The constructive membership problem for discrete two-generator subgroups of $\mathrm{SL}_2(\mathbb{R})$

Markus Kirschmer[1], Marion G. Rüther

Lehrstuhl D für Mathematik, RWTH Aachen University

Abstract

We describe a practical algorithm to solve the constructive membership problem for discrete two-generator subgroups of $\mathrm{SL}_2(\mathbb{R})$ or $\mathrm{PSL}_2(\mathbb{R})$. This algorithm has been implemented in Magma for groups defined over real algebraic number fields.

Keywords: Constructive membership, Fuchsian groups
2000 MSC: 20H10

1. Introduction

For a subgroup G of some group H, given by a set of generators $\{g_1, \ldots, g_n\} \subseteq H$, the constructive membership problem asks whether a given element $h \in H$ lies in G and if so, how to express h as a word in the generators $g_1, \ldots, g_n$.

Michailova [17, p. 42] showed that in general, the constructive membership problem is undecidable for infinite matrix groups. However, $\mathrm{SL}_2(\mathbb{R})$ is a topological group which acts on the upper half plane $\mathbb{H} = \{x + iy \mid x \in \mathbb{R}, y \in \mathbb{R}_{>0}\}$ via Möbius transformations. Using this action, Eick, Kirschmer&Leedham-Green [6] recently solved the constructive membership problem for discrete, free subgroups of $\mathrm{SL}_2(\mathbb{R})$ of rank 2. The purpose of this paper is to solve the problem for all discrete two-generator subgroups of $\mathrm{SL}_2(\mathbb{R})$, whether they are free or not; see Algorithm 3 for details.

In Section 4 we recall the classification of discrete two-generator subgroups of $\mathrm{SL}_2(\mathbb{R})$ and $\mathrm{PSL}_2(\mathbb{R})$ due to Rosenberger and Purzitsky [18, 19, 21, 23, 24, 27]. In Section 5 we exhibit explicit algorithms to decide whether $G = \langle A, B\rangle \leq \mathrm{SL}_2(\mathbb{R})$ is discrete.

The group G is called elementary if the commutators $[g, h] = ghg^{-1}h^{-1}$ of all pairs $g, h \in G$ of infinite order have trace 2. If G is elementary, the constructive membership problem can be solved directly, see Section 3 for details. Suppose now G is not elementary and let $\overline{G}$ be the image of G in $\mathrm{PSL}_2(\mathbb{R})$. In Section 6, we reduce the constructive membership problem for G to the corresponding problem for $\overline{G}$. By [27, Lemma 1], this leaves us with three types of groups $\overline{G}$ to consider:

1. $\overline{G}$ is a free product of two cyclic groups.

Email addresses: markus.kirschmer@math.rwth-aachen.de (Markus Kirschmer), marion.ruether@rwth-aachen.de (Marion G. Rüther)

[1]The first author was supported by DFG grant NE612/5-1.

2. $\overline{G}$ is a triangle group.
3. The commutator $[A, B]$ has finite order.

In [6], the constructive membership problem is solved for free groups $\overline{G} \leq \mathrm{PSL}_2(\mathbb{R})$ of rank 2 using the Ping-Pong Lemma and a suitable fundamental domain for the action of $\overline{G}$ on $\mathbb{H}$. This method extends immediately to free products, see Section 7. The groups in the remaining two cases are cocompact. In Sections 8 and 9 we solve the constructive membership problems for these groups using fundamental domains which are either triangles or squares.

We have implemented the above methods in MAGMA for subgroups G of $\mathrm{SL}_2(K)$ for real algebraic number fields K. A report on this implementation is given in Section 10 and it can be obtained from

`www.math.rwth-aachen.de/~Markus.Kirschmer/magma/sl2r.html`

2. Preliminaries

In this section we recall various well-known results on $\mathrm{GL}_2(\mathbb{R})$ and its geometry. For background and details we refer to the books by Beardon [1] and Katok [13].

2.1. Möbius transformations

The group $\mathrm{GL}_2(\mathbb{R})$ acts on the extended complex plane $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ via Möbius transformations. More precisely we have a group homomorphism

$$\varphi\colon \mathrm{GL}_2(\mathbb{R}) \to \mathrm{Aut}(\hat{\mathbb{C}}),\ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(z \mapsto M \cdot z := \frac{az+b}{cz+d} \right)$$

with $M \cdot \infty = \infty$ if $c = 0$, and $M \cdot \infty = a/c$ and $M \cdot (-d/c) = \infty$ if $c \neq 0$. Since the kernel of φ is $K = \{aI \mid a \in \mathbb{R},\ a \neq 0\}$, it induces an action of $\mathrm{PGL}_2(\mathbb{R}) = \mathrm{GL}_2(\mathbb{R})/K$ on $\hat{\mathbb{C}}$.

For a quadruple (x_1, x_2, x_3, x_4) of pairwise distinct elements in $\mathbb{C}$, the cross ratio is defined as

$$\mathrm{cross}(x_1, x_2, x_3, x_4) = \frac{(x_1 - x_3)(x_2 - x_4)}{(x_2 - x_3)(x_1 - x_4)}\,.$$

By continuity, this definition can be extended to quadruples of pairwise distinct elements in $\hat{\mathbb{C}}$. The map φ also induces an action of $\mathrm{GL}_2(\mathbb{R})$ on $\hat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$. It is 3-fold but not 4-fold transitive since Möbius transformations preserve cross ratios. More precisely, we have the following result, which we will use later on repeatedly.

Lemma 2.1. *Let (x_1, x_2, x_3) and (y_1, y_2, y_3) be triples of pairwise distinct elements in $\hat{\mathbb{R}}$. There exists some $M \in \mathrm{GL}_2(\mathbb{R})$ such that $M \cdot x_i = y_i$ for $i = 1, 2, 3$. Further, if $x_4 \in \hat{\mathbb{C}} \setminus \{x_1, x_2, x_3\}$ then $M \cdot x_4$ is uniquely determined by*

$$\mathrm{cross}(x_1, x_2, x_3, x_4) = \mathrm{cross}(y_1, y_2, y_3, M \cdot x_4)\,.$$

Proof. The Möbius transformation $f\colon z \mapsto \frac{(z-x_1)(x_2-x_3)}{(z-x_3)(x_2-x_1)}$ maps x_1, x_2, x_3 to $0, 1, \infty$ respectively. Similarly, we find a transformation g that maps y_1, y_2, y_3 to $0, 1, \infty$. Hence every $M \in \mathrm{GL}_2(\mathbb{R})$ with Möbius transformation $\mu\colon z \mapsto g^{-1}(f(z))$ satisfies $M \cdot x_i = y_i$ for all $i = 1, 2, 3$. The second assertion follows from the fact that Möbius transformations preserve cross ratios. □

2.2. Types of elements in $\mathrm{SL}_2(\mathbb{R})$

We consider in more detail the subgroup $\mathrm{SL}_2(\mathbb{R})$ of $\mathrm{GL}_2(\mathbb{R})$ and its action on the upper half plane

$$\mathbb{H} = \{x + iy \mid x \in \mathbb{R}, y \in \mathbb{R}_{>0}\}$$

induced by the homomorphism φ from paragraph 2.1. Given $M \in \mathrm{GL}_2(\mathbb{R})$, we denote by $\mathrm{tr}(M)$ its trace. We call $M \in \mathrm{SL}_2(\mathbb{R}) \setminus \{\pm I\}$

- *elliptic* if $|\mathrm{tr}(M)| < 2$,
- *parabolic* if $|\mathrm{tr}(M)| = 2$,
- *hyperbolic* if $|\mathrm{tr}(M)| > 2$.

The above properties can also be described in terms of fixed points on $\hat{\mathbb{R}}$. Elliptic, parabolic or hyperbolic elements have none, one or two fixed points on $\hat{\mathbb{R}}$ respectively.

2.3. Discrete subgroups of $\mathrm{SL}_2(\mathbb{R})$

The group $\mathrm{SL}_2(\mathbb{R})$ is a topological group. More precisely,

$$d\colon \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R}) \to \mathbb{R},\ (M, N) \mapsto \sqrt{\mathrm{tr}((M-N)(M-N)^t)}$$

is a metric on $\mathrm{SL}_2(\mathbb{R})$. A subgroup G of $\mathrm{SL}_2(\mathbb{R})$ is said to be *discrete* if it is discrete with respect to the topology induced by d, which is to say that

$$\inf\{d(M, I) \mid M \in G \setminus \{\pm I\}\} > 0\,.$$

Similarly, we say that a subgroup H of $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ is discrete if its full preimage under the canonical epimorphism

$$\overline{}\colon \mathrm{SL}_2(\mathbb{R}) \to \mathrm{PSL}_2(\mathbb{R}),\ M \mapsto \overline{M} = \{\pm M\}$$

is discrete. The result below characterizes the discrete, cyclic subgroups of $\mathrm{SL}_2(\mathbb{R})$.

Theorem 2.2. *A cyclic group* $\langle A\rangle \leq \mathrm{SL}_2(\mathbb{R})$ *is discrete if and only if* A *is either not elliptic or (elliptic) of finite order.*

Proof. See [13], Theorems 2.2.3 and 2.4.5. □

2.4. Free groups and Nielsen transformations

Given $n \in \mathbb{N}$, we denote by F_n the free group on the letters $f_1, \ldots, f_n$. Let $w \in F_n$ and let $g_1, \ldots, g_n$ be elements of some group G. Then $w(g_1, \ldots, g_n) \in G$ denotes the image of w under the homomorphism $F_n \to G$ which maps f_i to g_i.

Definition 2.3. An *elementary Nielsen transformation* takes as input a finite tuple $(g_1, g_2, \ldots, g_n)$ of elements in some group and outputs the tuple after performing one of the following operations on it.

- Interchange g_i and g_j for some $i \neq j$.
- Replace g_i by g_i^{-1}.

- Replace g_i by $g_i g_j^{-1}$ for some $i \neq j$.

Suppose g_i has finite order, n say. The transformation which replaces g_i by g_i^m with $m \in \mathbb{Z}$ and $\gcd(n, m) = 1$ is called an *E-transformation*. A *Nielsen transformation* is a finite product of elementary Nielsen transformations and an extended Nielsen transformation is a finite product of elementary Nielsen transformations and E-transformations. If an (extended) Nielsen transformation from $(f_1, \ldots, f_k)$ to $(g_1, \ldots, g_k)$ exists, then we write $(f_1, \ldots, f_k) \overset{N}{\sim} (g_1, \ldots, g_k)$ and $(f_1, \ldots, f_k) \overset{eN}{\sim} (g_1, \ldots, g_k)$ respectively.

An important property of extended Nielsen transformations is the fact that they do not change the generated group $\langle g_1, \ldots, g_k \rangle$.

2.5. Traces of elements of $\mathrm{SL}_2(\mathbb{R})$

Traces of elements of $\mathrm{SL}_2(\mathbb{R})$ play an important role throughout this paper. In particular, the following result will be used frequently.

Lemma 2.4. *Let* $U, V \in \mathrm{SL}_2(\mathbb{R})$. *Then*

1. $\mathrm{tr}(UV) + \mathrm{tr}(U^{-1}V) = \mathrm{tr}(U)\mathrm{tr}(V)$.
2. $\mathrm{tr}[U, V] = \mathrm{tr}(U)^2 + \mathrm{tr}(V)^2 + \mathrm{tr}(UV)^2 - \mathrm{tr}(U)\mathrm{tr}(V)\mathrm{tr}(UV) - 2$.
3. $\mathrm{tr}[U^k, V] = \left(\frac{\sin(k\theta)}{\sin(\theta)}\right)^2 (\mathrm{tr}[U, V] - 2)$, *if* $\mathrm{tr}(U) = 2\cos(\theta)$ *for some* $0 < \theta \leq \frac{\pi}{2}$ *and* $k \in \mathbb{N}$.

Note that $\cos(k\theta)$ with $k \in \mathbb{N}$ is the k-th Chebychev polynomial in $\cos(\theta)$, i.e.

$$\cos(k\theta) = \sum_{j=0}^{\lfloor k/2 \rfloor} (-1)^j \binom{k}{2j} (1 - \cos(\theta)^2)^j \cos(\theta)^{k-2j} .$$

Lemma 2.4 shows that if $U, V \in \mathrm{SL}_2(\mathbb{R})$ and $(U', V') \overset{N}{\sim} (U, V)$, then the commutators $[U, V]$ and $[U', V']$ have the same trace. It also shows that this is not necessarily the case if $(U', V') \overset{eN}{\sim} (U, V)$.

2.6. Computational model

Let x, y be real numbers. Throughout the paper, we assume that we have an oracle to decide if $x < y$. In particular, this allows us to decide if $x = y$. Further, we assume that we can compute square roots of $x \geq 0$ exactly as well as arbitrarily good approximations of trigonometric functions like $\cos(x)$.

Given any bound $B > 0$, we can then easily decide if $U \in \mathrm{SL}_2(\mathbb{R})$ has finite order $\leq B$ as follows: Continued fraction expansion yields the best rational approximation p/q to $\arccos(\mathrm{tr}(U)/2)/2\pi$ with $1 \leq q \leq B$. Assuming that we can compare reals, we can then decide if $U^q = I$.

For our Magma implementation, we further assume that matrices are given over some algebraic number field which is equipped with a real embedding, see Section 10 for details.

