The Identity Problem in the special affine group of $\mathbb{Z}^2$

Ruiwen Dong

University of Oxford

Oxford, United Kingdom

ruiwen.dong@kellogg.ox.ac.uk

Abstract—We consider semigroup algorithmic problems in the Special Affine group $\mathsf{SA}(2, \mathbb{Z}) = \mathbb{Z}^2 \rtimes \mathsf{SL}(2, \mathbb{Z})$, which is the group of affine transformations of the lattice $\mathbb{Z}^2$ that preserve orientation. Our paper focuses on two decision problems introduced by Choffrut and Karhumäki (2005): the *Identity Problem* (does a semigroup contain a neutral element?) and the *Group Problem* (is a semigroup a group?) for finitely generated sub-semigroups of $\mathsf{SA}(2, \mathbb{Z})$. We show that both problems are decidable and NP-complete. Since $\mathsf{SL}(2, \mathbb{Z}) \leq \mathsf{SA}(2, \mathbb{Z}) \leq \mathsf{SL}(3, \mathbb{Z})$, our result extends that of Bell, Hirvensalo and Potapov (SODA 2017) on the NP-completeness of both problems in $\mathsf{SL}(2, \mathbb{Z})$, and contributes a first step towards the open problems in $\mathsf{SL}(3, \mathbb{Z})$.

I. INTRODUCTION

Algorithmic problems in matrix semigroups

The computational theory of matrix groups and semigroups is one of the oldest and most well-developed parts of computational algebra. The area plays an essential role in analysing system dynamics, and has numerous applications in automata theory, program analysis, and interactive proof systems [1], [2], [3], [4], [5]. The earliest studied algorithmic problems for groups and semigroups are the *Semigroup Membership* and the *Group Membership* problems, introduced respectively by Markov [6] and Mikhailova [7] in the 1940s and 1960s. For both problems, we work in a fixed matrix group G. The input is a finite set of matrices $\mathcal{G} = \{A_1, \ldots, A_K\}$ in G and a target matrix $A \in G$. Denote by $\langle \mathcal{G} \rangle$ the semigroup generated by $\mathcal{G}$, and by $\langle \mathcal{G} \rangle_{grp}$ the group generated by $\mathcal{G}$.

   i. *(Semigroup Membership)* decide whether $\langle \mathcal{G} \rangle$ contains A.

   ii. *(Group Membership)* decide whether $\langle \mathcal{G} \rangle_{grp}$ contains A.

Both problems are undecidable in general matrix groups by classical results of Markov and Mikhailova [6], [7]. In this paper, we consider the *Identity Problem* and the *Group Problem*, introduced by Choffrut and Karhumäki [3] in 2005. These two decision problems concern the *structure* of semigroups rather than their *membership*. Fix a matrix group G, the input for both problems is a finite set of matrices $\mathcal{G} = \{A_1, \ldots, A_K\}$ in G.

   iii. *(Identity Problem)* decide whether $\langle \mathcal{G} \rangle$ contains the neutral element I of G.

   iv. *(Group Problem)* decide whether $\langle \mathcal{G} \rangle$ is a group.

Apart from their obvious use in determining structural properties of a semigroup[1], the Identity Problem and the Group Problem are closely related to[2] the more difficult Semigroup Membership problem. Usually, the solution to the Identity Problem is the most essential special case on the way to building an algorithm for the Semigroup Membership problem. We also point out that there are significantly more available algorithms for groups then there are for semigroups, therefore performing preliminary checks using the Group Problem can help decide Semigroup Membership in many special cases (see Section VI).

All four algorithmic problems remain undecidable even for matrices of small dimensions. The *Special Linear group* of dimension n, denoted by $\mathsf{SL}(n, \mathbb{Z})$, is defined as the group of $n \times n$ integer matrices with determinant one. Mikhailova famously showed undecidability of the Group Membership problem (and hence also Semigroup Membership) in $\mathsf{SL}(4, \mathbb{Z})$ [7]. Later, Bell and Potapov showed undecidability of the Identity Problem and the Group Problem in $\mathsf{SL}(4, \mathbb{Z})$ [9]. Both undecidability results stem from the fact that $\mathsf{SL}(4, \mathbb{Z})$ contains as a subgroup a direct product of two non-abelian free groups. In dimension two, the Semigroup Membership problem in $\mathsf{SL}(2, \mathbb{Z})$ was shown to be decidable in **EXPSPACE** by Choffrut and Karhumäki [3]; Group Membership was shown to be in **PTIME** by Lohrey [10]; the Identity Problem and the Group Problem were shown to be **NP**-complete by Bell, Hirvensalo and Potapov [11]. It remains an intricate open problem whether any of these four algorithmic problems is decidable in $\mathsf{SL}(3, \mathbb{Z})$. Nevertheless, Ko, Niskanen and Potapov [12] recently showed that $\mathsf{SL}(3, \mathbb{Z})$ cannot embed pairs of words over an alphabet of size two, suggesting that all four problems in $\mathsf{SL}(3, \mathbb{Z})$ might be decidable. The following table I summarizes the state of art as well as our result, the group $\mathsf{SA}(2, \mathbb{Z})$ will be introduced in the next subsection.

The Special Affine group $\mathsf{SA}(2, \mathbb{Z})$

In this paper we focus on an intermediate group between $\mathsf{SL}(2, \mathbb{Z})$ and $\mathsf{SL}(3, \mathbb{Z})$: the *Special Affine group* $\mathsf{SA}(2, \mathbb{Z})$. This affine analogue of $\mathsf{SL}(2, \mathbb{Z})$ is defined as the group of affine

---

[1]For example, given a decision procedure for the Group Problem, one can compute a generating set for the *group of units* (set of of invertible elements) of a finitely generated semigroup $\langle \mathcal{G} \rangle$ [8].

[2]In fact, decidability of Semigroup Membership subsumes decidability of the Identity Problem and the Group Problem.

	Semigrp Mem.	Group Mem.	Identity & Grp Prb.
$\mathsf{SL}(2,\mathbb{Z})$	EXPSPACE [3]	PTIME [10]	NP-complete [11]
$\mathsf{SA}(2,\mathbb{Z})$	?	Decidable [13]	NP-complete*
$\mathsf{SL}(3,\mathbb{Z})$	?	?	?
$\mathsf{SL}(4,\mathbb{Z})$	Undec. [7]	Undec. [7]	Undec. [9]

TABLE I
* = OUR RESULT.

transformations of $\mathbb{Z}^2$ that preserve orientation. Written as matrices, elements of $\mathsf{SA}(2,\mathbb{Z})$ are 3×3 integer matrices of the following form.

$$\mathsf{SA}(2,\mathbb{Z}) \coloneqq \left\{ \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix} \;\middle|\; A \in \mathsf{SL}(2,\mathbb{Z}), \boldsymbol{a} \in \mathbb{Z}^2 \right\}.$$

To be precise, elements of $\mathsf{SA}(2,\mathbb{Z})$ are represented using matrices with *binary encoded* entries. We denote by $(A, \boldsymbol{a})$ the element $\begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}$, then the neutral element of $\mathsf{SA}(2,\mathbb{Z})$ is $(I, \boldsymbol{0})$; multiplication in $\mathsf{SA}(2,\mathbb{Z})$ is given by

$$(A, \boldsymbol{a}) \cdot (B, \boldsymbol{b}) = (AB, A\boldsymbol{b} + \boldsymbol{a}).$$

Naturally, $\mathsf{SA}(2,\mathbb{Z})$ has a subgroup $\{(A, \boldsymbol{0}) \mid A \in \mathsf{SL}(2,\mathbb{Z})\} \cong \mathsf{SL}(2,\mathbb{Z})$.

Special Affine groups are important in the context of many fundamental problems, such as Lie groups [14], polyhedral geometry [15], dynamical systems [16], quadrics [17], computer vision [18], [19] and gauge theory [20]. Apart from the intrinsic interest to study $\mathsf{SA}(2,\mathbb{Z})$, we also point out that the Special Affine group has tight connections to various reachability problems. Some of the central questions in automated verification include reachability problems in *Affine Vector Addition Systems* and *Affine Vector Addition Systems with states (Affine VASS)* over the integers [21]. While both problems as well as many of their variations have been shown to be decidable in dimension one and undecidable for dimension three [22], [23], few results are known for dimension two. Since the study of these reachability problems in dimension two necessitates the study of sub-semigroups of $\mathsf{SA}(2,\mathbb{Z})$, the techniques introduced in our paper may provide insights into these open problems.

Currently, among the four algorithmic problems introduced in the beginning, the only known result in $\mathsf{SA}(2,\mathbb{Z})$ is decidability of the Group Membership problem. This can be deduced from the recent work of Delgado [13], who showed decidability of the Group Membership problem in the semidirect product $\mathbb{Z}^m \rtimes F$, where F is a free group. Delgado's result relies on a generalization of the Stalling automata, and can therefore be extended to the case where F is *virtually free*. This can then be applied to $\mathsf{SA}(2,\mathbb{Z}) = \mathbb{Z}^2 \rtimes \mathsf{SL}(2,\mathbb{Z})$, since $\mathsf{SL}(2,\mathbb{Z})$ is virtually free.

In this paper, we step further by considering sub-semigroups of $\mathsf{SA}(2,\mathbb{Z})$. We show decidability and **NP**-completeness of the Identity Problem and the Group Problem in $\mathsf{SA}(2,\mathbb{Z})$. This extends the **NP**-completeness result of Bell et al. for the Identity Problem and the Group Problem in $\mathsf{SL}(2,\mathbb{Z})$, and contributes a first step towards solving problems in $\mathsf{SL}(3,\mathbb{Z})$.

The **NP**-hard lower bounds in $\mathsf{SA}(2,\mathbb{Z})$ directly follows from its embedding of the subgroup $\mathsf{SL}(2,\mathbb{Z})$. In order to prove decidability and the **NP** upper bounds, our main idea is the following. Given a finitely generated sub-semigroup $\langle \mathcal{G} \rangle$ of $\mathsf{SA}(2,\mathbb{Z})$, we show that we can without loss of generality suppose its image under the natural projection $p \colon \mathsf{SA}(2,\mathbb{Z}) \to \mathsf{SL}(2,\mathbb{Z})$ to be a group, using a classic result for $\mathsf{SL}(2,\mathbb{Z})$. If $p(\langle \mathcal{G} \rangle)$ is a group, we then invoke an effective version of the *Tits alternative*, which shows that either $p(\langle \mathcal{G} \rangle)$ contains a non-abelian free subgroup, or it is virtually solvable. In the first case we show that $\langle \mathcal{G} \rangle$ is always a group, while in the second case we further simplify the problem by identifying six subcases for $p(\langle \mathcal{G} \rangle)$. Our proof combines two viewpoints: a group theoretic viewpoint of $\mathsf{SL}(2,\mathbb{Z})$ as a virtually free group, and a geometric viewpoint of $\mathsf{SA}(2,\mathbb{Z})$ as elements acting on the lattice $\mathbb{Z}^2$.

Beyond the Identity Problem and the Group Problem, we will discuss some obstacles to generalizing our results to the Semigroup Membership problem in $\mathsf{SA}(2,\mathbb{Z})$. Our results actually show that Semigroup Membership in $\mathsf{SA}(2,\mathbb{Z})$ is decidable in many cases under additional constraints. We identify one of the remaining difficult cases, namely when $\langle \mathcal{G} \rangle$ is isomorphic to a sub-semigroup of the semidirect product $\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}$, where λ is a quadratic integer. The Semigroup Membership problem in $\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}$ remains open. However, the group $\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}$ bears certain similarities to the *Baumslag-Solitar group* $\mathsf{BS}(1, q) \coloneqq \mathbb{Z}[\frac{1}{q}] \rtimes_q \mathbb{Z}$; and a recent result by Cadilhac, Chistikov and Zetzsche [24] showed decidability of the *rational subset membership problem*[3] in $\mathsf{BS}(1, q)$ by considering rational languages of *base-q expansions*. Despite some visible difficulties, it would be interesting in the future to adapt this approach to study the Semigroup Membership problem in $\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}$, namely by considering rational languages of *base-λ expansions* [25], where λ is an algebraic integer.

II. PRELIMINARIES

Words, semigroups and groups

Let G be an arbitrary group. Let $\mathcal{A} = \{a_1, \ldots, a_K\}$ be a set of elements in G. Considering $\mathcal{A}$ as an alphabet, denote by $\mathcal{A}^*$ the set of words over $\mathcal{A}$. For an arbitrary word $w = a_{i_1} a_{i_2} \cdots a_{i_m} \in \mathcal{A}^*$, by multiplying consecutively the elements appearing in w, we can evaluate w as an element $\pi(w)$ in G. We say that the word w *represents* the element $\pi(w)$. The semigroup $\langle \mathcal{A} \rangle$ generated by $\mathcal{A}$ is hence the set of elements in G that are represented by *non-empty* words in $\mathcal{A}^*$.

