



HAL
open science

Computing arithmetic Kleinian groups

Aurel Page

► **To cite this version:**

Aurel Page. Computing arithmetic Kleinian groups. *Mathematics of Computation*, 2015, 84 (295), pp.2361-2390. 10.1090/S0025-5718-2015-02939-1 . hal-00703043v3

HAL Id: hal-00703043

<https://hal.science/hal-00703043v3>

Submitted on 20 Sep 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

COMPUTING ARITHMETIC KLEINIAN GROUPS

AUREL PAGE

ABSTRACT. Arithmetic Kleinian groups are arithmetic lattices in $\mathrm{PSL}_2(\mathbb{C})$. We present an algorithm that, given such a group Γ , returns a fundamental domain and a finite presentation for Γ with a computable isomorphism.

CONTENTS

Introduction	2
1. Arithmetic Kleinian groups	3
1.1. Hyperbolic geometry	3
1.2. The unit ball model	3
1.3. The Lobachevsky function and volumes of tetrahedra	4
1.4. Kleinian groups, Dirichlet domains and exterior domains	4
1.5. Quaternion algebras and arithmetic Kleinian groups	7
2. Algorithms	7
2.1. Algorithms for polyhedra in the hyperbolic 3-space	7
2.2. The reduction algorithm	10
2.3. Normalized basis algorithms	11
2.4. Instantiation of the blackboxes	16
2.5. Floating-point implementation	20
2.6. Master algorithm	22
3. Examples	23
3.1. Comparison between subalgorithms	23
3.2. Relation to previous work	24
3.3. A larger example	25
3.4. Efficiency of the algorithm	26
References	27

INTRODUCTION

An arithmetic Kleinian group Γ is a discrete subgroup of $\mathrm{PGL}_2(\mathbb{C})$ with finite volume that is commensurable with the image of the integral points of a form of GL_2 defined over a number field under the natural surjection $\mathrm{GL}_2(\mathbb{C}) \rightarrow \mathrm{PGL}_2(\mathbb{C})$. Our main results are new deterministic and probabilistic algorithms for constructing fundamental domains for the action of arithmetic Kleinian groups Γ on hyperbolic three-space that produce a finite presentation for Γ . There is a substantial literature concerning such algorithms, some of which we review below. We compare our algorithms to recent ones and discuss numerical evidence suggesting that ours are more efficient. The algorithm presented here prepares the ground for computing the cohomology of these groups with the action of Hecke operators, which gives a concrete realization of certain automorphic forms by the Matsushima-Murakami formula [BW00]. By the Jacquet-Langlands correspondence [JL70], such forms are essentially the same as automorphic forms for GL_2 over some number field. They should have attached Galois representations, but the construction of these representations in general is still an open problem. More generally, the integral (co)homology of such groups has recently received a lot of attention: for example the size of their torsion [BV13] and arithmetic functoriality [CV12] are being actively studied. Our algorithm allows for empirical study of these objects.

The problem of computing fundamental domains for such groups is well studied. In the analogous Fuchsian group case, i.e. a subgroup of $\mathrm{PSL}_2(\mathbb{R})$, an algorithm may have been known to Klein and J. Voight [Voi09] has described and implemented an efficient algorithm exploiting reduction theory. In the special case of Bianchi groups, i.e. when the base field is imaginary quadratic and the group is split, R.G. Swan [Swa71] has described an algorithm, which was implemented by Riley [Ril83] and A. Rahm [Rah10]; D. Yasaki [Yas10] has described and implemented another algorithm based on Voronoi theory. C. Corrales, E. Jaspers, G. Leal and Á. del Río [CJLdR04] have described an algorithm for the general Kleinian group case. They implemented it for one nonsplit group with imaginary quadratic base field. Our algorithm and implementation are more general, and experimentally more efficient in practice. We have recently found an unpublished algorithm of K. N. Jones and A. W. Reid, mentioned and briefly described in [CFJR01, section 3.1] that solves the same problem.

The article is organized as follows. In the first section we recall basic definitions and properties of hyperbolic geometry, quaternion algebras and Kleinian groups. In the second section we describe our algorithms: basic procedures to work in the hyperbolic 3-space, algorithms for computing a Dirichlet domain and a presentation with a computable isomorphism for a cocompact Kleinian group, and how to apply these algorithms to arithmetic Kleinian groups. In the third section we show examples produced by our implementation of these algorithms and comment on their running time.

I would like to thank John Voight for proposing me this project and supervising my master thesis, and Karim Belabas and Andreas Enge for their helpful comments on earlier versions of this article. Experiments presented in this paper were carried out using the PLAFRIM experimental testbed, being developed under the Inria PlaFRIM development action with support from LABRI and IMB and other entities: Conseil Régional d'Aquitaine, FeDER, Université de Bordeaux and CNRS (see <https://plafrim.bordeaux.inria.fr/>). This research was partially funded by ERC Starting Grant ANTICS 278537.

1. ARITHMETIC KLEINIAN GROUPS

Here we recall basic definitions and properties of hyperbolic geometry, quaternion algebras and Kleinian groups. The general reference for this section is [MR03].

1.1. Hyperbolic geometry. The reader can find more about hyperbolic geometry in [Rat06]. The *upper half-space* is the Riemannian manifold $\mathcal{H}^3 = \mathbb{C} \times \mathbb{R}_{>0}$ with Riemannian metric given by

$$ds^2 = \frac{dx^2 + dy^2 + dt^2}{t^2}$$

where $(z, t) \in \mathcal{H}^3$, $z = x + iy$ and $t > 0$. For $w, w' \in \mathcal{H}^3$, $d(w, w')$ is the distance between w and w' . The set $\mathbb{P}^1(\mathbb{C})$ is called the *sphere at infinity*. The upper half-space is a model of the hyperbolic 3-space, i.e. the unique connected, simply connected Riemannian manifold with constant sectional curvature -1 . In this space, the volume of the ball of radius r is $\pi(\sinh(2r) - 2r)$.

The group $\mathrm{PSL}_2(\mathbb{C})$ acts on \mathcal{H}^3 in the following way. Consider the ring of Hamiltonians $\mathbb{H} = \mathbb{C} + \mathbb{C}j$ with multiplication given by $j^2 = -1$ and $jz = \bar{z}j$ for $z \in \mathbb{C}$, and identify \mathcal{H}^3 with the subset $\mathbb{C} + \mathbb{R}_{>0}j \subset \mathbb{H}$. Then for an element $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$ and $w \in \mathcal{H}^3$, the formula

$$g \cdot w = (aw + b)(cw + d)^{-1} = (wc + d)^{-1}(wa + b)$$

defines an action of $\mathrm{PSL}_2(\mathbb{C})$ on \mathcal{H}^3 by orientation-preserving isometries. This action is transitive and the stabilizer of the point $j \in \mathcal{H}^3$ in $\mathrm{PSL}_2(\mathbb{C})$ is the subgroup $\mathrm{PSU}_2(\mathbb{C})$.

The trace of an element of $\mathrm{PSL}_2(\mathbb{C})$ is defined up to sign, and we have the following classification of conjugacy classes in $\mathrm{PSL}_2(\mathbb{C})$:

- If $\mathrm{tr}(g) \in \mathbb{C} \setminus [-2, 2]$, then g has two distinct fixed points in $\mathbb{P}^1(\mathbb{C})$, no fixed point in \mathcal{H}^3 and stabilizes the geodesic between its fixed points, called its *axis*. The element g is conjugate to $\pm \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ with $|\lambda| > 1$; it is called *loxodromic*.
- If $\mathrm{tr}(g) \in (-2, 2)$, then g has two distinct fixed points in $\mathbb{P}^1(\mathbb{C})$, and fixes every point in the geodesic between these two fixed points. The element g is conjugate to $\pm \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$ with $\theta \in \mathbb{R} \setminus (\pi + 2\pi\mathbb{Z})$; it is called *elliptic*.
- If $\mathrm{tr}(g) = \pm 2$, then g has one fixed point in $\mathbb{P}^1(\mathbb{C})$ and no fixed point in \mathcal{H}^3 . It is conjugate to $\pm \begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix}$; it is called *parabolic*.

1.2. The unit ball model. In actual computations we are going to work with another model of the hyperbolic 3-space. The *unit ball* \mathcal{B} is the open ball of center 0 and radius 1 in $\mathbb{R}^3 \cong \mathbb{C} + \mathbb{R}j \subset \mathbb{H}$, equipped with the Riemannian metric

$$ds^2 = \frac{4(dx^2 + dy^2 + dt^2)}{(1 - |w|^2)^2}$$

where $w = (z, t) \in \mathcal{B}$, $z = x + iy$ and $|w|^2 = x^2 + y^2 + t^2 < 1$. The *sphere at infinity* $\partial\mathcal{B}$ is the Euclidean sphere of center 0 and radius 1. The distance between two points $w, w' \in \mathcal{B}$ is given by the explicit formula

$$d(w, w') = \cosh^{-1} \left(1 + 2 \frac{|w - w'|^2}{(1 - |w|^2)(1 - |w'|^2)} \right).$$

The upper half-space and the unit ball are isometric, the isometry being given by

$$\eta: \begin{cases} \mathcal{H}^3 \longrightarrow \mathcal{B} \\ w \longmapsto (w - j)(1 - jw)^{-1} = (1 - wj)^{-1}(w - j), \end{cases}$$

and the corresponding action of an element $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{C})$ on a point $w \in \mathcal{B}$ is given by

$$(1) \quad g \cdot w = (Aw + B)(Cw + D)^{-1}$$

where

$$\begin{aligned} A &= a + \bar{d} + (b - \bar{c})j, & B &= b + \bar{c} + (a - \bar{d})j, \\ C &= c + \bar{b} + (d - \bar{a})j, & D &= d + \bar{a} + (c - \bar{b})j. \end{aligned}$$

In the unit ball model, the geodesic planes are the intersections with \mathcal{B} of Euclidean spheres and Euclidean planes orthogonal to the sphere at infinity, and the geodesics are the intersections with \mathcal{B} of Euclidean circles and Euclidean straight lines orthogonal to the sphere at infinity. A *half-space* is an open connected subset of \mathcal{B} with boundary consisting of a geodesic plane. A *convex polyhedron* is the intersection of a set of half-spaces, such that the corresponding set of geodesic planes is locally finite.

1.3. The Lobachevsky function and volumes of tetrahedra. We are going to compute hyperbolic volumes, and for this the main tool is going to be the Lobachevsky function, which we define here. The integral

$$- \int_0^\theta \ln |2 \sin u| \, du$$

converges for $\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$ and admits a continuous extension to \mathbb{R} that is odd and periodic with period π . This extension is called the *Lobachevsky function* $\mathcal{L}(\theta)$. The Lobachevsky function admits a power series expansion, converging for $\theta \in [-\pi, \pi]$:

$$\mathcal{L}(\theta) = \theta \left(1 - \ln(2|\theta|) + \sum_{n=1}^{\infty} \frac{\zeta(2n)}{n(2n+1)} \left(\frac{\theta}{\pi}\right)^{2n} \right).$$

With this function we can derive a formula for the volume of a certain standard tetrahedron. We will use it to compute the volume of convex polyhedra.

Proposition 1. *Let T be the tetrahedron in \mathcal{H}^3 with one vertex at ∞ and the other vertices A, B, C on the unit hemisphere projecting vertically onto A', B', C' in \mathbb{C} with $A' = 0$ to form a Euclidean triangle, with angles $\frac{\pi}{2}$ at B' and α at A' , and such that the angle along BC is γ . Then the volume of T is finite and given by*

$$\mathrm{Vol}(T) = \frac{1}{4} \left[\mathcal{L}(\alpha + \gamma) + \mathcal{L}(\alpha - \gamma) + 2\mathcal{L}\left(\frac{\pi}{2} - \alpha\right) \right].$$

Proof. This formula can be found in [MR03, paragraph 1.7]. □

1.4. Kleinian groups, Dirichlet domains and exterior domains. A subgroup Γ of $\mathrm{PSL}_2(\mathbb{C})$ is a *Kleinian group* if it acts discontinuously on \mathcal{H}^3 , or equivalently if it is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{C})$. A *fundamental domain* for Γ is an open subset \mathcal{F} of \mathcal{H}^3 such that

- (i) $\bigcup_{\gamma \in \Gamma} \gamma \bar{\mathcal{F}} = \mathcal{H}^3$;
- (ii) For all $\gamma \in \Gamma \setminus \{1\}$, $\mathcal{F} \cap \gamma \mathcal{F} = \emptyset$;
- (iii) $\mathrm{Vol}(\partial \mathcal{F}) = 0$

where Vol is the Riemannian volume on \mathcal{H}^3 . To compute a fundamental domain for a Kleinian group Γ , we are going to use the standard construction of Dirichlet domains. Let $p \in \mathcal{B}$ be a point with trivial stabilizer in Γ . Then the *Dirichlet domain* centered at p

$$D_p(\Gamma) = \{x \in \mathcal{B} \mid \text{for all } \gamma \in \Gamma \setminus \{1\}, d(x, p) < d(x, \gamma p)\}$$

is a convex fundamental polyhedron for Γ . If Γ has finite covolume, then the closure of $D_p(\Gamma)$ has finitely many faces. A Kleinian group Γ is *geometrically finite* if the closure of one (equivalently, every) Dirichlet domain for Γ has finitely many faces.