3. Elementary discrete groups

This section provides a method to decide if $G = \langle A, B\rangle \leq \mathrm{SL}_2(\mathbb{R})$ is discrete and elementary. If this is the case, a solution to the membership problem for G is also given. *Elementary* means that every pair of elements $M, N \in G$ of infinite order satisfies $\mathrm{tr}[M, N] = 2$. The condition $\mathrm{tr}[M, N] = 2$ can also be characterized as follows.

Lemma 3.1. *Two elements $M, N \in \mathrm{SL}_2(\mathbb{R})$ have a common fixed point in $\hat{\mathbb{C}}$ if and only if $\mathrm{tr}[M, N] = 2$ holds.*

Proof. See for example [1, Theorem 4.3.5]. □

The following discussion, which is taken from [1, p. 84–89], shows that there are three different types of elementary groups depending on the type of elements in G.

3.1. Every element of $G \setminus \{\pm I\}$ is elliptic

Since G is assumed to be discrete, every element of G has finite order. A result of Schur shows that G is finite, see for example [28, Theorem 5, Chapter 23]. Conversely, every finite subgroup G of $\mathrm{SL}_2(\mathbb{R})$ is elementary and discrete. Algorithms to decide if a matrix group is finite and the constructive membership problem for finite matrix groups are well-known, see for example [5, Section 3.2.2] and [11, Section 3.1.2].

3.2. G contains parabolic elements

Let $g \in G$ be parabolic with fixed point $z \in \hat{\mathbb{R}}$ and let $h \in G$. Then $x = h^{-1}gh$ is also parabolic. Hence $\mathrm{tr}[g, x] = 2$, since G is assumed to be elementary. Lemma 3.1 shows that z is a fixed point of x and thus $gh \cdot z = h \cdot z$. Consequently, $h \cdot z = z$, and therefore z is a common fixed point of all elements in G. After conjugating G with some element in $\mathrm{GL}_2(\mathbb{R})$ we can assume that $z = \infty$, see Lemma 2.1 for details. According to [1, p. 84–89], the two-generator group G is discrete if and only if it is a subgroup of

$$H = \left\{ \begin{pmatrix} a & \lambda \\ 0 & a^{-1} \end{pmatrix} \;\middle|\; a \in \{\pm 1\} \text{ and } \lambda \in \mathbb{R} \right\}.$$

Hence every element of $G \setminus \{\pm I\}$ is parabolic. In particular, this holds for A and B. Such a group G is easily recognized.

Let $\phi\colon H \to \{\pm 1\}$ be the projection onto the upper left entry and let $M \in H$. Initially, membership is decided for the case that $\phi(M) = \phi(A) = \phi(B) = 1$. Then $A = \left(\begin{smallmatrix} 1 & \lambda_1 \\ 0 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 1 & \lambda_2 \\ 0 & 1 \end{smallmatrix}\right)$ and $M = \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$. In this case, $M \in G$ if and only if $m = r_1\lambda_1 + r_2\lambda_2$ with $r_1, r_2 \in \mathbb{Z}$ and then $M = A^{r_1}B^{r_2}$. If λ_1, λ_2 are algebraic numbers, the computation of (r_1, r_2) is just linear algebra over $\mathbb{Z}$. In general, assuming some reasonable bound C on $|r_i|$, the computation of (r_1, r_2) can be done as follows. Using continued fractions one can decide if λ_1 and λ_2 are linearly dependent over $\mathbb{Q}$. If this is the case, then λ_2 and m must be rational multiplies of λ_1 and the computation of r_1 and r_2 becomes trivial. If λ_1 and λ_2 are linearly independent over $\mathbb{Q}$, then one decides if there are integers $q_i \leq C$ such that $\lambda_1 q_1 + \lambda_2 q_2 = mq_3$ using some integer relation algorithm like PSLQ [7]. The assumption on the linear independence then shows that $r_1 = q_1/q_3$ and $r_2 = q_2/q_3$ are the only rational numbers satisfying $\lambda_1 r_1 + \lambda_2 r_2 = m$. This solves the constructive membership test in the special case that $\phi(M) = \phi(A) = \phi(B) = 1$.

In the general case, it suffices to decide if $XM \in \langle A^2, B^2 \rangle$ as X runs through

$$\left\{ Y \in \{I, A, B, AB\} \mid \phi(Y) = \phi(M) \right\}.$$

This can be done using the method outlined before.

3.3. G contains hyperbolic elements

Suppose $g \in G$ is hyperbolic and without loss of generality one may assume that g fixes 0 and ∞. Let $h \in G$. As in the previous case, $gh \cdot 0 = h \cdot 0$ and $gh \cdot \infty = h \cdot \infty$. Hence h either fixes both 0 and ∞ or exchanges these two points. Therefore

$$H = \{g \in G \mid g \cdot 0 = 0 \text{ and } g \cdot \infty = \infty\}$$

is a normal subgroup of G of index at most 2.

Consider first the case that $G = H$. In this case, every element in $G \setminus \{\pm I\}$ is hyperbolic and after conjugation, $A = \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} b & 0 \\ 0 & b^{-1} \end{smallmatrix}\right)$ with $a, b \in \mathbb{R}^*$. By [1, p. 84–89], the group G is discrete if and only if $|a| = \lambda^n$ and $|b| = \lambda^m$ with $\lambda \neq 1$ and coprime integers $n, m \in \mathbb{Z}$, i.e. $|a| = |b|^{\frac{n}{m}}$. Such groups G are easily recognized.

We now want to solve the constructive membership problem for G. Initially, it is assumed that a and b are positive. Then G is generated by $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$. In this case the membership problem is trivial. If a or b is negative, one tests $YM \in \langle A^2, B^2 \rangle$ for $Y \in \{I, A, B, AB\}$ as in Section 3.2.

Now assume that the index of H in G is 2. At least one of the matrices A, B and AB fixes both 0 and ∞. Without loss of generality, this is A. Then B interchanges 0 and ∞. Hence B^2 has at least 3 fixed points in $\hat{\mathbb{C}}$ and thus $B^4 = I$. Section 3.2 shows that G contains no parabolic elements. Hence

$$\operatorname{tr}[A, B] = \operatorname{tr}[A, A^{-1}BA] = 2$$

shows that A and B commute. Such groups G are easily recognized. Conversely, every finite extension of a discrete cyclic group is necessarily discrete.

For the solution of the membership problem $M \in G$ it suffices to decide if $MB^j \in \langle A \rangle$ for some $0 \leq j \leq 3$. This is trivial since A is a diagonal matrix.

4. Classification of discrete two-generator groups

The classification of all non-elementary, discrete two-generator subgroups of $\mathrm{PSL}_2(\mathbb{R})$ was developed by Knapp [15], Purzitsky [18, 19, 21], Rosenberger [24, 27] and Purzitsky & Rosenberger [23]. The following summary is taken from Rosenberger's very nice overview [27].

Theorem 4.1. *A non-elementary, discrete two-generator subgroup $H \leq \mathrm{PSL}_2(\mathbb{R})$ has one and only one of the following descriptions in terms of generators and relations:*

(1.1) $H = \langle U, V \mid - \rangle$, *i.e. H is free of rank two.*
(1.2) $H = \langle U, V \mid U^p = 1 \rangle$ *for some integer $p \geq 2$.*
(1.3) $H = \langle U, V \mid U^p = V^q = 1 \rangle$ *for some integers $2 \leq p \leq q$ with $p + q \geq 5$.*

(1.4) $H = \langle U, V \mid U^p = V^q = (UV)^r = 1\rangle$ *for some integers* $2 \le p \le q \le r$ *with* $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$.
(1.5) $H = \langle U, V \mid [U,V]^p = 1\rangle$ *for some integer* $p \ge 2$.
(1.6) $H = \langle U, V, W \mid U^2 = V^2 = W^2 = (UVW)^p = 1\rangle$ *for some odd integer* p.

In (1.1)–(1.3), H *is a free product of the two cyclic subgroups* $\langle U\rangle$ *and* $\langle V\rangle$. *In (1.4),* H *is a* (p,q,r)*-triangle group and in (1.6),* $H = \langle UV, WU\rangle$ *and* $[UV, WU] = (UVW)^2$.

Proof. See [27, Lemma 1]. □

For an integer $n \ge 2$ let $\lambda_n = 2\cos\left(\frac{\pi}{n}\right)$.

Theorem 4.2. *Let* $A, B \in \mathrm{SL}_2(\mathbb{R})$ *with* $\mathrm{tr}[A,B] > 2$. *Then* $G = \langle A, B\rangle \le \mathrm{SL}_2(\mathbb{R})$ *is discrete if and only if* $(\overline{A}, \overline{B}) \overset{eN}{\sim} (\overline{U}, \overline{V})$ *with* $U, V \in \mathrm{SL}_2(\mathbb{R})$ *such that*

$$\begin{aligned} 0 \le \mathrm{tr}(U) \le \mathrm{tr}(V) &\le -\mathrm{tr}(UV), \\ \mathrm{tr}(U) = \lambda_p \quad &or \quad \mathrm{tr}(U) \ge 2, \\ \mathrm{tr}(V) = \lambda_q \quad &or \quad \mathrm{tr}(V) \ge 2, \\ \mathrm{tr}(UV) = -\lambda_r \quad &or \quad \mathrm{tr}(UV) \le -2 \end{aligned}$$

for some integers $p, q, r \ge 2$. *Moreover, if* G *is discrete then* $\overline{G}$ *is of type (1.1)–(1.4) in Theorem 4.1.*

Proof. See [27, Theorem 2]. □

Theorem 4.3. *Let* $A, B \in \mathrm{SL}_2(\mathbb{R})$ *with* $0 \le \mathrm{tr}(A)$, $0 \le \mathrm{tr}(B)$ *and* $\mathrm{tr}[A,B] < 2$. *Then* $G = \langle A, B\rangle \le \mathrm{SL}_2(\mathbb{R})$ *is discrete if and only if one of the following holds:*

(2.1) $\mathrm{tr}[A,B] \le -2$.
(2.2) $\mathrm{tr}[A,B] = -2\cos\left(\frac{\pi}{p}\right)$ *for some integer* $p \ge 2$.
(2.3) $\mathrm{tr}[A,B] = -2\cos\left(\frac{2\pi}{p}\right)$ *for some odd integer* $p \ge 3$.
(2.4) $\mathrm{tr}[A,B] = -2\cos\left(\frac{6\pi}{r}\right)$ *for some integer* $r \ge 7$ *coprime to* 6 *and* $(\overline{A}, \overline{B}) \overset{eN}{\sim} (\overline{R}, \overline{S})$ *with* $R, S \in \mathrm{SL}_2(\mathbb{R})$ *such that* $\mathrm{tr}(R) = \mathrm{tr}(S) = \mathrm{tr}(RS)$.
(2.5) $\mathrm{tr}[A,B] = -2\cos\left(\frac{4\pi}{r}\right)$ *for some odd integer* $r \ge 5$ *and* $(\overline{A}, \overline{B}) \overset{eN}{\sim} (\overline{R}, \overline{S})$ *with* $R, S \in \mathrm{SL}_2(\mathbb{R})$ *such that* $\mathrm{tr}(RS) = \frac{1}{2}(\mathrm{tr}(R))^2$.
(2.6) $\mathrm{tr}[A,B] = -2\cos\left(\frac{3\pi}{r}\right)$ *for some integer* $r \ge 4$ *coprime to* 3 *and* $(\overline{A}, \overline{B}) \overset{eN}{\sim} (\overline{R}, \overline{S})$ *with* $R, S \in \mathrm{SL}_2(\mathbb{R})$ *such that* $\mathrm{tr}(R) = \mathrm{tr}(S) = \mathrm{tr}(RS)$.
(2.7) $\mathrm{tr}[A,B] = -2\cos\left(\frac{4\pi}{7}\right)$ *and* $(\overline{A}, \overline{B}) \overset{eN}{\sim} (\overline{R}, \overline{S})$ *with* $R, S \in \mathrm{SL}_2(\mathbb{R})$ *such that* $\mathrm{tr}(S) = \mathrm{tr}(RS) = \mathrm{tr}(R) + 1$.

Moreover, if G *is discrete then* $\overline{G}$ *is of type (1.1) in (2.1), of type (1.5) in (2.2), of type (1.6) in (2.3), a* $(2,3,r)$*-triangle group in (2.4), a* $(2,4,r)$*-triangle group in (2.5), a* $(3,3,r)$*-triangle group in (2.6) and a* $(2,3,7)$*-triangle group in (2.7).*

Proof. See [27, Theorem 3]. □

The next section will explain in detail how the pairs (U,V) and (R,S) mentioned in Theorems 4.2 and 4.3 can be constructed from A and B.

5. Deciding discreteness

This section discusses an algorithm to decide if a non-elementary subgroup $\langle A, B\rangle$ of $\mathrm{SL}_2(\mathbb{R})$ is discrete. The method used here is much simpler than the one given by Gilman [10, Theorem 14.4.1]. We discuss the cases $\mathrm{tr}[A, B] < 2$ and $\mathrm{tr}[A, B] > 2$ separately.

5.1. The case tr[A,B] < 2

Suppose $G = \langle A, B\rangle \leq \mathrm{SL}_2(\mathbb{R})$ and $\mathrm{tr}[A, B] < 2$. Purzitsky [19] and Rosenberger [12, 14] both give a similar method to decide if G is discrete. It is based on the following lemma.