A word w over the alphabet $\mathcal{A}$ is called *full-image* if every letter in $\mathcal{A}$ has at least one occurrence in w.

Lemma 1. *Let $\mathcal{A} = \{a_1, \ldots, a_K\}$ be a set of elements in a group G. Consider the following conditions:*

(i) The neutral element I of G is represented by a full-image word over $\mathcal{A}$.

(ii) The semigroup $\langle \mathcal{A} \rangle$ is a group.

---

[3]The rational subset membership problem subsumes the Semigroup Membership problem.

(iii) Every element $A \in \langle \mathcal{A} \rangle$ is represented by a full-image word over $\mathcal{A}$.

Then $(i) \Longleftrightarrow (ii)$, and $(ii) \Longrightarrow (iii)$.

Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$ be a set of elements in $\mathsf{SA}(2, \mathbb{Z})$. Suppose that an element $A \in \langle A_1, \ldots, A_K \rangle$ in $\mathsf{SL}(2, \mathbb{Z})$ is represented by a full-image word w in the alphabet $\{A_1, \ldots, A_K\}$. Then replacing each letter A_i in w by $(A_i, \boldsymbol{a}_i)$, we obtain a product $(A, \boldsymbol{a}) \in \mathsf{SA}(2, \mathbb{Z})$ for some $\boldsymbol{a} \in \mathbb{Z}^2$, represented by a full-image word over $\mathcal{G}$.

The following observation shows that decidability of the Group Problem implies decidability of the Identity Problem.

Lemma 2 ([9]). *Given a subset $\mathcal{A}$ of a group G, the semigroup $\langle \mathcal{A} \rangle$ contains the neutral element I if and only if there exists a non-empty subset $\mathcal{H} \subseteq \mathcal{A}$ such that $\langle \mathcal{H} \rangle$ is a group.*

Linear algebra

For an arbitrary matrix $A \in \mathsf{SL}(2, \mathbb{Z})$, an *invariant subspace* of A is a $\mathbb{C}$-linear subspace V of $\mathbb{C}^2$ such that $AV = V$. If the eigenvalues of A are reals, then one can suppose that the invariant spaces of A are subspaces of $\mathbb{R}^2$. Denote by $\mathrm{Lat}(A)$ the set of *dimension one* invariant subspaces of A. It is easy to see that if $A \notin \{I, -I\}$, then $\mathrm{Lat}(A)$ has one or two elements.

Two matrices A and B are called *conjugates* over a field $\mathbb{K}$ if $P^{-1}AP = B$ for some matrix P with entries in $\mathbb{K}$. This is denoted as $A \overset{\mathbb{K}}{\sim} B$. Two matrices $A, B \in \mathsf{SL}(2, \mathbb{Z})$ are called *simultaneously triangularizable* if there exists a complex matrix P such that $P^{-1}AP$ and $P^{-1}BP$ are both upper-triangular. It is easy to see that if $\mathrm{Lat}(A) \cap \mathrm{Lat}(B) \neq \emptyset$, then A and B are simultaneously triangularizable.

Group theory

For a general reference on group theory, see [26].

Definition 3. *A group G is called* solvable *if its derived series*
$$G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \cdots,$$
where $G^{(i+1)}$ is the commutator subgroup[4] of $G^{(i)}$, eventually reaches the trivial group.

Every subgroup of a solvable group is solvable [26, Proposition 13.91]. Abelian groups are obviously solvable. For any field $\mathbb{K}$ and integer n, denote by $\mathsf{T}(n, \mathbb{K})$ the group of $n \times n$ invertible upper-triangular matrices with entries in $\mathbb{K}$. Then $\mathsf{T}(n, \mathbb{K})$ is a solvable group [27]. In particular, if two matrices $A, B \in \mathsf{SL}(2, \mathbb{Z})$ are simultaneously triangularizable, then the group G they generate is isomorphic to a subgroup of $\mathsf{T}(2, \mathbb{C})$; thus G is solvable.

Given an alphabet Σ, define the corresponding group alphabet $\Sigma^{\pm} := \Sigma \cup \{a^{-1} \mid a \in \Sigma\}$, where a^{-1} is a new symbol. There is a natural involution $(\cdot)^{-1}$ over $(\Sigma^{\pm})^*$ defined by $(a^{-1})^{-1}$ and $(a_1 \cdots a_m)^{-1} = a_m^{-1} \cdots a_1^{-1}$. A word over the alphabet is called *reduced* if it does not contain consecutive letters aa^{-1} or $a^{-1}a$. For a word w over the alphabet $\Sigma^{\pm}$,

---

[4]The commutator subgroup of a group H is the subgroup generated by the elements $ghg^{-1}h^{-1}$ where $g, h \in H$.

define $\mathrm{red}(w)$ to be the reduced word obtained by iteratively replacing consecutive letters aa^{-1} and $a^{-1}a$ with the empty string. The *free group* $F(\Sigma)$ over Σ is then defined as the set of reduced words over the alphabet $\Sigma^{\pm}$, where multiplication is given by $v \cdot w = \mathrm{red}(vw)$, and inversion is given by the involution $(\cdot)^{-1}$. A group is called *free* if it is a free group over some alphabet. The free group $F(\Sigma)$ is abelian if and only if the cardinality of Σ is zero or one, in which case $F(\Sigma)$ is trivial or isomorphic to the infinite cyclic group $\mathbb{Z}$.

Theorem 4 (Nielsen–Schreier [28, Chapter I, Theorem 5]). *Every subgroup of a free group is free.*

Given an arbitrary group G with neutral element I. An element $T \in G$ is called *torsion* if $T \neq I$ and $T^m = I$ for some $m > 1$. A group is called *torsion-free* if it does not contain a torsion element. In particular, a free group is torsion-free.

A group is called *virtually solvable* if it admits a finite index subgroup that is solvable. Similarly, a group is called *virtually free* if it admits a finite index subgroup that is free. The following is a classic result.

Theorem 5 ([29]). *The group $\mathsf{SL}(2, \mathbb{Z})$ is virtually free. Moreover, it contains a finite index free subgroup $F(\{S, T\})$ over two generators.*

Based on this fact, Bell et al. showed the following complexity result.

Theorem 6 ([11]). *The Identity Problem and the Group Problem in $\mathsf{SL}(2, \mathbb{Z})$ are **NP**-complete.*

Here, the input elements in $\mathsf{SL}(2, \mathbb{Z})$ are represented using matrices with binary encoded entries.

Classification of elements in $\mathsf{SL}(2, \mathbb{Z})$

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix in $\mathsf{SL}(2, \mathbb{Z})$. The characteristic polynomial of A is $f(X) = X^2 - (a + d)X + (ad - bc) = X^2 - (a + d)X + 1$. Consider the five following cases.

(i) $a + d = 0$.

In this case, $A \overset{\mathbb{Q}(i)}{\sim} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, the eigenvalues of A are i and $-i$. We have $A^4 = I$, so A is a torsion element.

(ii) $|a + d| = 1$.

In this case, $A \overset{\mathbb{Q}(\omega)}{\sim} \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$, where $\omega = \frac{1 + \sqrt{3}i}{2}$ or $\frac{-1 + \sqrt{3}i}{2}$. In both cases, we have $A^6 = I$, so A is a torsion element.

(iii) $a + d = 2$.

In this case, either $A = I$, or $A \overset{\mathbb{Q}}{\sim} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. In the second situation, we call A a *shear*. The only eigenvalue of A is 1. If A is a shear, then $\mathrm{Lat}(A)$ has exactly one element. See Figure 2 for an illustration.

(iv) $a + d = -2$.

In this case, either $A = -I$, or $A \overset{\mathbb{Q}}{\sim} \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$. In the second situation, we call A a *twisted inversion*. In

particular, if A is a twisted inversion, then $(A+I)^2 = 0$, and A^2 is a shear, and $\mathrm{Lat}(A)$ has exactly one element.

(v) $|a + d| \geq 3$.

In this case, $A \overset{\mathbb{R}}{\sim} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, where λ is the root of $f(X)$ such that $|\lambda| \geq 1$. Furthermore, λ is real. In this case, we call A a *scale*. If $\lambda > 0$, we call A a *positive scale*; if $\lambda < 0$, we call A an *inverting scale*. In both cases, $\mathrm{Lat}(A)$ has two elements, one element is the invariant space corresponding to the eigenvalue λ, and is called the *stretching direction*; the other element is the invariant space corresponding to the eigenvalue λ^{-1}, and is called the *compressing direction*. See Figure 1 for an illustration.
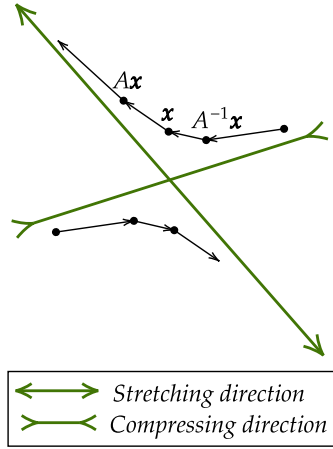

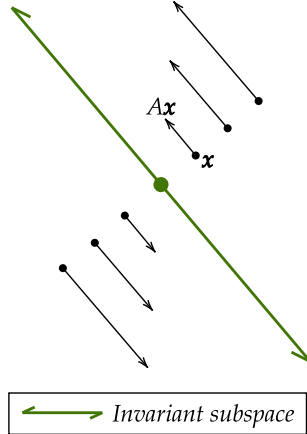Fig. 1. Illustration for a (positive) scale.

Fig. 2. Illustration for a shear.

III. OVERVIEW OF DECISION PROCEDURES

In this section we give an overview of the decision procedures for the Identity Problem and the Group Problem in $\mathsf{SA}(2,\mathbb{Z})$. We state two propositions (Propositions 9 and 10) regarding the structure of sub-semigroups of $\mathsf{SA}(2,\mathbb{Z})$. Assuming these propositions, we prove **NP**-completeness of

the Identity Problem and the Group Problem in $\mathsf{SA}(2,\mathbb{Z})$. The proofs of propositions 9 and 10 are delayed until Section IV and V.

We now first focus on solving the Group Problem, because by Lemma 2, decidability of the Group Problem will imply decidability of the Identity Problem. Fix a set $\mathcal{G} := \{(A_1, \boldsymbol{a}_1), \dots, (A_K, \boldsymbol{a}_K)\}$ of elements in $\mathsf{SA}(2,\mathbb{Z})$. The following lemma shows that, if the semigroup $G := \langle A_1, \dots, A_K \rangle$ is not a group, then $\langle \mathcal{G} \rangle$ is also not a group. Therefore, to decide whether $\langle \mathcal{G} \rangle$ is a group, we can focus on the case where G is a group.

Lemma 7. *Let* $\mathcal{G} := \{(A_1, \boldsymbol{a}_1), \dots, (A_K, \boldsymbol{a}_K)\}$ *be a set of elements of* $\mathsf{SA}(2,\mathbb{Z})$. *If the semigroup* $G := \langle A_1, \dots, A_K \rangle$ *is not a group, then the semigroup* $\langle \mathcal{G} \rangle$ *is also not a group.*

Proof. If $\langle \mathcal{G} \rangle$ is a group, then $(A_i^{-1}, -A_i^{-1}\boldsymbol{a}_i) = (A_i, \boldsymbol{a}_i)^{-1} \in \langle \mathcal{G} \rangle$ for all i. Therefore, $A_i^{-1} \in \langle A_1, \dots, A_K \rangle$ for all i. Thus $\langle A_1, \dots, A_K \rangle$ is a group. $\square$

Suppose now that G is a group. The key idea of solving the Group Problem is the following dichotomy known as the *Tits alternative*.

Theorem 8 (Tits alternative [30, Theorem 1], effective version [27, Theorem 1.1]). *For any* n, *given a finitely generated subgroup* G *of* $\mathsf{SL}(n,\mathbb{Z})$, *exactly one of the following is true:*

(i) G contains a non-abelian free subgroup.

(ii) G is virtually solvable.

Furthermore, given a set of generators of G, *it is decidable in PTIME which of the two cases is true.*

In case of G containing a non-abelian free subgroup, we will prove the following Proposition 9, which shows that the semigroup $\langle \mathcal{G} \rangle$ must be a group.

Proposition 9. *Let* $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \dots, (A_K, \boldsymbol{a}_K)\}$ *be a set of elements of* $\mathsf{SA}(2,\mathbb{Z})$, *such that the semigroup* $G := \langle A_1, \dots, A_K \rangle$ *is a group. If* G *contains a non-abelian free subgroup, then* $\langle \mathcal{G} \rangle$ *is a group.*

The proof of Proposition 9 is highly non-trivial and will be given in Section IV. The proof is mainly geometric - it consists of analysing the action of $\mathsf{SA}(2,\mathbb{Z})$ on the lattice $\mathbb{Z}^2$.

