LMS J. Comput. Math. 17 (1) (2014) 345–359
doi:10.1112/S1461157014000047

The constructive membership problem for discrete free subgroups of rank 2 of $\mathrm{SL}_2(\mathbb{R})$

B. Eick, M. Kirschmer and C. Leedham-Green

Abstract

We exhibit a practical algorithm for solving the constructive membership problem for discrete free subgroups of rank 2 in $\mathrm{PSL}_2(\mathbb{R})$ or $\mathrm{SL}_2(\mathbb{R})$. This algorithm, together with methods for checking whether a two-generator subgroup of $\mathrm{PSL}_2(\mathbb{R})$ or $\mathrm{SL}_2(\mathbb{R})$ is discrete and free, have been implemented in Magma for groups defined over real algebraic number fields.

Supplementary materials are available with this article.

1. *Introduction*

The Tits alternative asserts that a finitely generated subgroup G of $\mathrm{GL}_n(K)$ for a field K is either solvable-by-finite or contains a non-cyclic free subgroup. Algorithms to decide the Tits alternative over the rational field $\mathbb{Q}$ have been described by Beals [2], Ostheimer [13] and Assmann and Eick [1]. An algorithm for arbitrary fields has been introduced by Detinko, Flannery and O'Brien [7].

The case that the matrix group G is solvable-by-finite is considered to be the 'tame' case. In this case, further structural investigations of the group G are possible, see for example [1] and [7]. The case that the matrix group G contains a non-cyclic free subgroup is considered to be the 'wild' case. In this case there seem hardly any methods available to investigate the structure of G further. In particular, there is no algorithm available to construct explicit generators of a non-cyclic free subgroup of G in general.

An important general problem in algorithmic group theory is the so-called constructive membership problem. The problem is solved for a group H by an algorithm that takes as input a subgroup G of H, given by a finite generating set $\{g_1, \ldots, g_m\}$, and an element g of H, and returns a word in $\{g_1, \ldots, g_m\}$ that evaluates to g if g lies in G, and returns false otherwise. In the 'tame' case that G is solvable-by-finite, there is some hope that the structure of G can be used to solve the constructive membership problem, see [1] for a special case and [6] for a discussion of the problem. In the 'wild' case that G contains a non-cyclic free subgroup, there is no general method available to solve this problem. In fact, Michailova [12, p. 42] showed that this problem is undecidable in general.

Here, we first show how the constructive membership problem can be solved for a free group acting on a topological space provided that a certain special type of fundamental domain for the group is available, see Theorem 2.1 and Algorithm 1. We then show how this can be used to solve the constructive membership problem for discrete free two-generator subgroups of $\mathrm{PSL}_2(\mathbb{R})$ or $\mathrm{SL}_2(\mathbb{R})$ using the action of these groups via Möbius transformations. This extends the work on $\mathrm{PSL}_2(\mathbb{R})$ by Purzitsky [14, 15], see § 4.

In Algorithm 2 we give a method of deciding whether a given two-generator subgroup G of $\mathrm{SL}_2(\mathbb{R})$ or $\mathrm{PSL}_2(\mathbb{R})$ is discrete and free. This algorithm is implicitly contained in Kern-Isberner and Rosenberger [10, 17]. If the group G is discrete and free, then this algorithmproduces as a

Received 26 February 2013; revised 1 February 2014.

2010 Mathematics Subject Classification 20H10 (primary).

side-product a special generating set for G which will underpin our solution to the constructive membership problem.

A report on an implementation in MAGMA [4] of our methods for subgroups G of $\mathrm{SL}_2(K)$ for real algebraic number fields K is included as supplementary material available with the online version of this paper.

2. *The constructive membership problem*

Let G be a group acting on a topological space $\mathbb{X}$. For $\mathbb{Y} \subseteq \mathbb{X}$ let $\mathbb{Y}^o$ denote the interior of $\mathbb{Y}$ and let $\mathbb{Y}^c$ denote the closure of $\mathbb{Y}$. Further, 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 $g \in G$ so that $g \cdot x \in \mathbb{F}^c$, and (2) if $z \in \mathbb{F}^o$ and $g \in G \setminus \{1\}$, then $g \cdot z \notin \mathbb{F}^c$. The following theorem and its attached algorithm show how the constructive membership problem can be solved for free groups acting on a topological space with a special type of fundamental domain.

THEOREM 2.1. *Let $G = \langle g_1, \ldots, g_m \rangle$ act on the topological space $\mathbb{X}$. Suppose that there exist pairwise disjoint subsets $\mathbb{X}_1^+, \ldots, \mathbb{X}_m^+, \mathbb{X}_1^-, \ldots, \mathbb{X}_m^-$ of $\mathbb{X}$ so that:*

(a) *$g_i \cdot (\mathbb{X} \setminus (\mathbb{X}_i^+)^o) \subseteq \mathbb{X}_i^-$ and $g_i^{-1} \cdot (\mathbb{X} \setminus (\mathbb{X}_i^-)^o) \subseteq \mathbb{X}_i^+$ for $1 \leqslant i \leqslant m$; and*

(b) *$\mathbb{F} = \mathbb{X} \setminus (\mathbb{X}_1^+ \cup \ldots \cup \mathbb{X}_m^+ \cup \mathbb{X}_1^- \cup \ldots \cup \mathbb{X}_m^-)$ is a fundamental domain for G with $\mathbb{F}^o \neq \emptyset$.*

Then G is free on $\{g_1, \ldots, g_m\}$ and the constructive membership problem can be solved by the following algorithm.

ALGORITHM 1. (ConstructiveMembership)
Let H be a group that acts on a topological space $\mathbb{X}$.
Input: Generators $g_1, \ldots, g_m$ for a subgroup G of H, sets $\mathbb{X}_i^+ \subset \mathbb{X}$ and $\mathbb{X}_i^- \subset \mathbb{X}$ for $1 \leqslant i \leqslant m$ satisfying the conditions of Theorem 2.1, some point $z' \in \mathbb{F}^o$ and an element $g \in H$.
Output: A word $w = w(f_1, \ldots, f_m)$ with $w(g_1, \ldots, g_m) = g$ if g is an element of G and false otherwise; here $f_1, \ldots, f_m$ are abstract elements generating a free group F.

(1) Initialize $w = 1 \in F$ and let $z = g \cdot z'$.
(2) While $z \notin \mathbb{F}^c$ do
  (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.
(3) Evaluate $v = w(g_1, \ldots, g_m)$.
(4) If $z = z'$ and $v = g$ then return w; otherwise return false.

Proof. We first observe that G is free. Suppose $g = g_{i_n}^{e_n} \ldots g_{i_2}^{e_2} g_{i_1}^{e_1}$ where $n \geqslant 1$, $e_j \neq 0$ and $i_j \in \{1, \ldots, m\}$ for $1 \leqslant j \leqslant n$ such that $i_j \neq i_{j+1}$ for $1 \leqslant j < n$. Let $z \in \mathbb{F}^o$. By induction on n, we have $g \cdot z \in \mathbb{X}_{i_n}^+ \cup \mathbb{X}_{i_n}^-$. Thus $g \cdot z \neq z \in \mathbb{F}^o$ and therefore $g \neq 1$. In fact, this part of the proof is a version of the well-known ping-pong lemma.

We now consider Algorithm 1 and show as a first step that this always terminates. By the definition of a fundamental domain, there exists a minimal reduced word W in the free group F whose evaluation $V = W(g_1, \ldots, g_m)$ satisfies $V \cdot z \in \mathbb{F}^c$. Suppose that W ends with g_i. Then $z \in V^{-1} \cdot \mathbb{F}^c \subseteq \mathbb{X}_i^+$ and hence the algorithm would set $w = f_i^{-1}$ during the first iteration and replace z by $g_i \cdot z$. Similarly, if W ends with g_i^{-1}, then $z \in V^{-1} \cdot \mathbb{F}^c \subseteq \mathbb{X}_i^-$ and hence the algorithm would set $w = f_i$ during the first iteration and replace z by $g_i^{-1} \cdot z$. By induction on the length of W, it follows that the while loop in Step (2) of the algorithm terminates after finitely many iterations.