Lemma 5.1. *Let $A, B \in \mathrm{SL}_2(\mathbb{R})$ such that $\mathrm{tr}[A, B] < 2$. Then*

1. *A and B are both hyperbolic.*
2. *There exist $U, V \in \mathrm{SL}_2(\mathbb{R})$ with $(\overline{U}, \overline{V}) \overset{N}{\sim} (\overline{A}, \overline{B})$ such that*

$$2 < \mathrm{tr}(U) \leq \mathrm{tr}(V) \leq \mathrm{tr}(UV) \leq \tfrac{1}{2}\mathrm{tr}(U)\mathrm{tr}(V).$$

Moreover, $(\mathrm{tr}(U), \mathrm{tr}(V), \mathrm{tr}(UV))$ is uniquely determined.

Proof. See [12, Lemma 2.5] and [14, Lemma 1] or [19]. □

A pair (U, V) as in Lemma 5.1 can be obtained from (A, B) by applying Nielsen transformations in a trace minimizing manner:

Algorithm 1. *Input: $A, B \in \mathrm{SL}_2(\mathbb{R})$ with $\mathrm{tr}[A, B] < 2$.*
Output: $U, V \in \mathrm{SL}_2(\mathbb{R})$ with $\langle \overline{U}, \overline{V}\rangle = \langle \overline{A}, \overline{B}\rangle \leq \mathrm{PSL}_2(\mathbb{R})$ and

$$2 < \mathrm{tr}(U) \leq \mathrm{tr}(V) \leq \mathrm{tr}(UV) \leq \tfrac{1}{2}\mathrm{tr}(U)\mathrm{tr}(V).$$

1. *Initialize $U := \pm A$ and $V := \pm B$ such that $\mathrm{tr}(U), \mathrm{tr}(V) \geq 0$.*
2. *If $\mathrm{tr}(V) < \mathrm{tr}(U)$, swap U and V.*
3. *If $\mathrm{tr}(U^e V) < \mathrm{tr}(V)$ for some $e \in \{\pm 1\}$ then replace V by $U^e V$ and go to step (2).*
4. *If $\mathrm{tr}(UV) \leq \mathrm{tr}(U^{-1}V)$ then return (U, V) otherwise return (U^{-1}, V).*

Proof. See for example [12] or [19]. □

Remark 5.2. By means of Algorithm 1, it can be decided if $G = \langle A, B\rangle \leq \mathrm{SL}_2(\mathbb{R})$ with $\mathrm{tr}[A, B] < 2$ is discrete. The first three cases of Theorem 4.3 can be checked directly. In the remaining cases let (U, V) be the output of Algorithm 1 when applied to (A, B). The matrices R, S in Theorem 4.3 also satisfy

$$2 < \mathrm{tr}(R) \leq \mathrm{tr}(S) \leq \mathrm{tr}(RS) \leq \tfrac{1}{2}\mathrm{tr}(R)\mathrm{tr}(S)\,.$$

Hence Lemma 5.1 shows that G is discrete if and only if $(R, S) := (U, V)$ satisfies one of the conditions (2.4)–(2.7) of Theorem 4.3.

5.2. The case tr[A,B] > 2

Suppose $G = \langle A, B\rangle \leq \mathrm{SL}_2(\mathbb{R})$ and $\mathrm{tr}[A, B] > 2$. In this case, applying Nielsen transformations in a trace minimizing manner is not enough to decide if G is discrete.

The proofs of Lemma 2 and Theorem 1 of [14] when combined with [26, p. 264] yield the following algorithm to decide if G is discrete. It uses extended Nielsen transformations to

- minimize the trace of the commutator of the generators,
- minimize the traces of non-elliptic generators,
- maximize the traces of elliptic generators,

where the first objective takes precedence over the others.

Algorithm 2. *Input: Some matrices* $A, B \in \mathrm{SL}_2(\mathbb{R})$ *with* $\mathrm{tr}[A, B] > 2$.
Output: True if $G = \langle A, B\rangle$ *is discrete and if so, a pair of matrices* (U, V) *in* $\mathrm{SL}_2(\mathbb{R})$ *with* $\overline{G} = \langle \overline{U}, \overline{V}\rangle$ *that satisfies the conditions of Theorem 4.2. Otherwise false is returned.*

1. *If* A *or* B *is elliptic of infinite order, return false.*
2. *For each* $X \in \{A, B\}$ *of finite order, replace* X *by an appropriate power such that* $|\mathrm{tr}(X)| = \lambda_n$ *where* n *denotes the order of* $\overline{X} \in \mathrm{PSL}_2(\mathbb{R})$.
3. *Initialize* $U := \pm A$ *and* $V := \pm B$ *such that* $\mathrm{tr}(U), \mathrm{tr}(V) \geq 0$.
4. *If* $\mathrm{tr}(U) < \mathrm{tr}(V)$ *exchange* U *and* V.
5. *Set* $S := \{UV, U^{-1}V\}$.
   (a) *If* S *contains an elliptic element of infinite order, return false.*
   (b) *If* S *contains no elliptic element, let* $m := \min\{|\mathrm{tr}(X)| \mid X \in S\}$. *If* $m < \mathrm{tr}(V)$, *replace* V *by some matrix in* $\{\pm X \mid X \in S\}$ *that has trace* m *and go to (4).*
   (c) *For each* $X \in S$ *of finite order, write* $|\mathrm{tr}(X)| = 2\cos\left(\frac{k\pi}{n}\right)$ *with* $1 \leq k \leq \frac{n}{2}$ *and* $\gcd(k, n) = 1$. *If* $\lambda_n < \mathrm{tr}(V)$ *or* $k \neq 1$, *replace* V *by* eX^ℓ *where* $e \in \{\pm 1\}$ *and* $\ell \in \mathbb{Z}$ *such that* $\mathrm{tr}(eX^\ell) = \lambda_n$. *Then go to (4).*
6. *If* $\mathrm{tr}(UV) > 0$ *then replace* V *by* V^{-1}.
7. *Return true and the pair* (U, V).

Proof. The proof is already implicitly contained in [14, 26]. To begin, some remarks on the algorithm are given. In each step, the matrices U and V have non-negative traces and if they are elliptic, they have finite order. Steps (3)–(5) ensure that $0 \leq \mathrm{tr}(U) \leq \mathrm{tr}(V)$ and the two traces are either at least 2 or of the form λ_n for some $n \in \mathbb{Z}$. Also note that the replacement in step (5) always yields generators U and V with $\mathrm{tr}[U, V] > 2$ as Lemma 2.4 shows.

Let us now show that the algorithm terminates. First assume that the algorithm iterates through step (5c) infinitely many times. Then after at most two iterations U, V and some element in S have finite order. After replacing V by V^{-1}, we may assume that $UV \in S$ has finite order. This implies that $\mathrm{tr}(U) = \lambda_p$, $\mathrm{tr}(V) = \lambda_q$ and $\mathrm{tr}(UV) = \pm 2\cos\left(\frac{k\pi}{n}\right)$ for some $2 \leq p \leq q$ and coprime integers $k, n \in \mathbb{Z}$. Lemma 2.4

then shows that $\mathrm{tr}(g) \in \mathbb{Q}(\lambda_p, \lambda_q, \lambda_n)$ for all $g \in G$. This field only contains finitely many elements of the form $\cos\left(\frac{r\pi}{s}\right)$. In particular, the set

$$\{\mathrm{tr}[U', V'] \mid U',\, V',\, U'V' \text{ have finite order and } (\overline{A}, \overline{B}) \overset{eN}{\sim} (\overline{U}', \overline{V}')\}$$

is finite by Lemma 2.4. Let $e \in \{\pm 1\}$ and $\ell \in \mathbb{Z}$ such that $\mathrm{tr}(e(UV)^\ell) = \lambda_n$. The assumption that the algorithm does not terminate implies that $k \neq 1$ or $n < q$. In the first case, $\mathrm{tr}[U, V] = \mathrm{tr}[U, UV] > \mathrm{tr}[U, e(UV)^\ell]$ by Lemma 2.4. Note that all other substitutions in step (5) are Nielsen transformations and thus do not change $\mathrm{tr}[U, V]$. Hence after some point $k = 1$ in step (5c). But then the algorithm reduces the order of $\overline{V}$ in each iteration.

So if the algorithm does not terminate, after a certain point, the algorithm only iterates through step (5b). The proof of [14, Lemma 2] shows that after finitely many steps, S contains an element of negative trace. Without loss of generality, suppose that $\mathrm{tr}(UV) < 0$. Then $\mathrm{tr}(U^{-1}V) \geq -\mathrm{tr}(UV)$ by Lemma 2.4. If $-\mathrm{tr}(UV) \geq \mathrm{tr}(V)$ there will be no replacement made in step (5c). Otherwise this step will replace (U, V) once more, this time by $(U, V' := -UV)$. But then in the following iteration, the set S will be $S = \{-V, -U^2V\}$. Note that this time $\mathrm{tr}(-U^2V) = \mathrm{tr}(V) - \mathrm{tr}(U)\mathrm{tr}(UV) \geq \mathrm{tr}(V) > \mathrm{tr}(V')$. So at this point, no replacement will be made. Thus eventually we will reach step (6) and the algorithm terminates.

Let us now prove the correctness of the algorithm. If the algorithm ever encounters an elliptic element of infinite order, then G is non-discrete by Theorem 2.2. Suppose this does not happen. The discussion above shows that after step (6) one of the matrices UV, $U^{-1}V$ has negative trace. Step (7) ensures that $\mathrm{tr}(UV) < 0$. Further, we can only ever reach step (7) if the traces of $U, V, -UV$ are greater than 2 or of the form λ_n with some integer $n \geq 2$. In other words, the pair (U, V) in step (7) satisfies the conditions of Theorem 4.2. This proves that G is discrete and finishes the proof. □

6. The constructive membership problem in $\mathrm{SL}_2(\mathbb{R})$

Let $A, B \in \mathrm{SL}_2(\mathbb{R})$ such that $G = \langle A, B\rangle$ is discrete. The constructive membership problem for G asks whether any given $M \in \mathrm{SL}_2(\mathbb{R})$ lies in G and if so, how to express M as a word in the generators A and B.

If G is elementary, this problem was already solved in Section 3. So let G be non-elementary. We will show that it suffices to solve the corresponding problem for $\overline{M}$ and $\overline{G}$. First, we introduce a more suitable pair of generators $(\overline{U}, \overline{V})$ for $\overline{G}$.

Definition 6.1. Let $G \leq \mathrm{SL}_2(\mathbb{R})$ be discrete and non-elementary. A pair (U, V) of elements in $\mathrm{SL}_2(\mathbb{R})$ with $0 \leq \mathrm{tr}(U) \leq \mathrm{tr}(V)$ and $\overline{G} = \langle \overline{U}, \overline{V}\rangle$ is called a *witness pair* for G if one of the following four conditions holds:

1. $\mathrm{tr}[U, V] \leq -2$.
2. $\mathrm{tr}[U, V] = -\lambda_p$ for some integer $p \geq 2$.
3. $\mathrm{tr}[U, V] = -2\cos\left(\frac{2\pi}{p}\right)$ for some odd integer $p \geq 3$.
4. $\mathrm{tr}[U, V] > 2$ and
   - $\mathrm{tr}(V) \leq -\mathrm{tr}(UV)$,

- $\operatorname{tr}(U) = \lambda_p$ or $\operatorname{tr}(U) \geq 2$,
- $\operatorname{tr}(V) = \lambda_q$ or $\operatorname{tr}(V) \geq 2$,
- $\operatorname{tr}(UV) = -\lambda_r$ or $\operatorname{tr}(UV) \leq -2$

with integers $p, q, r \geq 2$.

Note that a witness pair for G does not necessarily generate G, but its existence guarantees that G is discrete. Also note that Algorithms 1 and 2 construct a witness pair for $G = \langle A, B\rangle$ unless $\operatorname{tr}[A, B] < 2$ and $\overline{G}$ is a triangle group. Suppose now $\overline{G}$ is a triangle group such that $[A, B]$ has finite order. In [25, 27] Rosenberger expresses all pairs $(\overline{R}, \overline{S})$ of generators of $\overline{G}$ as words in some witness pair. Using these words, it is quite easy to reverse this situation.

Lemma 6.2. *Suppose $G = \langle A, B\rangle \leq \mathrm{SL}_2(\mathbb{R})$ satisfies one of the conditions (2.4)–(2.7) of Theorem 4.3. Further, let r be the order of $[\overline{A}, \overline{B}] \in \mathrm{PSL}_2(\mathbb{R})$ and let R, S be the output of Algorithm 1 when applied to A and B. Then the following matrices yield a witness pair (U, V) for G.*

(2.4) Let $V = [R, S]^{-2s}R$ and $U = V^{-2}SV^2$ where $6s \equiv 1 \pmod r$.
(2.5) Let $V = (-1)^{s+1}[R, S]^{-s}R$ and $U = V^2R^{-1}$ where $4s \equiv 1 \pmod r$.
(2.6) Let $U = -([R, S]^sS)^{-1}$ and $V = -[R, S]^{-s}R$ where $3s \equiv 1 \pmod r$.
(2.7) Let $U = -[S^{-1}, R] \cdot [S^{-1}RS, R] \cdot [R, RS^{-1}] \cdot [RS^{-1}, T] \cdot [S^{-1}R, T] \cdot [S^{-1}, T] \cdot T$ and $V = -([S^{-1}, R]^3 \cdot RS \cdot [T, S^{-1}R] \cdot [T, RS^{-1}] \cdot [RS^{-1}, R]^2 \cdot [R, S^{-1}]^2)^2$ where $T = (RS)^{-1}$.