In case of G being virtually solvable, we will prove the following Proposition 10 which refines the Tits alternative. In particular, it shows that virtually solvable subgroups of $\mathsf{SL}(2,\mathbb{Z})$ have relatively simple structure: it is either trivial, or it contains a torsion element, or it is infinite cyclic.

Proposition 10. *Let* $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \dots, (A_K, \boldsymbol{a}_K)\}$ *be a set of elements of* $\mathsf{SA}(2,\mathbb{Z})$, *such that the semigroup* $G := \langle A_1, \dots, A_K \rangle$ *is a group. If* G *is virtually solvable, then exactly one of the following six conditions holds:*

(i) G is the trivial group.

(ii) G contains a torsion element.

(iii) $G = \langle A \rangle_{grp}$, where A is a twisted inversion.

(iv) $G = \langle A \rangle_{grp}$, where A is a shear.

(v) $G = \langle A \rangle_{grp}$, where A is an inverting scale.

(vi) $G = \langle A \rangle_{grp}$, *where A is a positive scale.*

Furthermore, in cases (ii), (iii) and (v), the semigroup $\langle \mathcal{G} \rangle$ is a group. Overall, it is decidable in PTIME whether $\langle \mathcal{G} \rangle$ is a group.

Proposition 10 will be proved in Section V. The proof will be mainly algebraic - it consists of analysing the structure of sub-semigroups of a virtually solvable group. Lemma 7-Proposition 10 yield the decidability of the Group Problem (and consequently, the Identity Problem) in $\mathsf{SA}(2, \mathbb{Z})$. An overview of the procedure is given in Algorithm 1. The justification of each step is given in parentheses with reference to the corresponding lemmas or propositions.

Theorem 11. *The Group Problem and the Identity Problem in $\mathsf{SA}(2, \mathbb{Z})$ are NP-complete.*

Proof. The NP-hard lower bounds come from the NP-completeness of both problems in the subgroup $\mathsf{SL}(2, \mathbb{Z}) \cong \{(A, \mathbf{0}) \mid A \in \mathsf{SL}(2, \mathbb{Z})\} \leq \mathsf{SA}(2, \mathbb{Z})$ (see Theorem 6).

To show decidability and the NP upper bounds, we first solve the Group Problem. Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \dots, (A_K, \boldsymbol{a}_K)\}$ be a set in $\mathsf{SA}(2, \mathbb{Z})$. As a first step, we can check whether $\langle A_1, \dots, A_K \rangle$ is a group in NP (Theorem 6). If $\langle A_1, \dots, A_K \rangle$ is not a group, then $\langle \mathcal{G} \rangle$ is not a group by Lemma 7.

Suppose now that $\langle A_1, \dots, A_K \rangle$ is a group. As the second step, we check in PTIME whether $\langle A_1, \dots, A_K \rangle$ contains a non-abelian free subgroup using Theorem 8. If $\langle A_1, \dots, A_K \rangle$ contains a non-abelian free subgroup, then the Group Problem has a positive answer by Proposition 9. Otherwise, $\langle A_1, \dots, A_K \rangle$ is virtually solvable, and we can decide the Group Problem in PTIME using Proposition 10. In total, the Group Problem for $\mathcal{G}$ can be decided in NP.

Next we solve the Identity Problem. Note that by Lemma 2, $I \in \langle \mathcal{G} \rangle$ if and only if there exists a non-empty subset $\mathcal{H}$ of $\mathcal{G}$ such that the semigroup $\langle \mathcal{H} \rangle$ is a group. Therefore, it suffices to guess a non-empty subset $\mathcal{H}$ of $\mathcal{G}$, and check whether $\langle \mathcal{H} \rangle$ is a group. This can be done in NP using the above procedure of the Group Problem. $\square$

IV. NON ABELIAN FREE SUBGROUP

In this section we prove Proposition 9. Omitted proofs of technical results can be found in the appendix of the full version of this paper. Let A be a scale with $\mathrm{Lat}(A) = \{V, W\}$. Since V, W are distinct one dimensional subspaces of $\mathbb{R}^2$, every element $\boldsymbol{x} \in \mathbb{R}^2$ can be written uniquely as $\boldsymbol{x} = \boldsymbol{x}_V + \boldsymbol{x}_W$, where $\boldsymbol{x}_V \in V, \boldsymbol{x}_W \in W$. We will adopt this notation in the following lemma. For an element $\boldsymbol{y} \in \mathbb{R}^2$, $\boldsymbol{y}_V, \boldsymbol{y}_W$ are defined similarly.

Lemma 12. *Let $(A, \boldsymbol{a}), (B, \boldsymbol{b})$ be elements of $\mathsf{SA}(2, \mathbb{Z})$ such that $(A, \boldsymbol{a}) \cdot (B, \boldsymbol{b}) = (I, \boldsymbol{x})$ for some $\boldsymbol{x} \in \mathbb{Z}^2$. Suppose A is a scale; denote by V, W the elements of $\mathrm{Lat}(A)$, and suppose $\boldsymbol{x} \notin V \cup W$. Let $\boldsymbol{v}$ be any non-zero vector in the subspace V.*

Algorithm 1 Deciding the Group Problem for a subset of $\mathsf{SA}(2, \mathbb{Z})$.

Input: A subset $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \dots, (A_K, \boldsymbol{a}_K)\}$ of $\mathsf{SA}(2, \mathbb{Z})$.
Output: **True** or **False**.
1. Decide whether the semigroup $\langle A_1, \dots, A_K \rangle$ is a group by Theorem 6. If not a group, return **False**. (Lemma 7)
2. Let $G \coloneqq \langle A_1, \dots, A_K \rangle \leq \mathsf{SL}(2, \mathbb{Z})$, decide for G which case of Theorem 8 is true.
3. If G contains a non-abelian free subgroup, return **True**. (Proposition 9)
4. If G is virtually free, decide which case of Proposition 10 is true using Lemma 16.
   (i) If G is trivial, decide whether $n_1 \boldsymbol{a}_1 + \cdots n_K \boldsymbol{a}_K = \mathbf{0}$ has a solution over $\mathbb{Z}_{>0}^K$. If yes, return **True**, otherwise return **False**. (Proposition 17)
   (ii) If G contains a torsion element, return **True**. (Proposition 18)
   (iii) If $G = \langle A \rangle_{grp}$, where A is a twisted inversion, return **True**. (Proposition 19)
   (iv) If $G = \langle A \rangle_{grp}$, where A is a shear, compute the set $\varphi(\mathcal{G})$ defined by Equation (6). Decide whether $\langle \varphi(\mathcal{G}) \rangle$ is a group by Theorem 20. If yes, return **True**; if not, return **False**. (Corollary 21)
   (v) If $G = \langle A \rangle_{grp}$, where A is a inverting scale, return **True**. (Proposition 22)
   (vi) If $G = \langle A \rangle_{grp}$, where A is a positive scale, compute the set $\mathcal{S}$ defined by Equation (8). Decide whether the condition in Proposition 26 is satisfied for $\mathcal{S}$. If yes, return **True**; if not, return **False**. (Corollary 27)

Then for every $\varepsilon > 0$, there exists a word $w \in \{(A, \boldsymbol{a}), (B, \boldsymbol{b})\}^*$, such that $(A, \boldsymbol{a}) \cdot w \cdot (B, \boldsymbol{b}) = (I, \boldsymbol{y})$, where $\boldsymbol{y} \in \mathbb{Z}^2$ satisfies

$$1 - \frac{|\boldsymbol{v}^\top \boldsymbol{y}|}{|\boldsymbol{v}||\boldsymbol{y}|} < \varepsilon, \quad \boldsymbol{y}_V^\top \boldsymbol{x}_V > 0, \quad \boldsymbol{y}_W^\top \boldsymbol{x}_W > 0. \quad (1)$$

In other words, the angle θ between $\boldsymbol{y}$ and V satisfies $1 - \cos \theta < \varepsilon$. Also, $\boldsymbol{y}$ and $\boldsymbol{x}$ lie in same cone out of the four cut by V and W. See Figure 3 for an illustration.

The idea of proving Lemma 12 is to use the word $w = (A, \boldsymbol{a})^m (B, \boldsymbol{b})^m$ or $w = (B, \boldsymbol{b})^m (A, \boldsymbol{a})^m$ for large enough m, according to whether V is a stretching or compressing direction. A similar lemma can be proved for shears:

Lemma 13. *Let $(A, \boldsymbol{a}), (B, \boldsymbol{b})$ be elements of $\mathsf{SA}(2, \mathbb{Z})$ such that $(A, \boldsymbol{a}) \cdot (B, \boldsymbol{b}) = (I, \boldsymbol{x})$ for some $\boldsymbol{x} \in \mathbb{Z}^2$. Suppose A is a shear, $\mathrm{Lat}(A) = \{V\}$, and $\boldsymbol{x} \notin V$. Let $\boldsymbol{v}$ be any non-zero vector in the subspace V.*

Then for every $\varepsilon > 0$, there exists a word $w \in \{(A, \boldsymbol{a}), (B, \boldsymbol{b})\}^*$, such that $(A, \boldsymbol{a}) \cdot w \cdot (B, \boldsymbol{b}) = (I, \boldsymbol{y})$, where $\boldsymbol{y} \in \mathbb{Z}^2$ satisfies

$$1 - \frac{\boldsymbol{v}^\top \boldsymbol{y}}{|\boldsymbol{v}||\boldsymbol{y}|} < \varepsilon \quad (2)$$
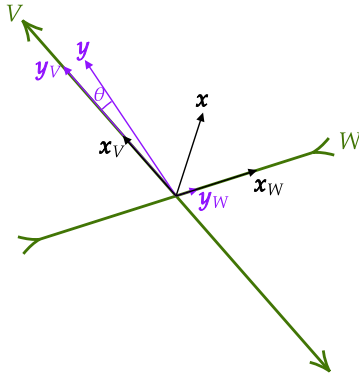
Fig. 3. Illustration for Lemma 12.
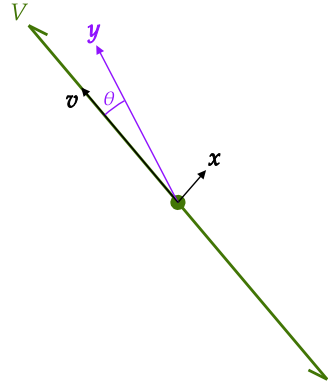
Fig. 4. Illustration for Lemma 13.

and $\boldsymbol{y}$ and $\boldsymbol{x}$ lie in same halfspace cut by V. In other words, the angle θ between $\boldsymbol{y}$ and $\boldsymbol{v}$ satisfies $1 - \cos\theta < \varepsilon$. See Figure 4 for an illustration.

We now prove Proposition 9.

Proposition 9. *Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$ be a set of elements of $\mathsf{SA}(2, \mathbb{Z})$, such that the semigroup $G := \langle A_1, \ldots, A_K \rangle$ is a group. If G contains a non-abelian free subgroup, then $\langle \mathcal{G} \rangle$ is a group.*

Proof. Suppose that the group $\langle A_1, \ldots, A_K \rangle$ contains a non-abelian free subgroup, in particular, it contains a subgroup isomorphic to the free group F_2 of two generators. Let A, B be elements of $\langle A_1, \ldots, A_K \rangle$ that generate a free group. Since A, B are non-torsion, they are twisted inversions, scales, or shears. Hence, $A^2, B^2 \in \langle A_1, \ldots, A_K \rangle$ are positive scales or shears. Since A and B generate a free group, A^2 and B^2 also generate a free group. Therefore, we can replace A, B by A^2, B^2, and without loss of generality suppose A and B to be positive scales or shears.

Since $\langle A_1, \ldots, A_K \rangle$ is a group, A and B can be represented by full-image words over the alphabet $\{A_1, \ldots, A_K\}$ due to Lemma 1. Hence, let $(A, \boldsymbol{a})$ and $(B, \boldsymbol{b})$ be elements in $\langle \mathcal{G} \rangle$ represented by full-image words.

