# Decidability of the Membership Problem for $2 \times 2$ integer matrices[*]

Igor Potapov[†]          Pavel Semukhin[‡]

The main result of this paper is the decidability of the membership problem for $2 \times 2$ nonsingular integer matrices. Namely, we will construct the first algorithm that for any nonsingular $2 \times 2$ integer matrices $M_1, \ldots, M_n$ and $M$ decides whether $M$ belongs to the semigroup generated by $\{M_1, \ldots, M_n\}$.

Our algorithm relies on a translation of the numerical problem on matrices into combinatorial problems on words. It also makes use of some algebraical properties of well-known subgroups of $\mathrm{GL}(2, \mathbb{Z})$ and various new techniques and constructions that help to limit an infinite number of possibilities by reducing them to the membership problem for regular languages.

## 1 Introduction

Matrices and matrix products play a crucial role in a representation and analysis of various computational processes, i.e., linear recurrent sequences [18, 26, 27], arithmetic circuits [15], hybrid and dynamical systems [25, 2], probabilistic and quantum automata [7], stochastic games, broadcast protocols [14], optical systems [16], etc. Unfortunately, many simply formulated and elementary problems for matrices are inherently difficult to solve even in dimension two, and most of these problems become undecidable in general starting from dimension three or four. One of such hard questions is the *Membership problem* in matrix semigroups:

**Membership problem:** Given a finite set of $m \times m$ matrices $F = \{M_1, M_2, \ldots, M_n\}$ and a matrix $M$. Determine if there exist an integer $k \geq 1$ and $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$ such that $M_{i_1} \cdot M_{i_2} \cdots M_{i_k} = M$. In other words, determine whether a matrix $M$ belongs to the semigroup generated by $F$.

In this paper we solve an open problem by showing that the membership is decidable for the semigroups of $2 \times 2$ nonsingular matrices over integers. The membership problem was intensively studied since 1947 when A.Markov showed that this problem is undecidable for matrices in $\mathbb{Z}^{6 \times 6}$ even for a specific fixed set $F$ [24]. Later, M. Paterson in 1970 showed that a special case of the membership problem when $M$ is equal to a zero matrix (known as *Mortality problem*) is undecidable for matrices in $\mathbb{Z}^{3 \times 3}$. The decidability status of another special case of the membership problem — the *Identity problem* (i.e., when $M = I$, the identity matrix) — was unknown for a long time and was only recently shown to be undecidable for integer matrices starting from dimension four [5], see also the solution to Problem 10.3 in [8]. The undecidability of the identity problem means that the

---

[†]Department of Computer Science, University of Liverpool. Email: `potapov@liverpool.ac.uk`

[‡]Department of Computer Science, University of Liverpool. Email: `semukhin@liverpool.ac.uk`

*Group problem* (of whether a matrix semigroup over integers forms a group) is undecidable starting from dimension four. A more recent survey of undecidable problems can be found in [9].

The undecidability proofs in matrix semigroups are mainly based on various techniques and methods for embedding universal computations into matrix products. The case of dimension two is the most intriguing since there is some evidence that if these problems are undecidable, then this cannot be proved using any previously known constructions. In particular, there is no injective semigroup morphism from pairs of words over any finite alphabet (with at least two elements) into complex $2 \times 2$ matrices [10], which means that the coding of independent pairs of words in $2 \times 2$ complex matrices is impossible and the exact encoding of the Post Correspondence Problem or a computation of the Turing Machine cannot be used directly for proving undecidability in $2 \times 2$ matrix semigroups over $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{C}$. The only undecidability in the case of $2 \times 2$ matrices has been shown so far is the membership, freeness and vector reachability problems over quaternions [3] or more precisely in the case of diagonal matrices over quaternions, which are simply double quaternions.

The problems for semigroups are rather hard, but there was a steady progress on decidable fragments over the last few decades. First, both membership and vector reachability problems were shown to be decidable in polynomial time for a semigroup generated by a single $m \times m$ matrix (known as the *Orbit problem*) by Kannan and Lipton [20] in 1986. Later, in 1996 this decidability result was extended to a more general case of commutative matrices [1]. The generalization of this result for a special class of non-commutative matrices (a class of row-monomial matrices over a commutative semigroup satisfying some natural effectiveness conditions) was shown in 2004 in [21]. Even now we still have long standing open problems for matrix semigroups generated by a single matrix, see, for example, the *Skolem Problem* about reaching zero in a linear recurrence sequence (LRS), which in matrix form is a question of whether any power of a given integer matrix $A$ has zero in the right upper corner [12, 13]. It was recently shown that the decidability of either Positivity or Ultimate Positivity for integer LRS of order 6 would entail some major breakthroughs in analytic number theory. The decidability of each of these problems, whether for integer, rational, or algebraic linear recurrence sequences, is open, although partial results are known [15, 25, 26, 27].