Proof. Suppose $\operatorname{tr}[A, B] = 2\cos\left(\frac{6\pi}{r}\right)$ with $r \geq 7$ and $\gcd(6, r) = 1$. Let (U', V') be a witness pair for G. By Theorem 4.3, $\overline{G}$ is a $(2, 3, r)$-triangle group. Thus $\operatorname{tr}(U) = \lambda_2 = 2$, $\operatorname{tr}(V) = \lambda_3 = 1$ and $\operatorname{tr}(UV) = -\lambda_r$. As suggested by [25, 27], let $R' := [U', V']$ and $S' := [V'^{-1}, U']$. Then $V' = [R', S']^{-2s}R'$ and $U' = V'^{-2}S'V'^2$. Lemma 2.4 shows that R' and S' satisfy

$$2 < \operatorname{tr}(R') = \operatorname{tr}(S') = \operatorname{tr}(R'S') \leq \frac{1}{2}\operatorname{tr}(R')\operatorname{tr}(S')\,.$$

Thus $\operatorname{tr}(R) = \operatorname{tr}(R')$, $\operatorname{tr}(S) = \operatorname{tr}(S')$ and $\operatorname{tr}(RS) = \operatorname{tr}(R'S')$. Induction on the word length shows that $\operatorname{tr}(w(R, S)) = \operatorname{tr}(w(R', S'))$ for all $w \in F_2$. In particular, $\operatorname{tr}(U) = \operatorname{tr}(U')$, $\operatorname{tr}(V) = \operatorname{tr}(V')$ and $\operatorname{tr}(UV) = \operatorname{tr}(U'V')$. Thus (U, V) is a witness pair for G.
In the cases (2.5)–(2.7) one can start with the words $(R', S') = (U'^{-1}V'^2, V'^{-1}U'^{-1}V'^3)$, $(U'V'^{-1}, V'^{-1}U')$ and $(U'V'^{-1}(U'V')^4U', U'V'^{-1}[U', V'^{-1}]^2)$ respectively. We leave the details to the reader. □

If one keeps track of the (extended) Nielsen transformations performed in Algorithms 1 and 2, one obtains words $w, w' \in F_2$ such that $\overline{U} = w(\overline{A}, \overline{B})$ and $\overline{V} = w'(\overline{A}, \overline{B})$. Using these words, one can decide if $-I \in G$ and if so, how to express $-I$ as a word in A and B. Our method is based on the following observation.

Lemma 6.3. *Let $G = \langle U, V\rangle \leq \mathrm{SL}_2(\mathbb{R})$. Suppose $\overline{G}$ has a finite presentation $\overline{G} \cong \langle F_2 \mid r_1, \ldots, r_n\rangle$ with $r_i \in F_2$ and the isomorphism is defined by $\overline{U} \mapsto f_1$, $\overline{V} \mapsto f_2$. Then $-I \in G$ if and only if $r_i(U, V) = -I$ for some $1 \leq i \leq n$.*

Proof. Suppose $-I \in G$, i.e. there exists a word $w \in F_2$ with $w(U,V) = -I$. Then w lies in the normal subgroup generated by the relations r_i. Hence $w = r_{i_1}^{g_{i_1}} \cdot \ldots \cdot r_{i_n}^{g_{i_n}}$ with $g_{i_j} \in F_2$. So $w(U,V) = -I$ is only possible if $r_j(U,V) = -I$ for some j. □

Now we can decide if $-I \in G$ as follows and if so, express $-I$ as a word in A and B.

Theorem 6.4. *Let $G = \langle A, B\rangle \leq \mathrm{SL}_2(\mathbb{R})$ be discrete and non-elementary.*

1. *If $\mathrm{tr}[A,B] \leq -2$ or $\mathrm{tr}[A,B] = -2\cos\left(\frac{\pi}{r}\right)$ for some odd integer $r \geq 3$ then $-I \notin G$.*
2. *Suppose $\mathrm{tr}[A,B] = -2\cos\left(\frac{n\pi}{r}\right)$ with $\gcd(n,r) = 1$. If nr is even, then $-I = [A,B]^r \in G$.*
3. *Suppose $\mathrm{tr}[A,B] = -2\cos\left(\frac{3\pi}{r}\right)$ with r odd. Let (R,S) be the output of Algorithm 1 when applied to (A,B). Let $w_1, w_2 \in F_2$ such that $\overline{R} = w_1(\overline{A},\overline{B})$ and $\overline{S} = w_2(\overline{A},\overline{B})$. Set $R' = w_1(A,B)$ and $S' = w_2(A,B)$. Further, let $U = ([R',S']^s \cdot S')^{-1}$ and $V = [R',S']^{-s}R'$ where $3s \equiv 1 \pmod r$. Then $-I \in G$ if and only if $-I = U^3$ or $-I = V^3$.*
4. *Suppose $\mathrm{tr}[A,B] > 2$.*
   (a) *Suppose Algorithm 2 applies an extended Nielsen transformation where $X \in \mathrm{SL}_2(\mathbb{R})$ is replaced by X^e for some even integer e. Further suppose that $\overline{X} = w(\overline{A},\overline{B})$ for some $w \in F_2$ and $w(A,B)$ has even order, o say. Then $-I = w(A,B)^{o/2} \in G$.*
   (b) *Suppose case (a) never occurs. Let (U,V) be the witness pair for G computed by Algorithm 2 and let $w, w' \in F_2$ such that $\overline{U} = w(\overline{A},\overline{B})$ and $\overline{V} = w'(\overline{A},\overline{B})$. Then $U' := w(A,B)$ and $V' := w'(A,B)$ generate G and $(\overline{U'},\overline{V'}) = (\overline{U},\overline{V})$ satisfies one (and only one) of the relations (1.1)–(1.4) of Theorem 4.1. In particular, Lemma 6.3 can be used to decide whether $-I \in G$ and if so, how to express $-I$ as a word in (U',V') and thus in (A,B).*

Proof. The first assertion follows from Lemma 6.3 while the second is clear. Suppose now $\mathrm{tr}[A,B] = -2\cos\left(\frac{3\pi}{r}\right)$ with r odd and suppose that $U^3 = V^3 = I$. We have to show that $-I \notin G$. Algorithm 1 only performs Nielsen transformations. Thus $G = \langle R', S'\rangle$. Lemma 6.2 shows that $(-U,-V)$ is a witness pair for G. By [20, Theorem 2], $[\overline{R}', \overline{S}']$ is conjugate to $(\overline{UV})^3$ in $\overline{G} = \langle \overline{U}, \overline{V}\rangle$. Comparing traces shows that $[R',S']$ is conjugate to $(UV)^3$ in $\langle U,V\rangle$. Hence $[R',S'] \in \langle U,V\rangle$ and thus $G = \langle U,V\rangle$. But then $-I \notin G$ by Lemma 6.3.
Suppose now $\mathrm{tr}[A,B] > 2$. If case (a) never occurs, then every extended Nielsen transformation that Algorithm 2 performs induces an extended Nielsen transformation of G. Hence $G = \langle U', V'\rangle$. □

In the subsequent sections, we solve the constructive membership problem for $\overline{G} \leq \mathrm{PSL}_2(\mathbb{R})$ using geometric methods. The solution to this problem and Theorem 6.4 yield a solution to the constructive membership problem for G.

Algorithm 3 (Constructive membership in $\mathrm{SL}_2(\mathbb{R})$)**.**
Input: Three matrices $A, B, M \in \mathrm{SL}_2(\mathbb{R})$.
Output: Decide if $G = \langle A, B\rangle \leq \mathrm{SL}_2(\mathbb{R})$ is discrete. If G is discrete and $M \in G$, a word $w \in F_2$ such that $M = w(A,B)$ is also returned.

1. *Using the methods of Section 3, decide if G is elementary and discrete. If so, solve the constructive membership using the methods presented there.*
2. *If either $\mathrm{tr}[A,B]=2$ or Algorithms 1 and 2 show that G is not discrete, then return "not discrete".*
3. *From Algorithms 1 and 2 and Lemma 6.2, one obtains a witness pair (U,V) of G as well as words $w_1, w_2 \in F_2$ such that $\overline{U}=w_1(\overline{A},\overline{B})$ and $\overline{V}=w_2(\overline{A},\overline{B})$.*
4. *Decide if $\overline{M} \in \overline{G}$. If not, then return false. Otherwise find some $v \in F_2$ such that $v(\overline{U},\overline{V})=\overline{M}$. This step depends on the isomorphism type of $\overline{G}$.*
   - *If U, V, UV all have finite order (i.e. $\overline{G}$ is a triangle group), then one can apply Algorithm 5.*
   - *If $[A,B]$ has finite order, but $\overline{G}$ is not a triangle group, then one can use Algorithm 6 together with Remark 9.5.*
   - *In all other cases, $\overline{G} \cong \langle \overline{U} \rangle * \langle \overline{V} \rangle$ is a free product and one can apply Algorithm 4 to the fundamental domain given in Theorem 7.8, 7.10, 7.12 or 7.13 depending on the traces of U, V and UV.*
5. *Let $w := v(w_1(f_1,f_2), w_2(f_1,f_2))$.*
6. *If $w(A,B)=M$ then return w.*
7. *Using Theorem 6.4, decide if $-I \in G$. If not, then return false. Otherwise return ww' where $w' \in F_2$ such that $w'(A,B)=-I$.*

7. Free Products

This section solves the constructive membership problem in the case that $\overline{G} \leq \mathrm{PSL}_2(\mathbb{R})$ is a free product. Our solution is based on a variant of the well known Ping-Pong Lemma.

Definition 7.1. Let G be a group operating on a topological space $\mathbb{X}$. For $\mathbb{Y} \subseteq \mathbb{X}$ let $\mathbb{Y}^o$, $\mathbb{Y}^c$ and $\partial\mathbb{Y}$ denote the interior, the closure and the boundary of $\mathbb{Y}$ respectively. A subset $\mathbb{F}$ of $\mathbb{X}$ is called a fundamental domain for G if the following two conditions are satisfied:

1. For each $x \in \mathbb{X}$ there exists some $g \in G$ such that $g \cdot x \in \mathbb{F}^c$.
2. If $z \in \mathbb{F}^o$ and $g \in G \setminus \{1\}$ then $g \cdot z \notin \mathbb{F}^c$.

Theorem 7.2. *Let $G=\langle g_1,\ldots,g_n\rangle$ be a group acting on a topological space $\mathbb{X}$ and suppose that at least one of the generators g_i has order greater than 2. Assume that there exists pairwise disjoint subsets*

$$\mathbb{X}_1^+,\ldots,\mathbb{X}_m^+,\mathbb{X}_1^-,\ldots,\mathbb{X}_m^-,\mathbb{X}_{m+1},\ldots,\mathbb{X}_n$$

of $\mathbb{X}$ with the following properties:

1. *$g_i \cdot (\mathbb{X} \setminus (\mathbb{X}_i^+)^o) \subseteq \mathbb{X}_i^-$ and $g_i^{-1} \cdot (\mathbb{X} \setminus (\mathbb{X}_i^-)^o) \subseteq \mathbb{X}_i^+$ for $1 \leq i \leq m$.*
2. *The elements $g_{m+1},\ldots,g_n$ have finite order and $g_i \cdot (\mathbb{X} \setminus \mathbb{X}_i^o) \subseteq \mathbb{X}_i$ for $m+1 \leq i \leq n$.*
3. *$\mathbb{F}=\mathbb{X} \setminus (\mathbb{X}_1^+ \cup \ldots \cup \mathbb{X}_m^+ \cup \mathbb{X}_1^- \cup \ldots \cup \mathbb{X}_m^- \cup \mathbb{X}_{m+1} \cup \ldots \cup \mathbb{X}_n)$ is a fundamental domain for G with $\mathbb{F}^o \neq \emptyset$.*

Then $g_1, \ldots, g_m$ have infinite order and G is a free product $G \cong \langle g_1 \rangle * \ldots * \langle g_n \rangle$.

Proof. If $1 \leq i \leq m$ and $r \geq 1$ then $g_i^r \cdot \mathbb{F}^o \subseteq g_i^{r-1} \cdot \mathbb{X}_i^- \subseteq \mathbb{X}_i^-$ shows that $g_i^r \cdot \mathbb{F}^o \neq \mathbb{F}^o$. Hence g_i has infinite order. The Ping-Pong Lemma shows that G is a free product of the cyclic subgroups $\langle g_i \rangle$, see [16, Proposition 12.2] for details. □

In the situation of Theorem 7.2, suppose that we have oracles to decide if any given $x \in \mathbb{X}$ lies in $\mathbb{Y}$ for $\mathbb{Y} = \mathbb{X}_i$, $\mathbb{Y} = \mathbb{X}_j^{\pm}$ and $\mathbb{Y} = \mathbb{F}^c$. Then we can solve the constructive membership problem for G by Algorithm 4 below. Note that in the sequel, the set $\mathbb{X}$ will be the upper half plane $\mathbb{H}$ and the sets $\mathbb{X}_i$, $\mathbb{X}_j^{\pm}$ and $\mathbb{F}$ will be polygons, i.e. intersections of hyperbolic half spaces. So in these cases, we always will have such inclusion tests.

