Vector and Scalar Reachability Problems in $\mathrm{SL}(2,\mathbb{Z})$[☆]

Igor Potapov[a], Pavel Semukhin[a,*]

[a] *Department of Computer Science, University of Liverpool, United Kingdom*

Abstract

This paper solves three open problems about the decidability of the vector and scalar reachability problems and the point to point reachability by fractional linear transformations over finitely generated semigroups of matrices from $\mathrm{SL}(2,\mathbb{Z})$. Our approach to solving these problems is based on the characterization of reachability paths between vectors or points, which is then used to translate the numerical problems on matrices into computational problems on words and regular languages. We will also give geometric interpretations of these results.

Keywords: Vector Reachability Problem, Scalar Reachability Problem, Matrix Semigroup, Special Linear Group, Linear Fractional Transformation, Automata and Formal Languages
2010 MSC: 68Q05, 68Q45

1. Introduction

Decision problems on matrices were intensively studied from 1947 when A. Markov showed the connection between classical computations and problems for matrix semigroups [1]. Moreover, matrix products play an essential role in the representation of various computational processes, i.e. linear recurrent sequences [2, 3, 4], arithmetic circuits [5], hybrid and dynamical systems [6, 7], probabilistic and quantum automata [8], stochastic games, broadcast protocols [9], optical systems, etc. New algorithms for solving reachability problems in matrix semigroups can be incorporated into software verification tools and used for analysis of mathematical models in physics, chemistry, biology, ecology, and economics.

However, many computational problems for matrix semigroups are inherently difficult to solve even when the problems are considered in dimension

[☆]This work was supported by EPSRC grant "Reachability problems for words, matrices and maps" (EP/M00077X/1).

[*]Corresponding author

Email addresses: potapov@liverpool.ac.uk (Igor Potapov), semukhin@liverpool.ac.uk (Pavel Semukhin)

two, and most of these problems become undecidable in general starting from dimension three or four. Examples of such problems are

- **The membership problem:** Let $S = \langle G \rangle$ be a semigroup generated by a finite set G of $n \times n$ matrices. Determine whether a given matrix M belongs to S, that is, determine whether there exists a sequence of matrices $M_1, M_2, \ldots, M_k$ in G such that $M = M_1 \cdot M_2 \cdot \ldots \cdot M_k$. If M is the zero or the identity matrix, then this problem is called the *mortality* or the *identity* problem, respectively.

- **The vector reachability problem:** Let $\mathbf{x}$ and $\mathbf{y}$ be two vectors and S be a given finitely generated semigroup of $n \times n$ matrices. Determine whether there is a matrix $M \in S$ such that $M\mathbf{x} = \mathbf{y}$.

- **The scalar reachability problem:** Let $\mathbf{x}$ and $\mathbf{y}$ be two vectors, λ be a scalar, and S be a given finitely generated semigroup of $n \times n$ matrices. Determine whether there is a matrix $M \in S$ such that $\mathbf{x}^\top M\mathbf{y} = \lambda$.

All the above problems are tightly connected with each other, including other problems such as the *emptiness* problem for matrix semigroups intersection and the *freeness* problem, i.e. to decide whether each element of $S = \langle G \rangle$ can be expressed uniquely as a product of generating matrices from G [10].

The vector reachability problem can be seen as a parameterized version of the membership problem, where some elements of a matrix M are either independent variables or variables linked by some equations. In contrast to the original membership problem, where all values of M are constants, in the vector reachability problem we may have an infinite set of matrices that transform a vector $\mathbf{x}$ to $\mathbf{y}$. Thus the decidability results for the membership cannot be directly applied to the vector reachability problem.

The scalar reachability can be viewed as a vector to hyperplane reachability problem. Indeed, we can rewrite the equation $\mathbf{x}^\top M\mathbf{y} = \lambda$ as a system of two equations: $M\mathbf{y} = \mathbf{z}$ and $\mathbf{x}^\top\mathbf{z} = \lambda$. So, the question becomes if there is a matrix $M \in S$ that maps a given vector $\mathbf{y}$ to a vector $\mathbf{z}$ that lies on a hyperplane $\mathbf{x}^\top\mathbf{z} = \lambda$. Because there are infinitely many vectors on a hyperplane, decidability of the scalar reachability problem does not follow directly from the decidability of the vector reachability problem.

Most of the problems such as membership, vector reachability and freeness are undecidable for 3×3 integer matrices. The undecidability proofs in matrix semigroups are mainly based on various techniques and methods of embedding universal computations into three and four dimensional matrices and their products. The case of dimension two is the most intriguing one since there is some evidence that if these problems are undecidable, then this cannot be proved using a construction similar to the one used for dimensions 3 and 4. In particular, there is no injective semigroup morphism from pairs of words over any finite alphabet (with at least two elements) into 2×2 matrices over $\mathbb{C}$ [11], which means that the encoding of independent pairs of words in 2×2 complex matrices is impossible, and a straightforward reduction from the Post Correspondence

Problem or a Halting Problem cannot be used to prove undecidability in 2×2 matrix semigroups over $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{C}$. The only undecidability result in dimension two for the vector reachability and the membership problems has been shown in the case of 2×2 matrices over quaternions [12].

The main hypothesis is that the reachability problems for 2×2 matrix semigroups over integer, rational or complex numbers are decidable, but not much is known about the status of these problems. There was some progress on the membership problem, which was shown to be decidable in $\mathrm{SL}(2, \mathbb{Z})$, and the identity problem, which was shown to be decidable in $\mathbb{Z}^{2\times 2}$ [13]. Later the decidability of the freeness problem was shown for $\mathrm{SL}(2, \mathbb{Z})$ [14] and for upper-triangular 2×2 matrices with rational entries when the products are restricted to certain bounded languages [15]. The mortality, identity and vector reachability problems were shown to be at least NP-hard for $\mathrm{SL}(2, \mathbb{Z})$ [16, 10], but for the finitely generated subgroups of the modular group $\mathrm{PSL}(2, \mathbb{Z})$ the membership problem was shown to be decidable in polynomial time by Gurevich and Schupp [17].

Recently, the membership problem was proven to be decidable for non-singular matrices from $\mathbb{Z}^{2\times 2}$ [18] and for matrices from $\mathbb{Z}^{2\times 2}$ with determinants 0 and ± 1 [19]. Furthermore, it was shown that the following problems in $\mathrm{SL}(2, \mathbb{Z})$ are NP-complete: identity, membership and non-freeness [20, 21].

The algorithmic properties of $\mathrm{SL}(2, \mathbb{Z})$ are important in the context of many fundamental problems in hyperbolic geometry [22, 23, 24], dynamical systems [25], Lorenz/modular knots [26], braid groups [27], particle physics, high energy physics [28], M/string theories [29], ray tracing analysis, music theory [30] and can lead to further decidability results for matrix semigroups in $\mathbb{Z}^{2\times 2}$ or $\mathbb{Q}^{2\times 2}$.

In this paper we solve three open problems about the decidability of the vector and scalar reachability problems over finitely generated semigroups of matrices from $\mathrm{SL}(2, \mathbb{Z})$ and the point to point reachability (over rational numbers) for fractional linear transformations $f_M(x) = \frac{ax+b}{cx+d}$, where the associated matrix $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ belongs to a semigroup in $\mathrm{SL}(2, \mathbb{Z})$. Our approach to solving these problems for 2×2 matrix semigroups is based on the analysis of reachability paths between vectors or points. This analysis is then used to translate the numerical problems on matrices into computational problems on words and regular languages. We also present a few extensions of our main results and give a geometric interpretation of reachability paths.

The decidability proof in dimension two presented in this paper is the first nontrivial new result concerning the vector reachability problem since 1996 when it was shown that the problem is decidable for any commutative matrix semigroup in any dimension [31] and for a special case of non-commuting matrices [32]. On the other hand, in the general case of non-commuting matrices the problem is known to be undecidable already for integer matrices in dimension three [33].

2. Preliminaries

The integers and rationals are denoted by $\mathbb{Z}$ and $\mathbb{Q}$, respectively, and $\mathrm{SL}(2,\mathbb{Z})$ is a group of 2×2 integer matrices with determinant 1. The notation $a \mid b$ means that a divides b, and $a \nmid b$ means that a does not divide b, where a and b are integer numbers. We also use the notations $\mathbf{e}_1 = \begin{bmatrix}1\\0\end{bmatrix}$, $\mathbf{e}_2 = \begin{bmatrix}0\\1\end{bmatrix}$ and $\mathbf{0} = \begin{bmatrix}0\\0\end{bmatrix}$.

Definition 1. With each matrix $M = \begin{bmatrix}a & b\\ c & d\end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ we associate a fractional linear map (also called Möbius transformation) $f_M : \mathbb{Q} \to \mathbb{Q}$ defined as

$$f_M(x) = \frac{ax+b}{cx+d}\,.$$

This definition can be extended to $f : \mathbb{Q}\cup\{\infty\} \to \mathbb{Q}\cup\{\infty\}$ in a natural way by setting $f_M(\infty) = \frac{a}{c}$ if $c \neq 0$, $f_M(\infty) = \infty$ if $c = 0$, and $f_M(x) = \infty$ if $cx+d = 0$.

Note that we have $f_{M_1} \circ f_{M_2} = f_{M_1 M_2}$ for any matrices M_1 and M_2.

Let $M_1, \ldots, M_n$ be a finite collection of matrices. Then $\langle M_1, \ldots, M_n\rangle$ denotes the multiplicative semigroup (including the identity matrix) generated by $M_1, \ldots, M_n$.

Definition 2. The *vector reachability problem (VRP)* in $\mathrm{SL}(2,\mathbb{Z})$ is defined as follows: Given two vectors $\mathbf{x}$ and $\mathbf{y}$ with integer coefficients and a finite collection of matrices $M_1, \ldots, M_n$ from $\mathrm{SL}(2,\mathbb{Z})$, decide whether there exists a matrix $M \in \langle M_1, \ldots, M_n\rangle$ such that $M\mathbf{x} = \mathbf{y}$.