Next we show that Algorithm 1 produces the desired output. First assume that the algorithm terminates with $z = z'$ and $v = g$. Then $g = w(g_1, \ldots, g_n) \in G$ and the algorithm produces the

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

correct output in this case. Conversely, if $g \in G$, then g has to respect the fundamental domain $\mathbb{F}$ and thus $z = z'$ and $v = g$ follows. Hence if the algorithm returns false, then $g \notin G$. □

REMARK 2.2. Write the word w determined by Algorithm 1 as $w = g_{i_1}^{e_1} \dots g_{i_r}^{e_r}$ with $e_i \in \mathbb{Z}$. Then Algorithm 1 determines w in $e_1 + \dots + e_r$ steps. The performance of the algorithm can be improved significantly if each syllable $g_{i_j}^{e_j}$ can be determined in one step instead of in e_j steps. In our later applications we exhibit some improvements of this type.

3. *Möbius transformations and* $\mathrm{GL}_2(\mathbb{R})$

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 book by Beardon [3].

The elements of $\mathrm{GL}_2(\mathbb{R})$ act via Möbius transformations on the extended complex plane $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. More precisely,

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ acts as } \mu : \hat{\mathbb{C}} \to \hat{\mathbb{C}} : z \mapsto M \cdot z := \frac{az + b}{cz + d}$$

with $\mu(\infty) = \infty$ if $c = 0$, and $\mu(\infty) = a/c$ and $\mu(-d/c) = \infty$ if $c \neq 0$. This action induces a group homomorphism

$$\varphi : \mathrm{GL}_2(\mathbb{R}) \to \mathrm{Aut}(\hat{\mathbb{C}})$$

whose kernel is $K = \{aI \mid a \in \mathbb{R}, a \neq 0\}$. Hence φ also induces an action of $\mathrm{PGL}_2(\mathbb{R}) = \mathrm{GL}_2(\mathbb{R})/K$ on $\hat{\mathbb{C}}$.

The cross ratio of a quadruple $(x_1, \dots, x_4)$ of pairwise distinct elements in $\mathbb{C}$ is

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

By continuity, this definition can be extended to the case where one of the x_i equals ∞. The following lemma asserts that the cross ratio is invariant under the action of Möbius transformations.

LEMMA 3.1. (a) *Let* (x_1, x_2, x_3, x_4) *be a quadruple of pairwise distinct elements in* $\hat{\mathbb{C}}$ *and* $M \in \mathrm{GL}_2(\mathbb{R})$. *Then* $\mathrm{cross}(x_1, x_2, x_3, x_4) = \mathrm{cross}(M \cdot x_1, M \cdot x_2, M \cdot x_3, M \cdot x_4)$.

(b) *Given triples* (x_1, x_2, x_3) *and* (y_1, y_2, y_3) *of pairwise distinct elements in* $\hat{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$, *there exists an element* $M \in \mathrm{GL}_2(\mathbb{R})$ *such that* $M \cdot x_i = y_i$ *for* $i = 1, 2, 3$.

Proof. For a proof of part (a) see for example [3, § 4.4]. For part (b), note that the Möbius transformation $f : z \mapsto ((z - x_1)(x_2 - x_3))/((z - x_3)(x_2 - x_1))$ 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 $M \in \mathrm{GL}_2(\mathbb{R})$ with Möbius transformation $\mu : z \mapsto g^{-1}(f(z))$ has the desired form. □

We consider in more detail the subgroup $\mathrm{SL}_2(\mathbb{R})$ of $\mathrm{GL}_2(\mathbb{R})$. Traces of products and commutators $[M, N] = MNM^{-1}N^{-1}$ of elements in $\mathrm{SL}_2(\mathbb{R})$ play an important role throughout this paper. We note the following.

LEMMA 3.2. *Let* M *and* N *be elements of* $\mathrm{SL}_2(\mathbb{R})$. *Then:*

(a) $\mathrm{tr}(M)\mathrm{tr}(N) = \mathrm{tr}(MN) + \mathrm{tr}(MN^{-1}) = \mathrm{tr}(MN) + \mathrm{tr}(M^{-1}N)$;

(b) $\mathrm{tr}[M, N] = \mathrm{tr}(M)^2 + \mathrm{tr}(N)^2 + \mathrm{tr}(MN)^2 - \mathrm{tr}(M)\mathrm{tr}(N)\mathrm{tr}(MN) - 2$.

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

Recall that an element $M \in \mathrm{SL}_2(\mathbb{R})$ is:
(a) elliptic if $\mathrm{tr}(M)^2 \in [0, 4)$;
(b) parabolic if $\mathrm{tr}(M)^2 = 4$;
(c) hyperbolic if $\mathrm{tr}(M)^2 \in (4, \infty)$.

These properties can also be characterized by the number of fixed points on $\hat{\mathbb{R}}$. A non-trivial element of $\mathrm{SL}_2(\mathbb{R})$ is elliptic if it has no fixed point on $\hat{\mathbb{R}}$, it is parabolic if it has only one fixed point on $\hat{\mathbb{R}}$ and it is hyperbolic if it has two fixed points on $\hat{\mathbb{R}}$.

As observed in [3, p. 78], the group $\mathrm{SL}_2(\mathbb{R})$ is a topological group with respect to the metric d on $\mathrm{SL}_2(\mathbb{R})$ defined by $d(M, N) = ||M - N||$, where $||M|| = \sqrt{\mathrm{tr}(MM^t)}$. A subgroup G of $\mathrm{SL}_2(\mathbb{R})$ is said to be *discrete* if G is discrete with respect to this topology. In other words, a subgroup G of $\mathrm{SL}_2(\mathbb{R})$ is discrete if $\inf\{||M - I|| \mid M \in G, M \neq \pm I\} \neq 0$. The following theorem recalls some elementary facts about discrete groups.

THEOREM 3.3. *Let $G \leqslant \mathrm{SL}_2(\mathbb{R})$.*
(a) *If G contains an elliptic element of infinite order, then G is not discrete.*
(b) *If G contains no elliptic elements, then G is elementary or discrete.*

Proof. See [9, Theorems 2.4.5 and 2.2.3]. □

A subgroup G of $\mathrm{SL}_2(\mathbb{R})$ in which $\mathrm{tr}[M, N] = 2$ holds for every pair $M, N \in G$ of infinite order is called *elementary*. The following lemma shows that two-generator elementary subgroups of $\mathrm{SL}_2(\mathbb{R})$ are solvable.

LEMMA 3.4. (a) *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.*
(b) *Let $G = \langle M, N\rangle \leqslant \mathrm{SL}_2(\mathbb{R})$ with $\mathrm{tr}[M, N] = 2$. Then G is solvable, and $\mathrm{tr}[S, T] = 2$ holds for every pair $S, T \in G$.*

Proof. (a) See for example [3, Theorem 4.3.5].
(b) If $\mathrm{tr}[M, N] = 2$, then M and N have a common fixed point in $\hat{\mathbb{C}}$ by (a). As M and N generate G, it follows that this fixed point is fixed by every element in G. We conjugate G so that this fixed point is ∞. This conjugates G into the subgroup of upper triangular matrices U in $\mathrm{SL}_2(\mathbb{C})$. As U is solvable, it follows that G is solvable. Further, G' consists of unitriangular elements and hence each element in G' has trace 2. □

As a final point in this introductory section, we introduce some notation that we use throughout. Consider the natural homomorphism $\mathrm{SL}_2(\mathbb{R}) \to \mathrm{PSL}_2(\mathbb{R})$ with kernel $\{\pm I\}$. Then for $M \in \mathrm{SL}_2(\mathbb{R})$ or $G \leqslant \mathrm{SL}_2(\mathbb{R})$ we denote with $\overline{M}$ or $\overline{G}$, respectively, their images under this natural homomorphism. Thus each element $\overline{M} \in \mathrm{PSL}_2(\mathbb{R})$ has exactly two preimages in $\mathrm{SL}_2(\mathbb{R})$, namely M and $-M$. Let H be a subgroup of $\mathrm{PSL}_2(\mathbb{R})$. Then H is said to be discrete if the preimage of H under the natural homomorphism $\mathrm{SL}_2(\mathbb{R}) \to \mathrm{PSL}_2(\mathbb{R})$ is discrete.