Algorithm 4. *Let H be a group acting on a topological space $\mathbb{X}$.*
Input: Generators $g_1, \ldots, g_n$ of a subgroup G of H, subsets $\mathbb{X}_i^{\pm} \subseteq \mathbb{X}$ for $1 \leq i \leq m$ and $\mathbb{X}_i \subseteq \mathbb{X}$ for $m < i \leq n$ satisfying the conditions of Theorem 7.2. Further, $z' \in \mathbb{F}^o$ and $g \in H$.
Output: A word $w = w(f_1, \ldots, f_n) \in F_n$ with $w(g_1, \ldots, g_n) = g$ if g is an element of G and false otherwise.

1. *Initialize $w = 1 \in F_n$ and let $z = g \cdot z'$.*
2. *While $z \notin \mathbb{F}^c$:*
   (a) *If $z \in \mathbb{X}_i^+$ for some $i \in \{1, \ldots, m\}$, then replace z by $g_i \cdot z$ and w by wf_i^{-1}.*
   (b) *If $z \in \mathbb{X}_i^-$ for some $i \in \{1, \ldots, m\}$, then replace z by $g_i^{-1} \cdot z$ and w by wf_i.*
   (c) *If $z \in \mathbb{X}_i$ for some $i \in \{m+1, \ldots, n\}$, then replace z by $g_i^{-1} \cdot z$ and w by wf_i.*
3. *Evaluate $v = w(g_1, \ldots g_n)$.*
4. *If $z = z'$ and $v = g$ return w and false otherwise.*

Proof. We first show that the algorithm terminates. For $m < i \leq n$ let o_i denote the order of g_i. As $\mathbb{F}$ is a fundamental domain, there exists a unique $v \in G$ such that $v^{-1} \cdot z \in \mathbb{F}^c$. Then $v = g_{i_1}^{e_1} \cdot \ldots \cdot g_{i_r}^{e_r}$ with $1 \leq i_j \leq n$, $i_j \neq i_{j+1}$, $e_j \in \mathbb{Z} \setminus \{0\}$ and $1 \leq e_j < o_j$ whenever $j > m$. If $r = 0$, then the algorithm certainly terminates, so suppose $r > 0$. If $e_1 < 0$ then $z \in v \cdot \mathbb{F}^c \subseteq \mathbb{X}_{i_1}^+$. Hence the algorithm would set $w = f_{i_1}^{-1}$ during the first iteration and replace z by $g_{i_1} \cdot z$. Similarly, if $e_1 > 0$, then we set $w = f_{i_1}$ and replace z by $g_{i_1}^{-1} \cdot z$ in the first iteration. Induction on $\sum_j |e_j|$ shows that the iterations through step (2) simply reconstruct v and hence the algorithm terminates.
Now we show that the output of the algorithm is correct. If it terminates with $z = z'$ and $v = g$, then $g = w(g_1, \ldots, g_n) \in G$. Conversely, if $g \in G$, then $z, z' \in \mathbb{F}^o$ implies $z = z'$ and $g = v$ since $\mathbb{F}$ is a fundamental domain. □

Fundamental domains for cyclic groups show up repeatedly in the sequel. In most cases, we can choose these fundamental domains to be of a canonical form, the so-called isometric circles.

Definition 7.3. Let

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) .$$

Then the isometric circle of U is defined as

$$I_U = \{z \in \mathbb{H} \mid |cz + d| < 1\} .$$

Note that if $c \neq 0$, i.e. $U \cdot \infty \neq \infty$, then the boundary of I_U is a geodesic with center $-d/c$ and radius $|c|^{-1}$.

Lemma 7.4. *Let $U \in \mathrm{SL}_2(\mathbb{R})$ with $U \cdot \infty \neq \infty$. Then a fundamental domain of the group $\langle \overline{U} \rangle \leq \mathrm{PSL}_2(\mathbb{R})$ is given by*

$$\mathbb{F}_U = \mathbb{H} \setminus \bigcup_{k \in \mathbb{Z},\, U^k \neq \pm I} I_{U^k}.$$

Proof. See [8, Chapter II, Theorem 7]. □

Remark 7.5. Let U be either

1. hyperbolic or
2. elliptic with $\mathrm{tr}(U) = 2\cos\left(\frac{\pi}{n}\right)$ and $U \cdot i = i$.

Then every isometric circle of an element of $\langle U \rangle \setminus \{\pm I\}$ is contained in $I_U \cup I_{U^{-1}}$. Thus the set $\mathbb{F}_U = \mathbb{H} \setminus (I_U \cup I_{U^{-1}})$ is a fundamental domain of $\langle U \rangle$. Further, if U is elliptic, then $U \cdot (\mathbb{H} \setminus (I_U \cup I_{U^{-1}})) \subseteq I_U \cup I_{U^{-1}}$.

If $G = G_1 * G_2$ is a free product, one can sometimes combine the fundamental domains of G_1 and G_2 to obtain a fundamental domain for G.

Theorem 7.6 (Klein's Combination Theorem)**.** *Let G_1, G_2 be discrete subgroups of $\mathrm{PSL}_2(\mathbb{R})$ and let $\mathbb{F}_i$ be a fundamental domain for the action of G_i on $\hat{\mathbb{C}}$. If $\hat{\mathbb{C}} \setminus \mathbb{F}_1^o \subseteq \mathbb{F}_2^o$ and $\hat{\mathbb{C}} \setminus \mathbb{F}_2^o \subseteq \mathbb{F}_1^o$, then $\mathbb{F}_1 \cap \mathbb{F}_2$ is a fundamental domain for $G = \langle G_1, G_2 \rangle$ and $G \cong G_1 * G_2$.*

Proof. See for example [9, pp. 190–192]. □

For the remainder of this section, let $G = \langle A, B \rangle \leq \mathrm{SL}_2(\mathbb{R})$ be discrete such that $\overline{G}$ is a free product of two cyclic subgroups. Further, let (U, V) be a witness pair for G. Depending on the isomorphism type of $\overline{G}$, we give fundamental domains for $\overline{G}$ that are of the form described by Theorem 7.2. This solves the constructive membership problem for $\overline{G}$ and, as we have seen in Section 6, also for G.

7.1. U and V are both elliptic

Lemma 7.7. *Suppose U and V both have finite order. Then U and V can be conjugated simultaneously in $\mathrm{GL}_2(\mathbb{R})$ to the form*

$$U = \begin{pmatrix} \cos\left(\frac{\pi}{\ell}\right) & \sin\left(\frac{\pi}{\ell}\right) \\ -\sin\left(\frac{\pi}{\ell}\right) & \cos\left(\frac{\pi}{\ell}\right) \end{pmatrix}, \quad V = \begin{pmatrix} \cos\left(\frac{\pi}{m}\right) & b \\ c & \cos\left(\frac{\pi}{m}\right) \end{pmatrix},$$

with $\ell, m \in \mathbb{N}$, $|c| < |b|$, $b > 0$ and $c < 0$.

Proof. The geodesic g through the fixed points of U and V intersects $\hat{\mathbb{R}}$ in x_1 and x_2 say. Lemma 2.1 shows that there exists some $S \in \mathrm{GL}_2(\mathbb{R})$ such that $S \cdot x_1 = 0$ and $S \cdot x_2 = \infty$. So conjugating U and V with S maps g on the imaginary axis, i.e. the fixed points of U and V are ri and si with $r, s > 0$. After replacing S by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & r \end{smallmatrix}\right) S$ one may

assume that $r = 1$. Replacing S with $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)S$ if necessary brings U to the desired form. Finally, replacing S by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)S$ if necessary ensures that $s > 1$. Then

$$V = \begin{pmatrix} \cos\left(\frac{\pi}{m}\right) & b \\ -b/s^2 & \cos\left(\frac{\pi}{m}\right) \end{pmatrix}$$

for some $m \in \mathbb{N}$. The condition $\operatorname{tr}(UV) < 0$ forces b to be positive. □

Theorem 7.8. *Let (U, V) be as in Lemma 7.7. Then ui with $u = \sqrt{-b/c}$ is the fixed point of V in $\mathbb{H}$. Let $\mathbb{X}_U = I_U \cup I_{U^{-1}}$ and let $\mathbb{X}_V$ be the region of $\mathbb{H}$ that is bounded by the two geodesics through ui that enclose an angle of $\pm\frac{\pi}{m}$ with the imaginary axis. Then $\mathbb{X}_U$ and $\mathbb{X}_V$ satisfy the conditions of Theorem 7.2. In particular, $\mathbb{F} := \mathbb{H} \setminus (\mathbb{X}_U \cup \mathbb{X}_V)$ is a fundamental domain for $\overline{G} = \langle \overline{U}, \overline{V} \rangle$ and $z' := \frac{u+1}{2} i \in \mathbb{F}^o$. The sets $\mathbb{X}_U, \mathbb{X}_V$ and $\mathbb{F}$ are illustrated in Figure 1.*

Proof. Remark 7.5 shows that $\mathbb{H} \setminus \mathbb{X}_U$ is a fundamental domain for $\langle U \rangle$. The matrix V rotates at ui by an angle of $\frac{2\pi}{m}$ counter clockwise and $\mathbb{H} \setminus \mathbb{X}_V$ is a fundamental domain for $\langle V \rangle$, see [15, Lemma 2.1] for details.
If $\operatorname{tr}(UV) < -2$, the two regions $\mathbb{X}_U$ and $\mathbb{X}_V$ are not tangent. Thus $\mathbb{F}$ is a fundamental domain for $\overline{G}$ by Klein's Combination Theorem. If $\operatorname{tr}(UV) = -2$, the tangent points of $\mathbb{X}_U$ and $\mathbb{X}_V$ are precisely the fixed points of the parabolic elements UV and VU and thus $\mathbb{F}$ is a fundamental domain by [22, Theorem 1]. The inclusion $z' \in \mathbb{F}^o$ is clear. □

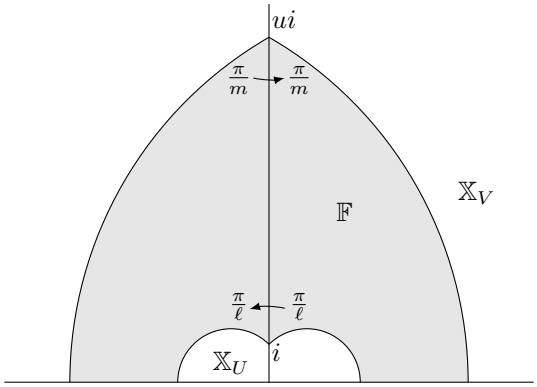


Figure 1: The fundamental domain in the case of two elliptic generators.

7.2. U is elliptic and V is parabolic

Lemma 7.9. *Suppose U has finite order and V is parabolic. Then U and V can be conjugated simultaneously in $\mathrm{GL}_2(\mathbb{R})$ to the form*

$$U = \begin{pmatrix} \cos\left(\frac{\pi}{\ell}\right) & \sin\left(\frac{\pi}{\ell}\right) \\ -\sin\left(\frac{\pi}{\ell}\right) & \cos\left(\frac{\pi}{\ell}\right) \end{pmatrix}, \quad V = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix},$$

with $\ell \in \mathbb{N}$ and $\lambda > 0$.

Proof. The details are omitted as the proof is similar to the proof of Lemma 7.7. □

Theorem 7.10. *Let U and V be as in Lemma 7.9. Then $\mathbb{X}_U = I_U \cup I_{U^{-1}}$,*

$$\mathbb{X}_V^+ = \{x + iy \in \mathbb{H} \mid x \leq -\lambda/2\} \quad \textit{and} \quad \mathbb{X}_V^- = \{x + iy \in \mathbb{H} \mid x \geq \lambda/2\}$$

satisfy the conditions of Theorem 7.2. In particular, $\mathbb{F} := \mathbb{H} \setminus (\mathbb{X}_U \cup \mathbb{X}_V^+ \cup \mathbb{X}_V^-)$ is a fundamental domain for $\overline{G}$ and $z' = 2i \in \mathbb{F}^o$. The sets $\mathbb{X}_U, \mathbb{X}_V^\pm$ and $\mathbb{F}$ are illustrated in Figure 2.

Proof. Remark 7.5 shows that $\mathbb{F}_U := \mathbb{H} \setminus \mathbb{X}_U$ is a fundamental domain for $\langle U \rangle$ and $\mathbb{X}_U$ satisfies the condition of Theorem 7.2. The set $\mathbb{F}_V := \mathbb{H} \setminus (\mathbb{X}_V^- \cup \mathbb{X}_V^+)$ is a fundamental domain for $\langle V \rangle$ as V acts on $\mathbb{H}$ as a translation by λ. If $\mathrm{tr}(UV) < -2$, then $\mathbb{F}_U$ and $\mathbb{F}_V$ are not tangent and thus $\mathbb{F}$ is a fundamental domain for $\overline{G}$ by Klein's Combination Theorem. If $\mathrm{tr}(UV) = -2$, then $\mathbb{F}_U$ and $\mathbb{F}_V$ are tangent. But the tangent points $\pm\lambda/2$ are the fixed points of the elliptic elements UV and UV^{-1}. Hence $\mathbb{F}$ is a fundamental domain by [22, Theorem 1]. □

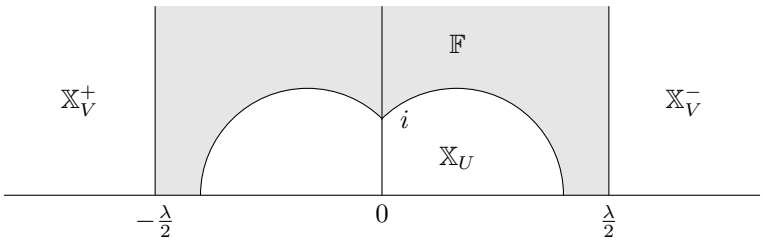


Figure 2: The fundamental domain in the case of an elliptic and a parabolic generator.