Definition 3. The *reachability problem by fractional linear transformations (FLT)* in $\mathrm{SL}(2,\mathbb{Z})$ is defined as follows: Given two rational numbers x and y and a finite collection of matrices $M_1, \ldots, M_n$ from $\mathrm{SL}(2,\mathbb{Z})$, decide whether there exists a matrix $M \in \langle M_1, \ldots, M_n\rangle$ such that $f_M(x) = y$.

Definition 4. The *scalar reachability problem* in $\mathrm{SL}(2,\mathbb{Z})$ is defined as follows: Given two vectors $\mathbf{x}$, $\mathbf{z}$ with integer coefficients, an integer number λ, and a finite collection of matrices $M_1, \ldots, M_n$ from $\mathrm{SL}(2,\mathbb{Z})$, decide whether there exists a matrix $M \in \langle M_1, \ldots, M_n\rangle$ that satisfies the equation $\mathbf{z}^\top M\mathbf{x} = \lambda$.

3. Overview of the main results

The main result of this paper is that the vector and scalar reachability problems as well as the reachability problem by fractional linear transformations in $\mathrm{SL}(2,\mathbb{Z})$ are decidable (Theorem 14 and Theorem 16). Both proofs follow the same pattern. We will use the fact that any matrix M from $\mathrm{SL}(2,\mathbb{Z})$ can be expressed as product of matrices $S = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$ and $R = \begin{bmatrix}0 & -1\\ 1 & 1\end{bmatrix}$. So we can represent any $M \in \mathrm{SL}(2,\mathbb{Z})$ by a word w in the alphabet $\{S, R\}$.

The main idea of our proof is to show that the solution set of the equation $M\mathbf{x} = \mathbf{y}$ is either empty or has the form

$$\left\{ B \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^t C \ : \ t \in \mathbb{Z} \right\},$$

where B and C are some matrices from $\mathrm{SL}(2,\mathbb{Z})$ that can be computed in polynomial time from $\mathbf{x}$ and $\mathbf{y}$ (Theorem 7 and Corollary 8). Similarly, the solution set of the equation $f_M(x) = y$ can be presented as a union of two sets of this form (Theorem 9). After translating matrices into words, these sets become regular languages. On the other hand, the semigroup $\langle M_1, \ldots, M_n \rangle$ can be also described by a regular language. Indeed, if M_i is represented by a word w_i, then the semigroup $\langle M_1, \ldots, M_n \rangle$ corresponds to the language $(w_1 \cup \cdots \cup w_n)^*$.

The final step of the proof is to show that the emptiness problem of the intersection of two regular subsets in $\mathrm{SL}(2,\mathbb{Z})$ is decidable (Proposition 13). The idea of the proof relies on the fact that the intersection of two regular languages is regular, and that the emptiness problem for regular languages is decidable. The problem here is that we cannot apply these facts directly because for each matrix $M \in \mathrm{SL}(2,\mathbb{Z})$ there are infinitely many words $w \in \{S, R\}^*$ that correspond to M, and only some of them may appear in a given language. However there is only one *canonical* word that corresponds to M, that is, the word that does not have substrings of the form SS or RRR. So, our solution is to take any automaton $\mathcal{A}$ and turn it into a new automaton $\mathrm{Can}(\mathcal{A})$ that accepts only canonical words and defines the same subset of $\mathrm{SL}(2,\mathbb{Z})$ as $\mathcal{A}$.

The construction of the automaton $\mathrm{Can}(\mathcal{A})$ was inspired by the work of Choffrut and Karhumaki [13]. In a simplified form it looks like this. Note that in $\mathrm{SL}(2,\mathbb{Z})$ we have an equality $S^2 = R^3 = -I$. So, to construct $\mathrm{Can}(\mathcal{A})$ we do the following: for every pair of states q and q' that are connected by a path labelled by SS or RRR, we add a new transition from q to q' labelled by X, where X is a special symbol that represents $-I$. Furthermore, we add ϵ-transitions for every pair of states q and q' that are connected by a path labelled by XX. We apply these steps iteratively until no new transitions can be added.

Now to solve the emptiness problem for the intersection of two regular subsets of $\mathrm{SL}(2,\mathbb{Z})$ defined by regular languages L_1 and L_2, we take finite automata $\mathcal{A}_1$ and $\mathcal{A}_2$ that accept L_1 and L_2, respectively, and construct new automata $\mathrm{Can}(\mathcal{A}_1)$ and $\mathrm{Can}(\mathcal{A}_2)$ as described above. After that we check whether the languages of $\mathrm{Can}(\mathcal{A}_1)$ and $\mathrm{Can}(\mathcal{A}_2)$ have nonempty intersection.

In the end of Section 5 we will show how to extend these decidability results to arbitrary regular subsets of $\mathrm{SL}(2,\mathbb{Z})$, i.e. subsets that are defined by arbitrary finite automata. Using this technique we will show how to algorithmically solve the equation

$$M_1^{x_1} \cdots M_k^{x_k} \mathbf{x} = N_1^{y_1} \cdots N_\ell^{y_\ell} \mathbf{y},$$

where $\mathbf{x}, \mathbf{y}$ are fixed vectors from $\mathbb{Z} \times \mathbb{Z}$, the matrices $M_1, \ldots, M_k$ and $N_1, \ldots, N_\ell$ are from $\mathrm{SL}(2,\mathbb{Z})$, and $x_1, \ldots, x_k$ and $y_1, \ldots, y_\ell$ are unknown non-negative integers.

Finally, in Section 6 we will prove that the scalar reachability problem in $\mathrm{SL}(2,\mathbb{Z})$ is decidable.

We will also give geometric interpretations of reachability paths for the vector and scalar reachability problems and for the reachability problem by fractional linear transformations (Figures 1, 2 and 4).

4. Solutions of the equations $M\mathbf{x} = \mathbf{y}$ and $f_M(x) = y$ in $\mathbf{SL(2,\mathbb{Z})}$

A characterization of the matrices $M \in \mathrm{SL}(2,\mathbb{Z})$ that satisfy the equations $M\mathbf{x} = \mathbf{y}$ and $f_M(x) = y$ are given in Corollary 8 to Theorem 7 and in Theorem 9, respectively. But first we prove one simple lemma which states that the gcd of a vector's coefficients is preserved under multiplication by matrices from $\mathrm{SL}(2,\mathbb{Z})$. We will use this fact several times in our arguments.

Lemma 5. *Let* $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ *and* $\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ *be vectors from* $\mathbb{Z} \times \mathbb{Z}$ *and let* M *be a matrix from* $\mathrm{SL}(2,\mathbb{Z})$ *such that* $M\mathbf{x} = \mathbf{y}$. *Then* $\gcd(x_1, x_2) = \gcd(y_1, y_2)$.

Proof. Take any $k \in \mathbb{Z}$ such that $k \mid x_1, x_2$ and let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then from $M\mathbf{x} = \mathbf{y}$ we have $y_1 = ax_1 + bx_2$ and $y_2 = cx_1 + dx_2$. Thus $k \mid y_1, y_2$. Now since $M \in \mathrm{SL}(2,\mathbb{Z})$, M^{-1} is also in $\mathrm{SL}(2,\mathbb{Z})$, and $M\mathbf{x} = \mathbf{y}$ is equivalent to $M^{-1}\mathbf{y} = \mathbf{x}$. So, if $k \in \mathbb{Z}$ is any number such that $k \mid y_1, y_2$, then $k \mid x_1, x_2$. Therefore, $\gcd(x_1, x_2) = \gcd(y_1, y_2)$. □

Definition 6. Suppose $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ is a nonzero vector such that $\gcd(x_1, x_2) = 1$. Let u and v be integer numbers such that $x_1u + x_2v = 1$. Define the matrix $A(\mathbf{x}) = A(x_1, x_2)$ as follows $A(\mathbf{x}) = A(x_1, x_2) = \begin{bmatrix} x_1 & -v \\ x_2 & u \end{bmatrix}$. Then we have that $A(\mathbf{x}) \in \mathrm{SL}(2,\mathbb{Z})$ and $A(\mathbf{x})\mathbf{e}_1 = \mathbf{x}$.

Note that there are infinitely many pairs of u, v which satisfy the equation $x_1u + x_2v = 1$. For our proofs it does not matter which particular values of u and v are chosen in the definition of $A(\mathbf{x})$. For definiteness, we assume that u and v are the integers produced by the extended Euclidean algorithm. So the matrix $A(\mathbf{x})$ can be constructed in PTIME from $\mathbf{x}$.

Theorem 7. *Let* $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ *and* $\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ *be integer vectors such that*

$$\gcd(x_1, x_2) = \gcd(y_1, y_2) = 1.$$

Then all solutions of the equation $M\mathbf{x} = \mathbf{y}$, *where* M *belongs to* $\mathrm{SL}(2,\mathbb{Z})$, *are given by*

$$\{A(\mathbf{y})T^t A(\mathbf{x})^{-1} \ : \ t \in \mathbb{Z}\},$$

where $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z})$.

Proof. First, let us find a particular solution to the equation $M\mathbf{x} = \mathbf{y}$ which belongs to $\mathrm{SL}(2, \mathbb{Z})$. Consider the matrices $A(\mathbf{x})$ and $A(\mathbf{y})$ constructed as in Definition 6. In this case $A(\mathbf{x})\mathbf{e}_1 = \mathbf{x}$ and $A(\mathbf{y})\mathbf{e}_1 = \mathbf{y}$. So, $A(\mathbf{x})^{-1}\mathbf{x} = \mathbf{e}_1$ and hence $A(\mathbf{y})A(\mathbf{x})^{-1}\mathbf{x} = A(\mathbf{y})\mathbf{e}_1 = \mathbf{y}$.

So, $M_0 = A(\mathbf{y})A(\mathbf{x})^{-1}$ is a particular solution to $M\mathbf{x} = \mathbf{y}$. Now the equation $M\mathbf{x} = \mathbf{y}$ becomes equivalent to $(M - M_0)\mathbf{x} = \mathbf{0}$. Therefore, we need to describe all solutions of the equation $M'\mathbf{x} = \mathbf{0}$, where M' is a 2×2 integer matrix such that $\det(M' + M_0) = 1$.