Note that since Γ acts properly discontinuously on \mathcal{B} , every point outside a zero measure, closed subset of \mathcal{B} has a trivial stabilizer in Γ . In the unit ball model, the Dirichlet domain centered at 0 has a simple description. Consider an element $g \in \mathrm{SL}_2(\mathbb{C})$ not fixing 0 $\in \mathcal{B}$. Let

- $I(g) = \{w \in \mathcal{B} \mid d(w, 0) = d(gw, 0)\}$;
- $\mathrm{Ext}(g) = \{w \in \mathcal{B} \mid d(w, 0) < d(gw, 0)\}$;
- $\mathrm{Int}(g) = \{w \in \mathcal{B} \mid d(w, 0) > d(gw, 0)\}$.

We call $I(g)$ the *isometric sphere* of g . For a subset $S \subset \mathrm{SL}_2(\mathbb{C})$ such that no element of S fixes 0, the *exterior domain* of S is $\mathrm{Ext}(S) = \bigcap_{g \in S} \mathrm{Ext}(g)$. The set S is a *defining set* for $\mathrm{Ext}(S)$. A *minimal defining set* for $\mathrm{Ext}(S)$ is a subset $S' \subset S$ such that $\mathrm{Ext}(S') = \mathrm{Ext}(S)$ and for all $g \in S'$, the geodesic plane $I(g)$ contains a face of $\overline{\mathrm{Ext}(S)}$.

With these definitions it is clear that $D_0(\Gamma) = \mathrm{Ext}(\Gamma \setminus \{1\})$. Note that for all $p \in \mathcal{B}$ with trivial stabilizer in Γ , $D_p(\Gamma) = uD_0(u^{-1}\Gamma u)$ where $u \in \mathrm{PSL}_2(\mathbb{C})$ is such that $p = u \cdot 0$, so there is no harm in restricting to the Dirichlet domain centered at 0. Consider an element $g \in \mathrm{SL}_2(\mathbb{C})$ and A, B, C, D as in formula (1). Then $g \cdot 0 = 0$ if and only if $C = 0$ and, if g does not fix 0, then a simple but lengthy computation reveals that $I(g)$ is the intersection of \mathcal{B} and the Euclidean sphere of center w and radius r , where

$$(2) \quad w = -C^{-1}D \text{ and } r = 2/|C|,$$

and that $\mathrm{Int}(g)$ is the interior of this sphere. The details are in [Pag10, Proposition 3.1.6].

Another property of Dirichlet domains is their rich structure: it gives a presentation for the group, and also necessary and sufficient conditions for an exterior domain to be a fundamental domain. Suppose Γ is a Kleinian group in which 0 has trivial stabilizer, and let $g, h \in \Gamma$. Then we have $I(g) = I(h)$ if and only if $g = h$. We also have $gI(g) = I(g^{-1})$, and a point $x \in I(g)$ is in the defining set of $D_0(\Gamma)$ if and only if $gx \in I(g^{-1})$ is too.

From this, we can group the faces of $\overline{D_0(\Gamma)}$ in pairs, one contained in some $I(g)$ and the other contained in $I(g^{-1})$, and g, g^{-1} send the faces to each other. This is the *face pairing* structure, and the elements g such that $I(g)$ contains a face of $\overline{D_0(\Gamma)}$ are called the *face pairing transformations*. They generate the group Γ .

Now we are going to look for relations. The first type comes from edge cycles: consider an edge e_1 of $\overline{D_0(\Gamma)}$ contained in some $I(g) \cap I(h)$, and let $g_1 = g$. We define inductively a sequence of edges and elements in Γ in the following way. We let $e_{n+1} = g_n e_n$. Then e_{n+1} is contained in $I(g_n^{-1}) \cap I(g_{n+1})$ for a unique $I(g_{n+1})$ (see Figure 1.1). If $\overline{D_0(\Gamma)}$ has finitely many faces, then the sequence $(e_n, g_n)_n$ is periodic, let m be its period. The sequence of edges $C = (e_1, \dots, e_m)$ is a *cycle* of edges, and m is its *length*. The *cycle transformation* at e_1 is $h = g_m g_{m-1} \dots g_1$, and has the property:

- (i) The cycle transformation at e_1 fixes e_1 pointwise.

This implies that h satisfies the *cycle relation* $h^\nu = 1$ for some integer ν . If $\nu \neq 1$, the cycle is called *elliptic*. At every edge e_i , the geodesic planes $I(g_i^{-1})$ and $I(g_{i+1})$ make an angle $\alpha(e_i)$ inside $D_0(\Gamma)$. The *cycle angle* of C is $\alpha(C) = \sum_{i=1}^m \alpha(e_i)$. Since the translates of $D_0(\Gamma)$ cover a neighborhood of e_1 , we have the property:

- (ii) The cycle angle is $\frac{2\pi}{\nu}$ where ν is the order of the cycle transformation.

The second type of relations comes from elements of order 2: it may happen that $I(g) = I(g^{-1})$, then the element g satisfies the *reflection relation* $g^2 = 1$.

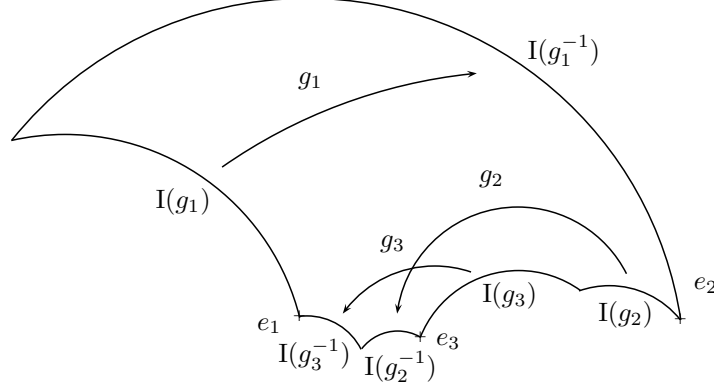


FIGURE 1.1. A length three cycle in a planar cut

Theorem 2 (Poincaré). *Let $D = D_0(\Gamma)$ be the Dirichlet domain of a geometrically finite Kleinian group Γ . Then the face pairing transformations generate the group Γ , and the reflection relations together with the cycle relations form a complete set of relations for Γ .*

Remark 3. In the presentation given by the theorem we consider only one element for each pair of face-pairing transformation g, g^{-1} . If we take both in the set of generators, we have to add the “inverse” relation $g g^{-1} = 1$.

We are now looking for sufficient conditions for an exterior domain to be a fundamental domain. There is another necessary condition, coming from cycles of some special points at infinity. A point $z \in \partial\mathcal{B}$ is a *tangency vertex* if it is a point of tangency $z = f \cap f'$ of two faces $f \subset I(g), f' \subset I(g')$ of $D_0(\Gamma)$. If $z_1 = I(g_0) \cap I(g_1)$ is a tangency vertex, then we define a sequence by letting $z_{i+1} = g_i \cdot z_i = I(g_i^{-1}) \cap I(g_{i+1})$ while z_{i+1} is a tangency vertex (otherwise the sequence ends at z_i). If such a sequence (z_i) is infinite and $D_0(\Gamma)$ has finitely many faces, then it is periodic. Let m be its period; then (z_1, \dots, z_m) is a *tangency vertex cycle* and the *tangency vertex transformation* is $h = g_m g_{m-1} \dots g_1$. The fact that \mathcal{B}/Γ is complete implies the property:

(iii) The tangency vertex transformation is parabolic.

Actually all these definitions can make sense for any exterior domain. Suppose $\text{Ext}(S)$ is an exterior domain with $S \subset \Gamma$ a finite minimal defining set. We say that it has a face pairing if $S = S^{-1}$ and for every $g \in S$ the image by g of the face contained in $I(g)$ is the face contained in $I(g^{-1})$ – equivalently, the image of every edge of $\overline{\text{Ext}(S)}$ by the pairing transformation of an adjacent face is an edge of $\overline{\text{Ext}(S)}$. This implies that every cycle is well-defined. We say that it satisfies the *cycle condition* if every cycle satisfies the properties (i) and (ii), and that it is *complete* if every tangency vertex cycle satisfies the property (iii).

Theorem 4 (Poincaré). *Let $D = \text{Ext}(S)$ be an exterior domain with S finite. Suppose D has a face pairing, satisfies the cycle condition, and is complete. Let Γ' be the group generated by the face pairing transformations. Then D is a fundamental polyhedron for Γ' .*

Proof. Both theorems are a special case of the second Theorem in [Mas71]. \square

1.5. Quaternion algebras and arithmetic Kleinian groups. We can now describe the construction of arithmetic Kleinian groups using orders in quaternion algebras. The reader can find more about quaternion algebra in [Vig80]. A *quaternion algebra* B over a field F is a central simple algebra of dimension 4 over F . Equivalently, if $\text{char } F \neq 2$, there exists $a, b \in F^\times$ such that $B = F + Fi + Fj + Fij$ with multiplication table given by $i^2 = a$, $j^2 = b$, $ji = -ij$. Such an algebra is written $B = \left(\frac{a,b}{F}\right)$. A quaternion algebra either is isomorphic to the matrix ring $\mathcal{M}_2(F)$, or is a division algebra. Given an element $w = x + yi + zj + tij \in \left(\frac{a,b}{F}\right)$, we define its *conjugate* $\bar{w} = x - yi - zj - tij$, its *reduced trace* $\text{trd}(w) = w + \bar{w} = 2x \in F$ and its *reduced norm* $\text{nrd}(w) = w\bar{w} = x^2 - ay^2 - bz^2 + abt^2 \in F$.

Let F be a number field, let \mathbb{Z}_F be its ring of integers and let B be a quaternion algebra over F . An *order* $\mathcal{O} \subset B$ is a finitely generated \mathbb{Z}_F -submodule with $F\mathcal{O} = B$ that is also a subring. We write $\mathcal{O}^1 \subset \mathcal{O}^\times$ the subgroup of elements of reduced norm 1.

A place v of F is *split* or *ramified* depending on whether $B \otimes_F F_v$ is isomorphic to the matrix ring or not. The set of ramified places is finite and the *discriminant* of B is the product of the ramified finite places, viewed as an ideal in \mathbb{Z}_F . The number field F is *almost totally real* (or *ATR*) if it has exactly one complex place. A quaternion algebra over an ATR field is *Kleinian* if it is ramified at every real place.

Theorem 5. *Let F be an ATR number field of degree n , B a Kleinian quaternion algebra over F and \mathcal{O} be an order in B . Let $\rho : B \hookrightarrow \mathcal{M}_2(\mathbb{C})$ be an algebra homomorphism extending a complex embedding of F . Then the group $\Gamma(\mathcal{O}) = \rho(\mathcal{O}^1)/\{\pm 1\} \subset \text{PSL}_2(\mathbb{C})$ is a Kleinian group. It has finite covolume, and it is cocompact if and only if B is a division algebra. Furthermore, if \mathcal{O} is maximal, we have*

$$(3) \quad \text{Covol}(\Gamma(\mathcal{O})) = \frac{|\Delta_F|^{3/2} \zeta_F(2) \Phi(\Delta_B)}{(4\pi^2)^{n-1}}$$

where Δ_F is the discriminant of F , ζ_F is the Dedekind zeta function of F , Δ_B is the discriminant of B and $\Phi(\mathfrak{N}) = N(\mathfrak{N}) \cdot \prod_{\mathfrak{p}|\mathfrak{N}} (1 - N(\mathfrak{p})^{-1})$ for every ideal \mathfrak{N} of F .