4. *Deciding if a two-generator subgroup of* $\mathrm{SL}_2(\mathbb{R})$ *is discrete and free*

Suppose that we are given two matrices $A, B \in \mathrm{SL}_2(\mathbb{R})$ and denote $G = \langle A, B\rangle$. Our aim in this section is to describe a practical method to check whether G is discrete and free of rank 2. If this is the case, then G is free on $\{A, B\}$ as well as on any other generating set with two elements (see [11, Proposition 2.7]). The following preliminary remark asserts that this problem for subgroups of $\mathrm{SL}_2(\mathbb{R})$ is equivalent to the corresponding problem for $\mathrm{PSL}_2(\mathbb{R})$.

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

LEMMA 4.1. *Let $G \leqslant \mathrm{SL}_2(\mathbb{R})$ be a two-generator group with image $\overline{G} \leqslant \mathrm{PSL}_2(\mathbb{R})$. Then G is discrete and free of rank 2 if and only if $\overline{G}$ is free and discrete of rank 2.*

Proof. Clearly G is discrete if and only if $\overline{G}$ is discrete by the definition of discreteness. Let $\varphi\colon G \to \overline{G}$ be the natural epimorphism. If G is free, then it contains no element of finite order. Conversely, if $\overline{G}$ is free, then there is a homomorphism $\overline{G} \to G$ which maps $\overline{A}$ and $\overline{B}$ to A and B respectively. Thus, in both cases, φ is one to one. □

DEFINITION 4.2. 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 $i \neq j$.

A *Nielsen transformation* is a finite product of elementary Nielsen transformations.

LEMMA 4.3. *Let $G = \langle A, B\rangle$ be a subgroup of $\mathrm{SL}_2(\mathbb{R})$ which is discrete and free of rank 2. If $U, V \in \mathrm{SL}_2(\mathbb{R})$ such that $\overline{G} = \langle \overline{U}, \overline{V}\rangle$ then $\mathrm{tr}[U, V] = \mathrm{tr}[A, B]$. In particular, $\mathrm{tr}[A, B]$ is an invariant of G and does not depend on the generators (A, B).*

Proof. The group $\overline{G}$ is free by Lemma 4.1. Hence there exists some Nielsen transformation t such that $(\overline{A}, \overline{B}) = t(\overline{U}, \overline{V})$ (see [**11**, Proposition 4.1]). Thus $(rA, sB) = t(U, V)$ for some $r, s \in \{\pm 1\}$. The result now follows from $\mathrm{tr}[A, B] = \mathrm{tr}[rA, sB]$ and the fact that Nielsen transformations preserve traces of commutators. □

The following theorem provides the basis for our algorithm to determine whether a two-generator subgroup of $\mathrm{SL}_2(\mathbb{R})$ is discrete and free.

THEOREM 4.4. *Let $A, B \in \mathrm{SL}_2(\mathbb{R})$ and let $G = \langle A, B\rangle$.*

(a) *If G is discrete and free of rank 2, then $|\mathrm{tr}(M)| \geqslant 2$ for all $M \in G$.*

(b) *Suppose that $|\mathrm{tr}(A)| \geqslant 2$ and $|\mathrm{tr}(B)| \geqslant 2$.*

  (i) *If $\mathrm{tr}[A, B] = 2$, then G is solvable.*

  (ii) *If $\mathrm{tr}[A, B] \in (-2, 2)$, then G is not free of rank 2 or not discrete.*

  (iii) *If $\mathrm{tr}[A, B] \leqslant -2$, then G is discrete and free of rank 2.*

  (iv) *If $\mathrm{tr}[A, B] > 2$, then G is discrete and free of rank 2 if and only if there exist $U, V \in \mathrm{SL}_2(\mathbb{R})$ with $\overline{G} = \langle \overline{U}, \overline{V}\rangle$ and $\mathrm{tr}(U) \geqslant 2$ and $\mathrm{tr}(V) \geqslant 2$ and $\mathrm{tr}(UV^{-1}) \leqslant -2$.*

  (v) *If $\mathrm{tr}[A, B] > 2$, then G is discrete and free of rank 2 if and only if there exist $U, V \in \mathrm{SL}_2(\mathbb{R})$ with $\overline{G} = \langle \overline{U}, \overline{V}\rangle$ and $2 \leqslant \mathrm{tr}(U) \leqslant \mathrm{tr}(V) \leqslant -\mathrm{tr}(UV^{-1})$.*

Proof. (a) If $M \in G$ and $|\mathrm{tr}(M)| < 2$ then either M is a non-trivial element of finite order and thus G is not free or M has infinite order and G is not discrete by Theorem 3.3(a).

(bi) This follows from Lemma 3.4.

(bii) This is an immediate consequence of (a).

(biii) and (biv) These cases are covered by [**17**, Satz 1].

(bv) If a pair (U, V) as in (bv) is given, then this satisfies the condition of (biv). Conversely, if a pair (U, V) as in (biv) is given, then it is not difficult to construct a pair (U', V') as needed for (bv). After exchanging U and V we may assume that $\mathrm{tr}(U) \leqslant \mathrm{tr}(V)$. Thus if $-\mathrm{tr}(UV^{-1}) \geqslant \mathrm{tr}(V)$ we can simply choose $U' = U$ and $V' = V$. Otherwise set $U' = U$ and $V' = -UV^{-1}$. Then $-\mathrm{tr}(U'V'^{-1}) = \mathrm{tr}(V) \geqslant \mathrm{tr}(V')$. Hence, after exchanging U' and V' if necessary, the traces satisfy $2 \leqslant \mathrm{tr}(U') \leqslant \mathrm{tr}(V') \leqslant -\mathrm{tr}(U'V'^{-1})$. □

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

DEFINITION 4.5. Let $G = \langle A, B\rangle \leqslant \mathrm{SL}_2(\mathbb{R})$ and suppose that G is discrete and free of rank 2. We call a pair of matrices (U, V) in $\mathrm{SL}_2(\mathbb{R})$ a *witness pair* for G if:

(a) $\overline{G} = \langle \overline{U}, \overline{V}\rangle$;

(b) $2 \leqslant \mathrm{tr}(U) \leqslant \mathrm{tr}(V)$ if $\mathrm{tr}[A, B] \leqslant -2$;

(c) $2 \leqslant \mathrm{tr}(U) \leqslant \mathrm{tr}(V) \leqslant -\mathrm{tr}(UV^{-1})$ if $\mathrm{tr}[A, B] > 2$.

Note that property (a) implies that $\mathrm{tr}[A, B] = \mathrm{tr}[U, V]$ (see Lemma 4.3). Also note that a witness pair generates a subgroup $\tilde{G}$ of $\mathrm{SL}_2(\mathbb{R})$ which is isomorphic to G, but not necessarily equal. However, its action via Möbius transformations is equal to that of G as G and $\tilde{G}$ have the same image in $\mathrm{PSL}_2(\mathbb{R})$.

The following algorithm decides whether a two-generator subgroup of $\mathrm{SL}_2(\mathbb{R})$ is discrete and free of rank 2.

ALGORITHM 2. (Discrete-And-Free-of-Rank-2)
Input: $A, B \in \mathrm{SL}_2(\mathbb{R})$.
Output: If $G = \langle A, B\rangle$ is discrete and free of rank 2, then the algorithm returns true and a witness pair for G. Otherwise the algorithm returns false.

(1) If $|\mathrm{tr}(A)| < 2$ or $|\mathrm{tr}(B)| < 2$ or $\mathrm{tr}[A, B] \in (-2, 2]$, then return false.

(2) Choose $U, V \in \mathrm{SL}_2(\mathbb{R})$ such that $\overline{A} = \overline{U}$, $\overline{B} = \overline{V}$ and $\mathrm{tr}(U), \mathrm{tr}(V) > 0$.