Note that A, B are not simultaneously triangularizable, oth-

erwise the group they generate is isomorphic to a subgroup of the group of upper-triangular matrices over complex numbers, which is solvable [27]. This contradicts that fact that A, B generate a non-abelian free group (see Theorem 8). Therefore, $\mathrm{Lat}(A) \cap \mathrm{Lat}(B) = \emptyset$. There are three cases to consider:

1. Both A and B are positive scales.
2. One of A and B is a shear.
3. Both A and B are shears.

Case 1. Both A and B are positive scales. Denote $Y = A^{-1}B^{-1} \in \langle A_1, \ldots, A_K \rangle$, we have $AYB = I$. Let $\boldsymbol{y} \in \mathbb{Z}^2$ be such that $(Y, \boldsymbol{y}) \in \langle \mathcal{G} \rangle$, and let $\boldsymbol{x} \in \mathbb{Z}^2$ be such that $(A, \boldsymbol{a})(Y, \boldsymbol{y})(B, \boldsymbol{b}) = (I, \boldsymbol{x})$. If $\boldsymbol{x} = \boldsymbol{0}$, then $(I, \boldsymbol{0})$ can be represented as a full-image word over $\mathcal{G}$, since $(A, \boldsymbol{a})$ can. In this case, $\langle \mathcal{G} \rangle$ is a group by Lemma 1. Otherwise, there are two subcases. Starting from any one-dimension subspace S, rotate S counter-clockwise and consider its sequence of encounters with $\mathrm{Lat}(A)$ and $\mathrm{Lat}(B)$ before finishing a full cycle. Either the sequence of encounters is a cyclic permutation of $(\mathrm{Lat}(A), \mathrm{Lat}(A), \mathrm{Lat}(B), \mathrm{Lat}(B))$, or it is a cyclic permutation of $(\mathrm{Lat}(A), \mathrm{Lat}(B), \mathrm{Lat}(A), \mathrm{Lat}(B))$.

(i) First consider the case of $(\mathrm{Lat}(A), \mathrm{Lat}(A), \mathrm{Lat}(B), \mathrm{Lat}(B))$. An illustration for the proof of this case is shown in Figure 5. Denote by V_A, W_A, V_B, W_B be these subspaces in this order. Since $\boldsymbol{x} \neq \boldsymbol{0}$, either $\boldsymbol{x} \notin V_A \cup W_A$, or $\boldsymbol{x} \notin V_B \cup W_B$. Without loss of generality suppose $\boldsymbol{x} \notin V_B \cup W_B$.

Let c be the maximum of the cosines of angles between all pairs of subspaces in V_A, W_A, V_B, W_B. Let $0 < \varepsilon < (1 - |c|)/2$. Apply Lemma 12 to ε, to the elements $(A', \boldsymbol{a}') := (A, \boldsymbol{a})(Y, \boldsymbol{y})$ and $(B, \boldsymbol{b})$, and to the subspaces V_B, W_B of $\mathrm{Lat}(B) = \mathrm{Lat}(A')$. (Note that $A' = B^{-1}$, so $\mathrm{Lat}(A') = \mathrm{Lat}(B)$.) Since $(A', \boldsymbol{a}')(B, \boldsymbol{b}) = (A, \boldsymbol{a})(Y, \boldsymbol{y})(B, \boldsymbol{b}) = (I, \boldsymbol{x})$, Lemma 12 shows there exists an element $w \in \langle \mathcal{G} \rangle$ such that $(A', \boldsymbol{a}') \cdot w \cdot (B, \boldsymbol{b}) = (I, \boldsymbol{x}_1)$, with

$$1 - \frac{|\boldsymbol{v}_B^\top \boldsymbol{x}_1|}{|\boldsymbol{v}_B||\boldsymbol{x}_1|} < \varepsilon, \quad (\boldsymbol{x}_1)_{V_B}^\top \boldsymbol{x}_{V_B} > 0, \quad (\boldsymbol{x}_1)_{W_B}^\top \boldsymbol{x}_{W_B} > 0. \tag{3}$$

where $\boldsymbol{v}_B, \boldsymbol{w}_B$ are a non-zero vectors in V_B, W_B. In other words, when ε is sufficiently small, the angle between $\boldsymbol{x}_1$ and V_B is also sufficiently small. Also, $\boldsymbol{x}_1$ and $\boldsymbol{x}$ lie in same cone out of the four cut by V_B and W_B. This gives us an element $(Y_1, \boldsymbol{y}_1) := (Y, \boldsymbol{y}) \cdot w$ such that $(A, \boldsymbol{a})(Y_1, \boldsymbol{y}_1)(B, \boldsymbol{b}) = (I, \boldsymbol{x}_1)$ with $\boldsymbol{x}_1$ satisfying (3), see Figure 5.

Next, apply Lemma 12 to ε, to the elements $(A, \boldsymbol{a})$ and $(B', \boldsymbol{b}') := (Y_1, \boldsymbol{y}_1)(B, \boldsymbol{b})$ of $\mathsf{SA}(2, \mathbb{Z})$, and to the subspaces V_A, W_A in $\mathrm{Lat}(A)$. Same as above, we obtain an element $(Y_2, \boldsymbol{y}_2)$ such that $(A, \boldsymbol{a})(Y_2, \boldsymbol{y}_2)(B, \boldsymbol{b}) = (I, \boldsymbol{x}_2)$ with $\boldsymbol{x}_2$ satisfying

$$1 - \frac{|\boldsymbol{v}_A^\top \boldsymbol{x}_2|}{|\boldsymbol{v}_A||\boldsymbol{x}_2|} < \varepsilon, \quad (\boldsymbol{x}_1)_{V_A}^\top \boldsymbol{x}_{V_A} > 0, \quad (\boldsymbol{x}_1)_{W_A}^\top \boldsymbol{x}_{W_A} > 0. \tag{4}$$

In other words, when ε is sufficiently small, the angle between $\boldsymbol{x}_2$ and V_A is also sufficiently small. Hence, one

can take ε such that $\boldsymbol{x}_2$ and $-\boldsymbol{x}_1$ lie in the same cone out of the four cut by V_B and W_B. Furthermore, $\boldsymbol{x}_2$ and $\boldsymbol{x}_1$ lie in same cone out of the four cut by V_A and W_A. We follow this pattern and apply Lemma 12 again on $(A', \boldsymbol{a}') \coloneqq (A, \boldsymbol{a})(Y_2, \boldsymbol{y}_2)$ and $(B, \boldsymbol{b})$, and to the subspaces V_B, W_B. This yields an element $(Y_3, \boldsymbol{y}_3)$ such that $(A, \boldsymbol{a})(Y_3, \boldsymbol{y}_3)(B, \boldsymbol{b}) = (I, \boldsymbol{x}_3)$ with $\boldsymbol{x}_3$ very close to V_B, but lie in the same cone cut by V_B and W_B as $\boldsymbol{x}_2$.

Finally we apply Lemma 12 again on $(A, \boldsymbol{a})$ and $(B', \boldsymbol{b}') \coloneqq (Y_3, \boldsymbol{y}_3)(B, \boldsymbol{b})$, and to the subspaces V_A, W_A. This yields $(Y_4, \boldsymbol{y}_4)$ such that $(A, \boldsymbol{a})(Y_4, \boldsymbol{y}_4)(B, \boldsymbol{b}) = (I, \boldsymbol{x}_4)$ with $\boldsymbol{x}_4$ very close to V_A, but lie in the same cone cut by V_A and W_A as $\boldsymbol{x}_3$.

When ε is small enough, the angles of the vectors $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4$ are sufficiently close to V_B, V_A, V_B, V_A, with opposing directions. Hence, they generate $\mathbb{Q}^2$ as a $\mathbb{Q}_{\geq 0}$-cone. In other words, there exist *positive* integers n_1, n_2, n_3, n_4 such that $n_1 \boldsymbol{x}_1 + n_2 \boldsymbol{x}_2 + n_3 \boldsymbol{x}_3 + n_4 \boldsymbol{x}_4 = \boldsymbol{0}$. Therefore,

$$(I, \boldsymbol{x}_1)^{n_1}(I, \boldsymbol{x}_2)^{n_2}(I, \boldsymbol{x}_3)^{n_3}(I, \boldsymbol{x}_4)^{n_4} = (I, \boldsymbol{0}).$$

Since the element $(A, \boldsymbol{a})$ can be represented as a full-image word over $\mathcal{G}$, the elements $(I, \boldsymbol{x}_1)$ and hence $(I, \boldsymbol{0})$ can be represented by full-image words as well. Therefore, $\langle \mathcal{G} \rangle$ is a group.

(ii) Next consider the case $(\mathrm{Lat}(A), \mathrm{Lat}(B), \mathrm{Lat}(A), \mathrm{Lat}(B))$. Denote by V_A, V_B, W_A, W_B be these subspaces in this order. Without loss of generality suppose $\boldsymbol{x} \notin V_B \cup W_B$. The strategy is exactly the same as the previous case, see Figure 6. However, in the present case, we need to apply Lemma 12 for a total of six times, where V will be the subspaces $V_B, W_A, W_B, V_A, V_B, W_A$ respectively. In this way, we obtain $(I, \boldsymbol{x}_1), (I, \boldsymbol{x}_2), (I, \boldsymbol{x}_3), (I, \boldsymbol{x}_4), (I, \boldsymbol{x}_5), (I, \boldsymbol{x}_6)$ with $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_6$ generating $\mathbb{Q}^2$ as a $\mathbb{Q}_{\geq 0}$-cone. Hence, there exist positive integers $n_1, \ldots, n_6$ such that

$$(I, \boldsymbol{x}_1)^{n_1} \cdots (I, \boldsymbol{x}_6)^{n_6} = (I, \boldsymbol{0}).$$

Similarly, since the element $(A, \boldsymbol{a})$ can be represented as a full-image word over $\mathcal{G}$, $\langle \mathcal{G} \rangle$ is a group.

This concludes case 1.

Case 2. One of A and B is a shear. The approach is similar to case 1(a), but we have to apply Lemma 12 and Lemma 13 alternately. See Figure 7 for an illustration.

Without loss of generality, let A be the shear and B be the positive scale. Starting from any one-dimension subspace S, rotate S counter-clockwise and consider its sequence of encounters with $\mathrm{Lat}(A)$ and $\mathrm{Lat}(B)$ before finishing a full cycle. The sequence of encounters must a cyclic permutation of $(\mathrm{Lat}(A), \mathrm{Lat}(B), \mathrm{Lat}(B))$. Denote by V_A, V_B, W_B be these subspaces in this order. Without loss of generality suppose $\boldsymbol{x} \notin V_B \cup W_B$, the case where $\boldsymbol{x} \notin V_A$ is analogous.

For a small enough ε, apply Lemma 12 to $\boldsymbol{x}$ to obtain $\boldsymbol{x}_1$ that is sufficiently close to V_B; then apply Lemma 13 to $\boldsymbol{x}_1$ to obtain $\boldsymbol{x}_2$ that is sufficiently close to V_A; then apply Lemma 12 to $\boldsymbol{x}_2$ to obtain $\boldsymbol{x}_3$ that is sufficiently close to W_B; finally,
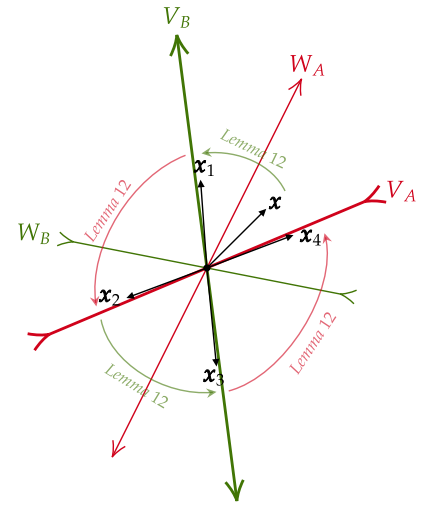
Fig. 5. Illustration for case 1(a).
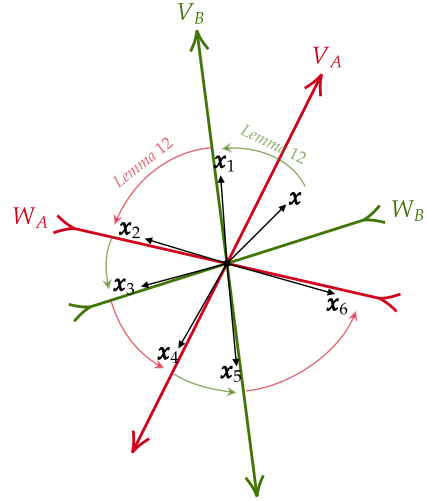
Fig. 6. Illustration for case 1(b).

apply Lemma 13 to $\boldsymbol{x}_3$ to obtain $\boldsymbol{x}_4$ that is sufficiently close to V_A. In this way, we obtain $(I, \boldsymbol{x}_1), (I, \boldsymbol{x}_2), (I, \boldsymbol{x}_3), (I, \boldsymbol{x}_4)$ with $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_4$ generating $\mathbb{Q}^2$ as a $\mathbb{Q}_{\geq 0}$-cone. Hence, there exist positive integers $n_1, \ldots, n_4$ such that

$$(I, \boldsymbol{x}_1)^{n_1} \cdots (I, \boldsymbol{x}_4)^{n_4} = (I, \boldsymbol{0}).$$

Since the element $(A, \boldsymbol{a})$ can be represented as a full-image word over $\mathcal{G}$, $\langle \mathcal{G} \rangle$ is a group.