Proof. This theorem can be found in [MR03, Theorems 8.2.2, 8.2.3 and 11.1.3]. \square

An *arithmetic Kleinian group* is a Kleinian group that is commensurable with a group $\Gamma(\mathcal{O})$ as in the previous theorem. This is equivalent to the definition given in the introduction. The object of the next section is to describe an algorithm that, given such a group, computes a fundamental domain for $\Gamma(\mathcal{O})$, and a presentation with a computable isomorphism.

2. ALGORITHMS

We describe every algorithm in ideal arithmetic. In section 2.5, we explain how to implement these algorithms using floating-point arithmetic.

2.1. Algorithms for polyhedra in the hyperbolic 3-space. We start with low-level algorithms for dealing with hyperbolic polyhedra. A point in \mathcal{B} is represented by a vector in $\mathbb{C} + \mathbb{R}j$; a geodesic plane not containing 0 is represented by the Euclidean center and radius of the corresponding Euclidean sphere; a geodesic not containing 0 is represented by the Euclidean center and radius of a Euclidean sphere and a basis of a Euclidean plane containing the center of the sphere, such that the geodesic is the intersection of \mathcal{B} , this sphere and this plane.

Using these representations, it is an exercise in computational geometry to see that we can compute the faces, edges and vertices of a convex polyhedron given by a finite set of half-spaces containing 0. The details can be found in [Pag10, section II.3.3]. A harder task is to compute the volume of such a polyhedron. We describe an algorithm here; it is essentially the same as the one described in [MR03, section 1.7] but for the sake of completeness we provide all the details here.

Algorithm 1 computes the volume of a convex polyhedron with finitely many faces.

Algorithm 1 Volume of a convex polyhedron

Input: A convex polyhedron P with finitely many faces

Output: The hyperbolic volume of P

- 1: Split every face of P into triangles
 - 2: Split P into tetrahedra
 - 3: Using the map η^{-1} , send every tetrahedron back to \mathcal{H}^3
 - 4: Express every tetrahedron as a difference of two tetrahedra, each having a vertex in the sphere at infinity
 - 5: For every tetrahedron having a vertex in the sphere at infinity, apply an isometry to map it to a tetrahedron with one vertex at ∞ and the other vertices on the unit hemisphere
 - 6: Express every such tetrahedron as a sum and difference of tetrahedra of the same type having one vertex at j
 - 7: Express every such tetrahedron as a sum and difference of tetrahedra of the same type with projected Euclidean triangle having a right angle not at 0
 - 8: For every such tetrahedron, compute the angles α and γ and use Proposition 1 to compute the volume
 - 9: $\text{Vol}(P) \leftarrow$ sum of every contribution
 - 10: **return** $\text{Vol}(P)$
-

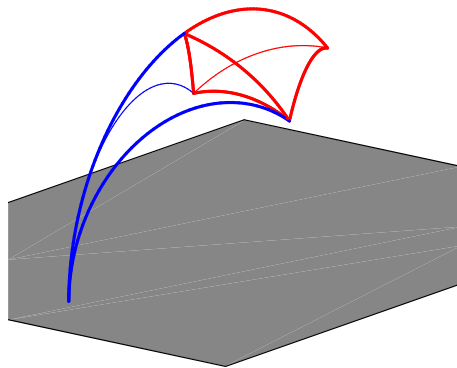


FIGURE 2.1. Step 4 in Algorithm 1

Remarks 6.

- For step 1, choose a vertex of the face and link it to every other vertex;
- For step 2, choose a vertex of P and link it to every computed triangle;

- For step 4, choose an edge and consider a geodesic ray containing it, then the tetrahedron appears as the difference between two tetrahedra, each having the geodesic ray as an edge and a face of the initial tetrahedron as a base (see Figure 2.1);
- In step 6, the signs that appear in the sum are the signs of certain determinants;
- In step 8, the angle α is an angle in a Euclidean triangle and can be computed by elementary trigonometry, and since the upper half-space model is conformal, the angle γ is the Euclidean angle of intersection of the sphere and plane representing the faces of the tetrahedron.

The values of the Lobachevsky function are computed with the following lemma. It may be well-known, but we include it for the sake of completeness.

Lemma 7. *For all $\theta \in (-\pi, \pi)$ we have the formula*

$$\mathcal{L}(\theta) = \pi \ln \left(\frac{\pi - \theta}{\pi + \theta} \right) + \theta \left(3 - \ln \left[2|\theta| \left(1 - \left(\frac{\theta}{\pi} \right)^2 \right) \right] \right) + \sum_{n=1}^{\infty} \frac{\zeta(2n) - 1}{n(2n+1)} \left(\frac{\theta}{\pi} \right)^{2n}$$

and the bounds

$$\begin{aligned} \sum_{n>r} \frac{\zeta(2n)}{n(2n+1)} \left(\frac{\theta}{\pi} \right)^{2n} &\leq \frac{2}{3} \frac{1}{1 - \left(\frac{\theta}{\pi} \right)^2} \left(\frac{\theta}{\pi} \right)^{2r+2} \\ \sum_{n>r} \frac{\zeta(2n) - 1}{n(2n+1)} \left(\frac{\theta}{\pi} \right)^{2n} &\leq \frac{1}{1 - \left(\frac{\theta}{2\pi} \right)^2} \left(\frac{\theta}{2\pi} \right)^{2r+2}. \end{aligned}$$

Proof. To derive the first expression we use the previous power series expansion and extract the first term of the series expansion of the zeta function. For all $\theta \in (-\pi, \pi)$ we have

$$\sum_{n=1}^{\infty} \frac{\zeta(2n)}{n(2n+1)} \left(\frac{\theta}{\pi} \right)^{2n} = \sum_{n=1}^{\infty} \frac{1}{n(2n+1)} \left(\frac{\theta}{\pi} \right)^{2n} + \sum_{n=1}^{\infty} \frac{\zeta(2n) - 1}{n(2n+1)} \left(\frac{\theta}{\pi} \right)^{2n}$$

since all these series converge. We only need to compute the power series that appears. By taking derivatives twice we find that for all $x \in (-1, 1)$ we have

$$\sum_{n=1}^{\infty} \frac{x^{2n+1}}{n(2n+1)} = 2x - x \ln(1 - x^2) + \ln \left(\frac{1-x}{1+x} \right).$$

Letting $x = \frac{\theta}{\pi}$ in this expression gives the first formula.

To prove the inequalities we are going to bound the values $\zeta(2n)$ and $\zeta(2n) - 1$ for $n \geq 1$. By series-integral comparison we get

$$\sum_{k=r}^{\infty} k^{-2n} \leq \frac{(r-1)^{1-2n}}{2n-1},$$

giving

$$\zeta(2n) = 1 + \sum_{k=2}^{\infty} k^{-2n} \leq 1 + \frac{1}{2n-1} \leq 2$$

for the first value, and

$$\zeta(2n) - 1 = 2^{-2n} + \sum_{k=3}^{\infty} k^{-2n} \leq \left(1 + \frac{2}{2n-1} \right) 2^{-2n} \leq 3 \cdot 2^{-2n}$$

for the second one. Using these inequalities and the bound $\frac{1}{n(2n+1)} \leq \frac{1}{3}$, and computing the geometric sum gives the result. \square

Remarks 8.

- With the same method, for any k we can obtain a formula with remainder term $O\left(\left(\frac{\theta}{k\pi}\right)^{2r}\right)$.
- In practise, we precompute the coefficients of the power series we are using. By periodicity and oddness, we can always reduce to the case where $\theta \in [0, \frac{\pi}{2}]$: if the precision is fixed, we know a priori the maximal number of terms needed to evaluate the Lobachevsky function.

2.2. The reduction algorithm. When we have a fundamental domain, it is natural to ask for an algorithm that, given a point in the hyperbolic 3-space, computes an equivalent point in the fundamental domain and an element in the group that sends one point to the other.

Definition 9. Let S be a subset of a Kleinian group Γ . A point $z \in \mathcal{B}$ is S -reduced if for all $g \in S$, we have $d(z, 0) \leq d(gz, 0)$, i.e. if $z \in \overline{\text{Ext}(S)}$.

Algorithm 2 Reduction algorithm

Input: A point $w \in \mathcal{B}$, a finite ordered subset $S \subset \text{PSL}_2(\mathbb{C})$

Output: A point w' and an element $\delta \in \langle S \rangle$ s.t. w' is S -reduced and $w' = \delta w$

- 1: $w' \leftarrow w, \delta \leftarrow 1$
 - 2: $g \leftarrow 1$
 - 3: **repeat**
 - 4: $w' \leftarrow gw', \delta \leftarrow g\delta$
 - 5: $g \leftarrow$ the first $g \in S$ such that $d(gw', 0)$ is minimal
 - 6: **until** $d(gw', 0) \geq d(w', 0)$
 - 7: **return** w', δ
-

Proposition 10. Given S a finite subset of a Kleinian group Γ and a point $w \in \mathcal{B}$, Algorithm 2 returns a point w' and $\delta \in \langle S \rangle$ such that w' is S -reduced and $w' = \delta w$.

Proof. After step 4, we have $w' = \delta w$ and $\delta \in \langle S \rangle$. Because of the loop condition, while the algorithm runs the distance $d(w', 0)$ decreases. Since w' stays in the orbit of w under Γ and this orbit is discrete, the algorithm terminates. When it happens, g is an element in S such that $d(gw', 0)$ is minimal and $d(gw', 0) \geq d(w', 0)$, so w' is S -reduced. \square

Remark 11. At step 5, the g achieving the minimal $d(gw', 0)$ may not be unique. We can pick any of these elements. Ordering S gives us a canonical choice.

Reducing points can give interesting information about the elements of the group, because if w has a trivial stabilizer, then the orbit map $\gamma \mapsto \gamma \cdot w$ is a bijection. This is the reason for introducing the following definition:

Definition 12. Let S be a subset of a Kleinian group Γ and $w \in \mathcal{B}$. An element $\gamma \in \text{PSL}_2(\mathbb{C})$ is (S, w) -reduced if γw is S -reduced, i.e. if $\gamma w \in \overline{\text{Ext}(S)}$.

Given a finite S , w and γ , we can now compute an (S, w) -reduced element $\bar{\gamma}$ such that $\bar{\gamma} \equiv \gamma \pmod{S}$ as follows: we reduce γw with respect to S ; if $\delta \in \langle S \rangle$ is such that $\delta(\gamma w)$ is S -reduced, then $\bar{\gamma} = \delta\gamma$ is (S, w) -reduced. We also write the reduced element $\bar{\gamma} = \text{Red}_S(\gamma; w)$ and simply $\text{Red}_S(\gamma) = \text{Red}_S(\gamma; 0)$. A priori this reduced element could depend on the chosen ordering in Algorithm 2.

Proposition 13. Suppose that $\text{Ext}(S)$ is a fundamental domain for $\langle S \rangle$. Then for $w \in \mathcal{B}$ outside of a zero measure, closed subset of \mathcal{B} , the following holds: for every $\gamma \in \Gamma$, there exists a unique (S, w) -reduced $\bar{\gamma} \equiv \gamma \pmod{S}$. If $w \in \text{Ext}(S)$ then $\bar{\gamma} = 1$ if and only if $\gamma \in \langle S \rangle$.

Proof. Let $w \in \Gamma \cdot \text{Ext}(S)$. The existence follows from Algorithm 2. For uniqueness, suppose $\bar{\gamma}$ and $\bar{\gamma}'$ are (S, w) -reduced and $\bar{\gamma} \equiv \bar{\gamma}' \equiv \gamma \pmod{S}$. Then $\bar{\gamma}w, \bar{\gamma}'w \in \text{Ext}(S)$, and since w is in the orbit of $\text{Ext}(S)$, they are in fact in $\text{Ext}(S)$. Since these two points are in the same $\langle S \rangle$ -orbit, we have $\bar{\gamma} = \bar{\gamma}'$. Now assume $w \in \text{Ext}(S)$. If $\bar{\gamma} = 1$ then $\gamma \equiv \bar{\gamma} \equiv 1 \pmod{S}$, i.e. $\gamma \in \langle S \rangle$. If $\gamma \in \langle S \rangle$ then $\gamma \equiv 1 \pmod{S}$ and 1 is (S, w) -reduced so by uniqueness $\bar{\gamma} = 1$. Moreover the complement of $\Gamma \cdot \text{Ext}(S)$ in \mathcal{B} is a locally finite union of faces of $\text{Ext}(S)$, so it is closed with zero measure. \square

Since this provides an algorithm to write an element of the group as a word in the generators and to compute modulo $\langle S \rangle$ with explicit unique representatives, that particular kind of generating set deserves a name.