Let $M' = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where a, b, c, d are integer numbers. Then the equation $M'\mathbf{x} = \mathbf{0}$ can be written as $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ or as a system

$$\begin{cases} ax_1 + bx_2 = 0 \\ cx_1 + dx_2 = 0 \end{cases}$$

Since $\gcd(x_1, x_2) = 1$, we conclude from the above equations that x_1 divides both b and d. So we can write $b = kx_1$ and $d = \ell x_1$ where k, ℓ are integers. Then it's easy to see that $a = -kx_2$ and $c = -\ell x_2$. So M' has the form

$$M' = \begin{bmatrix} -kx_2 & kx_1 \\ -\ell x_2 & \ell x_1 \end{bmatrix} = \begin{bmatrix} k \\ \ell \end{bmatrix} [-x_2,\, x_1].$$

Recall that M' must satisfy the property $\det(M' + M_0) = 1$, which will give us a restriction on k and ℓ. Suppose $M_0 = \begin{bmatrix} a_0 & b_0 \\ c_0 & d_0 \end{bmatrix}$, then

$$\det(M' + M_0) = \det \begin{bmatrix} a_0 - kx_2 & b_0 + kx_1 \\ c_0 - \ell x_2 & d_0 + \ell x_1 \end{bmatrix}$$

So, k and ℓ must satisfy the equation

$$(a_0 - kx_2)(d_0 + \ell x_1) - (b_0 + kx_1)(c_0 - \ell x_2) = 1 \quad \text{or}$$
$$a_0 d_0 + a_0 \ell x_1 - kx_2 d_0 - kx_2 \ell x_1 - b_0 c_0 + b_0 \ell x_2 - kx_1 c_0 + kx_1 \ell x_2 = 1$$

Using that $a_0 d_0 - b_0 c_0 = 1$, we obtain

$$a_0 \ell x_1 - kx_2 d_0 + b_0 \ell x_2 - kx_1 c_0 = 0 \quad \text{or}$$
$$\ell(a_0 x_1 + b_0 x_2) - k(c_0 x_1 + d_0 x_2) = 0$$

Recall that $M_0\mathbf{x} = \mathbf{y}$, that is, $\begin{bmatrix} a_0 & b_0 \\ c_0 & d_0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$. So, the above equation becomes $\ell y_1 - k y_2 = 0$, which gives us a restriction on k and ℓ. By the assumption, $\gcd(y_1, y_2) = 1$. Hence y_1 must divide k, and we can write $k = t y_1$, where t is an integer. Substituting this into $\ell y_1 - k y_2 = 0$ we obtain that $\ell = t y_2$. Therefore,

$$M' = \begin{bmatrix} k \\ \ell \end{bmatrix} [-x_2,\, x_1] = t \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} [-x_2,\, x_1].$$

Note that $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = A(\mathbf{y})\mathbf{e}_1$ and $[-x_2,\, x_1] = [0,\, 1]\begin{bmatrix} u & v \\ -x_2 & x_1 \end{bmatrix} = \mathbf{e}_2^\top A(\mathbf{x})^{-1}$, where u, v are integers used in the definition of $A(\mathbf{x})$.[1]

Therefore, $M' = tA(\mathbf{y})\mathbf{e}_1\mathbf{e}_2^\top A(\mathbf{x})^{-1}$. So, the general solution to $M\mathbf{x} = \mathbf{y}$ in $\mathrm{SL}(2,\mathbb{Z})$ has the form

$$\begin{aligned} M = M_0 + M' &= A(\mathbf{y})A(\mathbf{x})^{-1} + tA(\mathbf{y})\mathbf{e}_1\mathbf{e}_2^\top A(\mathbf{x})^{-1} \\ &= A(\mathbf{y})(I + t\mathbf{e}_1\mathbf{e}_2^\top)A(\mathbf{x})^{-1} \end{aligned}$$

Using that $\mathbf{e}_1\mathbf{e}_2^\top = \begin{bmatrix} 1 \\ 0 \end{bmatrix}[0,\, 1] = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, we obtain

$$\begin{aligned} M = A(\mathbf{y})(I + t\mathbf{e}_1\mathbf{e}_2^\top)A(\mathbf{x})^{-1} &= A(\mathbf{y})\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + t\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\right)A(\mathbf{x})^{-1} \\ = A(\mathbf{y})\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}A(\mathbf{x})^{-1} &= A(\mathbf{y})T^tA(\mathbf{x})^{-1} \end{aligned}$$

So, all solutions to the equation $M\mathbf{x} = \mathbf{y}$ in $\mathrm{SL}(2,\mathbb{Z})$ are given by

$$\{A(\mathbf{y})T^tA(\mathbf{x})^{-1} \;:\; t \in \mathbb{Z}\}.$$

□

Corollary 8. *Let* $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ *and* $\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ *be two nonzero integer vectors.*

(1) *If* $\gcd(x_1, x_2) \neq \gcd(y_1, y_2)$*, then* $M\mathbf{x} = \mathbf{y}$ *has no solution in* $\mathrm{SL}(2,\mathbb{Z})$.

(2) *If* $\gcd(x_1, x_2) = \gcd(y_1, y_2) = d$*, then all solutions to* $M\mathbf{x} = \mathbf{y}$ *in* $\mathrm{SL}(2,\mathbb{Z})$ *are exactly*

$$\{A(\tfrac{1}{d}\mathbf{y})T^tA(\tfrac{1}{d}\mathbf{x})^{-1} \;:\; t \in \mathbb{Z}\}.$$

Proof. The first item is a direct corollary from Lemma 5. To prove the second item, suppose $\gcd(x_1, x_2) = \gcd(y_1, y_2) = d$ and let $\mathbf{x}' = \frac{1}{d}\mathbf{x}$ and $\mathbf{y}' = \frac{1}{d}\mathbf{y}$. Obviously, the equation $M\mathbf{x} = \mathbf{y}$ is equivalent to $M\mathbf{x}' = \mathbf{y}'$. Note that $\gcd(x_1', x_2') = \gcd(y_1', y_2') = 1$. Hence by Theorem 7 all solutions to the equation $M\mathbf{x}' = \mathbf{y}'$ are $\{A(\mathbf{y}')T^tA(\mathbf{x}')^{-1} \;:\; t \in \mathbb{Z}\}$. □

In the case when $\gcd(x_1, x_2) = \gcd(y_1, y_2) = d$, the solutions

$$\{A(\tfrac{1}{d}\mathbf{y})T^tA(\tfrac{1}{d}\mathbf{x})^{-1} \;:\; t \in \mathbb{Z}\}.$$

have the following geometric interpretation: first, we apply $A(\frac{1}{d}\mathbf{x})^{-1}$ to $\mathbf{x}$ and arrive at $\begin{bmatrix} d \\ 0 \end{bmatrix}$, then we loop at $\begin{bmatrix} d \\ 0 \end{bmatrix}$ for t many times using T, and finally apply

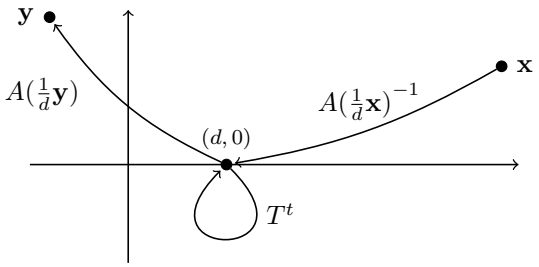

Figure 1: Geometric interpretation of the transformation $\mathbf{y} = A(\frac{1}{d}\mathbf{y})T^tA(\frac{1}{d}\mathbf{x})^{-1}(\mathbf{x})$.

$A(\frac{1}{d}\mathbf{y})$ to move from $\begin{bmatrix} d \\ 0 \end{bmatrix}$ to $\mathbf{y}$. Figure 1 gives an illustration of these transformations.

Theorem 7 and Corollary 8 provide us with a characterization of the matrices $M \in \mathrm{SL}(2, \mathbb{Z})$ that map vector $\mathbf{x}$ to vector $\mathbf{y}$. This characterization will be used later to prove the decidability of the vector reachability problem. We now give a similar characterization of the matrices $M \in \mathrm{SL}(2, \mathbb{Z})$ for which the fractional linear transformation f_M maps a number x to number y. In fact, we will do this by reducing this problem to the problem of finding all solutions of the equation $M\mathbf{x} = \mathbf{y}$ which we discussed above.

Theorem 9. *Let $x = \frac{x_1}{x_2}$ and $y = \frac{y_1}{y_2}$ be rational numbers, where x_1, x_2, y_1, y_2 are integers such that $\gcd(x_1, x_2) = \gcd(y_1, y_2) = 1$. Also let $\mathcal{F}(x, y)$ be the following set of matrices from $\mathrm{SL}(2, \mathbb{Z})$:*

$$\mathcal{F}(x, y) = \{M \in \mathrm{SL}(2, \mathbb{Z}) \ : \ f_M(x) = y\}.$$

Then $\mathcal{F}(x, y) = \{\pm A(y_1, y_2)T^tA(x_1, x_2)^{-1} \ : \ t \in \mathbb{Z}\}$.

Proof. Consider the equation $f_M(x) = y$, where $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is an unknown matrix from $\mathrm{SL}(2, \mathbb{Z})$. We can rewrite it as

$$\frac{a\frac{x_1}{x_2} + b}{c\frac{x_1}{x_2} + d} = \frac{y_1}{y_2} \quad \text{or} \quad \frac{ax_1 + bx_2}{cx_1 + dx_2} = \frac{y_1}{y_2}\,. \tag{1}$$

Consider the vectors $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, $\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$, and $\mathbf{z} = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$, where $\mathbf{z}$ is the vector with coordinates $z_1 = ax_1 + bx_2$ and $z_2 = cx_1 + dx_2$. So we have that $\mathbf{z} = M\mathbf{x}$. In this notation Equation (1) is equivalent to the fact that vector $\mathbf{z} = M\mathbf{x}$ belongs to the set $\{k\mathbf{y} : k \in \mathbb{Z}\}$.