7.3. U is elliptic and V is hyperbolic

Lemma 7.11. *Suppose U is elliptic and V is hyperbolic. Then U and V can be conjugated simultaneously in $\mathrm{GL}_2(\mathbb{R})$ to the form*

$$U = \begin{pmatrix} \cos\left(\frac{\pi}{\ell}\right) & \sin\left(\frac{\pi}{\ell}\right) \\ -\sin\left(\frac{\pi}{\ell}\right) & \cos\left(\frac{\pi}{\ell}\right) \end{pmatrix}, \quad V = \begin{pmatrix} m & \sqrt{m^2-1} \cdot k \\ \frac{\sqrt{m^2-1}}{k} & m \end{pmatrix}$$

with $\ell \in \mathbb{N}$ and $m, k > 1$.

Proof. Let z be the fixed point of U and let $z_{\pm 1}$ be the fixed points of V. Let g be the geodesic through z which is perpendicular to the geodesic through z_{-1} and z_1. Further, let z_0 be one of the intersection points of g and $\hat{\mathbb{R}}$. By Lemma 2.1, there exists some $S \in \mathrm{GL}_2(\mathbb{R})$ such that $S \cdot z_j = j$ for $j = -1, 0, 1$. Then S sends g to the imaginary axis. Hence after conjugating U and V with S, we may assume that $z_{-1} = -1$, $z_1 = 1$ and $z = ri$ for some $r > 0$. After replacing S with $\left(\begin{smallmatrix} 1 & 0 \\ 0 & r \end{smallmatrix}\right) S$, one may assume that $r = 1$. After replacing S with $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) S$ if necessary, U is of the desired form and

$$V = \begin{pmatrix} m & b \\ (m^2-1)/b & m \end{pmatrix}.$$

After replacing S with $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ if necessary, one may assume that $b > 0$. Finally, the condition $\operatorname{tr}(UV) < 0$ implies that $b > \sqrt{m^2-1}$, i.e. the fixed points of V are $\pm k$ with $k = b/\sqrt{m^2-1} > 1$. □

Theorem 7.12. *Let U and V be as in Lemma 7.11. Then $\mathbb{X}_U := I_U \cup I_{U^{-1}}$, $\mathbb{X}_V^+ := I_V$ and $\mathbb{X}_V^- := I_{V^{-1}}$ satisfy the conditions of Theorem 7.2. In particular, $\mathbb{F} := \mathbb{H} \setminus (\mathbb{X}_U \cup \mathbb{X}_V^+ \cup \mathbb{X}_V^-)$ is a fundamental domain for $\overline{G}$ and $z' = 2i \in \mathbb{F}^o$. The sets $\mathbb{X}_U, \mathbb{X}_V^\pm$ and $\mathbb{F}$ are illustrated in Figure 3.*

Proof. Remark 7.5 shows that $\mathbb{H} \setminus \mathbb{X}_U$ and $\mathbb{H} \setminus (\mathbb{X}_V^+ \cup \mathbb{X}_V^-)$ are fundamental domains for $\langle U \rangle$ and $\langle V \rangle$ respectively. The condition $\operatorname{tr}(UV) < -2$ implies that these sets are not tangent. Hence $\mathbb{F}$ is a fundamental domain for G by Klein's Combination Theorem. □

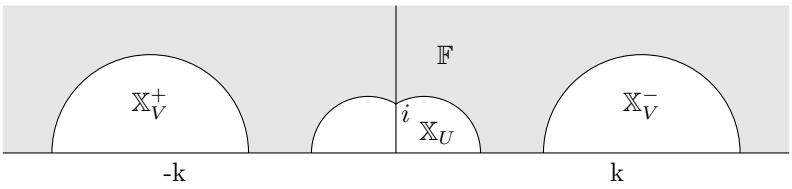


Figure 3: The fundamental domain in the case of an elliptic and a hyperbolic generator.

7.4. G is free

Fundamental domains which satisfy the conditions of Theorem 7.2 have been exhibited in [6] in the case that G (or equivalently $\overline{G}$) is free of rank 2. For sake of completeness, we recall the main result.

Theorem 7.13. *Let (U, V) be a witness pair for a free group $G \leq \mathrm{SL}_2(\mathbb{R})$ of rank 2.*

1. *Suppose $\operatorname{tr}[U,V] > 2$. After conjugation with some element from $\mathrm{GL}_2(\mathbb{R})$,*

$$(U,V) = \begin{cases} \left(\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ \mu & 1 \end{smallmatrix}\right)\right) & \text{if } 2 = \operatorname{tr}(U) = \operatorname{tr}(V), \\ \left(\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)\right) & \text{if } 2 = \operatorname{tr}(U) < \operatorname{tr}(V), \\ \left(\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right), \left(\begin{smallmatrix} x & (x^2-1)/y \\ y & x \end{smallmatrix}\right)\right) & \text{if } 2 < \operatorname{tr}(U) \leq \operatorname{tr}(V), \end{cases}$$

   with $\lambda, \mu, b, y > 0$, $a > 1$ and $x \geq a$. Let $\mathbb{X}_V^\pm = I_{V^{\pm 1}}$ and

$$\mathbb{X}_U^+ = \begin{cases} \{x + iy \in \mathbb{H} \mid x \leq -\lambda/2\} & \text{if } \operatorname{tr}(U) = 2, \\ I_U & \text{if } \operatorname{tr}(U) > 2 \end{cases}$$

$$\mathbb{X}_U^- = \begin{cases} \{x + iy \in \mathbb{H} \mid x \geq \lambda/2\} & \text{if } \operatorname{tr}(U) = 2, \\ I_{U^{-1}} & \text{if } \operatorname{tr}(U) > 2. \end{cases}$$

2. *Suppose* $\operatorname{tr}[U,V] \leq -2$. *After conjugation with some element from* $\mathrm{GL}_2(\mathbb{R})$,

$$U = \begin{pmatrix} k & 0 \\ 0 & 1/k \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} a & b \\ 1 & d \end{pmatrix}$$

for some $k > 1$ *and* $a, d > 0$ *with* $ad \geq \left(\frac{k^2+1}{k^2-1}\right)^2 > 1$. *Let*

$$\begin{aligned} \mathbb{X}_U^+ &= \{z \in \mathbb{H} \mid |z - (r+s)/2| \leq |r-s|/2\}, \\ \mathbb{X}_U^- &= \{z \in \mathbb{H} \mid |z - k^2(r+s)/2| \leq k^2|r-s|/2\}, \\ \mathbb{X}_V^+ &= \{z \in \mathbb{H} \mid |z+d|^2 \leq d/a\}, \\ \mathbb{X}_V^- &= \{z \in \mathbb{H} \mid |z-a|^2 \leq a/d\} \end{aligned}$$

where $r = \frac{a(k^2+1)+\sqrt{a/d}(1-k^2)}{2k^2}$ *and* $s = -\frac{d(k^2+1)+\sqrt{d/a}(1-k^2)}{2k^2}$.

Then $\mathbb{X}_U^+$, $\mathbb{X}_U^-$, $\mathbb{X}_V^+$ *and* $\mathbb{X}_V^-$ *satisfy the conditions of Theorem 7.2. In particular,* $\mathbb{F} := \mathbb{H} \setminus (\mathbb{X}_U^+ \cup \mathbb{X}_U^- \cup \mathbb{X}_V^+ \cup \mathbb{X}_V^-)$ *is a fundamental domain for* $\overline{G}$.

8. Triangle Groups

Throughout this section it is assumed that (U,V) is a witness pair for $G \leq \mathrm{SL}_2(\mathbb{R})$ and $\overline{G}$ is a (p,q,r)-triangle group. By Lemma 7.7 we may assume that

$$U = \begin{pmatrix} \cos\left(\frac{\pi}{p}\right) & \sin\left(\frac{\pi}{p}\right) \\ -\sin\left(\frac{\pi}{p}\right) & \cos\left(\frac{\pi}{p}\right) \end{pmatrix}, \quad V = \begin{pmatrix} \cos\left(\frac{\pi}{q}\right) & b \\ c & \cos\left(\frac{\pi}{q}\right) \end{pmatrix}$$

with $|c| < |b|$, $b > 0$ and $c < 0$. Let $u = \sqrt{-b/c}$ and let $\mathbb{F}$ be the region of $\mathbb{H}$ which is bounded by ∂I_U, $\partial I_{U^{-1}}$ and the two geodesics through the fixed point ui of V that enclose an angle of π/q with the imaginary axis, see Figure 4 for details.

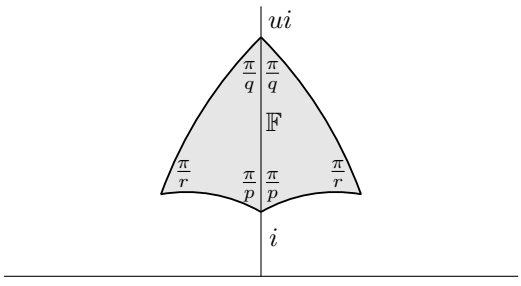


Figure 4: Fundamental domain for a triangle group.

By [1, Section 10], $\mathbb{F}$ is known to be a fundamental domain for $\overline{G}$. Since $\mathbb{F}$ has finite hyperbolic volume, G (or $\overline{G}$) is a cocompact group. We will give a different description of $\mathbb{F}$ in terms of the hyperbolic distance $\rho\colon \mathbb{H} \times \mathbb{H} \to \hat{\mathbb{R}}$. This characterization will yield an immediate solution of the constructive membership problem for $\overline{G}$.

Definition 8.1. For $w \in \mathbb{H}$ and $g \in \mathrm{SL}_2(\mathbb{R})$ with $g \cdot w \neq g$ define

$$L_g(w) = \{z \in \mathbb{H} \mid \rho(z,w) = \rho(z, g \cdot w)\}$$

and

$$H_g(w) = \{z \in \mathbb{H} \mid \rho(z,w) < \rho(z, g \cdot w)\} = \{z \in \mathbb{H} \mid \rho(z,w) < \rho(g^{-1} \cdot z, w)\}\,.$$

Let $G \leq \mathrm{SL}_2(\mathbb{R})$ and suppose that $g \cdot w \neq w$ for all elliptic elements $g \in G$. Then

$$D_G(w) = \bigcap_{g \in G \setminus \{\pm I\}} H_g(w)$$

is called the *Dirichlet polygon* for G with center w.

Lemma 8.2. *Let $g \in \mathrm{SL}_2(\mathbb{R})$, $w = x_1 + iy_1 \in \mathbb{H}$ and $g \cdot w = x_2 + iy_2$ with $x_1, x_2, y_1, y_2 \in \mathbb{R}$. If $g \cdot w \neq w$ then $L_g(w)$ is a geodesic, more precisely*

$$L_g(w) = \begin{cases} \{x + iy \in \mathbb{H} \mid x = (x_1 + x_2)/2\} & \text{if } y_1 = y_2, \\ \left\{ z \in \mathbb{H} \mid |z - \frac{x_1 y_2 - x_2 y_1}{y_2 - y_1}|^2 = y_1 y_2 (1 + \frac{(x_2 - x_1)^2}{(y_2 - y_1)^2}) \right\} & \text{if } y_1 \neq y_2. \end{cases}$$

Proof. For $z = x + iy \in L_g(w)$, the hyperbolic distance $\rho(z,w)$ satisfies

$$\cosh(\rho(z,w)) = 1 + \frac{|z-w|^2}{2yy_1} = 1 + \frac{(x-x_1)^2 + (y-y_1)^2}{2yy_1}\,.$$

From $\rho(z,w) = \rho(z, g \cdot w)$ we obtain

$$\frac{(x-x_1)^2 + (y-y_1)^2}{2yy_1} = \frac{(x-x_2)^2 + (y-y_2)^2}{2yy_2}\,.$$

The result follows. □

Hence the geodesic $L_g(w)$ divides $\mathbb{H}$ into two half planes and $H_g(w)$ is the one that contains w.

Theorem 8.3. *Let $G \leq \mathrm{SL}_2(\mathbb{R})$ be discrete and let $w \in \mathbb{H}$ be a point which is not fixed by any elliptic element of G. Then the Dirichlet polygon $D_G(w)$ is a fundamental domain for $\overline{G}$.*

Proof. See for example [1, Theorem 9.4.2]. □

By construction, $D_G(w)$ is the set of all points in $\mathbb{H}$ with a shorter distance to w than to every other point in the orbit $G \cdot w = \{g \cdot w \mid g \in G\}$. If G is cocompact, then there exists a finite subset X of $G \setminus \{\pm I\}$ with $D_G(w) = \bigcap_{g \in X} H_g(w)$ and [29] gives an algorithm to compute such a set. With such a set X at hand, the constructive membership problem for $\overline{G}$ can be solved using the following algorithm.