Definition 14. A subset S of a Kleinian group Γ is a *basis* if $\text{Ext}(S)$ is a fundamental domain for $\langle S \rangle = \Gamma$. If S is also a minimal defining set for $\text{Ext}(S)$, it is called a *normalized basis* for Γ .

2.3. Normalized basis algorithms. Now we describe a general algorithm that computes a normalized basis for a cocompact Kleinian group Γ . We will then apply it to arithmetic groups. First note that, after conjugating the group by a suitable element in $\text{PSL}_2(\mathbb{C})$, we may assume that $0 \in \mathcal{B}$ has a trivial stabilizer in Γ and that every elliptic cycle has length 1.

We will use two blackbox subalgorithms, `Enumerate` and `IsFullGroup`:

- `Enumerate(Γ, n)` takes as an input a positive integer n and returns a finite set of elements in Γ (the integer n is a parameter for iteration, it does not have any mathematical meaning);
- `IsFullGroup(Γ, S)` takes as an input a finite normalized basis S for a subgroup $\langle S \rangle \subset \Gamma$ and returns **true** or **false** according to whether $\langle S \rangle = \Gamma$ or not.

In every algorithm, an exterior domain $\text{Ext}(S)$ with finite S is represented as a polyhedron in \mathcal{B} . We begin with a naive algorithm.

Algorithm 3 Naive normalized basis algorithm

Input: A Kleinian group Γ

Output: A normalized basis S for Γ

- 1: $S \leftarrow \emptyset, n \leftarrow 0$
 - 2: **repeat**
 - 3: **repeat**
 - 4: $n \leftarrow n + 1$
 - 5: add `Enumerate(Γ, n)` to S
 - 6: $S \leftarrow$ minimal defining set of $\text{Ext}(S)$
 - 7: **until** $\text{Ext}(S)$ has a face-pairing **and** $\text{Ext}(S)$ is complete **and** $\text{Ext}(S)$ satisfies the cycle condition
 - 8: **until** `IsFullGroup(Γ, S)`
 - 9: **return** S
-

We say that `Enumerate` is a *complete enumeration* of Γ if we have

$$\bigcup_{n>0} \text{Enumerate}(\Gamma, n) = \Gamma.$$

Proposition 15. *If Γ is geometrically finite and `Enumerate` is a complete enumeration of Γ , then Algorithm 3 terminates after a finite number of steps and the output S is a normalized basis for Γ .*

Proof. The Dirichlet domain centered at 0 for Γ has finitely many faces by geometric finiteness. Since Enumerate is a complete enumeration, a defining set for this Dirichlet domain will be enumerated after a finite number of steps. The algorithm will then terminate as all the conditions are satisfied by Dirichlet domains. The output will then be a normalized basis for Γ by Step 6 and Theorem 4. \square

We will now use the reduction algorithm to improve upon Algorithm 3. The main ideas are

- reducing the elements that we have to find smaller ones
- when the face-pairing condition, the cycle condition or the completeness condition fails, using this fact to find elements that make the exterior domain smaller.

For clarity, we divide Algorithm 4 into four routines. Algorithm 4 uses these routines to compute a normalized basis for a geometrically finite Kleinian group Γ .

Algorithm 4 Normalized basis algorithm

Input: A Kleinian group Γ

Output: A normalized basis S for Γ

```

1:  $S \leftarrow \emptyset$ ,  $n \leftarrow 0$ 
2: repeat
3:   repeat
4:      $n \leftarrow n + 1$ 
5:     add Enumerate( $\Gamma, n$ ) to  $S$ 
6:      $S \leftarrow$  KeepSameGroup( $S$ )
7:      $S \leftarrow$  CheckPairing( $S$ )
8:      $S \leftarrow$  CheckCycleCondition( $S$ )
9:      $S \leftarrow$  CheckComplete( $S$ )
10:  until Ext( $S$ ) does not change
11: until IsFullGroup( $\Gamma, S$ )
12: return  $S$ 

```

The first routine, KeepSameGroup, reduces elements as much as possible to eliminate redundant ones and find smaller ones.

Algorithm 5 KeepSameGroup

Input: A finite subset $S \subset \text{PSL}_2(\mathbb{C})$

Output: A new S generating the same group with smaller elements

```

1: repeat
2:    $U \leftarrow$  minimal defining set of Ext( $S$ )
3:   for all  $g \in S$  do
4:      $\bar{g} \leftarrow$  Red $_U$ ( $g$ )
5:     if  $\bar{g} \neq \pm 1$  then
6:       add  $\bar{g}$  to  $U$ 
7:     end if
8:   end for
9:    $S \leftarrow U$ 
10: until Ext( $S$ ) does not change
11: return  $S$ 

```

Proposition 16. *If S is a subset of a Kleinian group, then Algorithm 5 terminates and does not change the group generated by S .*

Proof. We first prove the second claim. Every element added to S belongs to the group generated by S as it is a reduction by $U \subset S$ of an element in S . Moreover, every element that is discarded has $\text{Red}_U(g) = \pm 1$ so at the end of the loop we have $g \in \langle S \rangle$, and every other element $g \in S \setminus U$ is replaced by $\bar{g} = \text{Red}_U(g) \in \langle U \rangle g$, so the group generated by S does not change.

Now we prove that the algorithm terminates. First consider the initial S . Let $M = \max\{d(g \cdot 0, 0) : g \in S\}$ and $X_0 = \{g \in \langle S \rangle : d(g \cdot 0, 0) \leq M\}$. The set X_0 is finite since $\langle S \rangle$ is a Kleinian group, and we have $S \subset X_0$. By definition of reduction, every element added to U is in X_0 . Moreover, by Step 2 if an element g is discarded then its isometric sphere $I(g)$ does not intersect $\overline{\text{Ext}(S)}$, so $g \cdot 0$ is in the complement of $\text{Ext}(S)$: g cannot be the reduction of any element, so it cannot be added again. Similarly if $g \in S \setminus U$ is replaced by $\bar{g} \neq g$, then g is not reduced so it cannot be added again. Hence the algorithm terminates. \square

The second routine, `CheckPairing`, checks whether $\text{Ext}(S)$ has a face-pairing. If it does not, it finds elements that make $\text{Ext}(S)$ smaller.

Algorithm 6 `CheckPairing`

Input: A finite subset $S \subset \text{PSL}_2(\mathbb{C})$

Output: A new S such that $\text{Ext}(S)$ is smaller if it did not have a face-pairing

- 1: $S \leftarrow S \cup S^{-1}$
 - 2: **for all** e edge in $I(g)$ and $g \in S$, s.t. ge not an edge of $\overline{\text{Ext}(S)}$ **do**
 - 3: $x \leftarrow x \in e$ such that $gx \notin \overline{\text{Ext}(S)}$
 - 4: $\bar{g} \leftarrow \text{Red}_S(g; x)$
 - 5: add \bar{g}, \bar{g}^{-1} to S
 - 6: **end for**
 - 7: **return** S
-

Proposition 17. *If $\text{Ext}(S)$ does not have a face-pairing, then after applying Algorithm 6, $\text{Ext}(S)$ is strictly smaller.*

Proof. If there is a nonpaired edge, at Step 5, since $x \in I(g)$ we have $d(gx, 0) = d(x, 0)$ and since $gx \notin \overline{\text{Ext}(S)}$ we have $d(gx, 0) > d(\bar{g}x, 0)$. Putting these two together gives $d(\bar{g}x, 0) < d(x, 0)$, i.e. $x \in \text{Int}(\bar{g})$ so finally we have $\text{Ext}(S \cup \{\bar{g}\}) \subsetneq \text{Ext}(S)$. \square

We give a second possible algorithm for `CheckPairing`. It is simpler but less efficient in practice. It uses the fact that if a non-elliptic cycle has length three (which is generically the case), then it is of the form $e \subset I(g) \cap I(h)$, $ge \subset I(g^{-1}) \cap I(gh^{-1})$, $he \subset I(hg^{-1}) \cap I(h^{-1})$.

Algorithm 7 `CheckPairing'`

Input: A finite subset $S \subset \text{PSL}_2(\mathbb{C})$

Output: A new S such that $\text{Ext}(S)$ is smaller if it did not have a face-pairing

- 1: $S \leftarrow S \cup S^{-1}$
 - 2: **for all** $g, h \in S$ s.t. $I(g) \cap I(h) \neq \emptyset$ and $h \neq g^{-1}$ **do**
 - 3: add gh^{-1}, hg^{-1} to S
 - 4: **end for**
 - 5: **return** S
-

Proposition 18. *If $\text{Ext}(S)$ does not have a face-pairing, then after applying Algorithm 7, $\text{Ext}(S)$ is strictly smaller.*

Proof. If there is a nonpaired edge, then there exists elements $g, h \in S$ in the minimal defining set of $\text{Ext}(S)$ and a point $x \in I(g^{-1}) \cap \overline{\text{Ext}(S)}$ such that $g^{-1}x \in \text{Int}(h)$ (so that $h \neq g^{-1}$). Since we also have $g^{-1}x \in I(g)$ and $I(g)$ is not contained in $\text{Int}(h)$, we get $I(g) \cap I(h) \neq \emptyset$, so these elements will be considered in the loop. On the other hand we have $d(x, 0) = d(g^{-1}x, 0) > d(g^{-1}hx, 0)$, so $x \in \text{Int}(g^{-1}h)$: we have $\text{Ext}(S \cup \{g^{-1}h\}) \subsetneq \text{Ext}(S)$. \square

Remark 19. Although this algorithm is less efficient than Algorithm 6, it is interesting as it gives a geometric understanding of the method described in [Lip02]: “we consider words that are two-word combinations of those forming the sides of the existing domain to modify the domain. (...) This procedure has proven to be fast and effective in practice.” Proposition 18 explains why taking products of two elements forming the sides of the domain is useful, and in Algorithm 7 we get a geometric description of the the products that we should form. Actually, the computation in the proof of Proposition 7 also shows that if $I(g^{-1}h)$ reduces $\text{Ext}(S)$, then $I(g) \cap I(h) \neq \emptyset$.

The third routine, `CheckCycleCondition`, checks whether $\text{Ext}(S)$ satisfies the cycle condition. If it does not, it finds elements that make $\text{Ext}(S)$ smaller.

Algorithm 8 `CheckCycleCondition`

Input: A finite subset $S \subset \text{PSL}_2(\mathbb{C})$

Output: A new S s.t. $\text{Ext}(S)$ is smaller if it did not satisfy the cycle condition

```

1: Compute every well-defined edge cycle
2: for all  $g$  cycle transformation for the edge  $e$  do
3:   if  $g \neq \pm 1$  fixes at most one point in  $e$  then
4:      $S \leftarrow S \cup \{g, g^{-1}\}$ 
5:   else if  $g \neq \pm 1$  fixes every point in  $e$  then
6:      $S \leftarrow S \cup \langle g \rangle$ 
7:   else
8:      $m \leftarrow$  length of the cycle
9:     for all  $0 < i < m$  do
10:       $h \leftarrow g_i \dots g_1$ 
11:      add  $h, h^{-1}$  to  $S$ 
12:     end for
13:   end if
14: end for
15: return  $S$ 

```

Remarks 20.

- If we assume that every non-elliptic cycle has length three, then the steps 8–12 are unnecessary, as in this case the partial cycle transformations at an edge contained in $I(g) \cap I(h)$ are $g, h = (hg^{-1})g, 1 = h^{-1}(hg^{-1})g$.
- If we know in advance that the group Γ is torsion-free, then we can omit the steps 3–6.
- Assuming both, we can omit `CheckCycleCondition` completely.

Lemma 21. *Suppose $S \subset \Gamma$ is a subset of a Kleinian group Γ such that 0 has a trivial stabilizer in Γ , and suppose there is an element $h \in \Gamma \setminus \{\pm 1\}$ and a point $x \in \text{Ext}(S)$ such that $hx \in \text{Ext}(S)$. Then $\text{Ext}(S \cup \{h, h^{-1}\}) \subsetneq \text{Ext}(S)$.*

Proof. First suppose that $d(x, 0) < d(hx, 0)$. Then writing $x = h^{-1}(hx) = h^{-1}y$ we get $d(h^{-1}y, 0) < d(y, 0)$ i.e. $y \in \text{Int}(h)$. Since we also have $y \in \text{Ext}(S)$, we obtain $\text{Ext}(S \cup \{h\}) \subsetneq \text{Ext}(S)$.