Case 3. Both A and B are shears. The approach is similar to case 1(a), but we have to apply Lemma 13 only. See Figure 8 for an illustration.

Denote by V_A, V_B respectively the elements of $\mathrm{Lat}(A)$ and $\mathrm{Lat}(B)$. Without loss of generality suppose $\boldsymbol{x} \notin V_B$, the case where $\boldsymbol{x} \notin V_A$ is analogous. For a small enough ε, apply Lemma 13 to $\boldsymbol{x}$ to obtain $\boldsymbol{x}_1$ that is sufficiently close to V_B; then apply Lemma 13 again to $\boldsymbol{x}_1$ to obtain $\boldsymbol{x}_2$ that is sufficiently close to V_A; then apply Lemma 13 to $\boldsymbol{x}_2$ to obtain $\boldsymbol{x}_3$ that is sufficiently close to V_B; finally, apply
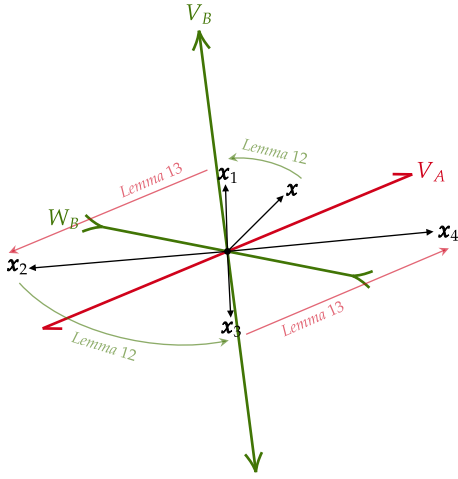
Fig. 7. Illustration for case 2.
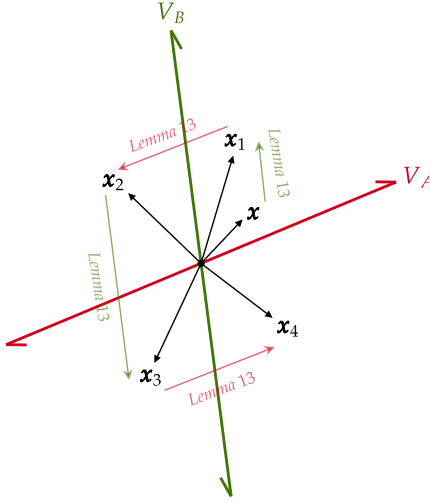
Fig. 8. Illustration for case 3.

Lemma 13 to $\boldsymbol{x}_3$ to obtain $\boldsymbol{x}_4$ that is sufficiently close to V_A. In this way, we obtain $(I, \boldsymbol{x}_1), (I, \boldsymbol{x}_2), (I, \boldsymbol{x}_3), (I, \boldsymbol{x}_4)$ with $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_4$ generating $\mathbb{Q}^2$ as a $\mathbb{Q}_{\geq 0}$-cone. Hence, there exist positive integers $n_1, \ldots, n_4$ such that

$$(I, \boldsymbol{x}_1)^{n_1} \cdots (I, \boldsymbol{x}_4)^{n_4} = (I, \boldsymbol{0}).$$

Since the element $(A, \boldsymbol{a})$ can be represented as a full-image word over $\mathcal{G}$, $\langle \mathcal{G} \rangle$ is a group. $\square$

V. Virtual solvability

In this section we prove Proposition 10. As in the statement of the proposition, we fix a set $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$ of elements in $\mathsf{SA}(2, \mathbb{Z})$, such that $G := \langle A_1, \ldots, A_K \rangle$ is a virtually solvable group.

Lemma 14. *Let G be a virtually solvable subgroup of $\mathsf{SL}(2, \mathbb{Z})$. Then G is either finite, or it contains a finite index subgroup H isomorphic to $\mathbb{Z}$.*

Proof. By Theorem 5, let $F \leq \mathsf{SL}(2, \mathbb{Z})$ be a free subgroup over two generators, such that the index $[\mathsf{SL}(2, \mathbb{Z}) : F]$ is finite. Then $[G : F \cap G] \leq [\mathsf{SL}(2, \mathbb{Z}) : F]$, so the group $H := F \cap G$ is of finite index in G. But H is a subgroup of the free group F, so it must be free by Theorem 4. Hence, H is a subgroup of the virtually solvable group G, so H is virtually solvable. Since $H \leq \mathsf{SL}(2, \mathbb{Z})$ is virtually solvable and free, it must be abelian by Theorem 8. Therefore $H \cong \mathbb{Z}$ or $H = \{I\}$, in the second case, G is finite. $\square$

Lemma 15. *Let $G \leq \mathsf{SL}(2, \mathbb{Z})$ be a group which contains a finite index subgroup H isomorphic to $\mathbb{Z}$. Then either G contains a torsion element, or it is also isomorphic to $\mathbb{Z}$.*

Proof. Suppose G torsion-free. Since G is virtually free and torsion-free, by [31, Theorem B], it is free. Hence either $G \cong \mathbb{Z}$, or G is a non-abelian free group. But a non-abelian free group is not virtually solvable (Theorem 8), so it cannot contain a finite index subgroup H isomorphic to $\mathbb{Z}$. Therefore, we must have $G \cong \mathbb{Z}$. $\square$

By Lemma 14 and 15, we can already prove the first part of Proposition 10. In particular, by Lemma 14, G is finite or contains a finite index subgroup isomorphic to $\mathbb{Z}$. If G is finite, then either it is trivial or it contains a torsion element. If G contains a finite index subgroup isomorphic to $\mathbb{Z}$, then by Lemma 15, either it contains a torsion element, or it is isomorphic to $\mathbb{Z}$. Therefore, we have proved that exactly one of the following holds.

(1) G is the trivial group.
(2) G contains a torsion element.
(3) G is isomorphic to $\mathbb{Z}$.

In case (3), the generator of G is either a twisted inversion, a shear, an inverting scale, or a positive scale. This corresponds to the cases (iii)-(vi) of Proposition 10. We have thus proved the first part of Proposition 10. The following lemma shows that one can decide which of the six cases in Proposition 10 is true.

Lemma 16. *Let $A_1, \ldots, A_K$ be matrices in $\mathsf{SL}(2, \mathbb{Z})$. The following can be done in PTIME:*

 (i) *decide whether the group $G := \langle A_1, \ldots, A_K \rangle_{grp}$ is trivial.*
 (ii) *decide whether G is isomorphic to $\mathbb{Z}$.*
(iii) *compute a generator A of G in case $G \cong \mathbb{Z}$.*

Proof. (i). G is trivial if and only if $A_i = I$ for all i.

(ii). First we check whether G is abelian, this is done simply by checking whether $A_i A_j = A_j A_i$ for all $1 \leq i, j \leq K$. If G is not abelian, then it is not isomorphic to $\mathbb{Z}$.

Suppose G is abelian. Then the group homomorphism

$$\varphi \colon \mathbb{Z}^K \longrightarrow G$$
$$(n_1, \ldots, n_K) \longmapsto A_1^{n_1} \cdots A_K^{n_K}$$

is surjective. By a classic result of Babai et al. [32], the kernel

$$\Lambda := \ker(\varphi) = \{(n_1, \ldots, n_K) \mid A_1^{n_1} \cdots A_K^{n_K} = I\}$$

is a lattice of $\mathbb{Z}^K$, and a $\mathbb{Z}$-basis of Λ is computable in PTIME.

Let $\boldsymbol{\ell}_1, \ldots, \boldsymbol{\ell}_m$ be a $\mathbb{Z}$-basis of Λ. Define

$$\overline{\Lambda} := \big\{ \boldsymbol{n} \in \mathbb{Z}^K \mid \boldsymbol{n} = q_1 \boldsymbol{\ell}_1 + \cdots + q_m \boldsymbol{\ell}_m, \\ \text{where } q_1, \ldots, q_m \in \mathbb{Q} \big\}$$

the lattice of integer points in the $\mathbb{Q}$-linear space spanned by Λ. A basis of $\overline{\Lambda}$ is effectively computable in PTIME using the *Hermite Normal Form* [33]. It is then decidable in PTIME whether $\overline{\Lambda} = \Lambda$, again using the Hermite Normal Form.

We claim that G is torsion-free if and only if $\overline{\Lambda} = \Lambda$. Indeed, let $T = A_1^{n_1} \cdots A_K^{n_K}$ be a torsion element of G, then $T^m = I$ for some $m > 1$. Therefore $A_1^{mn_1} \cdots A_K^{mn_K} = I$, so $(mn_1, \ldots, mn_K) \in \Lambda$. This shows $(n_1, \ldots, n_K) \in \overline{\Lambda}$. But $T \neq I$, so $(n_1, \ldots, n_K) \notin \Lambda$. Hence, $T = A_1^{n_1} \cdots A_K^{n_K}$ is a torsion element if and only if $(n_1, \ldots, n_K) \in \overline{\Lambda} \setminus \Lambda$.

This proves the claim. Therefore it is decidable in PTIME whether G contains a torsion element. By Lemma 15, it is decidable in PTIME whether $G \cong \mathbb{Z}$.

(iii). If G is isomorphic to $\mathbb{Z}$, then the quotient group $\mathbb{Z}^K / \Lambda \cong G \cong \mathbb{Z}$. Using Hermite Normal Form, one can in PTIME compute an element $\boldsymbol{x} = (x_1, \ldots, x_K) \in \mathbb{Z}^K$ such that $\boldsymbol{x}\mathbb{Z} + \Lambda = \mathbb{Z}^K$. Then $\boldsymbol{x} + \Lambda$ generates $\mathbb{Z}^K / \Lambda$. Therefore $A := \varphi(\boldsymbol{x}) = A_1^{x_1} \cdots A_K^{n_K}$ generates G. $\qquad \square$

Recall $G := \langle A_1, \ldots, A_K \rangle$. We now proceed to prove the PTIME decidability claim of Proposition 10 for all six cases.

G is trivial

In this case, $\mathcal{G} = \{(I, \boldsymbol{a}_1), \cdots, (I, \boldsymbol{a}_K)\}$.

Proposition 17. *Let $\mathcal{G} = \{(I, \boldsymbol{a}_1), \cdots, (I, \boldsymbol{a}_K)\}$. Then $\langle \mathcal{G} \rangle$ is a group if and only if the equation*

$$n_1 \boldsymbol{a}_1 + n_2 \boldsymbol{a}_2 + \cdots n_K \boldsymbol{a}_K = \boldsymbol{0} \tag{5}$$

has a solution $(n_1, \ldots, n_K) \in \mathbb{Z}_{>0}^K$. In particular, this is decidable in PTIME.

Proof. Note that the matrices in $\mathcal{G}$ commute. Therefore by the equivalence of (i) and (ii) in Lemma 1, $\langle \mathcal{G} \rangle$ is a group if and only if Equation (5) has a solution $(n_1, \ldots, n_K) \in \mathbb{Z}_{>0}^K$.

By the homogeneity of Equation (5), it has a solution in $\mathbb{Z}_{>0}^K$ if and only if it has a solution in $\mathbb{Q}_{>0}^K$. This is decidable in PTIME by linear programming. $\qquad \square$

G contains a torsion element

We show that $\langle \mathcal{G} \rangle$ is always a group in case G contains a torsion element.

Proposition 18. *Let $\mathcal{G} := \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$ be a set of elements of $\mathsf{SA}(2, \mathbb{Z})$. If the semigroup $\langle A_1, \ldots, A_K \rangle$ is a group containing a torsion element, then $\langle \mathcal{G} \rangle$ is a group.*

Proof. Suppose $\langle A_1, \ldots, A_K \rangle$ contains a torsion element T. Let $m > 0$ be such that $T^m = I$. Let $\boldsymbol{t} \in \mathbb{Z}^2$ be a vector such that $(T, \boldsymbol{t})$ is an element in $\langle \mathcal{G} \rangle$ represented by a full-image word (such a word exists by Lemma 1). Then

$$(T, \boldsymbol{t})^m = (T^m, (I + T + \cdots + T^{m-1})\boldsymbol{t}) \\ = (I, (I - T)^{-1}(I - T^m)\boldsymbol{t}) = (I, \boldsymbol{0}).$$

Here, $I - T$ is invertible because $T \in \mathsf{SL}(2, \mathbb{Z})$ is torsion, so the eigenvalues of T are all different from one (see the classification of element of $\mathsf{SL}(2, \mathbb{Z})$ in Section II). We conclude that $(I, \boldsymbol{0})$ can be represented by a full-image word over the alphabet $\mathcal{G}$. Hence, $\langle \mathcal{G} \rangle$ is a group by Lemma 1. $\qquad \square$

In the next four cases, G is isomorphic to $\mathbb{Z}$. Let A be a generator of G. The *Jordan Normal Form* of A can be computed in PTIME [34]. Consequently, one can decide whether A is a twisted inversion, a shear or a scale.