Algorithm 5. *Input: A discrete subgroup $G = \langle g_1, \ldots, g_n \rangle \leq \mathrm{SL}_2(\mathbb{R})$, some point $z' \in \mathbb{H}$ which is not fixed by any elliptic element in G, a finite set $X \subset G$ such that $D_G(z') = \bigcap_{g \in X} H_g(z')$ and some matrix $M \in \mathrm{SL}_2(\mathbb{R})$. Further, we assume that for $g \in X$ we know some word $w_g \in F_n$ such that $w_g(\overline{g_1}, \ldots, \overline{g_n}) = \overline{g}$.*
Output: A word $w \in F_n$ with $w(\overline{g_1}, \ldots, \overline{g_n}) = \overline{M}$ if $\overline{M} \in \overline{G}$ and false otherwise.

1. *Initialize* $w = 1 \in F_n$ *and* $z = M \cdot z'$.
2. *Compute* $g \in X$ *such that* $m := \rho(g^{-1} \cdot z, z')$ *is minimal. If* $m < \rho(z, z')$*, then replace* w *by* ww_g*, replace* z *by* $g^{-1} \cdot z$ *and repeat step (2).*
3. *If* $z = z'$ *and* $w(\overline{g_1}, \ldots, \overline{g_n}) = \overline{M}$ *then return* w *and false otherwise.*

Proof. Suppose first the algorithm terminates. Then w and z in step (3) satisfy $z = w(\overline{g_1}, \ldots, \overline{g_n})^{-1}\overline{M} \cdot z' \in D_G(z')^c$. If $\overline{M} \in \overline{G}$ this implies that $w(\overline{g_1}, \ldots, \overline{g_n}) = \overline{M}$ and $z = z'$. Hence the output is correct.
Let $B = \{\tilde{z} \in \mathbb{H} \mid \rho(z', \tilde{z}) \leq \rho(z', M \cdot z')\}$. The group G acts properly discontinuously on $\mathbb{H}$ and thus $G \cdot (M \cdot z') \cap B$ is finite, see [13, Corollary 2.2.7] for details. Hence the algorithm terminates, as in each iteration through step (2) it chooses a point in $G \cdot (M \cdot z') \cap B$ which is closer to z' than before. □

Lemma 8.4. *Let* U, V *and* $\mathbb{F}$ *be as in the beginning of this section. Then*

$$\mathbb{F}^o = D_G(z') = \bigcap_{g \in X} H_g(z')$$

with $X = \{U^{\pm 1}, V^{\pm 1}\}$ *and* $z' = \frac{1+u}{2}i \in \mathbb{F}^o$.

Proof. By Lemma 8.2, the geodesics $L_U(z')$ and $\partial I_{U^{-1}}$ share the same center, which is $-\cot(\pi/p)$. Further, both contain the fixed point of U. Hence $L_U(z') = \partial I_{U^{-1}}$. Similarly, $L_g(z') = \partial I_{g^{-1}}$ for all $g \in X$. Thus $\mathbb{F}^o = \bigcap_{g \in X} H_g(z') \supseteq D_G(z')$. The sets $\mathbb{F}$ and $D_G(z')$ are both fundamental domains for the cocompact group $\overline{G}$. Hence they share the same hyperbolic volume and thus $\mathbb{F}^o = D_G(z')$. □

In particular, the constructive membership problem for $\overline{G}$ can be solved using Algorithm 5 with $X = \{U^{\pm 1}, V^{\pm 1}\}$ and $z' = \frac{1+u}{2}i$.

9. Groups with commutators of finite order

Let $G = \langle A, B \rangle$ be a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ such that $[A, B]$ has finite order but $\overline{G}$ is not a triangle group. Theorem 4.3 shows that such groups G are characterized by the fact that A, B are both hyperbolic and either

- $\mathrm{tr}[A, B] = -2\cos\left(\frac{\pi}{p}\right)$ for some integer $p \geq 2$ or
- $\mathrm{tr}[A, B] = -2\cos\left(\frac{2\pi}{p}\right)$ for some odd integer $p \geq 3$.

These two cases correspond to the presentations (1.5) and (1.6) of Theorem 4.1. In both cases, the following result of Purzitsky [21] shows that $\overline{G}$ embeds into a subgroup $H \leq \mathrm{PSL}_2(\mathbb{R})$ such that $[H : \overline{G}] \leq 2$. The group H has a triangle as fundamental domain which yields a method to solve the membership problem for H and hence for $\overline{G}$. We provide a proof of this result since the proof not only gives a construction for H, but it also reveals a relation between the generators of $\overline{G}$ and H which will be needed later on.

Lemma 9.1. *Let* $A, B \in \mathrm{SL}_2(\mathbb{R})$ *be hyperbolic such that* $\mathrm{tr}[A, B] \neq 2$.

1. *There exists some* $U \in \mathrm{SL}_2(\mathbb{R})$ *such that* $UAU^{-1} = A^{-1}$ *and* $UBU^{-1} = B^{-1}$. *Moreover,* U *is unique up to scalars and has order* 4.
2. *The elements* $V = UA$ *and* $W = BU$ *have order* 4 *and satisfy* $(UVW)^2 = -[A, B]$.
3. *If* $\mathrm{tr}[A, B] = -2\cos\left(\frac{2\pi}{p}\right)$ *for some odd integer* $p \geq 3$, *then* $|\mathrm{tr}(UVW)| = \lambda_p$ *and* $\langle \overline{A}, \overline{B}\rangle = \langle \overline{U}, \overline{V}, \overline{W}\rangle$.
4. *If* $\mathrm{tr}[A, B] = -2\cos\left(\frac{\pi}{p}\right)$ *for some integer* $p \geq 2$, *then* $|\mathrm{tr}(UVW)| = \lambda_{2p}$ *and* $X \in \langle \overline{U}, \overline{V}, \overline{W}\rangle$ *lies in* $\langle \overline{A}, \overline{B}\rangle$ *if and only if* X *is a word of even length in* $\overline{U}, \overline{V}, \overline{W}$. *In particular,*
$$[\langle \overline{U}, \overline{V}, \overline{W}\rangle : \langle \overline{A}, \overline{B}\rangle] = 2\,.$$

Proof. Let z_1, z_2 be the fixed points of A and let z_3, z_4 be the fixed points of B. Lemma 3.1 shows that these points are pairwise distinct. Hence the cross ratio $\mathrm{cross}(z_1, z_2, z_3, z_4)$ is defined and equals $\mathrm{cross}(z_2, z_1, z_4, z_3)$. Suppose first that there exists some matrix U as in part (1). Then U acts on $\{z_1, z_2\}$. As U does not commute with A, it must interchange z_1 and z_2. Similarly it interchanges z_3 and z_4. These two conditions determine the image $\overline{U} \in \mathrm{PSL}_2(\mathbb{R})$ uniquely and the fact that U^2 has at least 4 fixed points shows that $U^2 = -I$. Conversely, the existence of some $U \in \mathrm{SL}_2(\mathbb{R})$ that interchanges z_1 and z_2 as well as z_3 and z_4 follows from Lemma 2.1. To see that $UAU^{-1} = A^{-1}$, one may suppose that A fixes 0 and ∞. Then $A = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{smallmatrix}\right)$ with $|\lambda| \neq 1$. Since U interchanges 0 with ∞, it is of the form $\left(\begin{smallmatrix} 0 & b \\ -1/b & 0 \end{smallmatrix}\right)$ for some $b \neq 0$. Hence $UAU^{-1} = A^{-1}$ as claimed. The same argument shows that $UBU^{-1} = B^{-1}$. The second assertion is verified directly.
Let $G = \langle \overline{A}, \overline{B}\rangle$ and $H = \langle \overline{U}, \overline{V}, \overline{W}\rangle$. Suppose $\mathrm{tr}[A, B] = -2\cos\left(\frac{2\pi}{p}\right)$ for some odd integer p. Part (2) and Lemma 2.4 show that $|\mathrm{tr}(UVW)| = \lambda_p$ and thus

$$\overline{I} = (\overline{UVW})^p = [\overline{A}, \overline{B}]^{\frac{p-1}{2}}(\overline{UVW}) = [\overline{A}, \overline{B}]^{\frac{p-1}{2}}\overline{AW}\,. \tag{1}$$

Hence $\overline{W} \in G$ and thus $G = H$. This shows the third assertion.
Finally suppose $\mathrm{tr}[\overline{A}, \overline{B}] = -2\cos\left(\frac{\pi}{p}\right)$ for some $p \geq 2$. Part (2) and Lemma 2.4 show that $|\mathrm{tr}(UVW)| = \lambda_{2p}$. Every word in $\overline{U}$, $\overline{V}$, $\overline{W}$ of even length is a word in $\overline{A} = \overline{UV}$ and $\overline{B} = \overline{WU}$, see also Remark 9.5 below. Thus $[H : G] \leq 2$. Conversely, H/H' is an elementary abelian 2-group but Theorem 4.1 shows that G/G' is isomorphic to $\mathbb{Z}^2$. Hence $G \neq H$. □

Theorem 9.2. *Let* $U, V, W \in \mathrm{SL}_2(\mathbb{R})$ *be of order* 4 *such that* $|\mathrm{tr}(UVW)| = \lambda_p$ *for some* $p \geq 2$. *Then the hyperbolic triangle* $\mathbb{F}$ *whose vertices are the fixed points of* UVW, VWU *and* WUV *is a fundamental domain for* $\langle \overline{U}, \overline{V}, \overline{W}\rangle \leq \mathrm{PSL}_2(\mathbb{R})$.

Proof. The result follows from Poincaré's Theorem, see [1, Theorem 9.8.4]. □

Definition 9.3. Two distinct points $x, y \in \mathbb{H}$ divide the unique geodesic through them into three components. Let $[x, y]$ denote the part between x and y. Given a fundamental domain $\mathbb{F}$ for a subgroup H of $\mathrm{PSL}_2(\mathbb{R})$, let

$$d_{H,\mathbb{F}} \colon \mathbb{H} \times \mathbb{H} \to \mathbb{Z} \cup \{\infty\},\ (x, y) \mapsto |\{h \cdot \mathbb{F} \mid h \in H\} \cap [x, y]|$$

be the distance function corresponding to H and $\mathbb{F}$.

Note that $d_{H,\mathbb{F}}$ is H-invariant, i.e. $d_{H,\mathbb{F}}(x,y) = d_{H,\mathbb{F}}(h \cdot x, h \cdot y)$ for all $h \in H$ and $x, y \in \mathbb{H}$. We are now ready to solve the membership problem for the group $\langle \overline{U}, \overline{V}, \overline{W} \rangle$ from Lemma 9.1. A similar approach is used in [3].

Algorithm 6. *Input: Matrices $U, V, W \in \mathrm{SL}_2(\mathbb{R})$ of order 4 with $|\mathrm{tr}(UVW)| = \lambda_p$ for some $p \geq 2$ and $M \in \mathrm{SL}_2(\mathbb{R})$.*
Output: A word $w \in F_3$ such that $w(\overline{U}, \overline{V}, \overline{W}) = \overline{M}$ if $\overline{M} \in H := \langle \overline{U}, \overline{V}, \overline{W} \rangle$ and false otherwise.

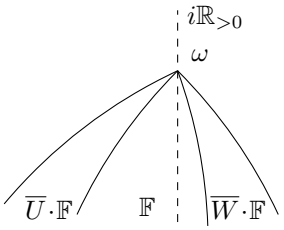
1. *Let $\mathbb{F}$ be the fundamental domain for H of Theorem 9.2 and pick some $z' \in \mathbb{F}^o$.*
2. *Initialize $w = 1 \in F_3$ and let $z = M \cdot z'$.*
3. *While $z \notin \mathbb{F}^c$ do:*
   (a) *If one of the three vertices of $\mathbb{F}^c$ lies on $[z, z']$, compute some $v \in F_3$ such that $v(\overline{U}, \overline{V}, \overline{W}) \cdot \mathbb{F}^c$ and $[z, z']$ have a point $\tilde{z}$ outside of $\mathbb{F}^c$ in common; see Remark 9.4 for details.*
   (b) *If none of the vertices of $\mathbb{F}$ lies on $[z, z']$, let $v \in \{f_1, f_2, f_3\}$ such that $[z, z']$ and $v(\overline{U}, \overline{V}, \overline{W}) \cdot \mathbb{F}$ have a point $\tilde{z}$ in common; see Remark 9.4 for details.*
   (c) *Replace z by $v(\overline{U}, \overline{V}, \overline{W})^{-1} \cdot z$ and z' by $v(\overline{U}, \overline{V}, \overline{W})^{-1} \cdot \tilde{z}$.*
   (d) *Replace w by wv.*
4. *If $w(\overline{U}, \overline{V}, \overline{W}) = \overline{M}$ then return w and false otherwise.*

Proof. By [1, Theorem 9.2.6] $\mathbb{F}$ is locally finite and $[z, z']$ is compact. Therefore, $[z, z']$ only intersects finitely many elements of $\{g \cdot \mathbb{F}^c \mid g \in H\}$ and thus $d_{H,\mathbb{F}}(z, z')$ is finite. The point $\tilde{z}$ from step (3a) or (3b) satisfies $d_{H,\mathbb{F}}(\tilde{z}, z) < d(z', z)$. Since $d_{H,\mathbb{F}}$ is H-invariant, we see that $d_{H,\mathbb{F}}(z, z')$ decreases in each iteration through step (3). Hence the algorithm terminates.
If $\overline{M} \notin H$, then no word $w \in F$ with $w(\overline{U}, \overline{V}, \overline{W}) = \overline{M}$ can be found. Conversely, if $\overline{M} \in H$, then $v^{-1}\overline{M} \cdot z' \in \mathbb{F}^o$ and thus $v = \overline{M}$ by the definition of a fundamental domain. So the output of the algorithm is correct. □

Before we continue our discussion, we explain how steps (3a) and (3b) of Algorithm 6 can be done in practice.