Othewise we have $d(hx, 0) \leq d(x, 0)$. This means that $x \in \overline{\text{Int}(h^{-1})}$, but since $x \in \text{Ext}(S)$ we get $\text{Ext}(S \cup \{h^{-1}\}) \subsetneq \text{Ext}(S)$. \square

Proposition 22. *If $\text{Ext}(S)$ does not satisfy the cycle condition, then after applying Algorithm 8, $\text{Ext}(S)$ is strictly smaller.*

Proof. Since the cycle transformation at an edge stabilizes it, if the edge is not equal to a geodesic then the cycle transformation fixes it pointwise and condition (i) is automatically satisfied. Suppose that there is a cycle for an edge e equal to a geodesic and that does not satisfy condition (i), and let g be the corresponding cycle transformation. Then the transformation g is either loxodromic, or elliptic of order 2 with exactly one fixed point in e . In both cases, Step 4 is executed. In the first case, since the interior of the isometric sphere of a loxodromic element contains one of its fixed points and the interior of the isometric sphere of its inverse contains the other, we have $\overline{\text{Ext}(\{g, g^{-1}\})} \cap e \subsetneq e$ so $\text{Ext}(S \cup \{g, g^{-1}\}) \subsetneq \text{Ext}(S)$. In the second case, the edge e contains exactly one fixed point of g in \mathcal{H}^3 , so we again have $\overline{\text{Ext}(\{g\})} \cap e \subsetneq e$ and we get $\text{Ext}(S \cup \{g, g^{-1}\}) \subsetneq \text{Ext}(S)$.

Now suppose some cycle angle for a non-elliptic cycle is larger than 2π . Then considering the images $P = \text{Ext}(S), g_1^{-1}P, \dots, (g_i \dots g_1)^{-1}P$ of $P = \text{Ext}(S)$ that glue one after another around e , we see that there is an overlap: there exists a point $x \in P$ such that $hx \in P$ for some h considered in Step 10. In this case after Step 11 we have $\text{Ext}(S \cup \{h, h^{-1}\}) \subsetneq \text{Ext}(S)$ by Lemma 21. Since the cycle transformation is the identity, the angle cannot be smaller than 2π .

Finally suppose some cycle angle for an elliptic cycle at an edge e with cycle transformation g with order ν does not satisfy condition (ii). The cycle has length 1, so $e \subset I(g) \cap I(g^{-1})$, and the angle at e is a multiple of $\frac{2\pi}{\nu}$. After running Step 6 the domain $\text{Ext}(\{g, g^{-1}\})$ is replaced by the Dirichlet domain of the finite group $\langle g \rangle$, which satisfies the cycle condition, so the new angle at e is equal to $\frac{2\pi}{\nu}$. \square

The fourth routine, CheckComplete, checks whether $\text{Ext}(S)$ is complete. If it is not, it finds elements that make $\text{Ext}(S)$ smaller.

Algorithm 9 CheckComplete

Input: A finite subset $S \subset \text{PSL}_2(\mathbb{C})$

Output: A new S such that $\text{Ext}(S)$ is smaller if it was not complete

- 1: Compute every tangency vertex cycle
 - 2: **for all** h tangency vertex transformation **do**
 - 3: **if** $h \neq 1$ is loxodromic **then**
 - 4: add h, h^{-1} to S
 - 5: **end if**
 - 6: **end for**
 - 7: **return** S
-

Remark 23. If we know in advance that the group Γ is cocompact, we can omit CheckComplete in Algorithm 4 and simply test whether $\text{Ext}(S)$ is bounded.

Proposition 24. *If $\text{Ext}(S)$ is not complete, then after applying Algorithm 8, $\text{Ext}(S)$ is strictly smaller.*

Proof. If h is a tangency vertex transformation at $z = I(g) \cap I(g') \in \partial\mathcal{B}$, then it fixes z . By looking at the successive images of the polyhedron along the cycle we see that $I(g')$ separates $I(g)$ from $hI(g)$, so h has infinite order. If $\text{Ext}(S)$ is not complete, then h is loxodromic. Being a fixed point of h , the point z is contained in $\text{Int}(h) \cup \text{Int}(h^{-1})$, so we get $\text{Ext}(S \cup \{h, h^{-1}\}) \subsetneq \text{Ext}(S)$. \square

Proposition 25. *Let Γ be a Kleinian group. The following holds for Algorithm 4 applied to Γ :*

- (i) *Suppose the algorithm terminates. Then the output is a normalized basis for Γ .*
- (ii) *Suppose that Γ is geometrically finite and Enumerate is a complete enumeration of Γ . Then the algorithm terminates.*

Remark 26. In practise Algorithm 4 runs much faster than the naive Algorithm 3 (see section 3.1.1), but unfortunately we could not prove it. What we believe is that in Algorithm 4 the blackbox Enumerate only needs to find a set of generators for the group, and then the other routines find the elements of the normalized basis; in Algorithm 3 the blackbox Enumerate needs to find directly the elements of the normalized basis, which is harder. The natural idea would be to put the routines in a loop that would not contain Enumerate in Algorithm 4, but then it is not clear whether this internal loop would terminate; actually in general it is false, since Γ may admit finitely generated subgroups that are not geometrically finite.

Proof.

- (i) If the algorithm terminates, then by Theorem 4, since $\text{Ext}(S)$ is complete, has a face-pairing and satisfies the cycle condition, the set S is a normalized basis for $\langle S \rangle$. It is then valid to use IsFullGroup to check that $\langle S \rangle = \Gamma$.
- (ii) The closure of the Dirichlet domain centered at 0 for Γ has finitely many faces by geometric finiteness. Since Enumerate is a complete enumeration, a defining set for this Dirichlet domain will be enumerated after a finite number of steps. The algorithm will then terminate as all the conditions are satisfied by the Dirichlet domain.

□

2.4. Instantiation of the blackboxes.

2.4.1. Enumerate and IsFullGroup for a group given by generators. Suppose the group Γ is given by a finite set of generators G . We can take for Enumerate the algorithm that writes every word of length n in the generators, and we can take for IsFullGroup the algorithm that reduces every element in G with respect to the given normalized basis S and returns whether every generator reduces to ± 1 : by Proposition 13, this is equivalent to $\Gamma \subset \langle S \rangle$.

2.4.2. Enumerate and IsFullGroup for an arithmetic group. We provide a possible instantiation of the blackboxes Enumerate and IsFullGroup for an arithmetic group $\Gamma(\mathcal{O})$ attached to a maximal order \mathcal{O} in a Kleinian quaternion algebra B with base field F of degree n .

We describe IsFullGroup first. A subgroup is proper if and only if its covolume is infinite or at least twice the covolume of Γ , the quotient of the covolumes being the index of the subgroup. Since Γ comes from a maximal order, the covolume of Γ is given by (3), which we can compute, and the covolume of a subgroup can be computed with Algorithm 1 once we have a normalized basis. We take for IsFullGroup the algorithm that computes the covolume $\text{Covol}(\Gamma)$ by the formula and the volume V of $\text{Ext}(S)$ for the given normalized basis S , and returns whether $\frac{V}{\text{Covol}(\Gamma)} < 2$. Since S is a normalized basis for $\langle S \rangle$, the polyhedron $\text{Ext}(S)$ is a fundamental domain for $\langle S \rangle$ so the volume V equals the covolume of $\langle S \rangle$.

We now describe an instantiation of the blackbox Enumerate for the Kleinian group associated with an order \mathcal{O} in B . Under the natural embedding $\mathcal{O} \subset B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R}$, the order \mathcal{O} is discrete. Now suppose that we have a positive definite quadratic form $Q : B \otimes_{\mathbb{Q}} \mathbb{R} \rightarrow \mathbb{R}$. Then \mathcal{O} becomes a full lattice in a real vector space of dimension $4n$. We can use lattice enumeration algorithms such as the

Kannan-Fincke-Pohst algorithm [FP85, Kan83] to enumerate elements in \mathcal{O} that are short with respect to Q . We can then select the elements having reduced norm 1. As we increase the bound on the values of Q , we will get every element in \mathcal{O}^1 . A priori any such quadratic form would work, but here we describe one that has a geometric meaning.

Recall we can embed B in $M_2(\mathbb{C})$ in such a way that \mathcal{O}^1 becomes discrete in $\mathrm{SL}_2(\mathbb{C})$. This embedding is only defined up to conjugation by an element of $\mathrm{PSL}_2(\mathbb{C})$. Let ρ be such an embedding. If $B = \left(\frac{a,b}{F}\right)$ we can take for example

$$\rho : x + yi + zj + tij \mapsto \begin{pmatrix} x + y\alpha & z + t\alpha \\ (z - t\alpha)\beta & x - y\alpha \end{pmatrix}$$

where σ is a complex embedding of F , $\beta = \sigma(b)$ and α is a square root of $\sigma(a)$.

For $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$, we define $\mathrm{inrad}(m) = |(c + \bar{b}) + (d - \bar{a})j|^2$.

Proposition 27. *The quadratic form $Q : B \otimes \mathbb{R} \rightarrow \mathbb{R}$ defined by*

$$Q(x) = \mathrm{inrad}(\rho(x)) + \mathrm{tr}_{F/\mathbb{Q}}(\mathrm{nrd}(x)) \text{ for all } x \in B$$

is positive definite and satisfies

$$Q(x) = \frac{4}{\mathrm{rad}(\rho(x))^2} + n \text{ for all } x \in \mathcal{O}^1$$

where $\mathrm{rad}(g)$ denotes the Euclidean radius of the isometric sphere of $g \in \mathrm{SL}_2(\mathbb{C})$ if $g \cdot 0 \neq 0$, and ∞ otherwise.

Proof. We show first that Q is positive definite. For a matrix $m \in \mathcal{M}_2(\mathbb{C})$ we have $\mathrm{inrad}(m) = |c + \bar{b}|^2 + |d - \bar{a}|^2 = \|m\|^2 - 2\Re(\det m)$ where $\|\cdot\|$ is the usual L^2 norm on $\mathcal{M}_2(\mathbb{C})$, so that $\|\cdot\|^2$ is a positive definite quadratic form on $\mathcal{M}_2(\mathbb{C})$. Since nrd is a positive definite quadratic form on \mathbb{H} and we have the decomposition $B \otimes \mathbb{R} \cong \mathcal{M}_2(\mathbb{C}) \oplus \mathbb{H}^{n-2}$, we can construct a positive definite quadratic form on $B \otimes \mathbb{R}$ by letting for all $x \in B \otimes \mathbb{R}$

$$Q(x) = \|m\|^2 + \mathrm{nrd}(h_1) + \cdots + \mathrm{nrd}(h_{n-2}) = \mathrm{inrad}(m) + \mathrm{tr}_{F \otimes \mathbb{R}/\mathbb{R}}(\mathrm{nrd}(x))$$

where

$$x = m + h_1 + \cdots + h_{n-2} \in \mathcal{M}_2(\mathbb{C}) \oplus \mathbb{H}^{n-2},$$

since $2\Re(\det m) + \mathrm{nrd}(h_1) + \cdots + \mathrm{nrd}(h_{n-2}) = \mathrm{tr}_{F \otimes \mathbb{R}/\mathbb{R}}(\mathrm{nrd}(x))$. This gives the positive definiteness.

For the formula on \mathcal{O}^1 , note that according to (2), it is

$$\mathrm{inrad}(g) = |(c + \bar{b}) + (d - \bar{a})j|^2 = \frac{4}{\mathrm{rad}(g)^2}$$

for $g \in \mathrm{SL}_2(\mathbb{C})$ not fixing 0 in \mathcal{B} , and if g fixes 0 then $\mathrm{inrad}(g) = 0$. \square

We obtain the following enumeration algorithm. It is a complete enumeration of $\Gamma(\mathcal{O})$, and depends on a parameter: a sequence of bounds $A_n \rightarrow \infty$.

Algorithm 10 Enumerate

Input: A positive integer n

Output: A finite subset $L \subset \Gamma(\mathcal{O})$

- 1: $L \leftarrow \emptyset$
 - 2: **for all** $x \in \mathcal{O}$ such that $Q(x) \leq A_n$ **do**
 - 3: **if** $\text{nrd}(x) = 1$ **then**
 - 4: Add $\rho(x)$ to L
 - 5: **end if**
 - 6: **end for**
 - 7: **return** L
-

We are now going to present a probabilistic enumeration algorithm. It is not a complete enumeration, but performs better in practice (see section 3.1.2). It uses variants of the former quadratic form.