Recall that $\gcd(x_1, x_2) = 1$ and hence, by Lemma 5, $\gcd(z_1, z_2) = 1$. Thus if $\mathbf{z} = k\mathbf{y}$ for some $k \in \mathbb{Z}$, then $k = \pm 1$. In other words, we showed that

[1] Here one can see why a particular choice of u and v is not important.

Equation (1) is equivalent to two matrix equations: $M\mathbf{x} = \mathbf{y}$ or $M\mathbf{x} = -\mathbf{y}$. Therefore,

$$\mathcal{F}(x, y) = \{M \in \mathrm{SL}(2, \mathbb{Z}) \ : \ M\mathbf{x} = \mathbf{y}\} \cup \{M \in \mathrm{SL}(2, \mathbb{Z}) \ : \ M\mathbf{x} = -\mathbf{y}\}.$$

Since $\gcd(x_1, x_2) = \gcd(y_1, y_2) = 1$, by Theorem 7 we have that

$$\mathcal{F}(x, y) = \{A(\mathbf{y})T^t A(\mathbf{x})^{-1} \ : \ t \in \mathbb{Z}\} \cup \{A(-\mathbf{y})T^t A(\mathbf{x})^{-1} \ : \ t \in \mathbb{Z}\}.$$

To finish the proof, we note that $A(-\mathbf{y}) = -A(\mathbf{y})$. □

The transformation $y = f_M(x)$, where $M = A(y_1, y_2)T^t A(x_1, x_2)^{-1}$, has the following geometric interpretation: first it maps x to ∞ using $f_{A(x_1,x_2)^{-1}}$, then it loops at ∞ for t many times using f_T, and finally maps ∞ to y using $f_{A(y_1,y_2)}$. Figure 2 gives an illustration of these transformations.

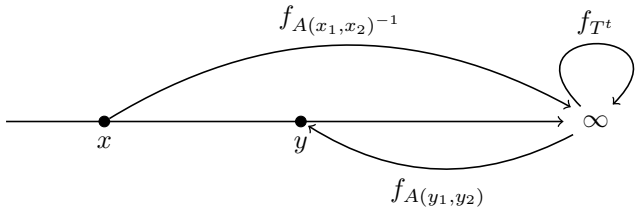

Figure 2: Geometric interpretation of the transformation $y = f_{A(y_1,y_2)T^t A(x_1,x_2)^{-1}}(x)$.

5. Decidability of VRP and FLT

We now prove that the intersection emptiness problem of two regular subsets in $\mathrm{SL}(2, \mathbb{Z})$ is decidable (Proposition 13). Then in the proof of Theorem 14 we will show that the solution sets of the equations $M\mathbf{x} = \mathbf{y}$ and $f_M(x) = y$ are regular subsets of $\mathrm{SL}(2, \mathbb{Z})$. Using these results and the fact that the semigroups in $\mathrm{SL}(2, \mathbb{Z})$ are also regular subsets, we will conclude that the vector reachability problem and the reachability problem by fractional linear transformations in $\mathrm{SL}(2, \mathbb{Z})$ are decidable.

Consider an alphabet $\Sigma = \{S, R, X\}$ consisting of three symbols S, R and X and define the mapping $\varphi : \Sigma \to \mathrm{SL}(2, \mathbb{Z})$ as follows:

$$\varphi(S) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \ \varphi(R) = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \text{ and } \varphi(X) = -I = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

We can extend this mapping to the morphism $\varphi : \Sigma^* \to \mathrm{SL}(2, \mathbb{Z})$ in a natural way. The matrices $\varphi(S)$ and $\varphi(R)$ are in fact generators of $\mathrm{SL}(2, \mathbb{Z})$, so φ is surjective.

Definition 10. A word $w \in \Sigma^*$ is called *reduced* if it does not have substrings of the form SS or RRR. We say that w is *canonical* if it is reduced and either w does not contain X or X appears only once as the first letter in w.

In our proof we will make use of the following well-known fact.

Theorem 11 ([34, 35, 36])**.** *For every $M \in \mathrm{SL}(2,\mathbb{Z})$, there exists a unique reduced word $w \in \{S,R\}^*$ such that either $M = \varphi(w)$ or $M = -\varphi(w)$.*

Therefore, for every $M \in \mathrm{SL}(2,\mathbb{Z})$, there exists a unique canonical word $w \in \Sigma^*$ such that $M = \varphi(w)$.

Definition 12. (1) We call two words w_1 and w_2 from Σ^* *equivalent*, denoted $w_1 \sim w_2$, if $\varphi(w_1) = \varphi(w_2)$.

(2) Two languages $L_1, L_2 \subseteq \Sigma^*$ are called *equivalent*, denoted $L_1 \sim L_2$, if for any $w_1 \in L_1$, there is $w_2 \in L_2$ such that $w_1 \sim w_2$, and vice versa if for any $w_2 \in L_2$, there is $w_1 \in L_1$ such that $w_2 \sim w_1$. In other words, $L_1 \sim L_2$ if and only if $\varphi(L_1) = \varphi(L_2)$, i.e. they define equal subsets of $\mathrm{SL}(2,\mathbb{Z})$.

(3) Two finite automata $\mathcal{A}_1$ and $\mathcal{A}_2$ over alphabet Σ are called *equivalent*, denoted $\mathcal{A}_1 \sim \mathcal{A}_2$, if $L(\mathcal{A}_1) \sim L(\mathcal{A}_2)$.

Note that by Theorem 11 for every $w \in \Sigma^*$ there exists a unique canonical word w' such that $w' \sim w$.

Let $\mathcal{A}$ be a finite automaton over alphabet Σ. We now show how to construct a new automaton $\mathrm{Can}(\mathcal{A})$ equivalent to $\mathcal{A}$ that accepts only canonical words. This construction was inspired by the work of Choffrut and Karhumaki [13]. It also appeared in our other paper [18] in a more general form. We will use it later in Proposition 13 to prove that the emptiness problem for the intersection of two regular subsets in $\mathrm{SL}(2,\mathbb{Z})$ is decidable.

First, we apply the following procedure to $\mathcal{A}$:

(1) For any pair of states q, q' in $\mathcal{A}$, if there is a path from q to q' labelled by XX, we add an ϵ-transition $q \xrightarrow{\epsilon} q'$.

(2) For any pair of states q, q' in $\mathcal{A}$, if there is a path from q to q' labelled by[2] $SX^{\alpha}S$, where $\alpha \in \{0,1\}$, we add a new transition $q \xrightarrow{X^{\beta}} q'$, where $\beta = 1 - \alpha$.

(3) For any pair of states q, q' in $\mathcal{A}$, if there is a path from q to q' labelled by $RX^{\alpha_1}RX^{\alpha_2}R$, where $\alpha_1, \alpha_2 \in \{0,1\}$, we add a new transition $q \xrightarrow{X^{\gamma}} q'$, where $\gamma \in \{0,1\}$ is such that $\gamma \equiv \alpha_1 + \alpha_2 + 1 \pmod 2$.

We repeat the above steps iteratively until no new transitions can be added. Obviously, this procedure eventually terminates because we do not add new states to $\mathcal{A}$. Let $\mathcal{A}_1$ be the resulting automaton. It is not hard to see that $\mathcal{A}_1 \sim \mathcal{A}$ because $XX \sim \epsilon$, $SX^{\alpha}S \sim X^{1-\alpha}$ and $RX^{\alpha_1}RX^{\alpha_2}R \sim X^{\gamma}$, where $\gamma \in \{0,1\}$ and $\gamma \equiv \alpha_1 + \alpha_2 + 1 \pmod 2$.

Figure 3 gives an illustration of this construction. At the first iteration we add transitions $q_0 \xrightarrow{X} q_3$ and $q_3 \xrightarrow{X} q_5$. Then at the second iteration we add an ϵ-transition $q_0 \xrightarrow{\epsilon} q_5$. At the next iteration no new transitions can be added, so the procedure terminates.

[2] In our notation X^0 denotes the empty word.

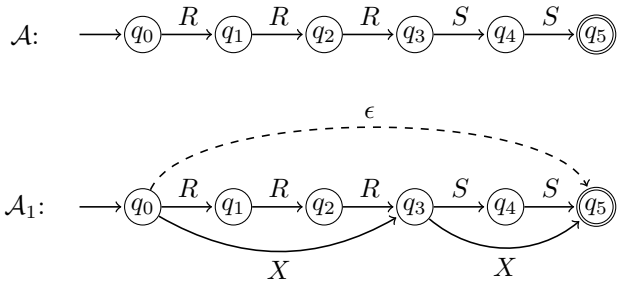

Figure 3: An example of an automaton $\mathcal{A}_1$ (below) constructed from an automaton $\mathcal{A}$ (above).

By construction, for every $w \in L(\mathcal{A})$ there is $w_1 \in L(\mathcal{A}_1)$ such that $w_1 \sim w$ and w_1 does not contain subwords $SX^\alpha S$ or $RX^{\alpha_1}RX^{\alpha_2}R$ for $\alpha, \alpha_1, \alpha_2 \in \{0, 1\}$. That is, w_1 is almost in canonical form except that letter X may appear in the middle of w_1.

To get rid of these extra X's we do the following: for every transition $q \xrightarrow{S} q'$ which appears in $\mathcal{A}_1$, we add new states p_1, p_2 and a new path of the form

$$q \xrightarrow{X} p_1 \xrightarrow{S} p_2 \xrightarrow{X} q'.$$

Similarly, for every transition $q \xrightarrow{R} q'$ which appears in $\mathcal{A}_1$, we add new states p_1, p_2 and a new path of the form

$$q \xrightarrow{X} p_1 \xrightarrow{R} p_2 \xrightarrow{X} q'.$$

Let $\mathcal{A}_2$ be the resulting automaton. Note that since $S \sim XSX$ and $R \sim XRX$, A_2 is equivalent to $\mathcal{A}_1$.

Finally, for any pair of states q, q' in $\mathcal{A}_2$, if there is a path from q to q' labelled by XX, we add an ϵ-transition $q \xrightarrow{\epsilon} q'$. Again, we apply this procedure iteratively until no new ϵ-transitions can be added. Let $\mathcal{A}_3$ be the resulting automaton. By construction, we have $\mathcal{A}_3 \sim \mathcal{A}_2 \sim \mathcal{A}_1 \sim \mathcal{A}$.