(3) If $\mathrm{tr}(V) < \mathrm{tr}(U)$, then exchange U and V.

(4) If $\mathrm{tr}[U, V] \leqslant -2$, then return true and (U, V).

(5) Set $S := \{UV, UV^{-1}\}$ and $m = \min\{|\mathrm{tr}(T)| : T \in S\}$.

(6) If $m < 2$, then return false.

(7) If $m < \mathrm{tr}(U)$, then
   (a) Replace V by U. Then replace U by a matrix in $\{\pm T \mid T \in S\}$ that has trace m.
   (b) Goto (5).

(8) If $m < \mathrm{tr}(V)$, then
   (a) Replace V by a matrix in $\{\pm T \mid T \in S\}$ that has trace m.
   (b) Goto (5).

(9) If $\mathrm{tr}(UV^{-1}) > 0$, then replace V by V^{-1}.

(10) Return true and the pair (U, V).

THEOREM 4.6. *Algorithm 2 terminates and produces the stated output.*

Proof. We first show that the algorithm terminates. The proof of [**10**, Lemma 2] shows that, after finitely many steps, the set S contains an element of negative trace. The proof of Theorem 4.4 shows that after at most one more iteration, the algorithm has produced a witness pair (U, V) for G.

We now show that the algorithm is correct. The replacements of the generating set in (7) and (8) are Nielsen transformations. Hence $\overline{G} = \langle \overline{U}, \overline{V}\rangle$ and $\mathrm{tr}[U, V] = \mathrm{tr}[A, B]$ hold throughout. Further, from step (4) onward, we have $2 \leqslant \mathrm{tr}(U) \leqslant \mathrm{tr}(V)$. If the algorithm returns false, then either it has encountered an elliptic element or $\mathrm{tr}[A, B] = 2$. Hence G is not discrete or not free of rank 2 by Theorem 4.4. If the algorithm returns true, it has produced a witness pair (U, V) for G. Thus G is discrete and free of rank 2 by Theorem 4.4. □

REMARK 4.7. If one keeps track of the Nielsen transformations performed in steps (3)–(9) of Algorithm 2, one can additionally produce explicit words u and v so that $\overline{U} = u(\overline{A}, \overline{B})$ and $\overline{V} = v(\overline{A}, \overline{B})$ hold.

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

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

Let $A, B \in \mathrm{SL}_2(\mathbb{R})$ and let $G = \langle A, B\rangle$ be discrete and free of rank 2. We consider an element $M \in \mathrm{SL}_2(\mathbb{R})$ and we wish to decide whether M is an element in G and, if so, then write it as a word in A and B. We first reduce this problem to the corresponding problem for witness pairs.

LEMMA 5.1. *Let (U, V) be a witness pair for G and let $M \in \mathrm{SL}_2(\mathbb{R})$. Let u and v be words with $\overline{U} = u(\overline{A}, \overline{B})$ and $\overline{V} = v(\overline{A}, \overline{B})$. Then M can be written as a word w' in $\{A, B\}$ if and only if $\overline{M}$ can be written as a word w in $\{\overline{U}, \overline{V}\}$ with $w(u(A, B), v(A, B)) = M$; in the latter case we obtain $w'(A, B)$ as $w'(A, B) = w(u(A, B), v(A, B))$.*

Proof. If $M \in G$, then $\overline{M} \in \overline{G}$ and thus $\overline{M} = w(\overline{U}, \overline{V})$. Hence $\overline{M} = w(u(\overline{A}, \overline{B}), v(\overline{A}, \overline{B}))$. As G is free on $\{A, B\}$, this implies that $M = w(u(A, B), v(A, B))$. □

We now show how Theorem 2.1 can be applied to solve the constructive membership problem for a witness pair (U, V). For this purpose we need to identify the regions $\mathbb{X}_j^{\pm}$ for $j \in \{1, 2\}$ and an element $z' \in \mathbb{F}^o$. We distinguish the cases that $\mathrm{tr}[A, B] \leqslant -2$ and $\mathrm{tr}[A, B] > 2$ in the following.

5.1. *The case* $\mathrm{tr}[A, B] \leqslant -2$

The regions which we define and use in this section have also been used by Purzitsky [**14**, Theorem 8] to show that the group $\overline{G}$ is discrete and free.

LEMMA 5.2. *Let (U, V) be a witness pair for $G = \langle A, B\rangle$ with $\mathrm{tr}[A, B] \leqslant -2$. Then U and V are both hyperbolic and, up to conjugation in $\mathrm{GL}_2(\mathbb{R})$, of the form*

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

for some $k > 1$ and $a, d > 0$ with $ad \geqslant ((k^2+1)/(k^2-1))^2 > 1$.

Proof. Let $t = \mathrm{tr}(U) \geqslant 0$. We may assume that

$$U = \begin{pmatrix} 0 & 1 \\ -1 & t \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then $\mathrm{tr}[U, V] = t^2 + \mathrm{tr}(V)^2 + \mathrm{tr}(UV)^2 - \mathrm{tr}(UV)\mathrm{tr}(V)t - 2$ and, as $\mathrm{tr}[U, V] \leqslant -2$, we see that $\mathrm{tr}(UV)\mathrm{tr}(V)t \geqslant t^2 + \mathrm{tr}(V)^2 + \mathrm{tr}(UV)^2$. Thus either $\min\{t, \mathrm{tr}(V), \mathrm{tr}(UV)\} > 2$ or $\mathrm{tr}(UV) = \mathrm{tr}(V) = t = 0$. In the first case, U and V are hyperbolic. In the second case, $\mathrm{tr}(UV) = 0$ shows $b = c$ and $\mathrm{tr}(V) = 0$ implies $d = -a$. But then $1 = \det(V) = -a^2 - b^2$ yields a contradiction. By Lemma 3.1 there exists some $S \in \mathrm{GL}_2(\mathbb{R})$ such that SUS^{-1} fixes 0 and ∞. After conjugating U and V with S or $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot S$ we may assume that

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

Then $c \neq 0$ by Lemma 3.4. After conjugating U and V with $\left(\begin{smallmatrix} c & 0 \\ 0 & 1 \end{smallmatrix}\right)$ we may finally assume that $c = 1$. The condition

$$-2 \geqslant \mathrm{tr}[U, V] = \underbrace{(2 - k^2 - 1/k^2)}_{<0} ad + (k^2 + 1/k^2)$$

implies that $ad \geqslant (k^2+1)^2/(k^2-1)^2 > 1$. Hence $a, d > 0$ since $\mathrm{tr}(V) = a + d > 2$. □

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

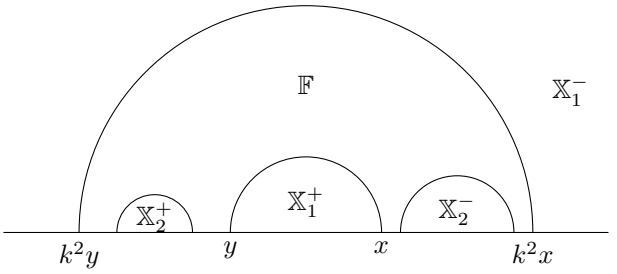

FIGURE 1. *Regions.*

If $U, V \in \mathrm{SL}_2(\mathbb{R})$ with $\mathrm{tr}[U,V] \leqslant -2$ have the form as in Lemma 5.2, then we say that they are *normalized*.

For the remainder of this section we suppose that the matrices

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

from Lemma 5.2 form a normalized witness pair for $G = \langle A, B \rangle$ with $\mathrm{tr}[A,B] \leqslant -2$.