Definition 28. Let $z_1, z_2 \in \mathcal{H}^3$. Let $h_1, h_2 \in \text{SL}_2(\mathbb{C})$ be such that $z_1 = h_1 \cdot j$ and $z_2 = h_2 \cdot j$. We then define the quadratic form Q_{z_1, z_2} by

$$Q_{z_1, z_2}(x) = \text{inrad}(h_2^{-1}\rho(x)h_1) + \text{tr}_{F/\mathbb{Q}}(\text{nrd}(x))$$

for all $x \in B$.

This family of quadratic forms has the following properties.

Proposition 29. Let $z_1, z_2 \in \mathcal{H}^3$. Then Q_{z_1, z_2} does not depend on the choice of $h_1, h_2 \in \text{SL}_2(\mathbb{C})$ such that $z_1 = h_1 \cdot j$ and $z_2 = h_2 \cdot j$. It is positive definite, and for all $g \in \mathcal{O}^1$ we have

$$Q_{z_1, z_2}(g) = 2 \cosh d(gz_1, z_2) - 2 + n.$$

Proof. The matrices h_1 and h_2 are defined up to right multiplication by $\text{SU}_2(\mathbb{C})$, the stabilizer of the point j . For all matrices $m \in \mathcal{M}_2(\mathbb{C})$ we have $\text{inrad}(m) = \|m\|^2 - 2\Re(\det m)$, which is not changed by left and right multiplication of m by elements of $\text{SU}_2(\mathbb{C})$, so that Q_{z_1, z_2} does not depend on the choice of h_1 and h_2 .

For $z_1 = z_2 = j$ the formula reads $\|g\|^2 = 2 \cosh d(gj, j)$ for all $g \in \text{SL}_2(\mathbb{C})$, which is well-known (and is a direct consequence of the explicit formulas for the hyperbolic distance). Then for arbitrary $z_1, z_2 \in \mathcal{H}^3$ we have

$$\|h_2^{-1}gh_1\|^2 = 2 \cosh d(h_2^{-1}gh_1j, j) = 2 \cosh d(gh_1j, h_2j) = 2 \cosh d(gz_1, z_2).$$

□

This family of quadratic forms is very useful, as it enables us to determine the elements $g \in \Gamma(\mathcal{O})$ such that gz_1 is close to z_2 . We propose the following probabilistic algorithm for enumerating elements in $\Gamma(\mathcal{O})$. It depends on a choice of some parameters: an increasing sequence of positive numbers $R_n \rightarrow \infty$ representing the radius of the search space, a sequence of positive integers $N_n \in \mathbb{Z}_{>0}$ representing the number of enumerations in small balls, and a positive number A being a bound on the quadratic form. For $w_1, w_2 \in \mathcal{B}$, we write $Q_{w_1, w_2} = Q_{\eta^{-1}(w_1), \eta^{-1}(w_2)}$.

Algorithm 11 Enumerate

Input: An positive integer n

Output: A finite subset $L \subset \Gamma(\mathcal{O})$

```
1:  $L \leftarrow \emptyset$ 
2: for  $i = 1$  to  $N_n$  do
3:   Draw a point  $w \in \mathcal{B}$  such that  $d(0, w) \leq R_n$  randomly, uniformly w.r.t. the
   hyperbolic volume
4:   for all  $x \in \mathcal{O}$  such that  $Q_{0,w}(x) \leq A$  do
5:     if  $\text{nr}(d(x)) = 1$  then
6:       Add  $\rho(x)$  to  $L$ 
7:     end if
8:   end for
9: end for
10: return  $L$ 
```

Remarks 30.

- We can also use these quadratic forms differently: if we miss an element of the group to “close off” the exterior domain around a point at infinity ξ , we can look for elements of small $Q_{j,z}$ where $z \rightarrow \xi$. This is a similar idea as in Remark 4.9 in [Voi09], but the quadratic form that was used there is the analogue of $Q_{z,z}$. If g is the element that we are looking for, $d(gz, z)$ is bounded by below by a positive constant if g is loxodromic, which is the generic case. On the contrary we have $d(gj, z) \rightarrow 0$ as $z \rightarrow gj$.
- The efficiency of this algorithm depends on the choice of the parameters N_n , R_n and A . Heuristics led us to the following choice, which works well in practise:
 - we use a small bound $A = \alpha \cdot |\Delta_F N(\Delta_B)|^{\frac{1}{4[F:\mathbb{Q}]}}$ so that the number of $x \in \mathcal{O}$ such that $Q_{0,w}(x) \leq A$ is approximately constant by Gaussian heuristic;
 - experimental evidence and [BGLS10, Theorem 1.5] suggest that a number of random elements of Γ proportional to $\text{Covol}(\Gamma)$ has a good probability to generate Γ , and by Gaussian heuristic we need $O(\text{Covol}(\Gamma))$ random centers to obtain one element of the group on average, so we choose $N_0 = \beta \cdot \text{Covol}(\Gamma)^2$, and we increase it exponentially fast: $N_n = (1 + \eta)^n N_0$;
 - the radius R_n has to be large enough to ensure good randomness of the elements of Γ , so we choose R_0 such that $\text{Vol}(\mathbb{B}(w, R_0)) = \text{Covol}(\Gamma)^\gamma$ and we increase it in arithmetic progression (so the volume increases exponentially fast): $R_n = R_0 + \epsilon \cdot n$. Because of our choice of N_n we take $\gamma > 2$.

Now we explain how we draw points at random in the ball $\mathbb{B}(0, R)$ of radius R . Since the hyperbolic volume is invariant by rotation around 0, it is equivalent to draw a random point uniformly on the sphere, and then multiply it by an appropriate random scalar independent from the point on the sphere. Thus we only have to determine the distribution of the distance from 0 of the points in the ball of radius R . Let X be a random variable with uniform distribution in $\mathbb{B}(0, R)$. The cumulative distribution function of the distance to 0 is

$$f_R(r) = \mathcal{P}_X(d(X, 0) \leq r) = \frac{\text{Vol}(\mathbb{B}(0, r))}{\text{Vol}(\mathbb{B}(0, R))}.$$

Recall that the volume $v(r)$ of the ball of radius r is $v(r) = \pi(\sinh(2r) - 2r)$. It is clear that the function $f_R : [0, R] \rightarrow [0, 1]$ is a continuous bijection. It implies that $d(0, X) = f_R^{-1}(U)$ where U is a uniform random variable in $[0, 1]$. We rewrite

that expression as $d(0, X) = v^{-1}(U')$ where U' is a uniform variable in $[0, v(R)]$. It is well-known how to draw a uniform variable in an interval and on a sphere, and v^{-1} can be computed by Newton iteration.

2.5. Floating-point implementation. Here we describe a floating-point implementation of the above algorithms. We start with a lemma giving us control on the error made when having an element of the group act on a point. We only study the stability of the algorithm, so we do not take into account the error made by rounding in elementary operations.

Lemma 31. *Let $g \in \text{SL}_2(\mathbb{C})$, $\tilde{g} \in \mathcal{M}_2(\mathbb{C})$ and $w, \tilde{w} \in \mathcal{B}$. Let $\epsilon = |w - \tilde{w}|$, $\eta = \|g - \tilde{g}\|$ and $\delta = \frac{1}{1 - |w|}$. Suppose that $(\|g\|\epsilon + 2\eta)^2 \leq \frac{1}{3\delta}$. Then the quantity $\tilde{g}\tilde{w}$ obtained by applying Formula (1) to \tilde{g} and \tilde{w} is well-defined, and we have*

$$|g \cdot w - \tilde{g}\tilde{w}| \leq 68 \delta^{\frac{3}{2}} \|g\|^3 \epsilon + 136 \delta^{\frac{3}{2}} \|g\|^2 \eta.$$

Proof. By direct computation we have $|A - \tilde{A}| \leq \sqrt{2}\eta$ and $|A| \leq \sqrt{2}\|g\|$, and the same inequalities for B, C, D . We write

$$g \cdot w = (Aw + B)(Cw + D)^{-1} = \frac{1}{|Cw + D|^2} (Aw + B)(\overline{wC} + \overline{D})$$

and similarly for \tilde{g}, \tilde{w} . Another direct computation gives

$$(4) \quad |w|^2 - |g \cdot w|^2 = \left(1 - \frac{4}{|Cw + D|^2}\right) (|w|^2 - 1),$$

showing that

$$\frac{1}{|Cw + D|^2} \leq \frac{1}{4}(1 + 2\delta) \leq \frac{3}{4}\delta \quad \text{and} \quad \frac{4}{3\delta} \leq |Cw + D|^2.$$

By the triangle inequality, adding and subtracting $A\tilde{w}$ gives

$$|Aw - \tilde{A}\tilde{w}| \leq \sqrt{2}\|g\|\epsilon + \sqrt{2}\eta$$

and the same inequality for Cw . We get

$$|(Cw + D) - (\tilde{C}\tilde{w} + \tilde{D})|^2 \leq 2(\|g\|\epsilon + 2\eta)^2 \leq \frac{|Cw + D|^2}{2}$$

since by hypothesis we have $(\|g\|\epsilon + 2\eta)^2 \leq \frac{1}{3\delta}$. In particular $\tilde{C}\tilde{w} + \tilde{D} \neq 0$ and $\tilde{g}\tilde{w}$ is well-defined. By the mean value theorem this gives

$$||Cw + D|^{-2} - |\tilde{C}\tilde{w} + \tilde{D}|^{-2}| \leq (6\delta)^{\frac{3}{2}} (\|g\|\epsilon + 2\eta)$$

We also get

$$\begin{aligned} & |(Aw + B)(\overline{wC} + \overline{D}) - (\tilde{A}\tilde{w} + \tilde{B})(\overline{\tilde{w}C} + \overline{\tilde{D}})| \\ & \leq |Aw + B|(\sqrt{2}\|g\|\epsilon + 2\sqrt{2}\eta) + 2|Cw + D|(\sqrt{2}\|g\|\epsilon + 2\sqrt{2}\eta) \\ & \leq (2\sqrt{2}\|g\|)(\sqrt{2}\|g\|\epsilon + 2\sqrt{2}\eta) + (2\sqrt{2}\|g\|)(2\sqrt{2}\|g\|\epsilon + 4\sqrt{2}\eta) \\ & = 12\|g\|^2\epsilon + 24\|g\|\eta. \end{aligned}$$

Finally we have

$$\begin{aligned} & |(Aw + B)(Cw + D)^{-1} - (\tilde{A}\tilde{w} + \tilde{B})(\tilde{C}\tilde{w} + \tilde{D})^{-1}| \\ & \leq |g \cdot w| |Cw + D|^{-2} (6\delta)^{\frac{3}{2}} (\|g\|\epsilon + 2\eta) + \frac{2}{|Cw + D|^2} (12\|g\|^2\epsilon + 24\|g\|\eta) \\ & \leq (24\sqrt{6} + 9)\delta^{\frac{3}{2}} \|g\|^3 \epsilon + (48\sqrt{6} + 18)\delta^{\frac{3}{2}} \|g\|^2 \eta \\ & \leq 68 \delta^{\frac{3}{2}} \|g\|^3 \epsilon + 136 \delta^{\frac{3}{2}} \|g\|^2 \eta \end{aligned}$$

as claimed. \square

In the following, we want to maintain the property $(\|g\|\epsilon + 2\eta)^2 \leq \frac{1}{3\delta}$ for every element g and every point w considered, where ϵ is the imprecision on the points in \mathcal{B} , η the imprecision on the elements g considered, and $\eta = \frac{8}{3}\epsilon$.

We now describe the modification of the algorithms for the floating-point version. In the reduction algorithm (Algorithm 2), we choose $\alpha > 0$ and in Step 6 we replace the inequality $d(gw', 0) \geq d(w', 0)$ by $\frac{4}{|Cw' + D|^2} \leq 1 + \alpha$. Since we have $w' \in \text{Ext}(g)$ if and only if $|Cw' + D|^2 \geq 4$, the modified condition is indeed an approximation of the exact condition.