The automaton $\mathcal{A}_3$ also has the property that for every $w \in L(\mathcal{A})$ there is a canonical word $w_3 \in L(\mathcal{A}_3)$ such that $w_3 \sim w$. Indeed, by the above observation, there is $w_1 \in L(\mathcal{A}_1)$ such that $w_1 \sim w$ and w_1 does not contain subwords $SX^\alpha S$ and $RX^{\alpha_1}RX^{\alpha_2}R$ for $\alpha, \alpha_1, \alpha_2 \in \{0, 1\}$. Suppose w_1 has the form

$$w_1 = u_1 X u_2 X \dots X u_{n-1} X u_n,$$

where $u_i \in \{S, R\}^*$ for $i = 1, \dots, n$. Consider a word w_2 which is obtained from w_1 as follows. If the number of X's in w_1 is even, then in each u_i with even i we replace S and R with XSX and XRX, respectively, and leave u_i with odd i unchanged. Similarly, if the number of X's in w_1 is odd, then in each u_i with odd i we replace S and R with XSX and XRX, respectively, and leave u_i with even i unchanged. By construction, $w_2 \sim w_1$ and $w_2 \in L(\mathcal{A}_2)$. Let w_3 be the word which is obtained from w_2 after removing all appearances of XX. Then

$w_3 \in L(\mathcal{A}_3)$, $w_3 \sim w_2 \sim w_1 \sim w$ and w_3 is a canonical word. This idea is illustrated by the following example. Suppose

$$w_1 = SRXSXRRX.$$

Since the number of X's in w_1 is odd, the word $w_2 \sim w_1$ has the form

$$\begin{aligned} w_2 &= (XSX)(XRX)XSX(XRX)(XRX)X \\ &= XS(XX)R(XX)S(XX)R(XX)R(XX). \end{aligned}$$

The parentheses in the above expression are inserted only to visually separate relevant subwords. After removing all occurrences of XX from w_2 we obtain

$$w_3 = XSRSRR \sim w_2,$$

which is a canonical word.

Let $\mathrm{Can}(\mathcal{A})$ be an automaton that recognizes the intersection $L(\mathcal{A}_3) \cap \mathcal{L}_{\mathrm{Can}}$, where $\mathcal{L}_{\mathrm{Can}}$ is a regular language consisting of all canonical words. By definition $\mathrm{Can}(\mathcal{A})$ accepts only canonical words. We need to show that $\mathrm{Can}(\mathcal{A}) \sim \mathcal{A}$. By the above argument, for every $w \in L(\mathcal{A})$, there is $w_3 \in L(\mathcal{A}_3)$ such that $w_3 \sim w$ and $w_3 \in \mathcal{L}_{\mathrm{Can}}$. Hence $w_3 \in L(\mathrm{Can}(\mathcal{A}))$. So, $\varphi(L(\mathcal{A})) \subseteq \varphi(L(\mathrm{Can}(\mathcal{A})))$. On the other hand,

$$\varphi(L(\mathrm{Can}(\mathcal{A}))) = \varphi(L(\mathcal{A}_3) \cap \mathcal{L}_{\mathrm{Can}}) \subseteq \varphi(L(\mathcal{A}_3)) = \varphi(L(\mathcal{A})).$$

Therefore, $\varphi(L(\mathrm{Can}(\mathcal{A}))) = \varphi(L(\mathcal{A}))$ and hence $\mathrm{Can}(\mathcal{A}) \sim \mathcal{A}$.

Proposition 13. *There is an algorithm that for any two regular languages L_1 and L_2 over the alphabet Σ, decides whether $\varphi(L_1) \cap \varphi(L_2)$ is empty or not.*

Proof. Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be finite automata that recognize the languages L_1 and L_2, respectively. Consider the automata $\mathrm{Can}(\mathcal{A}_1)$ and $\mathrm{Can}(\mathcal{A}_2)$. We have

$$\varphi(L_i) = \varphi(L(\mathcal{A}_i)) = \varphi(L(\mathrm{Can}(\mathcal{A}_i))) \quad \text{for } i = 1, 2.$$

We show that $\varphi(L_1) \cap \varphi(L_2) \neq \emptyset$ if and only if $L(\mathrm{Can}(\mathcal{A}_1)) \cap L(\mathrm{Can}(\mathcal{A}_2)) \neq \emptyset$. The statement of the proposition then follows from the fact that the emptiness problem for regular languages is decidable.

Suppose there is $w \in L(\mathrm{Can}(\mathcal{A}_1)) \cap L(\mathrm{Can}(\mathcal{A}_2))$. Then

$$\varphi(w) \in \varphi(L(\mathrm{Can}(\mathcal{A}_1))) \cap \varphi(L(\mathrm{Can}(\mathcal{A}_2))) = \varphi(L_1) \cap \varphi(L_2).$$

Hence $\varphi(L_1) \cap \varphi(L_2)$ is not empty.

Now assume there is $M \in \varphi(L_1) \cap \varphi(L_2) = \varphi(L(\mathrm{Can}(\mathcal{A}_1))) \cap \varphi(L(\mathrm{Can}(\mathcal{A}_2)))$. Hence there are words w_1, w_2 such that $M = \varphi(w_i)$ and $w_i \in L(\mathrm{Can}(\mathcal{A}_i))$ for $i = 1, 2$. Since $\mathrm{Can}(\mathcal{A}_1)$ and $\mathrm{Can}(\mathcal{A}_2)$ accept only canonical words, w_1 and w_2 must be canonical. By Theorem 11, there is only one canonical word w such that $M = \varphi(w)$. Hence $w_1 = w_2 \in L(\mathrm{Can}(\mathcal{A}_1)) \cap L(\mathrm{Can}(\mathcal{A}_2))$. □

We are ready to prove our main results.

Theorem 14. *The vector reachability problem (VRP) and the reachability problem by fractional linear transformations (FLT) in* $\mathrm{SL}(2,\mathbb{Z})$ *are decidable.*

Proof. Suppose $M_1, \ldots, M_n$ is a given finite collection of matrices from $\mathrm{SL}(2,\mathbb{Z})$. Let $w_1, \ldots, w_n \in \Sigma^*$ be canonical words such that $M_i = \varphi(w_i)$ for $i = 1, \ldots, n$. Let $\mathcal{L}_{semigr} = \{w_1 \cup \cdots \cup w_n\}^*$. It is not hard to see that $\mathcal{L}_{semigr}$ describes the semigroup $\langle M_1, \ldots, M_n \rangle$ in the sense that $\varphi(\mathcal{L}_{semigr}) = \langle M_1, \ldots, M_n \rangle$.

Recall that in the vector reachability problem we are given two integer vectors $\mathbf{x}$ and $\mathbf{y}$, and we ask if there is a matrix $M \in \langle M_1, \ldots, M_n \rangle$ such that $M\mathbf{x} = \mathbf{y}$. We want to construct a regular language $\mathcal{L}^{\mathrm{vrp}}_{\mathbf{x},\mathbf{y}}$ that describes the solution set of the equation $M\mathbf{x} = \mathbf{y}$ in $\mathrm{SL}(2,\mathbb{Z})$.

If $\mathbf{x} = \mathbf{0}$ and $\mathbf{y} \neq \mathbf{0}$ or if $\mathbf{x} \neq \mathbf{0}$ and $\mathbf{y} = \mathbf{0}$, then $\mathcal{L}^{\mathrm{vrp}}_{\mathbf{x},\mathbf{y}} = \emptyset$ because in these cases the equation $M\mathbf{x} = \mathbf{y}$ does not have a solution in $\mathrm{SL}(2,\mathbb{Z})$. On the other hand, if $\mathbf{x} = \mathbf{y} = \mathbf{0}$, then $\mathcal{L}^{\mathrm{vrp}}_{\mathbf{x},\mathbf{y}} = \Sigma^*$ because in this case any matrix $M \in \mathrm{SL}(2,\mathbb{Z})$ satisfies the equation $M\mathbf{0} = \mathbf{0}$.

Now suppose that both $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ and $\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ are nonzero integer vectors. If $\gcd(x_1, x_2) \neq \gcd(y_1, y_2)$, then my Lemma 5 the equation $M\mathbf{x} = \mathbf{y}$ has no solution in $\mathrm{SL}(2,\mathbb{Z})$ and hence we define $\mathcal{L}^{\mathrm{vrp}}_{\mathbf{x},\mathbf{y}} = \emptyset$.

Suppose that $d = \gcd(x_1, x_2) = \gcd(y_1, y_2)$. Then by Corollary 8 all solutions to $M\mathbf{x} = \mathbf{y}$ in $\mathrm{SL}(2,\mathbb{Z})$ are exactly $\{A(\frac{1}{d}\mathbf{y})T^t A(\frac{1}{d}\mathbf{x})^{-1} \ : \ t \in \mathbb{Z}\}$. We can rewrite it as a union

$$\{A(\tfrac{1}{d}\mathbf{y})T^t A(\tfrac{1}{d}\mathbf{x})^{-1} \ : \ t \geq 0\} \bigcup \{A(\tfrac{1}{d}\mathbf{y})(T^{-1})^t A(\tfrac{1}{d}\mathbf{x})^{-1} \ : \ t \geq 0\}.$$

Let u, v be canonical words such that $\varphi(u) = A(\frac{1}{d}\mathbf{y})$ and $\varphi(v) = A(\frac{1}{d}\mathbf{x})^{-1}$. It is easy to check that $T = \varphi(XSR)$ and $T^{-1} = \varphi(XRRS)$. Hence

$$\mathcal{L}^{\mathrm{vrp}}_{\mathbf{x},\mathbf{y}} = u\{XSR\}^* v \cup u\{XRRS\}^* v$$

is a regular language that describes all solutions to $M\mathbf{x} = \mathbf{y}$ in $\mathrm{SL}(2,\mathbb{Z})$.