G is generated by a twisted inversion A

We show that if A is a twisted inversion, then $\langle \mathcal{G} \rangle$ is always a group.

Proposition 19. *If the generator A of the group $\langle A_1, \ldots, A_K \rangle$ is a twisted inversion, then $\langle \mathcal{G} \rangle$ is a group.*

Proof. Since $\langle A_1, \ldots, A_K \rangle$ is isomorphic to $\mathbb{Z}$, we have $A, A^{-1} \in \langle A_1, \ldots, A_K \rangle$. Since $\langle A_1, \ldots, A_K \rangle$ is a group, let $(A, \boldsymbol{a})$ and $(A^{-1}, \boldsymbol{b})$ be elements of $\langle \mathcal{G} \rangle$ represented by full-image words over $\mathcal{G}$.

We claim that

$$(A, \boldsymbol{a})^2 \cdot (A^{-1}, \boldsymbol{b})^3 \cdot (A, \boldsymbol{a})^2 \cdot (A^{-1}, \boldsymbol{b}) = (I, \boldsymbol{0}).$$

By direct computation, $(A, \boldsymbol{a})^2 \cdot (A^{-1}, \boldsymbol{b})^3 \cdot (A, \boldsymbol{a})^2 \cdot (A^{-1}, \boldsymbol{b}) = (I, A^{-1}(A + I)^2 \boldsymbol{a} + (A + I)^2 \boldsymbol{b})$. But since A is a twisted inversion, we have $(A + I)^2 = 0$. Therefore, $(A, \boldsymbol{a})^2 \cdot (A^{-1}, \boldsymbol{b})^3 \cdot (A, \boldsymbol{a})^2 \cdot (A^{-1}, \boldsymbol{b}) = (I, \boldsymbol{0})$. We conclude that $(I, \boldsymbol{0})$ can be represented as a full-image word over $\mathcal{G}$. Hence, $\langle \mathcal{G} \rangle$ is a group. $\qquad \square$

G is generated by a shear A

If A is a shear, the main idea in this case is that the semigroup generated by $\mathcal{G}$ can be embedded as a sub-semigroup of the *Heisenberg group*:

$$\mathrm{H}_3(\mathbb{Q}) := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Q} \right\}.$$

Since A is a shear, it is triangularizable over $\mathbb{Q}$. Since $A_1, \ldots, A_K$ all commute, they all have the same eigenvalue one, and are simultaneously triangularizable. Let P be a matrix (with entries in $\mathbb{Q}$) such that $P^{-1}A_iP$ are all of the form $\begin{pmatrix} 1 & \lambda_i \\ 0 & 1 \end{pmatrix}$ with $\lambda_i \in \mathbb{Q}$. Hence, we have the following conjugation:

$$\begin{pmatrix} P^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A_i & \boldsymbol{a}_i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix} \\ = \begin{pmatrix} P^{-1}A_iP & P^{-1}\boldsymbol{a}_i \\ 0 & 1 \end{pmatrix} \in \mathrm{H}_3(\mathbb{Q}).$$

This shows that the map

$$\varphi : \mathcal{G} \to \mathrm{H}_3(\mathbb{Q}), \quad (A_i, \boldsymbol{a}_i) \mapsto \begin{pmatrix} P^{-1}A_iP & P^{-1}\boldsymbol{a}_i \\ 0 & 1 \end{pmatrix} \tag{6}$$

extends to an injective semigroup homomorphism from $\langle \mathcal{G} \rangle$ to $H_3(\mathbb{Q})$. Therefore, $\langle \mathcal{G} \rangle$ is a group if and only if $\langle \varphi(\mathcal{G}) \rangle$ is a group. This is decidable by the following theorem.

Theorem 20 ([8]). *The Group Problem in $H_3(\mathbb{Q})$ is decidable in PTIME.*

By this result, we immediately obtain:

Corollary 21. *If the generator A of the group $\langle A_1, \ldots, A_K \rangle$ is a shear, then the Group Problem for $\langle \mathcal{G} \rangle$ is equivalent to the Group Problem for $\langle \varphi(\mathcal{G}) \rangle$, which is decidable in PTIME.*

G is generated by an inverting scale A

We show that if A is an inverting scale, then $\langle \mathcal{G} \rangle$ is a group.

Proposition 22. *If the generator A of the group $\langle A_1, \ldots, A_K \rangle$ is an inverting scale, then $\langle \mathcal{G} \rangle$ is a group.*

G is generated by a positive scale A

This is the most technical case in our paper. We show that if A is a positive scale, then we can decide whether $\langle \mathcal{G} \rangle$ is a group in PTIME. Let $P = (\boldsymbol{x}_V, \boldsymbol{x}_W) \in \mathsf{SL}(2, \mathbb{R})$ be a change of basis matrix such that $P^{-1}AP = A'$, where A' is diagonal and can be written as

$$A' = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix},$$

where $\lambda > 1$. For $i = 1, \ldots, K$, let $A_i' := P^{-1}A_iP$ and $\boldsymbol{a}_i' := P^{-1}\boldsymbol{a}_i$, with

$$A_i' = \begin{pmatrix} \lambda^{z_i} & 0 \\ 0 & \lambda^{-z_i} \end{pmatrix}, \quad \boldsymbol{a}_i' = (a_i, b_i)^\top.$$

These are the forms of A_i and $\boldsymbol{a}_i$ under the new basis $(\boldsymbol{x}_V, \boldsymbol{x}_W)$. In particular we have $A\boldsymbol{x}_V = \lambda\boldsymbol{x}_V, A\boldsymbol{x}_W = \lambda^{-1}\boldsymbol{x}_W$.

Define the sets

$$J_+ := \{i \mid z_i > 0\}, \; J_- := \{i \mid z_i < 0\}, \; J_0 := \{i \mid z_i = 0\}.$$

Then $J_+ \cup J_- \cup J_0 = \{1, \ldots, K\}$. For all i, denote

$$n_i := \begin{cases} |z_i| & z_i \neq 0 \\ 1 & z_i = 0. \end{cases}$$

Since $\langle A_1, \ldots, A_K \rangle$ is isomorphic to $\mathbb{Z}$, we have $J_+ \neq \emptyset, J_- \neq \emptyset$.

Divide the set $\mathbb{R}^2$ into nine parts:

$$\begin{aligned} \mathcal{R}_{++} &:= \{(x, y) \mid x > 0, y > 0\}, \\ \mathcal{R}_{+0} &:= \{(x, y) \mid x > 0, y = 0\}, \\ \mathcal{R}_{+-} &:= \{(x, y) \mid x > 0, y < 0\}, \\ \mathcal{R}_{0+} &:= \{(x, y) \mid x = 0, y > 0\}, \\ \mathcal{R}_{00} &:= \{(x, y) \mid x = 0, y = 0\}, \\ \mathcal{R}_{0-} &:= \{(x, y) \mid x = 0, y < 0\}, \\ \mathcal{R}_{-+} &:= \{(x, y) \mid x < 0, y > 0\}, \\ \mathcal{R}_{-0} &:= \{(x, y) \mid x < 0, y = 0\}, \\ \mathcal{R}_{--} &:= \{(x, y) \mid x < 0, y < 0\}. \end{aligned}$$
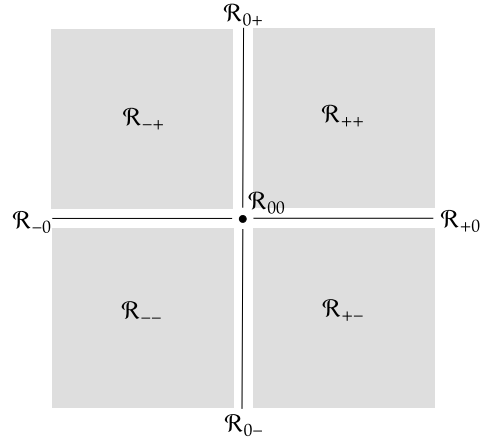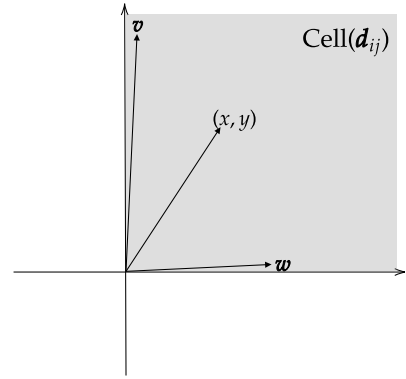

Fig. 9. Cells.

Fig. 10. Illustration for Lemma 23.

Each part is called a *cell*. See Figure 9.

For an element $\boldsymbol{x} \in \mathbb{R}^2$, denote by $\mathrm{Cell}(\boldsymbol{x})$ the cell which it belongs to. In other words, writing $\boldsymbol{x} = (x_1, x_2)^\top$, then

$$\mathrm{Cell}(\boldsymbol{x}) = \{(r_1 x_1, r_2 x_2)^\top \mid r_1, r_2 \in \mathbb{R}_{>0}\}. \quad (7)$$

In particular, $\boldsymbol{x}$ and $A'^z\boldsymbol{x}$ are in the same cell for all integers z.

For each tuple $(i, j) \in J_+ \times J_-$, define the vector

$$\boldsymbol{d}_{ij} := (d_{ija}, d_{ijb})^\top \in \mathbb{R}^2$$

where

$$d_{ija} := -\frac{a_i}{1 - \lambda^{n_i}} + \frac{a_j}{1 - \lambda^{-n_j}}, \quad d_{ijb} := \frac{b_i}{1 - \lambda^{n_i}} - \frac{b_j}{1 - \lambda^{-n_j}}.$$

For each element $k \in J_0$, define the vector

$$\boldsymbol{e}_k := (a_k, b_k)^\top \in \mathbb{R}^2.$$

Denote by $\mathcal{G}'$ the new alphabet $\{(A_1', \boldsymbol{a}_1'), \ldots, (A_K', \boldsymbol{a}_K')\}$.

Lemma 23. *Let (i, j) be a pair in $J_+ \times J_-$ and $(x, y)^\top \in \mathbb{R}^2$ be a vector in $\mathrm{Cell}(\boldsymbol{d}_{ij})$. If $\lambda > 1$, then there exist elements $(I, \boldsymbol{v})$ and $(I, \boldsymbol{w})$ in $\langle \mathcal{G}' \rangle$, where the vector $(x, y)^\top$ can be written as $r_1\boldsymbol{v} + r_2\boldsymbol{w}$ for some $r_1, r_2 \in \mathbb{R}_{>0}$. Furthermore, $(I, \boldsymbol{v})$ and $(I, \boldsymbol{w})$ are represented by words over the alphabet*

$\mathcal{G}'$, such that the letters $(A'_i, \boldsymbol{a}'_i)$ and $(A'_j, \boldsymbol{a}'_j)$ both occur. See Figure 10 for an illustration.

Proof. For any $p \in \mathbb{Z}_{>0}$, denote

$$(I, \boldsymbol{v}_p) := (A'_i, \boldsymbol{a}'_i)^{pn_j} (A'_j, \boldsymbol{a}'_j)^{pn_i},$$
$$(I, \boldsymbol{w}_p) := (A'_j, \boldsymbol{a}'_j)^{pn_i} (A'_i, \boldsymbol{a}'_i)^{pn_j}.$$

By direct computation, we have

$$\boldsymbol{v}_p = (1 - \lambda^{-pn_i n_j}) \cdot (\lambda^{pn_i n_j} d_{ija}, d_{ijb})^\top,$$
$$\boldsymbol{w}_p = (1 - \lambda^{-pn_i n_j}) \cdot (d_{ija}, \lambda^{pn_i n_j} d_{ijb})^\top.$$

Since $\lambda > 1$, we have $1 - \lambda^{-pn_i n_j} > 0$.

If $\mathrm{Cell}(\boldsymbol{d}_{ij})$ is of dimension one or zero, then either $d_{ija} = 0$ or $d_{ijb} = 0$. In both cases, $(x, y)^\top, \boldsymbol{v}_p, \boldsymbol{w}_p$ are linearly dependant and have the same direction, so $(x, y)^\top$ is in the $\mathbb{R}_{\geq 0}$-cone generated by $\boldsymbol{v}_p$ and $\boldsymbol{v}_q$.