Proposition 32. *Let $\beta = \alpha - 68\delta^{\frac{5}{2}}M^3\epsilon - 136\delta^{\frac{5}{2}}M^2\eta$ where $\delta = \frac{1}{1-|w|^2}$ and $M = \max_{g \in S} \|g\|$. If $\beta > 0$, then the floating-point version of the reduction algorithm terminates.*

Proof. Formula (4) may be rewritten

$$1 - |g \cdot w|^2 = \frac{4}{|Cw + D|^2}(1 - |w|^2),$$

which gives, if the modified condition of Step 6 is not satisfied

$$1 - |g \cdot w'|^2 \geq (1 + \alpha)(1 - |w'|^2).$$

Lemma 31 gives

$$1 - |\widetilde{g}w'|^2 \geq (1 + \beta)(1 - |w'|^2),$$

so $1 - |w'|^2$ is multiplied by $1 + \beta$ at each step of the algorithm. Since we also have $1 - |w'|^2 \leq 1$, the algorithm terminates. \square

We want to use a uniform α that tends to 0 as $\epsilon \rightarrow 0$. For this, we assume that we only consider points w such that $1 - |w|^2 \geq 2\epsilon^{\frac{2}{9}}$ and elements g such that $\|g\| \leq \epsilon^{-\frac{1}{9}}$. Assuming that $\epsilon < 10^{-9}$ we can then take $\alpha = 18\epsilon^{\frac{1}{9}}$. These assumptions also ensure that $(\|g\|\epsilon + 2\eta)^2 \leq \frac{1}{3\delta}$, and are compatible since the points $g \cdot 0$ that we have to consider satisfy $1 - |g \cdot 0|^2 = \frac{4}{\|g\|^2 + 2} \geq \frac{2}{\|g\|^2} \geq 2\epsilon^{\frac{2}{9}}$.

There is no change in KeepSameGroup (Algorithm 5): the same argument shows that the algorithm terminates, regardless of finite precision in the computations.

The routine CheckPairing (Algorithm 6) should only consider an edge e contained in $I(g)$ as not being paired if there is $x \in e$ and we have the stronger inequality $|C\widetilde{g}x + D|^2 < \frac{4}{1+\alpha}$ and C, D correspond to h for some $h \in S$. This ensures that the floating-point reduction will yield a non-trivial element, since at least one step of reduction will be performed.

The routines CheckCycleCondition (Algorithm 8) and CheckComplete (Algorithm 9) contain only finite loops regardless of the use of finite precision, so there is no change in them.

Proposition 33. *The floating-point version of the Normalized basis algorithm (Algorithm 4) terminates.*

Proof. By the arguments above, each of the routines terminates. Moreover, because of precision restriction we impose $\|g\| \leq \epsilon^{-\frac{1}{9}}$ for every element g of the group considered in the algorithm, so that only finitely many g can be used, so the algorithm terminates. \square

Of course if the precision chosen is insufficient, the algorithm may terminate with an error or a wrong answer, but with Riley's methods [Ril83], we can use Poincaré's theorem with the approximate fundamental domain to prove that the computed presentation is correct. Alternatively, we could check the fundamental domain algebraically, but this is likely to be time-consuming.

2.6. **Master algorithm.** As a summary, this is our master algorithm for computing an arithmetic Kleinian group associated with a maximal order.

Algorithm 12 Master algorithm

Input: A maximal order \mathcal{O} in a Kleinian quaternion algebra B

Output: A finitely presented group G , and two computable group homomorphism $\phi : G \rightarrow \Gamma(\mathcal{O})$ and $\psi : \Gamma(\mathcal{O}) \rightarrow G$, inverse of each other

- 1: Choose an embedding $\rho : B \hookrightarrow \mathcal{M}_2(\mathbb{C})$ s.t. the point 0 has trivial stabilizer in the group $\Gamma(\mathcal{O}) = \rho(\mathcal{O}^\times)/\{\pm 1\}$
 - 2: $V \leftarrow \text{Covol}(\Gamma(\mathcal{O}))$ computed with Formula (3)
 - 3: **function** IsFullGroup(S) **do**
 - 4: compute $V' = \text{Vol}(\text{Ext}(S))$ with Algorithm 1
 - 5: **return** $V' < 2V$
 - 6: **end function**
 - 7: Enumerate \leftarrow Algorithm 10 or Algorithm 11
 - 8: $S \leftarrow$ output of the Normalized Basis Algorithm 4
 - 9: $R \leftarrow$ inverse, cycle and reflection relations from Theorem 2
 - 10: $G \leftarrow \langle S | R \rangle$
 - 11: Let $\phi : G \rightarrow \Gamma(\mathcal{O})$ be the map that evaluates words in the generators
 - 12: Let $\psi : \Gamma(\mathcal{O}) \rightarrow G$ be the map that writes elements as words in the generators using Algorithm 2
 - 13: **return** G, ϕ, ψ
-

Remarks 34.

- If we want to compute the group that is the image of a smaller order, or more generally a finite index subgroup Γ' of the group $\Gamma(\mathcal{O})$ given by a maximal order \mathcal{O} , we can compute first a normalized basis for the larger group $\Gamma(\mathcal{O})$, and then compute the index by standard coset enumeration techniques. This gives the covolume of the smaller group, and even a set of generators for it, so we can then apply the same algorithm we described.
- We may also want to compute a maximal group in the commensurability class of $\Gamma(\mathcal{O})$. There are infinitely many conjugacy classes of such maximal groups, and they can be obtained as follow. Let \mathcal{O}' be a maximal order in B , and S a finite set of primes of F that split in B . Let $\mathcal{O}'' \subset \mathcal{O}'$ be an Eichler order of level \mathfrak{N} where \mathfrak{N} is the product of the primes in S , and define $\Gamma_{S, \mathcal{O}'}$ to be the normalizer of \mathcal{O}'' in B^\times . Then every maximal group in the commensurability class of $\Gamma(\mathcal{O})$ is conjugate to a group $\Gamma_{S, \mathcal{O}'}$ for some set S and some maximal order \mathcal{O}' , which can be taken from a set of representatives of the conjugacy classes of maximal orders in B . Note however that some of the groups $\Gamma_{S, \mathcal{O}'}$ may not be maximal. Since each of these groups is the image in $\text{PSL}_2(\mathbb{C})$ of the normalizer of an order in B , we may use the same enumeration techniques. The index is given in terms of a class group and a finite quotient of units in \mathbb{Z}_F , which can be computed, so again we get the covolume of this larger group, and can apply the same technique. The reader can refer to [Bor81] or [MR03, Section 11.4] for details on maximal groups.

3. EXAMPLES

The author has implemented the algorithm described in the previous section in the computer system Magma [BCP97]. Our package `KleinianGroups` is available at <http://www.normalesup.org/~page/software.html>. Here we show some examples of the output of this code. In sections 3.1 and 3.2, the computations are performed on a 1.73 GHz Intel i7 processor with Magma v2.18-4. The more extensive computations of sections 3.3 and 3.4 are run on a 2.5 GHz Intel Xeon E5420 processor from the PLAFRIM experimental testbed with Magma v2.17-12.

3.1. Comparison between subalgorithms.

3.1.1. *Comparison between the normalized basis algorithms.* Consider the ATR sextic field F of discriminant -92779 generated by an element t such that $t^6 - t^5 - 2t^4 + 3t^3 - t^2 - 2t + 1 = 0$, and let \mathbb{Z}_F be its ring of integers. Let $B = \left(\frac{-1, -1}{F}\right)$ be the quaternion algebra ramified only at the real places of F . Let \mathcal{O} be a maximal order in B ; the choice does not matter as they are all conjugate. The Kleinian group $\Gamma(\mathcal{O})$ has covolume $0.3007\dots$. We compare our algorithm with the naive Algorithm 3. Both need a precomputation of 3 seconds for the computation of the coefficients of the Lobachevsky power series and 4 seconds for the evaluation of the Dedekind zeta function at 2. Our algorithm then computes a Dirichlet domain in 2 seconds, and enumerates 37 elements of \mathcal{O} , yielding 21 elements of $\Gamma(\mathcal{O})$. The naive algorithm (actually we only removed the routine `CheckPairing`) computes the same Dirichlet domain in 48 seconds and has to enumerate 16 246 elements of \mathcal{O} , yielding 1713 elements of $\Gamma(\mathcal{O})$. The fundamental domain (Figure 3.1) has 18 faces and 42 edges.

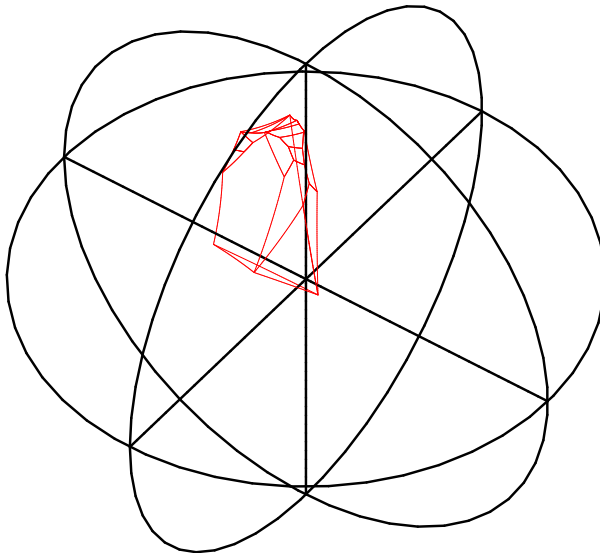


FIGURE 3.1. Dirichlet domain of a Kleinian group over a sextic field

3.1.2. *Comparison between the enumeration algorithms.* Consider the ATR number field F of degree 8 and discriminant -407793664 , generated by an element t such that $t^8 - 4t^7 + 4t^6 + 2t^5 - 8t^4 + 4t^3 + 5t^2 - 2t - 1 = 0$, and let \mathbb{Z}_F be its ring of integers. Let $B = \left(\frac{-1, -1}{F}\right)$ be the quaternion algebra ramified only at the real places of F . Let \mathcal{O} be a maximal order in B ; the choice does not matter as they are all

conjugate. The Kleinian group $\Gamma(\mathcal{O})$ has covolume $56.509\dots$. We compare the performance of our algorithm when using the enumeration algorithms 10 or 11. With the deterministic enumeration algorithm 10, our code computes a fundamental domain in 12 hours and 45 minutes (45943 seconds, most of which is enumeration), and enumerates 84 159 799 vectors, yielding 1600 group elements. With the probabilistic enumeration algorithm 11, our code computes the same Dirichlet domain in 71 seconds, and only needs to enumerate 3511 vectors, yielding 164 group elements. It spends 2 seconds for computing the value of the zeta function, 16 seconds for enumeration, 3 seconds for the routine `KeepSameGroup`, 40 for `CheckPairing` and 10 for computing the volume of the polyhedron. The fundamental domain (Figure 3.2) has 202 faces and 582 edges.

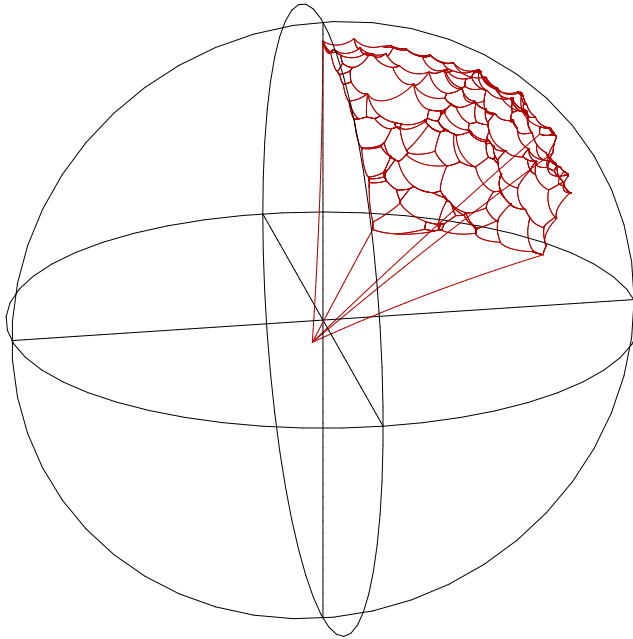


FIGURE 3.2. Dirichlet domain of a Kleinian group over an octic field

3.2. Relation to previous work. In this section we show how to recover examples covered by earlier work with our algorithm. When available, we provide a comparison of running times between public implementations and our code. The reader should keep in mind that these are only comparisons between implementations since the complexity of the algorithms is usually unknown.