Similarly, we can construct a regular language $\mathcal{L}^{\mathrm{flt}}_{x,y}$ that corresponds to the reachability problem by fractional linear transformations from $x = \frac{x_1}{x_2}$ to $y = \frac{y_1}{y_2}$. By Theorem 9, the set $\mathcal{F}(x,y)$ of matrices from $\mathrm{SL}(2,\mathbb{Z})$ that satisfy the equation $f_M(x) = y$ is equal to $\mathcal{F}(x,y) = \{\pm A(y_1,y_2)T^t A(x_1,x_2)^{-1} \ : \ t \in \mathbb{Z}\}$.

Let u and v be canonical words such that $\varphi(u) = A(y_1,y_2)$ and $\varphi(v) = A(x_1,x_2)^{-1}$. Then $\mathcal{F}(x,y)$ can be described by the following regular language

$$\mathcal{L}^{\mathrm{flt}}_{x,y} = u\{XSR\}^* v \cup u\{XRRS\}^* v \cup Xu\{XSR\}^* v \cup Xu\{XRRS\}^* v.$$

Finally, the vector reachability problem from $\mathbf{x}$ to $\mathbf{y}$ has a solution if and only if

$$\varphi(\mathcal{L}^{\mathrm{vrp}}_{\mathbf{x},\mathbf{y}}) \cap \varphi(\mathcal{L}_{semigr}) \neq \emptyset.$$

Similarly, the reachability problem by fractional linear transformations from x to y has a solution if and only if

$$\varphi(\mathcal{L}^{\mathrm{flt}}_{x,y}) \cap \varphi(\mathcal{L}_{semigr}) \neq \emptyset.$$

By Proposition 13 these problems are algorithmically decidable. □

Remark 1. In the definition of the vector reachability problem we consider vectors $\mathbf{x}$ and $\mathbf{y}$ only with integer coefficients. However, the above theorem still holds if we allow $\mathbf{x}$ and $\mathbf{y}$ to have rational coefficients. Indeed, the equation $M\mathbf{x} = \mathbf{y}$ is equivalent to $M(\lambda\mathbf{x}) = \lambda\mathbf{y}$ for any $\lambda \neq 0$. So if we multiply $M\mathbf{x} = \mathbf{y}$ by the greatest common divisor of all coefficients, we can transform it to an equivalent equation with integer coefficients.

Remark 2. Characterizations of the solution sets to the equations $M\mathbf{x} = \mathbf{y}$ and $f_M(x) = y$, which are given in Corollary 8 and Theorem 9, can be computed in polynomial time. However the overall complexity of the algorithm is in EXPTIME if the entries of the matrices are given in binary presentation. This is due to the fact that a canonical word w that corresponds to a given matrix M, i.e. such that $M = \varphi(w)$, has length exponential in the binary presentation of M. So computing symbolic presentations of given matrices and constructing automata for the languages $\mathcal{L}_{semigr}$, $\mathcal{L}^{\mathrm{vrp}}_{\mathbf{x},\mathbf{y}}$ and $\mathcal{L}^{\mathrm{flt}}_{x,y}$ takes exponential time. The next steps of the algorithm take only polynomial time in the size of these automata. However the PTIME algorithm for computing all matrices $M \in \mathrm{SL}(2,\mathbb{Z})$ that satisfy $M\mathbf{x} = \mathbf{y}$ could be combined with the result of Gurevich and Schupp [17] to produce a polynomial time algorithm for the vector reachability problem over finitely generated subgroups of the modular group $\mathrm{PSL}(2,\mathbb{Z})$.

In the rest of this section we will give some generalizations of the above theorem.

Consider a semigroup generated by matrices $M_1, \ldots, M_n$ from $\mathrm{SL}(2,\mathbb{Z})$. As we showed above, this semigroup can be described by a regular language which we called $\mathcal{L}_{semigr}$. It's not hard to see that the proof of Theorem 14 remains valid if we replace $\mathcal{L}_{semigr}$ by any other regular language, that is, a language defined by an arbitrary finite automaton or a labelled transition system.

Proposition 15. *Suppose that we are given a finite collection of matrices $M_1, \ldots, M_n$ from $\mathrm{SL}(2,\mathbb{Z})$ and a regular language $L \subseteq \{1, \ldots, n\}^*$. Consider the following generalized reachability problems:*

- **Generalized vector reachability problem.** *Given two vectors $\mathbf{x}$ and $\mathbf{y}$ with integer coefficients, decide whether there exists a word $i_1 \ldots i_k$ from the language L such that $M_{i_1} \cdots M_{i_k}\mathbf{x} = \mathbf{y}$.*
- **Generalized reachability problem by fractional linear transformations.** *Given two rational numbers x and y, decide whether there exists a word $i_1 \ldots i_k$ from L such that $f_{M_{i_1} \cdots M_{i_k}}(x) = y$.*

Then the above generalized reachability problems are decidable.

Proof. The proof of this proposition is similar to the proof of Theorem 14. Namely, it follows from the fact that a regular language L defines a regular subset in $\mathrm{SL}(2,\mathbb{Z})$ and from Proposition 13, where we proved that the emptiness problem for the intersection of two regular subsets in $\mathrm{SL}(2,\mathbb{Z})$ is decidable. □

As an application of Proposition 15 let us consider the follow matrix equation

$$M_1^{x_1} \cdots M_k^{x_k} \mathbf{x} = N_1^{y_1} \cdots N_\ell^{y_\ell} \mathbf{y}, \tag{2}$$

where $x_1, \ldots, x_k$ and $y_1, \ldots, y_\ell$ are non-negative integers. In [31] it was proved that if $M_1, \ldots, M_k$ and $N_1, \ldots, N_\ell$ are commuting $n \times n$ matrices over algebraic numbers and $\mathbf{x}, \mathbf{y}$ are vectors with algebraic coefficients, then it is decidable in polynomial time whether Equation (2) has a solution. On the other hand, in [37] it was shown that there is no algorithm for solving the equation $M_1^{x_1} \cdots M_k^{x_k} = Z$, where $M_1, \ldots, M_k$ are integer $n \times n$ matrices and Z is the zero matrix. Using the construction of Kronecker (or tensor) product of matrices, it is possible to show that the above-mentioned result implies that Equation (2) is algorithmically undecidable in general for non-commuting integer matrices $M_1, \ldots, M_k$ and $N_1, \ldots, N_\ell$.

However using Proposition 15 we can algorithmically solve Equation (2) in the case when $M_1, \ldots, M_k$ and $N_1, \ldots, N_\ell$ are matrices from $\mathrm{SL}(2, \mathbb{Z})$ and the vectors $\mathbf{x}, \mathbf{y}$ have integer coefficients. Indeed, since the matrices from $\mathrm{SL}(2, \mathbb{Z})$ are invertible, we can rewrite (2) as

$$(N_\ell^{-1})^{y_\ell} \cdots (N_1^{-1})^{y_1} M_1^{x_1} \cdots M_k^{x_k} \mathbf{x} = \mathbf{y}.$$

It is not hard to see that

$$\{ (N_\ell^{-1})^{y_\ell} \cdots (N_1^{-1})^{y_1} M_1^{x_1} \cdots M_k^{x_k} \ : \ x_1, \ldots, x_k, \ y_1, \ldots, y_l \in \mathbb{N} \cup \{0\} \}$$

is a regular subset of $\mathrm{SL}(2, \mathbb{Z})$. Hence this problem is decidable. Using the same idea we can algorithmically solve Equation (2) also in the case when $x_1, \ldots, x_k$ and $y_1, \ldots, y_\ell$ are arbitrary integers and the matrices are from $\mathrm{SL}(2, \mathbb{Z})$.

6. Decidability of the scalar reachability problem

Recall that the scalar reachability problem in $\mathrm{SL}(2, \mathbb{Z})$ is defined as follows: Given two integer vectors $\mathbf{x}$, $\mathbf{z}$, an integer number λ, and a finite collection of matrices $M_1, \ldots, M_n$ from $\mathrm{SL}(2, \mathbb{Z})$, decide whether there exists a matrix $M \in \langle M_1, \ldots, M_n \rangle$ that satisfies the equation

$$\mathbf{z}^\top M \mathbf{x} = \lambda \tag{3}$$

Theorem 16. *The scalar reachability problem in* $\mathrm{SL}(2, \mathbb{Z})$ *is decidable.*

Proof. The general idea of the proof is the same as in Theorem 14, that is, we will show that the set of matrices $M \in \mathrm{SL}(2, \mathbb{Z})$ that satisfy Equation (3) can be described by a regular language. The decidability of the scalar reachability problem then follows from Proposition 13 in which we showed that the emptiness problem for the intersection of two regular subsets in $\mathrm{SL}(2, \mathbb{Z})$ is decidable.

First, let us consider a geometric interpretation of this problem. We can rewrite Equation (3) as a system of two equations:

$$\begin{cases} M\mathbf{x} = \mathbf{y} \\ \mathbf{z}^\top \mathbf{y} = \lambda \end{cases}$$

So, M satisfies Equation (3) if and only if it maps a given vector $\mathbf{x}$ to some vector $\mathbf{y}$ that lies on the line L described by the equation $\mathbf{z}^\top \mathbf{y} = \lambda$. In other words, we have a *vector to line reachability problem* from $\mathbf{x}$ to L.

Let $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, $\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ and $\mathbf{z} = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$. The equation $\mathbf{z}^\top \mathbf{y} = \lambda$ can be written as $z_1 y_1 + z_2 y_2 = \lambda$. Note that if $\gcd(z_1, z_2) \nmid \lambda$, then this equation has no solution. On the other hand, if $\gcd(z_1, z_2) \mid \lambda$, then we can divide the equation $z_1 y_1 + z_2 y_2 = \lambda$ by $\gcd(z_1, z_2)$ and assume from now on that $\gcd(z_1, z_2) = 1$.