If $\mathrm{Cell}(\boldsymbol{d}_{ij})$ is of dimension two, then $d_{ija} \neq 0$ and $d_{ijb} \neq 0$. Let p be large enough so that $\frac{\lambda^{pn_i n_j} d_{ija}}{d_{ijb}} > \frac{x}{y} > \frac{d_{ija}}{\lambda^{pn_i n_j} d_{ijb}}$. Then $(x, y)^\top$ can be written as $r_1 \boldsymbol{v}_p + r_2 \boldsymbol{w}_p$ for some $r_1, r_2 \in \mathbb{R}_{>0}$. $\qquad\square$

A similar lemma can be shown for $\mathrm{Cell}(\boldsymbol{e}_k)$.

Lemma 24. *Let (i, j) be a pair in $J_+ \times J_-$, and k be an element in J_0, and $(x, y)^\top \in \mathbb{R}^2$ be a vector in $\mathrm{Cell}(\boldsymbol{e}_k)$. If $\lambda > 1$, then there exist elements $(I, \boldsymbol{v})$ and $(I, \boldsymbol{w})$ in $\langle \mathcal{G}' \rangle$, such that the vector $(x, y)^\top$ can be written as $r_1 \boldsymbol{v} + r_2 \boldsymbol{w}$ for some $r_1, r_2 \in \mathbb{R}_{>0}$. Furthermore, $(I, \boldsymbol{v})$ and $(I, \boldsymbol{w})$ are represented as words over the alphabet $\mathcal{G}'$, such that the letter $(A'_k, \boldsymbol{a}'_k)$ occurs.*

Define the *radical* $\widehat{(A'_i, \boldsymbol{a}'_i)}$ of $(A'_i, \boldsymbol{a}'_i)$ as

$$\widehat{(A'_i, \boldsymbol{a}'_i)} := \left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \begin{pmatrix} a_i \cdot \frac{1-\lambda}{1-\lambda^{n_i}} \\ b_i \cdot \frac{1-\lambda^{-1}}{1-\lambda^{-n_i}} \end{pmatrix} \right).$$

if $z_i = n_i > 0$, and

$$\widehat{(A'_i, \boldsymbol{a}'_i)} := \left(\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} a_i \cdot \frac{1-\lambda^{-1}}{1-\lambda^{-n_i}} \\ b_i \cdot \frac{1-\lambda}{1-\lambda^{n_i}} \end{pmatrix} \right).$$

if $z_i = -n_i < 0$, and

$$\widehat{(A'_i, \boldsymbol{a}'_i)} := (A'_i, \boldsymbol{a}'_i)$$

if $z_i = 0$. By direct computation, we have $\widehat{(A'_i, \boldsymbol{a}'_i)}^{n_i} = (A'_i, \boldsymbol{a}'_i)$ in all cases.

Define the alphabet

$$\widehat{\mathcal{G}} := \{\widehat{(A'_1, \boldsymbol{a}'_1)}, \ldots, \widehat{(A'_K, \boldsymbol{a}'_K)}\}.$$

Define the following union of cells:

$$\mathcal{S} := \left(\bigcup_{i \in J_+, j \in J_-} \mathrm{Cell}(\boldsymbol{d}_{ij}) \right) \bigcup \left(\bigcup_{k \in J_0} \mathrm{Cell}(\boldsymbol{e}_k) \right). \quad (8)$$

Lemma 25. *Let $w := (C_1, \boldsymbol{c}_1) \cdots (C_M, \boldsymbol{c}_M)$ be a full-image word over the alphabet $\widehat{\mathcal{G}}$, such that $(C_1, \boldsymbol{c}_1) \cdots (C_M, \boldsymbol{c}_M) = (I, \boldsymbol{x})$. Then there exists a finite non-empty set of vectors*

$\{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_m\} \subseteq \mathcal{S}$ *such that the following conditions are satisfied:*

(i) $r_1 \boldsymbol{s}_1 + \cdots + r_m \boldsymbol{s}_m = \boldsymbol{x}$ for some strictly positive reals $r_1, \ldots, r_m$.

(ii) For each $i \in J_+$, there exist $j \in J_-$ and $\ell \leq m$, such that $\boldsymbol{s}_\ell \in \mathrm{Cell}(\boldsymbol{d}_{ij})$.

(iii) For each $j \in J_-$, there exist $i \in J_+$ and $\ell \leq m$, such that $\boldsymbol{s}_\ell \in \mathrm{Cell}(\boldsymbol{d}_{ij})$.

(iv) For each $k \in J_0$, there exist $\ell \leq m$ such that $\boldsymbol{s}_\ell \in \mathrm{Cell}(\boldsymbol{e}_k)$.

Proposition 26. *The semigroup $\langle \mathcal{G} \rangle$ is a group if and only if there exists a finite set of vectors $\{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_m\} \subseteq \mathcal{S}$ that satisfies the four conditions (i)-(iv) in Lemma 25.*

Proof. First suppose there exist a finite set of vectors $\{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_m\} \subseteq \mathcal{S}$ satisfying (i)-(iv), we want to find a full-image word w over the alphabet $\mathcal{G}$, representing $(I, \boldsymbol{0})$.

For an arbitrary t, if $\boldsymbol{s}_t$ is an element of $\mathrm{Cell}(\boldsymbol{d}_{ij})$, then by Lemma 23, there exist $(I, \boldsymbol{v}), (I, \boldsymbol{w}) \in \langle \mathcal{G}' \rangle$ such that $\boldsymbol{s}_t = r_1 \boldsymbol{v} + r_2 \boldsymbol{w}$ for some $r_1, r_2 > 0$. Also, the letters $(A'_i, \boldsymbol{a}'_i)$ and $(A'_j, \boldsymbol{a}'_j)$ appear in some words representing $(I, \boldsymbol{v})$ and $(I, \boldsymbol{w})$. If $\boldsymbol{s}_t$ is an element of $\mathrm{Cell}(\boldsymbol{e}_k)$, then by Lemma 24, there exist $(I, \boldsymbol{v}), (I, \boldsymbol{w}) \in \langle \mathcal{G}' \rangle$ such that $\boldsymbol{s}_t = r_1 \boldsymbol{v} + r_2 \boldsymbol{w}$ for some $r_1, r_2 > 0$. Also, the letter $(A'_k, \boldsymbol{a}'_k)$ appears in some words representing $(I, \boldsymbol{v})$ and $(I, \boldsymbol{w})$.

Therefore, $\boldsymbol{s}_t$ can always be written as a strictly positive linear combination of vectors $\boldsymbol{v}$ with $(I, \boldsymbol{v}) \in \langle \mathcal{G}' \rangle$. Hence, by condition (i), there exist strictly positive reals $r_1, \ldots, r_M$ such that $r_1 \boldsymbol{v}'_1 + \cdots + r_M \boldsymbol{v}'_M = \boldsymbol{0}$, where $(I, \boldsymbol{v}'_t) \in \langle \mathcal{G}' \rangle$ for all t. Furthermore, conditions (ii), (iii) and (iv) show that every letter $(A'_i, \boldsymbol{a}'_i)$ in $\mathcal{G}'$ appears at least once in a word representing $(I, \boldsymbol{v}'_t)$ for some t.

Changing back to the original basis, this shows that $r_1 \boldsymbol{v}_1 + \cdots + r_M \boldsymbol{v}_M = \boldsymbol{0}$, where $(I, \boldsymbol{v}_i) \in \langle \mathcal{G} \rangle$ for all i. Since the entries of $\boldsymbol{v}_i$ are all integers, there exist strictly positive *integers* $t_1, \ldots, t_M$, such that $t_1 \boldsymbol{v}_1 + \cdots + t_M \boldsymbol{v}_M = \boldsymbol{0}$. Hence

$$(I, \boldsymbol{v}_1)^{t_1} \cdots (I, \boldsymbol{v}_M)^{t_M} = (I, \boldsymbol{0}).$$

Every letter $(A_i, \boldsymbol{a}_i)$ in $\mathcal{G}$ appears at least once in a word representing $(I, \boldsymbol{v}_t)$ for some t. Therefore, $(I, \boldsymbol{0})$ can be represented as a full-image word. This shows that $\langle \mathcal{G} \rangle$ is a group by Lemma 1.

Next, suppose $\langle \mathcal{G} \rangle$ is a group, we show that there exists a $\mathbb{R}_{>0}$-linear combination of elements in $\mathcal{S}$ equal to $\boldsymbol{0}$, that satisfies the conditions (ii), (iii) and (iv).

By Lemma 1, there exists a full-image word $w := (B'_1, \boldsymbol{b}'_1) \cdots (B'_m, \boldsymbol{b}'_m)$ over the alphabet $\mathcal{G}'$, representing $(I, \boldsymbol{0})$. Replacing each letter $(B'_i, \boldsymbol{b}'_i)$ in w with n_i consecutive letters $\widehat{(B'_i, \boldsymbol{b}'_i)}$, we obtain a full-image word

$$\hat{w} = (C_1, \boldsymbol{c}_1) \cdots (C_M, \boldsymbol{c}_M)$$

over the alphabet $\widehat{\mathcal{G}}$, representing $(I, \boldsymbol{0})$, satisfying the conditions (ii), (iii) and (iv).

Then by Lemma 25, the vector $\boldsymbol{0}$ can be written as a $\mathbb{R}_{>0}$-linear combination of a finite number of elements in $\mathcal{S}$, satisfying the conditions (ii), (iii) and (iv). $\qquad\square$

Corollary 27. *If the generator A of the group $\langle A_1, \ldots, A_K \rangle$ is a positive scale, it is the decidable in PTIME whether $\langle \mathcal{G} \rangle$ is a group.*

Proof. Since $\langle A_1, \ldots, A_K \rangle \cong \mathbb{Z}$, we have $J_+ \neq \emptyset, J_- \neq \emptyset$. Given $\mathcal{S}$ as a set of cells, it is decidable whether there exist a finite non-empty set of vectors $\{s_1, \ldots, s_m\} \subseteq \mathcal{S}$ satisfying conditions (ii), (iii) and (iv), as well as strictly positive reals $r_1, \ldots, r_m$ such that $r_1 s_1 + \cdots + r_m s_m = \mathbf{0}$. Indeed, this is true if and only if the largest linear subspace $\mathcal{L}$ of the $\mathbb{R}_{\geq 0}$-cone $\langle \mathcal{S} \rangle_{\mathbb{R}_{\geq 0}}$ generated by $\mathcal{S}$ contains some cell $\mathrm{Cell}(d_{i*})$ for all $i \in J_+$, some cell $\mathrm{Cell}(d_{*j})$ for all $j \in J_-$, and some cell $\mathrm{Cell}(e_k)$ for all $k \in J_0$. This is decidable in linear time since the number of cells is finite.

Given the input set $\mathcal{G}$, we can compute the set of cells in $\mathcal{S}$ in PTIME. Therefore, by Proposition 26, it is decidable in PTIME whether $\langle \mathcal{G} \rangle$ is a group. $\qquad\square$

We can now prove the main result of this section.

Proposition 10. *Let $\mathcal{G} = \{(A_1, a_1), \ldots, (A_K, a_K)\}$ be a set of elements of $\mathsf{SA}(2, \mathbb{Z})$, such that the semigroup $G := \langle A_1, \ldots, A_K \rangle$ is a group. If G is virtually solvable, then exactly one of the following six conditions holds:*

(i) G is the trivial group.
(ii) G contains a torsion element.
(iii) $G = \langle A \rangle_{grp}$, where A is a twisted inversion.
(iv) $G = \langle A \rangle_{grp}$, where A is a shear.
(v) $G = \langle A \rangle_{grp}$, where A is an inverting scale.
(vi) $G = \langle A \rangle_{grp}$, where A is a positive scale.

Furthermore, in cases (ii), (iii) and (v), the semigroup $\langle \mathcal{G} \rangle$ is a group. Overall, it is decidable in PTIME whether $\langle \mathcal{G} \rangle$ is a group.

Proof. Division into six cases has already been proved by Lemma 14 and 15 as well as the discussion that follows. In cases (ii), (iii) and (v), Proposition 18, 19 and 22 show that $\langle \mathcal{G} \rangle$ is a group. We now show PTIME decidability.

First, we decide in PTIME which of the six cases is true for G, using Lemma 16. In cases (ii), (iii) and (v), the Group Problem for $\langle \mathcal{G} \rangle$ has positive answer. In cases (i), (iv) and (vi), Proposition 17, Corollary 21 and Corollary 27 show the desired PTIME decidability result. $\qquad\square$

VI. EXTENSIONS AND OBSTACLES TO SEMIGROUP MEMBERSHIP

In previous sections we showed decidability and NP-completeness of the Identity Problem and the Group Problem in $\mathsf{SA}(2, \mathbb{Z})$. In this section we discuss possible extensions of our result and obstacles to solving the Semigroup Membership problem in $\mathsf{SA}(2, \mathbb{Z})$.