LEMMA 5.3. (a) *We have* $\mathrm{tr}[U,V] = -2$ *if and only if* $ad = (k^2+1)/(k^2-1)^2$.
(b) *If* $\mathrm{tr}[U,V] < -2$, *then there exist* $x, y \in \mathbb{Q}$ *such that*

$$\begin{aligned} 0 < x < a - \sqrt{a/d} \quad &\text{and} \quad a + \sqrt{a/d} < k^2 x, \\ -d + \sqrt{d/a} < y < 0 \quad &\text{and} \quad -d - \sqrt{d/a} > k^2 y. \end{aligned}$$

Proof. Part (a) follows immediately from $k^2 - \mathrm{tr}[U,V] + 1/k^2 = (k - 1/k)^2 ad$. Suppose now that $\mathrm{tr}[U,V] < -2$. Then $\sqrt{ad} > (k^2+1)/(k^2-1)$ or equivalently $k^2 > (\sqrt{ad}+1)/(\sqrt{ad}-1) = (a + \sqrt{a/d})/(a - \sqrt{a/d})$. Thus the interval $((a + \sqrt{a/d})/k^2,\ a - \sqrt{a/d})$ is non-empty. Any element x from this interval satisfies the first two inequalities. A similar argument shows how to choose y. □

If $\mathrm{tr}[U,V] = -2$ we set $x = a - \sqrt{a/d} > 0$ and $y = -d + \sqrt{d/a} < 0$. Otherwise we choose $x, y \in \mathbb{Q}$ satisfying the conditions of Lemma 5.3(b).

Let $\mathbb{H} := \{x' + iy' \in \mathbb{C} \mid y' > 0\}$ be the upper half complex plane and for two real numbers r, s let $C(r,s) := \{z \in \mathbb{H} \mid |z - (s+r)/2| \leqslant |s-r|/2\}$, that is, the region enclosed by the real axis and the geodesic which meets the real axis in r and s.

We define

$$\begin{aligned} \mathbb{X}_1^+ &:= C(x,y), & \mathbb{X}_1^- &:= \mathbb{H} \setminus (U \cdot \mathbb{X}_1^+)^o = \mathbb{H} \setminus C(k^2x, k^2y)^o, \\ \mathbb{X}_2^+ &:= C(-d - \sqrt{d/a}, -d + \sqrt{d/a}), & \mathbb{X}_2^- &:= V \cdot \mathbb{X}_2^+ = C(a - \sqrt{a/d}, a + \sqrt{a/d}). \end{aligned}$$

The sets $\mathbb{X}_1^+$, $\mathbb{X}_2^+$, $\mathbb{X}_1^-$, $\mathbb{X}_2^-$ and $\mathbb{F} = \mathbb{H} \setminus (\mathbb{X}_1^+ \cup \mathbb{X}_1^- \cup \mathbb{X}_2^+ \cup \mathbb{X}_2^-)$ are illustrated in Figure 1.

LEMMA 5.4. *The sets* $\mathbb{X}_1^+, \mathbb{X}_2^+, \mathbb{X}_1^-, \mathbb{X}_2^-$ *are pairwise disjoint and satisfy the conditions* (a) *and* (b) *of Theorem* 2.1 *for* $g_1 = U$ *and* $g_2 = V$. *Let* $\mathbb{F} = \mathbb{H} \setminus (\mathbb{X}_1^+ \cup \mathbb{X}_1^- \cup \mathbb{X}_2^+ \cup \mathbb{X}_2^-)$. *Then* $z' := i\sqrt{-xy}(1+k^2)/2 \in \mathbb{F}^o$ *where* $i = \sqrt{-1}$.

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

Proof. The sets are pairwise disjoint by Lemma 5.3. The inclusions in condition (a) involving U are obvious, as Lemma 5.2 implies that $Uh = k^2h$ for all $h \in \mathbb{H}$. For the inclusions involving V note that the fixed points $(a-d-\sqrt{(a+d)^2-4})/2$ and $(a-d+\sqrt{(a+d)^2-4})/2$ of V are contained in $\mathbb{X}_2^+$ and $\mathbb{X}_2^-$ respectively. Further, V maps the boundary of $\mathbb{X}_2^+$ to the boundary of $\mathbb{X}_2^-$.

Next we consider condition (b). First note that $\mathbb{F}_U = \mathbb{H} \setminus (\mathbb{X}_1^+ \cup \mathbb{X}_1^-)$ and $\mathbb{F}_V = \mathbb{H} \setminus (\mathbb{X}_2^+ \cup \mathbb{X}_2^-)$ are fundamental domains for $\langle U \rangle$ and $\langle V \rangle$, respectively. If $\operatorname{tr}[U,V] < -2$ then these two regions are not tangent. Thus it follows from Klein's combination theorem (see for example [**8**, pp. 190–192]) that $\mathbb{F} = \mathbb{F}_U \cap \mathbb{F}_V$ is a fundamental domain for G. In the case that $\operatorname{tr}[U,V] = -2$, the tangent points of the regions $\mathbb{F}_U$ and $\mathbb{F}_V$ are $a \pm \sqrt{a/d}$ and $d \pm \sqrt{d/a}$. These are precisely the fixed points of the four parabolic elements $[U^e, V^f] \in G$ where $e, f \in \{\pm 1\}$. In this case, the set $\mathbb{F}$ is also a fundamental domain for G (see [**16**, Theorem 1]).

Finally, the boundaries of the sets $\mathbb{X}_1^+$ and $\mathbb{X}_1^-$ intersect $L := \{\lambda i \mid \lambda > 0\}$ in $p := i\sqrt{-xy}$ and k^2p respectively. Thus $z' = (p + k^2p)/2$ is not contained in the closure of $\mathbb{X}_1^+ \cup \mathbb{X}_1^-$. Since $(\mathbb{X}_2^+)^c$ and $(\mathbb{X}_2^-)^c$ do not meet L, we obtain that $z' \in \mathbb{F}^o$. □

The following lemma and remark improve Algorithm 1 in the case considered in this section as suggested by Remark 2.2.

LEMMA 5.5. *Let $c = (x+y)/2$. If $z = x' + iy' \in \mathbb{X}_1^- \cup (\mathbb{X}_1^+)^o$, then $U^\ell \cdot z \in \mathbb{H} \setminus (\mathbb{X}_1^- \cup (\mathbb{X}_1^+)^o)$ for*

$$\ell = \left\lceil \frac{\log((cx' + \sqrt{(cx')^2 - |z|^2 xy})/|z|^2)}{\log(k^2)} \right\rceil. \tag{5.1}$$

Proof. The boundary of $\mathbb{X}_1^+$ is a circle with center c and radius $(x-y)/2$. Thus the condition $k^{2\ell} z = U^\ell \cdot z \notin (\mathbb{X}_1^+)^o$ is equivalent to

$$\begin{aligned} & (x-y)^2/4 \leqslant |k^{2\ell}(x'+iy') - c|^2 = k^{4\ell}|z|^2 - 2k^{2\ell}x'c + c^2 \\ \iff \quad & 0 \leqslant k^{4\ell}|z|^2 - 2k^{2\ell}x'c + xy \\ \iff \quad & k^{2\ell} \geqslant (x'c + \sqrt{(x'c)^2 - |z|^2 xy})/|z|^2. \end{aligned}$$

Hence the value ℓ given by equation (5.1) is the least ℓ such that $U^\ell \cdot z \notin (\mathbb{X}_1^+)^o$. □

REMARK 5.6. Let $\omega_1 < \omega_2$ be the two fixed points of V and let $S = \left(\begin{smallmatrix} 1 & -\omega_1 \\ -1 & \omega_2 \end{smallmatrix}\right)$. Then $V' := SVS^{-1} = \left(\begin{smallmatrix} k' & 0 \\ 0 & 1/k' \end{smallmatrix}\right)$ where $k' = (a+d+\sqrt{(a+d)^2-4})/2 > 1$. The matrix S maps the fundamental domain $\mathbb{F}_V = \mathbb{H} \setminus (\mathbb{X}_2^+ \cup \mathbb{X}_2^-)$ for $\langle V \rangle$ to a fundamental domain for $\langle V' \rangle$. Further, S maps geodesics to geodesics and $V' \cdot z = k'^2 z$ for all $z \in \mathbb{H}$. Hence

$$S \cdot \mathbb{X}_2^+ = C(x', y') \quad \text{and} \quad S \cdot \mathbb{X}_2^- = \mathbb{H} \setminus C(k'^2 x', k'^2 y')^o$$

for some $x' > 0 > y'$. In particular, given any $z \in \mathbb{H}$, we can use Lemma 5.5 to compute $\ell \in \mathbb{Z}$ such that $V^\ell \cdot z \in \mathbb{F}_V$.