Let u and v be the integers produced by the extended Euclidean algorithm such that

$$z_1 u + z_2 v = 1. \tag{4}$$

Now it is not hard to see that all solutions of the equation $z_1 y_1 + z_2 y_2 = \lambda$ have the form

$$\mathbf{y}^k = \begin{bmatrix} y_1^k \\ y_2^k \end{bmatrix} = \begin{bmatrix} \lambda u + k z_2 \\ \lambda v - k z_1 \end{bmatrix}, \text{ where } k \in \mathbb{Z}. \tag{5}$$

Recall that by Lemma 5 if $M\mathbf{x} = \mathbf{y}$, then $\gcd(x_1, x_2) = \gcd(y_1, y_2)$. So we are only interested in those $k \in \mathbb{Z}$ for which

$$\gcd(y_1^k, y_2^k) = \gcd(x_1, x_2) \tag{6}$$

To find all $k \in \mathbb{Z}$ that satisfy Equation (6), we will show that

$$\gcd(y_1^k, y_2^k) = \gcd(k, \lambda) \text{ for all } k \in \mathbb{Z}. \tag{7}$$

Indeed, let $d \in \mathbb{Z}$ be such that $d \mid k$ and $d \mid \lambda$, then from (5) it follows that $d \mid y_1^k$ and $d \mid y_2^k$. Conversely, if $d \mid y_1^k$ and $d \mid y_2^k$, then from (4) and (5) we have that $d \mid z_1 y_1^k + z_2 y_2^k = \lambda(z_1 u + z_2 v) = \lambda$ and $d \mid y_1^k v - y_2^k u = k(z_2 v + z_1 u) = k$.

So, Equation (6) becomes equivalent to

$$\gcd(k, \lambda) = \gcd(x_1, x_2) \tag{8}$$

Note that if $k \equiv k' \pmod{\lambda}$, then $\gcd(k, \lambda) = \gcd(k', \lambda)$. Therefore, we can describe all solutions of the Equation (8), and hence of (6), as follows

$$\{k + t\lambda \ : \ k \in X \text{ and } t \in \mathbb{Z}\},$$

where

$$X = \{k \ : \ 0 \leq k \leq \lambda - 1 \text{ and } \gcd(k, \lambda) = \gcd(x_1, x_2)\}.$$

Note that X is a finite set which can be algorithmically computed by trying all $k \in \{0, \ldots, \lambda - 1\}$.

So, we have the following equivalence: a matrix $M \in \mathrm{SL}(2, \mathbb{Z})$ satisfies the equation $\mathbf{z}^\top M \mathbf{x} = \lambda$ if and only if there exist $k \in X$ and $t \in \mathbb{Z}$ such that $M\mathbf{x} = \mathbf{y}^{k+t\lambda}$.

Let us fix $k \in X$ and consider the equation $M\mathbf{x} = \mathbf{y}^{k+t\lambda}$. By Corollary 8, all its solutions in $\mathrm{SL}(2, \mathbb{Z})$ are exactly

$$\{A(\tfrac{1}{d}\mathbf{y}^{k+t\lambda}) T^\ell A(\tfrac{1}{d}\mathbf{x})^{-1} \ : \ \ell \in \mathbb{Z}\}, \quad \text{where } d = \gcd(x_1, x_2).$$

We will now explicitly compute the matrix $A(\frac{1}{d}\mathbf{y}^{k+t\lambda})$. Note that since $k \in X$, we have $\gcd(k,\lambda) = \gcd(x_1,x_2) = d$. Let u_k and v_k be the integers produced by the extended Euclidean algorithm such that

$$ku_k + \lambda v_k = \gcd(k,\lambda) = \gcd(x_1,x_2) = d. \tag{9}$$

From (7) we obtain that for every $t \in \mathbb{Z}$,

$$\gcd(y_1^{k+t\lambda}, y_2^{k+t\lambda}) = \gcd(k+t\lambda,\lambda) = \gcd(k,\lambda) = \gcd(x_1,x_2) = d.$$

Our goal now is to find integer numbers $u_{k,t}$ and $v_{k,t}$ such that

$$y_1^{k+t\lambda}u_{k,t} + y_2^{k+t\lambda}v_{k,t} = d. \tag{10}$$

Since $y_1^{k+t\lambda} = \lambda u + (k+t\lambda)z_2$ and $y_2^{k+t\lambda} = \lambda v - (k+t\lambda)z_1$, we can rewrite Equation (10) as

$$\begin{aligned} (\lambda u + kz_2 + t\lambda z_2)u_{k,t} + (\lambda v - kz_1 - t\lambda z_1)v_{k,t} = d \qquad &\text{or as} \\ k(z_2u_{k,t} - z_1v_{k,t}) + \lambda((u+tz_2)u_{k,t} + (v-tz_1)v_{k,t}) = d \end{aligned}$$

On the other hand, Equation (9) states that $ku_k + \lambda v_k = d$. Hence, to find the desired $u_{k,t}$ and $v_{k,t}$, we need to solve the system of equations:

$$\begin{cases} z_2u_{k,t} - z_1v_{k,t} = u_k \\ (u+tz_2)u_{k,t} + (v-tz_1)v_{k,t} = v_k \end{cases}$$

In matrix form it looks like

$$\begin{bmatrix} z_2 & -z_1 \\ u+tz_2 & v-tz_1 \end{bmatrix}\begin{bmatrix} u_{k,t} \\ v_{k,t} \end{bmatrix} = \begin{bmatrix} u_k \\ v_k \end{bmatrix}$$

From Equation (4) we obtain that $\det\begin{bmatrix} z_2 & -z_1 \\ u+tz_2 & v-tz_1 \end{bmatrix} = z_2v + z_1u = 1$. So

$$\begin{bmatrix} u_{k,t} \\ v_{k,t} \end{bmatrix} = \begin{bmatrix} z_2 & -z_1 \\ u+tz_2 & v-tz_1 \end{bmatrix}^{-1}\begin{bmatrix} u_k \\ v_k \end{bmatrix} = \begin{bmatrix} v-tz_1 & z_1 \\ -(u+tz_2) & z_2 \end{bmatrix}\begin{bmatrix} u_k \\ v_k \end{bmatrix}$$

Thus $u_{k,t} = (v-tz_1)u_k + z_1v_k$ and $v_{k,t} = -(u+tz_2)u_k + z_2v_k$. Therefore, the matrix $A(\frac{1}{d}\mathbf{y}^{k+t\lambda})$ can we expressed as follows

$$\begin{aligned} A(\tfrac{1}{d}\mathbf{y}^{k+t\lambda}) &= \begin{bmatrix} \frac{1}{d}y_1^{k+t\lambda} & -v_{k,t} \\ \frac{1}{d}y_2^{k+t\lambda} & u_{k,t} \end{bmatrix} = \begin{bmatrix} \frac{\lambda}{d}u + \frac{k}{d}z_2 + t\frac{\lambda}{d}z_2 & uu_k + tz_2u_k - z_2v_k \\ \frac{\lambda}{d}v - \frac{k}{d}z_1 - t\frac{\lambda}{d}z_1 & vu_k - tz_1u_k + z_1v_k \end{bmatrix} \\ &= \begin{bmatrix} \frac{\lambda}{d}u + \frac{k}{d}z_2 & uu_k - z_2v_k \\ \frac{\lambda}{d}v - \frac{k}{d}z_1 & vu_k + z_1v_k \end{bmatrix} + t\begin{bmatrix} \frac{\lambda}{d}z_2 & z_2u_k \\ -\frac{\lambda}{d}z_1 & -z_1u_k \end{bmatrix} \end{aligned}$$

The first matrix in the above sum can be expressed as follows

$$\begin{bmatrix} \frac{\lambda}{d}u + \frac{k}{d}z_2 & uu_k - z_2v_k \\ \frac{\lambda}{d}v - \frac{k}{d}z_1 & vu_k + z_1v_k \end{bmatrix} = \begin{bmatrix} z_2 & u \\ -z_1 & v \end{bmatrix}\begin{bmatrix} \frac{k}{d} & -v_k \\ \frac{\lambda}{d} & u_k \end{bmatrix} = A(z_2,-z_1)A(\tfrac{k}{d},\tfrac{\lambda}{d})$$

The second matrix can be written as $\begin{bmatrix} \frac{\lambda}{d} z_2 & z_2 u_k \\ -\frac{\lambda}{d} z_1 & -z_1 u_k \end{bmatrix} = \begin{bmatrix} z_2 \\ -z_1 \end{bmatrix} [\frac{\lambda}{d},\, u_k]$. Note that $A(z_2, -z_1)\mathbf{e}_1 = \begin{bmatrix} z_2 \\ -z_1 \end{bmatrix}$ and $\mathbf{e}_2^\top A(\frac{k}{d}, \frac{\lambda}{d}) = [0,\, 1] \begin{bmatrix} \frac{k}{d} & -v_k \\ \frac{\lambda}{d} & u_k \end{bmatrix} = [\frac{\lambda}{d},\, u_k]$. Hence

$$\begin{aligned} A(\tfrac{1}{d}\mathbf{y}^{k+t\lambda}) &= A(z_2, -z_1)A(\tfrac{k}{d}, \tfrac{\lambda}{d}) + tA(z_2, -z_1)\mathbf{e}_1\mathbf{e}_2^\top A(\tfrac{k}{d}, \tfrac{\lambda}{d}) \\ &= A(z_2, -z_1)(I + t\mathbf{e}_1\mathbf{e}_2^\top)A(\tfrac{k}{d}, \tfrac{\lambda}{d}) \\ &= A(z_2, -z_1)\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & t \\ 0 & 0 \end{bmatrix}\right) A(\tfrac{k}{d}, \tfrac{\lambda}{d}) \\ &= A(z_2, -z_1)\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} A(\tfrac{k}{d}, \tfrac{\lambda}{d}) = A(z_2, -z_1)T^t A(\tfrac{k}{d}, \tfrac{\lambda}{d}) \end{aligned}$$

Therefore, all solutions of the equation $\mathbf{z}^\top M\mathbf{x} = \lambda$ in $\mathrm{SL}(2, \mathbb{Z})$ are exactly

$$\{A(z_2, -z_1)T^t A(\tfrac{k}{d}, \tfrac{\lambda}{d})T^\ell A(\tfrac{x_1}{d}, \tfrac{x_2}{d})^{-1} \;:\; \text{where } k \in X \text{ and } t, \ell \in \mathbb{Z}\}.$$

It is now not hard to see that this solution set can be described by a regular language. Therefore, the scalar reachability problem in $\mathrm{SL}(2, \mathbb{Z})$ is decidable.