Let $\mathcal{G} := \{(A_1, a_1), \ldots, (A_K, a_K)\}$ be a set of elements of $\mathsf{SA}(2, \mathbb{Z})$. This first obvious obstacle for deciding Semigroup Membership for $\langle \mathcal{G} \rangle$ is that we can no longer suppose $G := \langle A_1, \ldots, A_K \rangle$ to be a group, which we could do for the Identity Problem and the Group Problem. However, if we restrict the target element to be of the form (I, a), that is, if

we want to deciding whether $(I, a) \in \langle \mathcal{G} \rangle$, then we can still suppose G to be a group.

Indeed, if G is not a group, then at least one of the A_i is not invertible in G. Therefore, a word over $\mathcal{G}$ representing (I, a) cannot contain the letter (A_i, a_i). We can thus delete (A_i, a_i) from the alphabet $\mathcal{G}$ without changing whether $(I, a) \in \langle \mathcal{G} \rangle$. One can repeat this process until G becomes a group.

Under the additional assumption that G is a group, we can decide Semigroup Membership for $\langle \mathcal{G} \rangle$ in all except one cases. Recall Theorem 8, if G contains a non-abelian free subgroup, then $\langle \mathcal{G} \rangle$ is a group by Proposition 9. Hence Semigroup Membership reduces to Group Membership, and is decidable by the result of Delgado [13]. If G is virtually solvable, then consider the six cases in Proposition 10. Case (ii), (iii) and (v) are easy since $\langle \mathcal{G} \rangle$ becomes a group. In case (i), deciding whether $(I, a) \in \langle \mathcal{G} \rangle$ reduces to solving the linear equation $n_1 a_1 + n_2 a_2 + \cdots n_K a_K = a$ for $(n_1, \ldots, n_K) \in \mathbb{Z}_{\geq 0}^K \setminus \{\mathbf{0}\}$, and is decidable by integer programming. In case (iv), Semigroup Membership for $\langle \mathcal{G} \rangle$ reduces to Semigroup Membership in the Heisenberg group $\mathrm{H}_3(\mathbb{Q})$, which is decidable by the result of Colcombet et al. [35]. Only case (vi) remains unsolved.

We now show that solving the Semigroup Membership problem in case (vi) is equivalent to solving the Semigroup Membership problem in the group $\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}$. Given $\lambda > 1$ that satisfies a quadratic equation $\lambda^2 - a\lambda + 1 = 0$ for some $a \geq 3$, we define the following semidirect product:

$$\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z} := \left\{ \begin{pmatrix} \lambda^k & x \\ 0 & 1 \end{pmatrix} \;\middle|\; k \in \mathbb{Z}, x \in \mathbb{Z}[\lambda] \right\}.$$

Here, $\mathbb{Z}[\lambda]$ is the ring generated by 1 and λ. There exist an embedding of $\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}$ as a subgroup of $\mathsf{SA}(2, \mathbb{Z})$ in the following way. For a given λ satisfying $\lambda^2 - a\lambda + 1 = 0$, define the matrix $A_\lambda := \begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}$ in $\mathsf{SL}(2, \mathbb{Z})$. Since λ is a quadratic integer, every element $x \in \mathbb{Z}[\lambda]$ can be written uniquely as $x = x_1 + \lambda x_\lambda$ for some $x_1, x_\lambda \in \mathbb{Z}$. Define the map

$$\phi \colon \mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z} \longrightarrow \mathsf{SA}(2, \mathbb{Z})$$
$$\begin{pmatrix} \lambda^k & x \\ 0 & 1 \end{pmatrix} \longmapsto \left(A_\lambda^k, (x_1, x_\lambda)^\top \right).$$

It is easy to verify that ϕ is an injective group homomorphism. Furthermore, the image under ϕ of a sub-semigroup[5] of $\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}$ satisfies case (vi) of Proposition 10. Therefore, solving the hard case of the Semigroup Membership problem in $\mathsf{SA}(2, \mathbb{Z})$ necessitates solving the Semigroup Membership problem in $\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}$.

On the other hand, given any positive scale $A \in \mathsf{SL}(2, \mathbb{Z})$ with eigenvalue $\lambda > 1$, one can find a change of basis matrix $P \in \mathsf{SL}(2, \mathbb{Z})$ such that $P^{-1} A P = A_\lambda$ (see [36]). Therefore, any (finitely generated) semigroup $\langle \mathcal{G} \rangle$ satisfying case (vi) of

---

[5] We suppose that the upper-left entries of elements of the semigroup contain both positive and negative exponents of λ, otherwise deciding Semigroup Membership is easy.

Proposition 10 must be conjugate[6] to a (finitely generated) sub-semigroup of $\phi(\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}) \leq \mathsf{SA}(2, \mathbb{Z})$. Hence, solving Semigroup Membership in $\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}$ is sufficient for solving Semigroup Membership in the case (vi) of Proposition 10.

Although the Semigroup Membership problem in $\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}$ remains an open problem, the group bears certain similarities to the better studied *Baumslag-Solitar group* $\mathsf{BS}(1, q)$:

$$\mathsf{BS}(1, q) := \mathbb{Z}[\tfrac{1}{q}] \rtimes_q \mathbb{Z} = \left\{ \begin{pmatrix} q^k & x \\ 0 & 1 \end{pmatrix} \;\middle|\; k \in \mathbb{Z}, x \in \mathbb{Z}[\tfrac{1}{q}] \right\}.$$

Here, $q \geq 2$ is an integer. A recent result by Cadilhac, Chistikov and Zetzsche [24] showed decidability of the *rational subset membership problem* in $\mathsf{BS}(1, q)$ by considering rational languages of *base-q expansions*. This result subsumes decidability of the Semigroup Membership problem in $\mathsf{BS}(1, q)$. Therefore, it would be interesting to adapt this approach to study Semigroup Membership in $\mathbb{Z}[\lambda] \rtimes_\lambda \mathbb{Z}$ by considering rational languages of *base-λ expansions* [25], where λ is an algebraic integer. Nevertheless, adaptation of the previous result to a non-integer base of numeration poses various additional difficulties that we have not been able to surmount.

Acknowledgment

References

[1] R. Beals and L. Babai, "Las vegas algorithms for matrix groups," in *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*. IEEE, 1993, pp. 427–436.

[2] V. D. Blondel, E. Jeandel, P. Koiran, and N. Portier, "Decidable and undecidable problems about quantum automata," *SIAM Journal on Computing*, vol. 34, no. 6, pp. 1464–1473, 2005.

[3] C. Choffrut and J. Karhumäki, "Some decision problems on integer matrices," *RAIRO-Theoretical Informatics and Applications-Informatique Théorique et Applications*, vol. 39, no. 1, pp. 125–131, 2005.

[4] H. Derksen, E. Jeandel, and P. Koiran, "Quantum automata and algebraic groups," *Journal of Symbolic Computation*, vol. 39, no. 3-4, pp. 357–371, 2005.

[5] E. Hrushovski, J. Ouaknine, A. Pouly, and J. Worrell, "Polynomial invariants for affine programs," in *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, 2018, pp. 530–539.

[6] A. Markov, "On certain insoluble problems concerning matrices," *Doklady Akad. Nauk SSSR*, vol. 57, no. 6, pp. 539–542, 1947.

[7] K. A. Mikhailova, "The occurrence problem for direct products of groups," *Matematicheskii Sbornik*, vol. 112, no. 2, pp. 241–251, 1966.

[8] R. Dong, "On the Identity Problem and the Group Problem in nilpotent groups," *arXiv preprint arXiv:2208.02164*, 2022, submitted.

[9] P. C. Bell and I. Potapov, "On the undecidability of the identity correspondence problem and its applications for word and matrix semigroups," *International Journal of Foundations of Computer Science*, vol. 21, no. 06, pp. 963–978, 2010.

[10] M. Lohrey, "Subgroup membership in gl (2, z)," in *38th International Symposium on Theoretical Aspects of Computer Science (STACS 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021.

[11] P. C. Bell, M. Hirvensalo, and I. Potapov, "The identity problem for matrix semigroups in SL2(Z) is NP-complete," in *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*. SIAM, 2017, pp. 187–206.

[12] S. Ko, R. Niskanen, and I. Potapov, "On the identity problem for the special linear group and the heisenberg group," in *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018*, ser. LIPIcs, I. Chatzigiannakis, C. Kaklamanis, D. Marx, and D. Sannella, Eds., vol. 107. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018, pp. 132:1–132:15.

[13] J. Delgado Rodríguez, "Extensions of free groups: algebraic, geometric, and algorithmic aspects," Ph.D. dissertation, Universitat Politècnica de Catalunya, 2017.

[14] J. A. Wolf, "The affine group of a Lie group," in *Proc. Amer. Math. Soc.*, vol. 14, 1963, pp. 352–353.

[15] D. Mundici, "Invariant measure under the affine group over," *Combinatorics, Probability and Computing*, vol. 23, no. 2, pp. 248–268, 2014.

[16] L. M. Cabrer and D. Mundici, "Classifying orbits of the affine group over the integers," *Ergodic Theory and Dynamical Systems*, vol. 37, no. 2, pp. 440–453, 2017.

[17] A. R. Tarrida, *Affine Maps, Euclidean Motions and Quadrics*. Springer, 2011.

[18] L. A. Giefer, J. Clemens, and K. Schill, "Extended object tracking on the affine group aff (2)," in *2020 IEEE 23rd International Conference on Information Fusion (FUSION)*. IEEE, 2020, pp. 1–8.

[19] J. Kwon and F. C. Park, "Visual tracking via particle filtering on the affine group," *The International Journal of Robotics Research*, vol. 29, no. 2-3, pp. 198–217, 2010.

[20] L. F. Alday and Y. Tachikawa, "Affine SL(2) conformal blocks from 4d gauge theories," *Letters in Mathematical Physics*, vol. 94, no. 1, pp. 87–114, 2010.

[21] M. Raskin, F. Mazowiecki, C. Haase, and M. Blondin, "Affine extensions of integer vector addition systems with states," *Logical Methods in Computer Science*, vol. 17, 2021.

[22] A. Finkel, S. Göller, and C. Haase, "Reachability in register machines with polynomial updates," in *International Symposium on Mathematical Foundations of Computer Science*. Springer, 2013, pp. 409–420.

[23] S.-K. Ko, R. Niskanen, and I. Potapov, "Reachability problems in nondeterministic polynomial maps on the integers," in *International Conference on Developments in Language Theory*. Springer, 2018, pp. 465–477.

[24] M. Cadilhac, D. Chistikov, and G. Zetzsche, "Rational subsets of baumslag-solitar groups," in *47th International Colloquium on Automata, Languages, and Programming, ICALP 2020*, ser. LIPIcs, A. Czumaj, A. Dawar, and E. Merelli, Eds., vol. 168. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, pp. 116:1–116:16.

[25] F. Blanchard, "β-expansions and symbolic dynamics," *Theoretical Computer Science*, vol. 65, no. 2, pp. 131–141, 1989.

[26] C. Druțu and M. Kapovich, *Geometric group theory*. American Mathematical Soc., 2018, vol. 63.

[27] R. Beals, "Algorithms for matrix groups and the tits alternative," *Journal of computer and system sciences*, vol. 58, no. 2, pp. 260–279, 1999.

[28] J.-P. Serre, *Trees*. Springer Science & Business Media, 2002.

[29] M. Newman, "The structure of some subgroups of the modular group," *Illinois Journal of Mathematics*, vol. 6, no. 3, pp. 480–487, 1962.

[30] J. Tits, "Free subgroups in linear groups," *Journal of Algebra*, vol. 20, no. 2, pp. 250–270, 1972.

[31] R. G. Swan, "Groups of cohomological dimension one," *Journal of Algebra*, vol. 12, no. 4, pp. 585–610, 1969.

[32] L. Babai, R. Beals, J.-y. Cai, G. Ivanyos, and E. M. Luks, "Multiplicative equations over commuting matrices," in *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, 1996, pp. 498–507.

[33] M. Bremner, *Lattice basis reduction*. CRC Press New York, 2011.

[34] M. Giesbrecht, "Nearly optimal algorithms for canonical matrix forms," *SIAM Journal on Computing*, vol. 24, no. 5, pp. 948–969, 1995.

[35] T. Colcombet, J. Ouaknine, P. Semukhin, and J. Worrell, "On reachability problems for low-dimensional matrix semigroups," in *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019*, ser. LIPIcs, C. Baier, I. Chatzigiannakis, P. Flocchini, and S. Leonardi, Eds., vol. 132. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019, pp. 44:1–44:15.

[36] J. T. Campbell and E. C. Trouy, "When are two elements of GL(2,Z) similar?" *Linear Algebra and its Applications*, vol. 157, pp. 175–184, 1991.

---

[6] The conjugation is realized by the change-of-basis matrix $\mathrm{diag}(P, 1)$.