5.2. *The case* $\operatorname{tr}[A,B] > 2$

The regions we use have also been considered by Purzitsky in [**15**, § 3] to show that $\overline{G}$ is discrete and free. Throughout this section, we assume that (U,V) is a witness pair for G. Note that U and V have no common fixed points by Lemma 3.4. We distinguish three cases to determine sets $\mathbb{X}_1^+, \mathbb{X}_2^+, \mathbb{X}_1^-, \mathbb{X}_2^-$ that satisfy the requirements of Theorem 2.1.

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

5.2.1. *The case* $\mathrm{tr}(U) = \mathrm{tr}(V) = 2$. Here U and V both have a unique fixed point in $\hat{\mathbb{C}}$. After conjugating U and V simultaneously with some element in $\mathrm{GL}_2(\mathbb{R})$ (see Lemma 3.1) we may assume that U fixes ∞ and V fixes 0. Then

$$U = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}.$$

Further, $-2 \geqslant \mathrm{tr}(U^{-1}V) = 2 - \lambda\mu$ shows that (after conjugating U and V with $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ if necessary) we may assume that $\lambda, \mu > 0$. We define the sets

$$\mathbb{X}_1^+ := \{x + iy \in \mathbb{H} \mid x \leqslant -\lambda/2\}, \qquad \mathbb{X}_1^- := \{x + iy \in \mathbb{H} \mid x \geqslant \lambda/2\},$$
$$\mathbb{X}_2^+ := C(-2/\mu, 0), \qquad \mathbb{X}_2^- := C(0, 2/\mu).$$

5.2.2. *The case* $2 = \mathrm{tr}(U) < \mathrm{tr}(V)$. Now U has a unique fixed point and V has two fixed points in $\hat{\mathbb{R}}$. After conjugating U and V simultaneously with some element in $\mathrm{GL}_2(\mathbb{R})$ (see Lemma 3.1), we may assume that U fixes ∞ and V fixes ± 1. Then

$$U = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \text{ with } a > 1.$$

From $-2 > \mathrm{tr}(U^{-1}V) = 2a - b\lambda$ it follows that $\lambda b > 0$. Thus (after conjugating U and V with $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ if necessary) we may assume $\lambda > 0$, $b > 0$. Then we define the sets

$$\mathbb{X}_1^+ := \{x + iy \in \mathbb{H} \mid x \leqslant -\lambda/2\}, \qquad \mathbb{X}_1^- := \{x + iy \in \mathbb{H} \mid x \geqslant \lambda/2\},$$
$$\mathbb{X}_2^+ := C(-(a+1)/b, -(a-1)/b), \qquad \mathbb{X}_2^- := C((a-1)/b, (a+1)/b).$$

5.2.3. *The case* $2 < \mathrm{tr}(U) \leqslant \mathrm{tr}(V)$.

LEMMA 5.7. *Let (U, V) be a witness pair for $G = \langle A, B\rangle$ such that $2 < \mathrm{tr}(U) \leqslant \mathrm{tr}(V)$ and $\mathrm{tr}[A, B] > 2$. Further let ω_U, ω_U' and ω_V, ω_V' be the fixed points of U and V respectively. Then the cross ratio $c := \mathrm{cross}(\omega_U, \omega_U', \omega_V, \omega_V')$ is positive.*

Proof. Since the fixed points of U and V are pairwise different, the cross ratio exists. As cross ratios are preserved under Möbius transformations, we may assume that

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

just as in the proof of Lemma 5.2. Then $2 < \mathrm{tr}[U, V] = -(k - 1/k)^2 ad + k^2 + 1/k^2$ is equivalent to $ad < 1$. But then $(a - d)^2 > (a + d)^2 - 4$ shows that both fixed points of V have the same sign. Since the fixed points of U are 0 and ∞ this implies that $\mathrm{cross}(\omega_U, \omega_U', \omega_V, \omega_V') > 0$. □

Let c be the cross ratio from Lemma 5.7. Then $k := (1 + \sqrt{c})/(1 - \sqrt{c})$ satisfies $c = \mathrm{cross}(-1, 1, -k, k)$. Lemma 3.1 implies that there exists some $S \in \mathrm{GL}_2(\mathbb{R})$ such that SUS^{-1} fixes ± 1 and SVS^{-1} fixes $\pm k$.

Thus we may assume that

$$U = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} x & (x^2 - 1)/y \\ y & x \end{pmatrix} \quad \text{with } x \geqslant a > 1.$$

Further, since $-2 > \mathrm{tr}(U^{-1}V) = 2ax - by(1 + (x^2 - 1)/y^2)$ we may assume (after conjugating U and V with $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ if necessary) that $b > 0$, $y > 0$. We then define the sets

$$\mathbb{X}_1^+ := C(-(a+1)/b, -(a-1)/b), \qquad \mathbb{X}_1^- := C((a-1)/b, (a+1)/b),$$
$$\mathbb{X}_2^+ := C(-(x+1)/y, -(x-1)/y), \qquad \mathbb{X}_2^- := C((x-1)/y, (x+1)/y).$$

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

5.2.4. *Conclusion.* Similarly to § 5.1 we say that a pair $U, V \in \mathrm{SL}_2(\mathbb{R})$ with $\mathrm{tr}[U,V] > 2$ is *normalized* if (U,V) has the form as in §§ 5.2.1, 5.2.2 or 5.2.3.

We show that the sets $\mathbb{X}_1^+, \mathbb{X}_2^+, \mathbb{X}_1^-, \mathbb{X}_2^-$ satisfy the requirements of Theorem 2.1 in all cases discussed in this section. Let $\mathbb{F}_U = \mathbb{H} \setminus (\mathbb{X}_1^+ \cup \mathbb{X}_1^-)$ and $\mathbb{F}_V = \mathbb{H} \setminus (\mathbb{X}_2^+ \cup \mathbb{X}_2^-)$.

LEMMA 5.8. *The sets $\mathbb{X}_1^+, \mathbb{X}_2^+, \mathbb{X}_1^-, \mathbb{X}_2^-$ are pairwise disjoint and satisfy the conditions* (a) *and* (b) *of Theorem 2.1 for $g_1 = U$ and $g_2 = V$. If $\mathbb{F} = \mathbb{H} \setminus (\mathbb{X}_1^+ \cup \mathbb{X}_1^- \cup \mathbb{X}_2^+ \cup \mathbb{X}_2^-)$ then $z' := i \in \mathbb{F}^o$.*

Proof. The fact that the four sets are disjoint follows from a case by case discussion using $\mathrm{tr}(U), \mathrm{tr}(V), -\mathrm{tr}(U^{-1}V) \geqslant 2$. We only give the details for the case 5.2.3. By symmetry, it suffices to show that $\mathbb{X}_1^- \cap \mathbb{X}_2^-$ is empty. Using the identity $1 = \det(U) = a^2 - b^2$, we see that $-2 \geqslant \mathrm{tr}(U^{-1}V) = 2ax - by(1 + (x^2-1)/y^2)$ is equivalent to $by > (x+1)(a+1)$ or $by < (x-1)(a-1)$. These two inequalities are equivalent to $(x+1)/y < b/(a+1) = (a-1)/b$ and $(x-1)/y > b/(a-1) = (a+1)/b$ respectively. Hence $\mathbb{X}_1^- \cap \mathbb{X}_2^-$ is empty.