The above solution has the following geometric interpretation: first, $\mathbf{x}$ is mapped by $A(\frac{x_1}{d}, \frac{x_2}{d})^{-1}$ to $\begin{bmatrix} d \\ 0 \end{bmatrix}$, which is mapped to itself by T^ℓ. Next $A(\frac{k}{d}, \frac{\lambda}{d})$ maps $\begin{bmatrix} d \\ 0 \end{bmatrix}$ to $\begin{bmatrix} k \\ \lambda \end{bmatrix}$, and then T^t maps $\begin{bmatrix} k \\ \lambda \end{bmatrix}$ to $\begin{bmatrix} k + t\lambda \\ \lambda \end{bmatrix}$. Finally $A(z_2, -z_1)$ maps $\begin{bmatrix} k + t\lambda \\ \lambda \end{bmatrix}$ to $\mathbf{y}^{k+t\lambda} \in L$. Figure 4 gives an illustration of these transformations. In fact, it is easy to see that $A(z_2, -z_1)$ maps the dashed line that passes through the vectors $\begin{bmatrix} k \\ \lambda \end{bmatrix}$ and $\begin{bmatrix} k + t\lambda \\ \lambda \end{bmatrix}$ onto the line L defined by the equation $\mathbf{z}^\top \mathbf{y} = \lambda$.

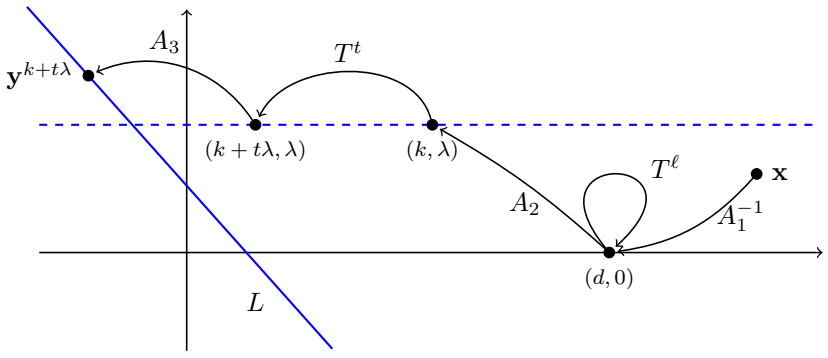

Figure 4: Geometric interpretation of the transformation $\mathbf{y}^{k+t\lambda} = A_3 T^t A_2 T^\ell A_1^{-1}(\mathbf{x})$, where $A_1 = A(\frac{x_1}{d}, \frac{x_2}{d})$, $A_2 = A(\frac{k}{d}, \frac{\lambda}{d})$ and $A_3 = A(z_2, -z_1)$.

□

We are grateful to the anonymous referees for their numerous comments and suggestions that helped us to simplify the proofs presented in this paper.

References

[1] A. Markov, On certain insoluble problems concerning matrices, Doklady Akad. Nauk SSSR 57 (6) (1947) 539–542.

[2] V. Halava, T. Harju, M. Hirvensalo, J. Karhumaki, Skolem's problem — on the border between decidability and undecidability, Tech. Rep. 683, Turku Centre for Computer Science (2005).

[3] J. Ouaknine, J. Worrell, On the positivity problem for simple linear recurrence sequences, in: Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part II, 2014, pp. 318–329.

[4] J. Ouaknine, J. Worrell, Ultimate positivity is decidable for simple linear recurrence sequences, in: Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part II, 2014, pp. 330–341.

[5] E. Galby, J. Ouaknine, J. Worrell, On Matrix Powering in Low Dimensions, in: E. W. Mayr, N. Ollinger (Eds.), 32nd International Symposium on Theoretical Aspects of Computer Science (STACS 2015), Vol. 30 of Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2015, pp. 329–340.

[6] J. Ouaknine, J. a. S. Pinto, J. Worrell, On termination of integer linear loops, in: Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA '15, SIAM, 2015, pp. 957–969.

[7] P. Bell, I. Potapov, On undecidability bounds for matrix decision problems, Theoretical Computer Science 391 (1-2) (2008) 3–13.

[8] V. D. Blondel, E. Jeandel, P. Koiran, N. Portier, Decidable and undecidable problems about quantum automata, SIAM J. Comput. 34 (6) (2005) 1464–1473.

[9] J. Esparza, A. Finkel, R. Mayr, On the verification of broadcast protocols, in: Logic in Computer Science, 1999. Proceedings. 14th Symposium on, 1999, pp. 352–359.

[10] P. C. Bell, I. Potapov, On the computational complexity of matrix semigroup problems, Fundam. Inf. 116 (1-4) (2012) 1–13.

[11] J. Cassaigne, T. Harju, J. Karhumaki, On the undecidability of freeness of matrix semigroups, International Journal of Algebra and Computation 09 (03n04) (1999) 295–305.

[12] P. Bell, I. Potapov, Reachability problems in quaternion matrix and rotation semigroups, Information and Computation 206 (11) (2008) 1353–1361.

[13] C. Choffrut, J. Karhumaki, Some decision problems on integer matrices, RAIRO-Theor. Inf. Appl. 39 (1) (2005) 125–131.

[14] J. Cassaigne, F. Nicolas, On the decidability of semigroup freeness, RAIRO - Theor. Inf. and Applic. 46 (3) (2012) 355–399.

[15] E. Charlier, J. Honkala, The freeness problem over matrix semigroups and bounded languages, Inf. Comput. 237 (2014) 243–256.

[16] P. C. Bell, M. Hirvensalo, I. Potapov, Mortality for 2x2 matrices is NP-hard, in: B. Rovan, V. Sassone, P. Widmayer (Eds.), Mathematical Foundations of Computer Science 2012, Vol. 7464 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2012, pp. 148–159.

[17] Y. Gurevich, P. Schupp, Membership problem for the modular group, SIAM J. Comput. 37 (2) (2007) 425–459.

[18] I. Potapov, P. Semukhin, Decidability of the membership problem for 2×2 integer matrices, in: Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19, 2017, pp. 170–186.

[19] I. Potapov, P. Semukhin, Membership problem in $\mathrm{GL}(2, \mathbb{Z})$ extended by singular matrices, in: 42nd International Symposium on Mathematical Foundations of Computer Science, MFCS 2017, August 21-25, 2017 - Aalborg, Denmark, 2017, pp. 44:1–44:13.

[20] P. C. Bell, M. Hirvensalo, I. Potapov, The identity problem for matrix semigroups in $\mathrm{SL}_2(\mathbb{Z})$ is NP-complete, in: Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19, 2017, pp. 187–206.

[21] S. Ko, I. Potapov, Matrix semigroup freeness problems in $\mathrm{SL}(2, \mathbb{Z})$, in: SOFSEM 2017: Theory and Practice of Computer Science - 43rd International Conference on Current Trends in Theory and Practice of Computer Science, Limerick, Ireland, January 16-20, 2017, pp. 268–279.

[22] D. Zagier, Elliptic modular forms and their applications, in: K. Ranestad (Ed.), The 1-2-3 of Modular Forms, Universitext, Springer Berlin Heidelberg, 2008, pp. 1–103.

[23] F. Chamizo, Non-euclidean visibility problems, Proceedings of the Indian Academy of Sciences - Mathematical Sciences 116 (2) (2006) 147–160.

[24] J. Elstrodt, F. Grunewald, J. Mennicke, Arithmetic applications of the hyperbolic lattice point theorem, Proc. London Math. Soc. s3-57 (1988) pp.239–283.

[25] L. Polterovich, Z. Rudnick, Stable mixing for cat maps and quasimorphisms of the modular group, Ergodic Theory and Dynamical Systems 24 (2004) 609–619.

[26] D. Mackenzie, A new twist in knot theory, What's Happening in the Mathematical Sciences Volume 7.

[27] I. Potapov, Composition problems for braids, in: 33nd International Conference on Foundations of Software Technology and Theoretical Computer Science, Vol. 24 of LIPIcs. Leibniz Int. Proc. Inform., Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2013, pp. 175–187.

[28] E. Witten, $SL(2,\mathbb{Z})$ action on three-dimensional conformal field theories with abelian symmetry, in: From fields to strings: circumnavigating theoretical physics. Vol. 2, World Sci. Publ., Singapore, 2005, pp. 1173–1200.

[29] M. P. García del Moral, I. Martín, J. M. Peña, A. Restuccia, Sl(2,z) symmetries, supermembranes and symplectic torus bundles, Journal of High Energy Physics 2011 (9) (2011) 1–12.

[30] T. Noll, Musical intervals and special linear transformations, Journal of Mathematics and Music: Mathematical and Computational Approaches to Music Theory, Analysis, Composition and Performance vol.1.

[31] L. Babai, R. Beals, J.-y. Cai, G. Ivanyos, E. M. Luks, Multiplicative equations over commuting matrices, in: Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA '96, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1996, pp. 498–507.

[32] A. Lisitsa, I. Potapov, Membership and reachability problems for row-monomial transformations, in: Mathematical Foundations of Computer Science 2004, 29th International Symposium, MFCS 2004, Prague, Czech Republic, August 22-27, 2004, Proceedings, 2004, pp. 623–634.

[33] V. Halava, T. Harju, M. Hirvensalo, Undecidability bounds for integer matrices using Claus instances, International Journal of Foundations of Computer Science 18 (05) (2007) 931–948.

[34] R. C. Lyndon, P. E. Schupp, Combinatorial group theory, Springer-Verlag, Berlin-New York, 1977, ergebnisse der Mathematik und ihrer Grenzgebiete, Band 89.

[35] W. Magnus, A. Karrass, D. Solitar, Combinatorial group theory, revised Edition, Dover Publications, Inc., New York, 1976, presentations of groups in terms of generators and relations.

[36] R. A. Rankin, Modular forms and functions, Cambridge University Press, Cambridge-New York-Melbourne, 1977.

[37] P. Bell, V. Halava, T. Harju, J. Karhumäki, I. Potapov, Matrix equations and Hilbert's tenth problem, Internat. J. Algebra Comput. 18 (8) (2008) 1231–1241.