Remark 9.4. In step (3) of Algorithm 6 one may assume (after conjugation with some element of $\mathrm{GL}_2(\mathbb{R})$), that the segment $[z, z']$ lies on the imaginary axis $i\mathbb{R}_{>0}$. Let ω be the intersection point of $[z, z']$ and the boundary of $\mathbb{F}$.

1. Suppose ω is not a vertex of $\mathbb{F}^c$. Without loss of generality, ω lies on the side of $\mathbb{F}^c$ which is opposite of the fixed point of UVW. Then $[z, z'] \cap (\overline{V} \cdot \mathbb{F}^o)$ is non-empty. Let ω' be the intersection point of $\overline{V} \cdot \mathbb{F}^c$ and $i\mathbb{R}_{>0}$. Then any point $\tilde{z}$ between ω and ω' can be chosen in step (3b).
2. Suppose ω is a vertex of $\mathbb{F}^c$, say $UVW \cdot \omega = \omega$. The element $\overline{UVW}$ rotates at ω by an angle of $\pm 2\pi/p$. So if p is even, then $g := (\overline{UVW})^{p/2}$ satisfies $([z, z'] \cap g \cdot \mathbb{F}^c) \setminus \mathbb{F}^c \neq \emptyset$. Suppose now p is odd. The neighborhood at ω is tessellated by $(\overline{UVW})^j \cdot (\mathbb{F}^c \cup \overline{U} \cdot \mathbb{F}^c \cup \overline{W} \cdot \mathbb{F}^c)$ for $0 \leq j < p$:



Since $\overline{UVW}$ rotates at ω by an angle of $\pm 2\pi/p$, one of the elements

$$g \in \{h \cdot (\overline{UVW})^{(p-e)/2} \mid h \in \{\overline{U}, \overline{I}, \overline{W}\} \text{ and } e \in \{\pm 1\}\}$$

satisfies $([z, z'] \cap g \cdot \mathbb{F}^c) \setminus \mathbb{F}^c \neq \emptyset$. A point $\tilde{z}$ in this set can be found as before.

3. Instead of moving the point z closer to the set $\mathbb{F}$, one could instead move the set $\mathbb{F}$ closer to z in step (3c). This way, the geodesic through z and z' would not be changed in each iteration. So after an initial conjugation, one may assume that $[z, z'] \subset i\mathbb{R}_{>0}$.

The constructive membership problem for discrete subgroups of $\mathrm{PSL}_2(\mathbb{R})$ with a presentation labeled (1.5) or (1.6) in Theorem 4.1 can now be solved as follows.

Remark 9.5. Let $A, B \in \mathrm{SL}_2(\mathbb{R})$ be hyperbolic such that $G = \langle A, B\rangle$ is discrete and $[A, B]$ has finite order. Let $U, V, W \in \mathrm{SL}_2(\mathbb{R})$ be as in Lemma 9.1. Further, let $M \in \mathrm{SL}_2(\mathbb{R})$.

1. Suppose $\mathrm{tr}([A, B]) = -2\cos\left(\frac{2\pi}{p}\right)$ for some odd integer $p \geq 3$. Algorithm 6 can be used to decide if $\overline{M} \in \overline{G}$ and if so, express $\overline{M}$ as a word in the generators $\overline{U}, \overline{V}, \overline{W}$. Using the relations

$$\overline{W} = [\overline{A}, \overline{B}]^{\frac{p-1}{2}}\overline{A}, \qquad \overline{U} = \overline{WB}, \qquad \overline{V} = \overline{UA},$$

from eq. (1) one can express $\overline{M}$ as a word in $\overline{A}$ and $\overline{B}$.

2. Suppose $\mathrm{tr}([A, B]) = -2\cos\left(\frac{\pi}{p}\right)$ for some integer $p \geq 2$. Algorithm 6 can be used to decide if $\overline{M} \in \langle \overline{U}, \overline{V}, \overline{W}\rangle$ and if so, express $\overline{M}$ as a reduced word w in $\overline{U}, \overline{V}, \overline{W}$. Then $\overline{M} \in \overline{G}$ if and only if $\overline{M} \in \langle \overline{U}, \overline{V}, \overline{W}\rangle$ and w has even length, say $w = w_1 w_2 \dots w_{2m}$ with $w_i \in \{\overline{U}, \overline{V}, \overline{W}\}$ such that $w_i \neq w_{i+1}$. Replacing each of the substrings $w_1w_2, w_3w_4, \dots, w_{2m-1}w_{2m}$ according to the following relations expresses $\overline{M}$ as a word in $\overline{A}$ and $\overline{B}$.

$w_{2i-1}w_{2i}$	$\overline{UV}$	$\overline{UW}$	$\overline{VU}$	$\overline{VW}$	$\overline{WU}$	$\overline{WV}$
word in $\overline{A}$ and $\overline{B}$	$\overline{A}$	$\overline{B}^{-1}$	$\overline{A}^{-1}$	$(\overline{BA})^{-1}$	$\overline{B}$	$\overline{BA}$

10. Implementation and examples

A Magma [2] implementation of our algorithms is available from

`www.math.rwth-aachen.de/~Markus.Kirschmer/magma/sl2r.html`

Below are some comments on this implementation.

10.1. Representing matrices

Let $A, B \in \mathrm{SL}_2(\mathbb{R})$ and let $K \subset \mathbb{R}$ be the subfield generated by the entries of A and B. Then $G = \langle A, B\rangle \leq \mathrm{SL}_2(K)$. Our implementation assumes that K is an algebraic number field together with an embedding $\varepsilon\colon K \to \mathbb{R}$. Then G acts on $\mathbb{H}$ via ε.

This approach allows us to decide if $X \in \mathrm{SL}_2(K)$ has finite order or is parabolic etc. Some of our algorithms require that the square roots of some elements are present in K. This can be checked using well known factorization routines for polynomials over global fields (see for example [4, Section 3.6.2]). If the square roots are not present in K, then we extend K and ε accordingly.

Hence, in summary, even if G is given by matrices over K, the constructive membership test may be performed over some finite extension K' of K.

10.2. Some examples

All timings were performed on an Intel Xeon E5-4617. In each example, we took 10 random words of the given length. The indicated timing is the one from the run that took the most time.

Example 10.1. Let $a = \sqrt{2\cos\left(\frac{2\pi}{7}\right)}$ and $G = \langle A, B\rangle \leq \mathrm{SL}_2(\mathbb{R})$ where

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } B = \frac{1}{2}\begin{pmatrix} 1 & -a^5 + a^4 + a^2 + 2a - 1 \\ -a^5 - a^4 - a^2 + 2a + 1 & 1 \end{pmatrix}.$$

Then $\overline{G}$ is the well known $(2, 3, 7)$-triangle group and (A, B) is a witness pair for G. Let M be a word of length k in A and B. The time needed for Algorithm 5 to test if $M \in G$ is summarized in Figure 5. Note $(U, V) := (A, B)$ satisfies the conditions of Lemma 7.7. Hence the membership test can be performed in $K = \mathbb{Q}(a)$ and $[K : \mathbb{Q}] = 6$.

k	≤ 100	≤ 1000	≤ 5000	≤ 10000	≤ 20000
sec	< 0.1	< 2	< 19	< 90	< 415

Figure 5: Timings for Example 10.1.

The main reason for the non-linear increase in time is the growth of the matrix entries of M when k becomes larger.

Example 10.2. Let $n \geq 2$ be some integer and let $G = \langle A, B\rangle \leq \mathrm{SL}_2(\mathbb{R})$ where

$$A = \begin{pmatrix} \cos(\pi/n) & \sin(\pi/n) \\ -\sin(\pi/n) & \cos(\pi/n) \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & \lceil 2\cot(\pi/(2n))\rceil \\ 0 & 1 \end{pmatrix}.$$

Then (A, B) is a witness pair for G. In particular, G is discrete. Let M be a word of length k in A and B. The time needed for Algorithm 5 to test if $M \in G$ is summarized in Figure 6. Note that $(U, V) := (A, B)$ satisfies the conditions of Lemma 7.9. Hence the membership test can be performed in $K = \mathbb{Q}(\cos(\pi/n), \sin(\pi/n))$ and $[K : \mathbb{Q}] = \phi(n)$ where ϕ denotes Euler's totient function.

n	$\phi(n)$	$k \leq 100$	$k \leq 500$	$k \leq 1000$	$k \leq 5000$	$k \leq 10000$
2	1	< 0.1	< 0.1	< 0.1	< 1	< 2
3	2	< 0.1	< 0.2	< 0.3	< 7	< 40
5	4	< 0.1	< 0.8	< 3	< 170	< 800
7	6	< 0.1	< 2	< 9	< 470	< 2600
16	8	< 0.3	< 10	< 54	< 2300	$< 32{,}000$
11	10	< 0.8	< 32	< 195	$< 15{,}000$	$< 120{,}000$

Figure 6: Timings for Example 10.2 in seconds.

References

[1] A. F. Beardon. *The geometry of discrete groups*. Springer New York, 1983.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[3] O. Braun, R. Coulangeon, G. Nebe, and S. Schönnenbeck. Computing in arithmetic groups with Voronoi's algorithm. *Journal of Algebra*, 435:263–285, 2015.

[4] H. Cohen. *A course in computational algebraic number theory*. Springer, 1993.

[5] A. S. Detinko and D. L. Flannery. On deciding finiteness of matrix groups. *J. Symbolic Comput.*, 44(8):1037–1043, 2009.

[6] B. Eick, M. Kirschmer, and C. Leedham-Green. The constructive membership problem for discrete free subgroups of rank 2 of $\mathrm{SL}_2(\mathbb{R})$. *LMS J. Comput. Math.*, 17:345–359, 2014.

[7] H. R. P. Ferguson, D. H. Bailey, and S. Arno. Analysis of PSLQ, an integer relation finding algorithm. *Math. Comp.*, 68(225):351–369, 1999.

[8] L. Ford. *Automorphic functions*. AMS Chelsea Pub., 1951.

[9] R. Fricke and F. Klein. *Vorlesungen über die Theorie der Automorphen Functionen*. Teubner, 1897.

[10] J. Gilman. *Two-generator Discrete Subgroups of PSL(2,R)*, volume 117 of *Memoirs of the AMS*. AMS, 1995.

[11] D. F. Holt, B. Eick, and E. A. O'Brien. *Handbook of computational group theory*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[12] R. Kalia and G. Rosenberger. Automorphisms of the Fuchsian groups of type $(0; 2, 2, 2, q; 0)$. *Communications in Algebra*, 6(11):1115–1129, 1978.

[13] S. Katok. *Fuchsian Groups*. Chicago Lectures in Mathematics, 1992.

[14] G. Kern-Isberner and G. Rosenberger. Über Diskretheitsbedingungen und die diophantische Gleichung $ax^2 + by^2 + cz^2 = dxyz$. *Archiv der Mathematik*, 34(1):481–493, 1980.

[15] A. W. Knapp. Doubly generated Fuchsian groups. *Michigan Math. J.*, 15(3):289–304, 1968.

[16] R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory*. Springer, 1977.

[17] C. F. Miller. *On group-theoretic decision problems and their classification*. Princeton University Press, 1971.

[18] N. Purzitsky. Two generator discrete free groups. *Math. Z.*, 126:209–223, 1972.

[19] N. Purzitsky. Real two-dimensional representations of two-generator free groups. *Math. Z.*, 127:95–104, 1972.

[20] N. Purzitsky. Canonical generators of Fuchsian groups. *Illinois J. Math.*, 18:484–490, 1974.

[21] N. Purzitsky. All two-generator Fuchsian groups. *Math. Z.*, 147(1):87–92, 1976.

[22] N. Purzitsky. A cutting and pasting of noncompact polygons with applications to Fuchsian groups. *Acta Mathematica*, 143(1):233–250, 1979.

[23] N. Purzitsky and G. Rosenberger. Two generator Fuchsian groups of genus one. *Math Z.*, 128:245–251, 1972. Correction: Math. Z. 132, 261–262 (1973).

[24] G. Rosenberger. Fuchssche Gruppen, die freies Produkt zweier zyklischer Gruppen sind, und die Gleichung $x^2 + y^2 + z^2 = xyz$. *Math. Ann.*, 199:213–227, 1972.

[25] G. Rosenberger. Von Untergruppen der Triangel-Gruppen. *Illinois J. Math.*, 22(3):405–413, 1978.

[26] G. Rosenberger. Eine Bemerkung zu einer Arbeit von T. Jørgensen. *Math. Z.*, 165:261–265, 1979.

[27] G. Rosenberger. All generating pairs of all two-generator Fuchsian groups. *Archiv der Mathematik*, 46(3):198–204, 1986.

[28] D. Suprunenko and K. Hirsch. *Matrix Groups*. Translations of Mathematical Monographs. AMS, 1976.
[29] J. Voight. Computing fundamental domains for Fuchsian groups. *Journal de Théorie des Nombres de Bordeaux*, 21(2):467–489, 2009.