The condition (a) from Theorem 2.1 can easily be checked. Let us now prove condition (b). The fact that $\mathbb{F}_U$ is a fundamental domain for $\langle U \rangle$ is obvious if $\mathrm{tr}(U) = 2$, since then U is a translation by λ and $\mathbb{F}_U$ is a vertical strip of width λ. A similar argument holds for V (after conjugation with $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$) whenever $\mathrm{tr}(V) = 2$. Suppose now $\mathrm{tr}(U) > 2$. One observes that $(\mathbb{X}_1^+)^o$ and $(\mathbb{X}_1^-)^o$ each contain one fixed point of U. Since U maps the boundary of $\mathbb{X}_1^+$ to the boundary of $\mathbb{X}_1^-$ it follows that $\mathbb{F}_U$ is a fundamental domain for $\langle U \rangle$. The case $\mathrm{tr}(V) > 2$ is handled similarly. The fact that $\mathbb{F}$ is a fundamental domain for G now follows from Klein's combination theorem. Note that the regions $\mathbb{F}_U$ and $\mathbb{F}_V$ are tangent if and only if $2 = \mathrm{tr}(U) = \mathrm{tr}(V) = -\mathrm{tr}(U^{-1}V)$. But then the tangent points are precisely the fixed points of the parabolic transformations $U^{-1}V$ and UV^{-1}. Finally, the inclusion $i \in \mathbb{F}^o$ follows directly. □

The following remark allows Algorithm 1 to be speeded up significantly in the way suggested by Remark 2.2.

REMARK 5.9. Suppose $z \in \mathbb{H}$. Again, one can easily compute the exponents $n_U, n_V \in \mathbb{Z}$ such that $U^{n_U} \cdot z \in \mathbb{F}_U$ and $V^{n_V} \cdot z \in \mathbb{F}_V$.

If U is a translation, the computation of n_U is obvious. Similarly, if $\mathrm{tr}(V) = 2$, then after conjugating with $S := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, SVS^{-1} is also a translation. Hence the computation of n_V is clear.

Finally, if $X \in \{U, V\}$ is hyperbolic, we proceed exactly as in Remark 5.6. There exists some $T \in \mathrm{GL}(2,\mathbb{R})$ such that TXT^{-1} is a diagonal matrix. Further, $T \cdot \mathbb{F}_X$ is the area between two geodesics, and the exponent n_X can now be computed using equation (5.1).

5.3. *The membership test*

Algorithms 1 and 2 together with our fundamental domains from §§ 5.1 and 5.2 finally yield a constructive membership test for all discrete and free two-generator subgroups of $\mathrm{SL}_2(\mathbb{R})$. We close this section by stating this algorithm explicitly.

ALGORITHM 3. (ConstructiveMembership$\mathrm{SL}_2(\mathbb{R})$)
Input: Three matrices $A, B, M \in \mathrm{SL}_2(\mathbb{R})$ such that $G = \langle A, B \rangle$ is discrete and free of rank 2.
Output: A word $w = w(a,b)$ with $w(A,B) = M$ if M is an element of G and false otherwise; here a, b are abstract elements freely generating a free group F.

(1) Compute a witness pair (U', V') for G and words $u, v \in F$ such that $\overline{U'} = u(\overline{A}, \overline{B})$ and $\overline{V'} = v(\overline{A}, \overline{B})$ using Algorithm 2.
(2) Compute some $S \in \mathrm{GL}_2(\mathbb{R})$ such that $(U,V) := (SU'S^{-1}, SV'S^{-1})$ is normalized.

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

(3) Let $z' \in \mathbb{H}$ and $\mathbb{X}_1^+, \mathbb{X}_1^-, \mathbb{X}_2^+, \mathbb{X}_2^-$ be as in Lemma 5.4 or 5.8 depending on whether $\mathrm{tr}[A,B] \leqslant -2$ or $\mathrm{tr}[A,B] > 2$.
(4) Decide if $\overline{SMS^{-1}}$ can be written as a word w' in $\overline{U}$ and $\overline{V}$. This is done by calling Algorithm 1 with input $g_1 = \overline{U}$, $g_2 = \overline{V}$, the sets $\mathbb{X}_j^{\pm}$, the point z' and $g = \overline{SMS^{-1}}$.
(5) If no such w' exists, then return false.
(6) If $w'(u(A,B), v(A,B)) \neq M$, then return false.
(7) Return true and $w := w'(u(a,b), v(a,b))$.

Note that if one omits step (6), then the algorithm decides membership in $\mathrm{PSL}_2(\mathbb{R})$.

6. *Implementation*

6.1. *Comments on the ground fields*

Our algorithms take as input two matrices A and B with entries in a field K such that there exists a field monomorphism $\varepsilon\colon K \to \mathbb{R}$. Via ε, we can view K as a subfield of $\mathbb{R}$ and the group G generated by A and B thus acts on $\mathbb{H}$.

Further, the algorithms require that given $a \in K$, the following tasks can be performed.

(1) Test whether $a > 0$.
(2) If $a \geqslant 0$, compute $\sqrt{a} \in K$. If $\sqrt{a} \notin K$, then it must be possible to extend K to $K(\sqrt{a})$.

Real algebraic number fields have these two properties (see [**5**, § 3.6.2]) and we have implemented Algorithms 2 and 3 in Magma [**4**] for this class of fields.

6.2. *Comparison with facilities already in* Magma

Currently, Magma can solve the constructive membership problem for infinite matrix groups only in the following two cases.

(1) For congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$, that is, subgroups that contain the kernel $\Gamma(N)$ of the canonical homomorphism $\mathrm{PSL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ for some integer $N \geqslant 2$. A congruence subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ is not free of rank 2, unless it has index 6 in $\mathrm{PSL}_2(\mathbb{Z})$.

(2) For arithmetic Fuchsian groups with no cusps. These are the full unit groups of orders in quaternion algebras ramified at all but one infinite place. Such groups are not free of rank 2.

Hence there is only small overlap between our implementation and existing features of Magma.

6.3. *Examples and runtimes*

We now exhibit some explicit runtimes. All timings are done on a Core i7 860.

Example 6.1. For $n \in \mathbb{N}$ let ζ_n be a primitive nth root of unity and $\theta_n = \zeta_n + \zeta_n^{-1}$. Let $K_n = \mathbb{Q}(\theta_n)$. Then K_n is the maximal totally real subfield of the cyclotomic number field $C_n = \mathbb{Q}(\zeta_n)$. The map $\varepsilon\colon C_n \to \mathbb{C}, \zeta_n \mapsto \exp(2\pi i/n)$ induces an embedding of K_n into $\mathbb{R}$. Let $d(n)$ denote the degree of K_n over $\mathbb{Q}$. Then every element in K_n can be described as $f(\theta_n)$ where $f(x) \in \mathbb{Q}[x]$ with $\deg(f) < d(n)$.

Let W_n denote the set of elements in K_n which can be written as $f(\theta)/b$ with some integer $1 \leqslant b \leqslant 100$ and some $f(x) \in \mathbb{Z}[x]$ with coefficients in the range $[-10^4, 10^4]$. Then W_n is a large, but finite, subset of K_n and we can choose random elements in W_n. Using these random elements in W_n we can determine a wide range of interesting examples of matrices in $\mathrm{SL}_2(K_n)$.

Using this strategy, we have chosen 10 000 pairs of matrices $A, B \in \mathrm{SL}_2(K_n)$ with $\mathrm{tr}(A), \mathrm{tr}(B) \geqslant 2$ and $\mathrm{tr}[A,B] > 2$. For each pair we called Algorithm 2 to see whether $G = \langle A, B\rangle$ is discrete and free of rank 2. If this was the case, we used Algorithm 3 to check if $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right) \in G$. The timings of these tests are summarized in Table 1.