3.2.1. Bianchi groups. Let F be an imaginary quadratic field with ring of integers \mathbb{Z}_F . Consider the quaternion algebra $B = \mathcal{M}_2(F)$ and the maximal order $\mathcal{O} = \mathcal{M}_2(\mathbb{Z}_F)$. Then the group $\Gamma(\mathcal{O}) = \mathrm{PSL}_2(\mathbb{Z}_F)$ is called a *Bianchi group*. There exists already several programs computing fundamental domains for these groups [Rah10, Yas10] but they only work for Bianchi groups while ours deals with general arithmetic Kleinian groups. Table 3.1 gives the running time (in seconds) of our Magma package and other public implementations. The first three columns correspond to the discriminant of the field, its class number and the covolume of $\mathrm{PSL}_2(\mathbb{Z}_F)$. The last four columns display running times in seconds: `Bianchi.gp` [Rah10] written in GP [The11] implementing Swan’s algorithm for $\mathrm{PSL}_2(\mathbb{Z}_F)$, our code `KleinianGroups` computing $\mathrm{PSL}_2(\mathbb{Z}_F)$, the code provided by Magma implementing the algorithm of [Yas10] using Voronoi theory

Δ_F	h_F	volume	Bianchi	KG, PSL ₂	Magma	KG, PGL ₂
-3	1	0.169	0.015	0.93	0.43	0.83
-15	2	3.139	0.152	0.92	0.8	2.32
-23	3	6.449	0.176	1.22	1.11	2.06
-39	4	13.80	2.37	9.44	3.05	4.36
-47	5	19.43	3.83	19.9	5.33	6.96
-71	7	37.53	21.6	36.6	17.8	13.2
-87	6	44.72	25.7	45.1	17.3	16.4
-95	8	57.06	41.4	43.8	33.9	19.3
-119	10	82.93	7080.	137.	99.5	25.6
-167	11	132.3	1545.	391.	188.	80.9
-199	9	148.5	3840.	393.	224.	92.7

TABLE 3.1. Running times for Bianchi groups

for $\mathrm{PGL}_2(\mathbb{Z}_F)$, and our code for $\mathrm{PGL}_2(\mathbb{Z}_F)$. Note that it is not surprising that computing $\mathrm{PGL}_2(\mathbb{Z}_F)$ is faster: the group is larger by an index 2, so the covolume is twice smaller and our computation is 4 times shorter (see also section 3.4).

3.2.2. Arithmetic Fuchsian groups. Let F be a totally real field and B a quaternion algebra ramified at every infinite place but one. Let \mathcal{O} be an order in B . Then the group $\Gamma(\mathcal{O}) = \mathcal{O}^\times / \{\pm 1\}$ embeds into $\mathrm{PSL}_2(\mathbb{R})$, in which it is discrete with finite covolume: it is an *arithmetic Fuchsian group*. Using the action of $\mathrm{PSL}_2(\mathbb{R})$ on the upper half-plane \mathbb{H} , Voight [Voi09] was able to compute fundamental domains for these groups. Since we have $\mathrm{PSL}_2(\mathbb{R}) \subset \mathrm{PSL}_2(\mathbb{C})$, a Fuchsian group can be seen as a Kleinian group leaving a geodesic plane stable. Using this we can also compute arithmetic Fuchsian groups with our code. Our probabilistic enumeration Algorithm 11 leads to an improvement in high degree. As an example, consider the totally real field F with discriminant 9685993193, generated by an element t such that $t^9 - 2t^8 - 7t^7 + 11t^6 + 15t^5 - 15t^4 - 10t^3 + 7t^2 + 2t - 1 = 0$. Let $B = \left(\frac{a,b}{F}\right)$ with $a = -3t^8 + 2t^7 + 30t^6 - 8t^5 - 93t^4 + 90t^2 + 2t - 26$ and $b = -1$. It is ramified at every real place but one. Let \mathcal{O} be a maximal order in B . The Fuchsian group $\Gamma(\mathcal{O})$ has coarea 103.67...; our code computes a fundamental domain for this group in 13 minutes (735 seconds). The code provided by Magma and implementing the algorithm of [Voi09] computes a fundamental domain for $\Gamma(\mathcal{O})$ in 1 hour and 10 minutes (4204 seconds).

3.2.3. The Hamiltonians over $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$. Consider the field $F = \mathbb{Q}(\sqrt{-7})$ and the quaternion division algebra $\left(\frac{-1,-1}{F}\right)$. Then $\mathcal{O} = \mathbb{Z}_F + \mathbb{Z}_F i + \mathbb{Z}_F j + \mathbb{Z}_F ij$ is a non-maximal order in B . A fundamental domain for this group was computed by C. Corrales, E. Jaspers, G. Leal and Á. del Río in [CJLdR04]. Using the method of Remark 34, our code can compute a fundamental domain for the group $\Gamma(\mathcal{O})$. It computes first a maximal order $\mathcal{O}' \supset \mathcal{O}$, and a fundamental domain for $\Gamma(\mathcal{O}')$ (having covolume 0.8889...). By coset enumeration, it finds that $\Gamma(\mathcal{O})$ has index 9 in the larger group, and computes a fundamental domain for the initial group $\Gamma(\mathcal{O})$. The overall computation takes 15 seconds.

3.3. A larger example. Consider the ATR field F generated by an element t such that $t^{10} + 4t^9 - 18t^7 - 27t^6 + 26t^5 + 57t^4 - 2t^3 - 33t^2 - 10t + 1 = 0$, having discriminant $-546829505431 \simeq -5.5 \cdot 10^{11}$. Let B be the quaternion algebra $\left(\frac{a,b}{F}\right)$ where $a = \frac{1}{2}(-25t^9 - 82t^8 + 61t^7 + 404t^6 + 376t^5 - 932t^4 - 718t^3 + 590t^2 + 368t - 33)$ and $b = -1$. It is ramified exactly at the real places of F . Let \mathcal{O} be a maximal order

in B . The group $\Gamma(\mathcal{O})$ has covolume $1783.7\dots$. Our code computes a fundamental domain for this group in 23 hours and 39 minutes (85150 seconds). It spends 5.3% of the time for enumeration, 5.8% for the routine `KeepSameGroup`, 87.7% for `CheckPairing` and 1.3% for computing the volume of the polyhedron. The fundamental domain has 5434 faces and 16252 edges.

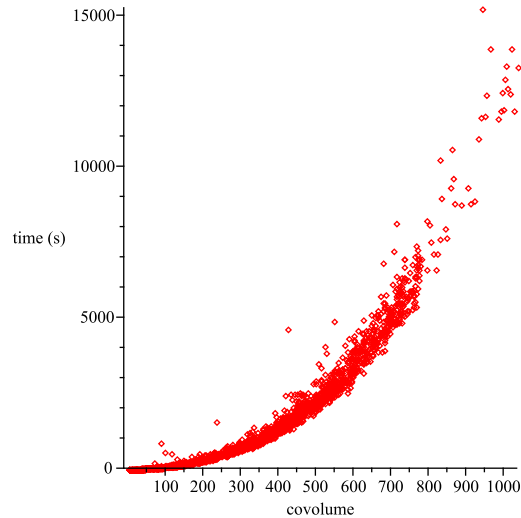


FIGURE 3.3. Running time of the algorithm

3.4. Efficiency of the algorithm. According to geometers, the parameter encoding the complexity of an arithmetic Kleinian group is the covolume. In practise it is simpler to vary the discriminant of the base field (and hence the degree) and the norm of the discriminant of the quaternion algebra. It seems hard to estimate the running time of the algorithm in terms of these parameters. First, we do not know any bound on the radii of the isometric spheres containing the faces of the closure of the Dirichlet domain, or of generators of the group, so we do not know how many elements we have to enumerate. Then, even if we have generators of the group, we do not know how long the normalized basis algorithm could run before terminating (see also Remark 26).

We present numerical data obtained in a family. Since the running time increases very quickly with the discriminant of the field, we fixed the base field and varied the discriminant of the algebra. The field we chose is the ATR cubic field of discriminant -23 . We computed groups $\Gamma(\mathcal{O})$ for every algebra with discriminant less than 10 000, and one algebra every ten with discriminant less than 15 000.

Analysis of this data shows that the running time is approximately proportional to the square of the covolume, with a few exceptionnally slow computations. We explain this as follows: in almost all cases, the enumeration appears to take negligible time, and the longest part is the computation of the fundamental domain itself; moreover the data (Figure 3.4) seem to indicate that the number of faces is proportional to the covolume (we have such a lower bound since the volume of a hyperbolic tetrahedron is bounded by $3\mathcal{L}(\frac{\pi}{3})$), and we know that our algorithm to compute the domain given the faces is quadratic.

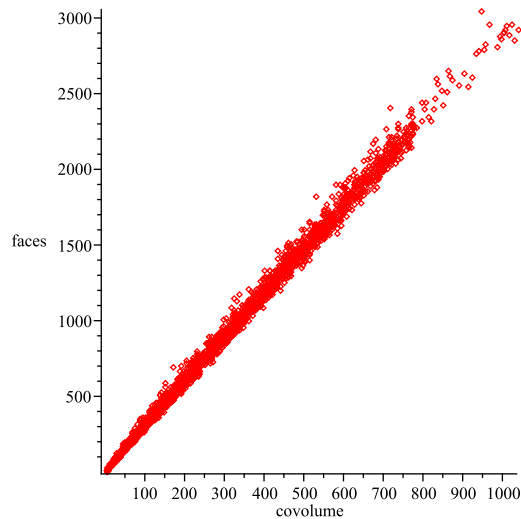


FIGURE 3.4. Number of faces of the closure of the Dirichlet domains

REFERENCES

- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [BGLS10] Mikhail Belolipetsky, Tsachik Gelander, Alexander Lubotzky, and Aner Shalev. Counting arithmetic lattices and surfaces. *Ann. of Math. (2)*, 172(3):2197–2221, 2010.
- [Bor81] A. Borel. Commensurability classes and volumes of hyperbolic 3-manifolds. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 8(1):1–33, 1981.
- [BV13] Nicolas Bergeron and Akshay Venkatesh. The asymptotic growth of torsion homology for arithmetic groups. *J. Inst. Math. Jussieu*, 12(2):391–447, 2013.
- [BW00] A. Borel and N. Wallach. *Continuous cohomology, discrete subgroups, and representations of reductive groups*, volume 67 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, second edition, 2000.
- [CFJR01] Ted Chinburg, Eduardo Friedman, Kerry N. Jones, and Alan W. Reid. The arithmetic hyperbolic 3-manifold of smallest volume. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 30(1):1–40, 2001.
- [CJLdR04] Capi Corrales, Eric Jespers, Guilherme Leal, and Angel del Río. Presentations of the unit group of an order in a non-split quaternion algebra. *Adv. Math.*, 186(2):498–524, 2004.
- [CV12] Frank Calegary and Akshay Venkatesh. A torsion Jacquet–Langlands correspondence. 2012. <http://arxiv.org/abs/1212.3847>.
- [FP85] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comp.*, 44(170):463–471, 1985.
- [JL70] H. Jacquet and R. P. Langlands. *Automorphic forms on GL(2)*. Lecture Notes in Mathematics, Vol. 114. Springer-Verlag, Berlin, 1970.
- [Kan83] Ravi Kannan. Improved algorithms for integer programming and related lattice problems. In *Proceedings of the fifteenth annual ACM symposium on Theory of computing*, STOC '83, pages 193–206, New York, NY, USA, 1983. ACM.
- [Lip02] M. Lipyanskiy. A computer-assisted application of Poincaré’s fundamental polyhedron theorem. Preprint available at <http://www.math.columbia.edu/~ums/Archive.html>, 2002.
- [Mas71] Bernard Maskit. On Poincaré’s theorem for fundamental polygons. *Advances in Math.*, 7:219–230, 1971.
- [MR03] Colin Maclachlan and Alan W. Reid. *The arithmetic of hyperbolic 3-manifolds*, volume 219 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003.
- [Pag10] Aurel Page. Computing fundamental domains for arithmetic Kleinian groups. Master’s thesis, Université Paris 7, August 2010.

- [Rah10] Alexander Rahm. *(Co)homologies et K-théorie de groupes de Bianchi par des modèles géométriques calculatoires*. Phd thesis, Université Joseph-Fourier - Grenoble I, October 2010.
- [Rat06] John G. Ratcliffe. *Foundations of hyperbolic manifolds*, volume 149 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2006.
- [Ril83] Robert Riley. Applications of a computer implementation of Poincaré's theorem on fundamental polyhedra. *Math. Comp.*, 40(162):607–632, 1983.
- [Swa71] Richard G. Swan. Generators and relations for certain special linear groups. *Advances in Math.*, 6:1–77 (1971), 1971.
- [The11] The PARI Group, Bordeaux. *PARI/GP, version 2.6.0*, 2011. available from <http://pari.math.u-bordeaux.fr/>.
- [Vig80] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.
- [Voi09] John Voight. Computing fundamental domains for Fuchsian groups. *J. Théor. Nombres Bordeaux*, 21(2):469–491, 2009.
- [Yas10] Dan Yasaki. Hyperbolic tessellations associated to Bianchi groups. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 385–396. Springer, Berlin, 2010.