchsian codes with rate $3\frac{p-1}{2}$. We have explicitly constructed Fuchsian codes attached to the groups $T^{(2)}$ for arithmetic Fuchsian groups T of signature $(1; e)$ classified by Takeuchi. Finally, the relevance of the code rate in terms of information compression and data rate has been numerically demonstrated.

Further research will consist of rigorously finding and proving a relation between the code rate and the data rate, and of the construction of an error-correcting outer system for our codes. Possible enabler of this is the excess of code rate that could be alternatively utilized for error correction, e.g., by using some kind of an analogy of a parity-check method. This would make our codes more suitable for the low-moderate SNR regime (SNR stands for the signal-to-noise ratio describing the channel quality), while at the moment the relevant application is the high-SNR regime. One instance of this is an optic-fiber channel.

References

[1] Alsina, M.; Bayer, P.: *Quaternion orders, quadratic forms and Shimura curves.* CRM Monograph Series, 22. American Mathematical Society, Providence, RI, 2004. xvi+196 pp. ISBN: 0-8218-3359-6.

[2] Blanco-Chacón, I.; Remón, D.; Hollanti, C.; Alsina, M.: Nonuniform Fuchsian codes for noisy channels. *Journal of the Franklin Institute* 351 (2014) 5076–5098.

[3] Bayer, P.; Remón, D.: A reduction point algorithm for cocompact Fuchsian groups and applications. Adv. Math. Commun. 8 (2014) 223–239.

[4] Blanco-Chacón, I.; Hollanti, C.; Remón, D.: Fuchsian codes for AWGN channels. PRE-PROCEEDINGS. The International Workshop on Coding and Cryptography, WCC 2013. p. 496–507. Bergen (2013). ISBN: 978-82-308-2269-2.

[5] Digital Video Broadcasting Consortium, *dvb.org*.

[6] Carvalho, E., Andrade, A., Palazzo, R., Filho, J.V.: Arithmetic Fuchsian groups and space–time block codes. Comput. Appl. Math. **30**, 485–498 (2011)

[7] Gertsenshtein, M., Vasilev, V.: Waveguides with random inhomogeneties and Brownian motion in the Lobachevsky plane. Theory Probab. Appl. **4**, 391–398 (1959)

[8] Hollanti, C., Lahtonen, J.: A new tool: Constructing STBCs from maximal orders in central simple algebras. In: IEEE Information Theory Workshop (ITW '06), Punta del Este, Uruguay, pp. 322–326 (2006)

[9] S. Johansson: On Fundamental Domains of Arithmetic Fuchsian Groups. *Math. Comp.* 69 (2000), no. 229, 339–349.

[10] Katok, S.: *Fuchsian Groups.* Chicago Lectures in Mathematics Series. The University of Chicago Press (1992).

[11] J. S. Milne: *Class field theory (4.02)* http://www.jmilne.org/math/CourseNotes/cft.html (2013)

[12] Oggier, F.; Viterbo, E.: Algebraic number theory and code design for Rayleigh fading channels. *Commun. Inf. Theory* 1(3) (2004), 333–416.

[13] Sethuraman, B.A., Rajan, B., Shashidhar, V.: Full-diversity, high-rate space–time block codes from division algebras. IEEE Transactions on Information Theory **49**(10), 2596–2616 (2003)

[14] G. Shimura: *Construction of class fields and zeta functions of algebraic curves*, Annals of Math., 85, 1967, 58-159.

[15] J. Sijsling: *Equations for arithmetic pointed tori*. Ph.D. Thesis, Universiteit Utrecht, 2010.

[16] da Silva, E.B., Firer, M., Costa, S.R., Palazzo, R.: Signal constellations in the hyperbolic plane: A proposal for new communication systems. Journal of the Franklin Institute **343**, 69–82 (2006)

[17] de Souza, M., Faria, M.B., Palazzo, R., Firer, M.: Edge-pairing isometries and counting dirichlet domains on the densest tessellation (12g-6,3) for signal set design. Journal of the Franklin Institute **349**, 1139–1152 (2012)

[18] Takeuchi, K.: A characterization of arithmetic Fuchsian groups. J. Math. Soc. Japan, 27, Number 4, 1975, 600-612.

[19] Takeuchi, K.: Arithmetic Fuchsian groups with signature $(1, e)$. J. Math. Soc. Japan, 35, Number 3, 1983, 381-407.

[20] Vieira, V.L., Palazzo, R., Faria, M.B.: On the arithmetic Fuchsian groups derived from quaternion orders. Proceedings of the International Telecommunications Symposium (ITS 2006), Fortaleza-Ce (Brazil) (2006)

[21] Vignéras, M. F.: *Arithmétique des algèbres de quaternions*. Lecture Notes in Mathematics 800. Springer, 1980. vii+169 pp. ISBN: 3-540-09983-2.

[22] J. Voight: Computing fundamental domains for Fuchsian groups. *J. Théorie des Nombres de Bordeaux* 21 (2009), 467–489.

[23] L.C. Washington: *Introduction to cyclotomic fields (second edition)*. Springer GTM, Number 83 (1982).

Department of Mathematics and Systems Analysis, Aalto University, Otakaari 1, M, FI-00076 Espoo, Finland

E-mail address: ivan.blancochacon@aalto.fi

Department of Mathematics and Systems Analysis, Aalto University, Otakaari 1, M, FI-00076 Espoo, Finland

E-mail address: camilla.hollanti@aalto.fi

Universitat Politècnica de Catalunya- BarcelonaTech, Dept. Applied Mathematics III - EPSEM,, University of Barcelona, Av. Bases de Manresa 61-73, 08242 Manresa (Spain)

E-mail address: montserrat.alsina@upc.edu

Faculty of Mathematics, University of Barcelona, Gran Via de les Corts Catalanes, 585, 08007 Barcelona, Spain

E-mail address: dremon@ub.edu