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

EXAMPLE 6.2. A well-known example of a discrete and free group is $G = \Gamma(2) = \langle A, B\rangle \leqslant \mathrm{SL}_2(\mathbb{Q})$ with

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

These generators satisfy $\mathrm{tr}[A, B] = 18 > 2$ and $\mathrm{tr}(A) = 2 = \mathrm{tr}(B)$. Hence we are in the case of § 5.2.1. Note that $\mathrm{tr}(AB^{-1}) = -2$ and hence (A, B) is a witness pair for G. Further, this pair is normalized as in § 5.2.1. Our implementation of Algorithm 3 chooses $S = I$, $(U, V) = (A, B)$, $z' = i \in \mathbb{H}$, $\mathbb{X}_1^+ = \{x + iy \in \mathbb{H} \mid x \leqslant -1\}$, $\mathbb{X}_1^- = \{x + iy \in \mathbb{H} \mid x \geqslant 1\}$, $\mathbb{X}_2^+ = C(-1, 0)$ and $\mathbb{X}_2^- = C(0, 1)$ in steps (2) and (3). Thus in this example we can choose $K = \mathbb{Q}$ and it is not necessary to extend K.

Let M be a random word of length k in $\{A, B\}$. Such a word can be constructed by multiplying k random elements in $\{A, B, A^{-1}, B^{-1}\}$ if one takes care that no two adjacent factors are mutually inverse.

We have summarized the time needed for the constructive membership test $M \in G$ in Table 2.

The main reason for the nonlinear increase in time is the growth of the matrix entries during the intermediate steps of the algorithm.

EXAMPLE 6.3. Let $G = \langle A, B\rangle \leqslant \mathrm{SL}_2(\mathbb{Q})$ where

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}.$$

Then $\mathrm{tr}(A) = 3$, $\mathrm{tr}(B) = 4$ and $\mathrm{tr}[A, B] = -9$. Hence G is discrete and free of rank 2 by Theorem 4.4 and (A, B) is a witness pair for G.

TABLE 1. *Timings for Example 6.1 (in seconds).*

n	2	5	11	25	55
$d(n)$	1	2	5	10	20
Time for 10 000 calls to Algorithm 2	0.2	13	25	74	272
Average time to decide if $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right) \in G$	<0.1	0.6	13	201	3924

TABLE 2. *Timings for Example 6.2.*

k	$\leqslant$100	$\leqslant$1000	$\leqslant$10 000	$\leqslant$20 000
sec	<0.1	<0.1	<5	<35

TABLE 3. *Timings for Example 6.3.*

k	$\leqslant$100	$\leqslant$1000	$\leqslant$2000	$\leqslant$10 000
sec	<0.1	<2	<10	<600

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press

Our implementation of Algorithm 3 now chooses

$$S = \frac{1}{10}\begin{pmatrix} 6\sqrt{5}+20 & 7\sqrt{5}+5 \\ -10 & 5\sqrt{5}+5 \end{pmatrix}, \qquad z' = \frac{74}{20}i,$$

$$U = SAS^{-1} = \frac{1}{2}\begin{pmatrix} \sqrt{5}+3 & 0 \\ 0 & -\sqrt{5}+3 \end{pmatrix}, \qquad V = SBS^{-1} = \frac{1}{5}\begin{pmatrix} 2\sqrt{5}+10 & 11 \\ 5 & -2\sqrt{5}+10 \end{pmatrix},$$

$$\mathbb{X}_1^+ = C\left(\frac{967}{1000}, \frac{-37}{100}\right), \qquad \mathbb{X}_1^- = C\left(\frac{2901\sqrt{5}+6769}{2000}, \frac{-111\sqrt{5}-259}{200}\right),$$

$$\mathbb{X}_2^+ = C\left(\frac{-\sqrt{5}-15}{10}, \frac{9\sqrt{5}-25}{10}\right) \quad \text{and} \qquad \mathbb{X}_2^- = C\left(\frac{-\sqrt{5}+15}{10}, \frac{9\sqrt{5}+25}{10}\right).$$

In particular, the membership test can be performed over the field $K' = \mathbb{Q}(\sqrt{5})$. Note that the choice of z' from above differs slightly from Lemma 5.4, as we try to keep the field K' as small as possible.

Let M be a word of length k in $\{A, B\}$. We have summarized the time needed for the constructive membership test $M \in G$ in Table 3.

7. *Open problems*

It would be of interest to extend the method for detecting whether an input group is discrete and free as well as the membership test for such groups to arbitrary rank $m \geqslant 2$. For this purpose one would need to find suitable fundamental domains as described in Theorem 2.1 for arbitrary m. Similarly, it would be of interest to extend the method described here to discrete free products of arbitrary cyclic groups. While Theorem 2.1 would generalize to free products of cyclic groups, again it is unclear how to determine the special fundamental domain for a given subgroup of $\mathrm{SL}_2(\mathbb{R})$ in this case.

Further, it would be of interest to generalize the method described here to $\mathrm{SL}_n(\mathbb{R})$ for arbitrary $n \geqslant 2$. This however incorporates the problem that one needs to find a suitable topological action of the matrix groups of higher degrees. And, clearly, one has to keep in mind that the constructive membership problem is not always decidable in larger degree matrix groups.

Acknowledgements. The authors would like to thank Gerhard Rosenberger and Norman Purzitsky for helpful discussions.

References

1. B. Assmann and B. Eick, 'Computing polycyclic presentations of polycyclic matrix groups', *J. Symbolic Comput.* 40 (2005) 1269–1284.
2. R. Beals, 'Improved algorithms for the Tits alternative', *Groups and computation III*, Ohio State University Mathematical Research Institute Publications 8 (eds W. M. Kantor and A. Seress; de Gruyter, New York, 2001) 63–77.
3. A. F. Beardon, *The geometry of discrete groups*, Graduate Texts in Mathematics 91 (Springer, New York, 1983).
4. W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) no. 3–4, 235–265.
5. H. Cohen, *A course in computational algebraic number theory* (Springer, 1993).
6. A. S. Detinko, B. Eick and D. L. Flannery, 'Computing with matrix groups over infinite fields', *Groups St Andrews 2009 in Bath Volume 1*, London Mathematical Society Lecture Note Series 387 (Cambridge University Press, Cambridge, 2010) 256–269.
7. A. S. Detinko, D. L. Flannery and E. A. O'Brien, 'Algorithms for the Tits alternative and related problems', *J. Algebra* 344 (2011) 397–406.

8. R. Fricke and F. Klein, *Vorlesungen über die Theorie der Automorphen Functionen* (Teubner, 1897).
9. S. Katok, *Fuchsian groups*, Chicago Lectures in Mathematics (University of Chicago Press, Chicago, IL, 1992).
10. G. Kern-Isberner and G. Rosenberger, 'Über Diskretheitsbedingungen und die Diophantische Gleichung $ax^2 + by^2 + cz^2 = dxyz$', *Arch. Math. (Basel)* 34 (1980) no. 6, 481–493.
11. R. C. Lyndon and P. E. Schupp, *Combinatorial group theory* (Springer, 1977).
12. C. F. Miller, *On group-theoretic decision problems and their classification* (Princeton University Press, Princeton, 1971).
13. G. Ostheimer, 'Practical algorithms for polycyclic matrix groups', *J. Symbolic Comput.* 28 (1999) no. 3, 361–379.
14. N. Purzitsky, 'Two-generator discrete free products', *Math. Z.* 126 (1972) 209–223.
15. N. Purzitsky, 'Real two-dimensional representations of two-generator free groups', *Math. Z.* 127 (1972) 95–104.
16. N. Purzitsky, 'A cutting and pasting of noncompact polygons with applications to Fuchsian groups', *Acta Math.* 143 (1979) 233–250.
17. G. Rosenberger, 'Fuchssche Gruppen, die freies Produkt zweier zyklischer Gruppen sind, und die Gleichung $x^2 + y^2 + z^2 = xyz$', *Math. Ann.* 199 (1972) 213–227.

B. Eick
Institut Computational Mathematics
TU Braunschweig, Pockelsstrasse 14
38106 Braunschweig
Germany

beick@tu-bs.de

M. Kirschmer
Lehrstuhl D für Mathematik
RWTH Aachen University
Templergraben 64
52062 Aachen
Germany

markus.kirschmer@math.rwth-aachen.de

C. Leedham-Green
School of Mathematical Sciences
Queen Mary College University of London
Mile End Road
London E1 4NS
United Kingdom

c.r.leedham-green@qmul.ac.uk

https://doi.org/10.1112/S1461157014000047 Published online by Cambridge University Press