Due to a severe lack of methods and techniques the status of decision problems for $2 \times 2$ matrices (like membership, vector reachability, freeness) is remaining to be a long standing open problem. More recently, a new approach of translating numerical problems of $2 \times 2$ integer matrices into variety of combinatorial and computational problems on words over group alphabet and studying their transformations as specific rewriting systems have led to a few results on decidability and complexity for some subclasses. In particular, this approach was successfully applied to proving the decidability of the membership problem for semigroups from $\mathrm{GL}(2, \mathbb{Z})$ [11] in 2005, designing the polynomial time algorithm for the membership problem for the modular group [17] in 2007, showing NP-hardness for most of the reachability problems in dimension two [6, 4] in 2012, and showing decidability of the vector/scalar reachability problems in $\mathrm{SL}(2, \mathbb{Z})$ [28] in 2015.

The main ingredient of the translation into combinatorial problems on words is the well-known result that the groups $\mathrm{SL}(2, \mathbb{Z})$ and $\mathrm{GL}(2, \mathbb{Z})$ are finitely generated. For example, $\mathrm{SL}(2, \mathbb{Z})$ can be generated by a pair of matrices:

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ and } R = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \text{ with the following relations: } S^4 = I, R^6 = I \text{ and } S^2 = R^3.$$

Hence we can represent a matrix $M \in \mathrm{SL}(2, \mathbb{Z})$ as a word in the alphabet $\{S, R\}$.

In [11] both the *Identity* and the *Group* problems are shown to be decidable in $\mathbb{Z}^{2 \times 2}$. Moreover, it was also claimed more generally that it is decidable whether or not a given nonsingular matrix belongs to a given finitely generated semigroup over integers. Unfortunately, it appears that the proof of this more general claim (i.e., when we consider matrices with determinants different from $\pm 1$)

has a significant gap, and it only works for a small number of special cases. Namely, after translating the membership from $\mathrm{GL}(2, \mathbb{Z})$ to $\mathrm{SL}(2, \mathbb{Z})$, the authors describe a very short reduction from the membership problems in $\mathbb{Z}^{2 \times 2}$ to the one in $\mathrm{SL}(2, \mathbb{Z})$ using some incorrect assumptions. For instance, it was assumed that if $X$ is an integer matrix with determinant one and $Z$ is a nonsingular integer matrix, then there exists an integer matrix $Y$ satisfying the following equation $ZX = YZ$. However, this is not true and here is a simple counter example. Let $Z = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ and $X = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, then from $ZX = YZ$ it follows that $Y = ZXZ^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \times \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 0 & -\frac{1}{2} \\ 2 & 0 \end{bmatrix}$. So $Y$ has fractional coefficients, and if the matrices $X$ and $Z$ were in the generating set, then the argument from [11] would not work.

The main result of this paper is that the membership problem is decidable for the semigroups of $2 \times 2$ nonsingular integer matrices. Our proof provides an algorithm for solving this problem, which is based on the translation of the numerical problem on matrices into combinatorial problems on words and regular languages. We will also makes use of some well-known algebraical results like the uniqueness of the Smith normal form of a matrix and a fact that certain subgroups of $\mathrm{GL}(2, \mathbb{Z})$ have finite index.

## 2 Preliminaries

The semigroup of $2 \times 2$ integer matrices is denoted by $\mathbb{Z}^{2 \times 2}$. We use $\mathrm{SL}(2, \mathbb{Z})$ to denote the special linear group of $2 \times 2$ matrices with integer coefficients, i.e., $\mathrm{SL}(2, \mathbb{Z}) = \{M \in \mathbb{Z}^{2 \times 2} : \det(M) = 1\}$ and $\mathrm{GL}(2, \mathbb{Z})$ to denote the general linear group, i.e., $\mathrm{GL}(2, \mathbb{Z}) = \{M \in \mathbb{Z}^{2 \times 2} : \det(M) = \pm 1\}$.

A matrix is called *nonsingular* if its determinant is not equal to zero.

If $F$ is a finite collection of matrices from $\mathbb{Z}^{2 \times 2}$, then $\langle F \rangle$ denotes the semigroup generated by $F$ (including the identity matrix), that is, $M \in \langle F \rangle$ if and only if $M = I$ or there are matrices $M_1, \ldots, M_n \in F$ such that $M = M_1 \cdots M_n$.

## 3 Main result

The main result of our paper is presented in Theorem 1 which states that membership problem in dimension two is decidable.

**Theorem 1.** *There is an algorithm that decides for a given finite collection $F$ of nonsingular matrices from $\mathbb{Z}^{2 \times 2}$ and a matrix $M \in \mathbb{Z}^{2 \times 2}$ whether $M \in \langle F \rangle$.*

*Proof sketch.* Let $\{M_1, \ldots, M_n\}$ be all matrices from $F$ whose determinant is different from $\pm 1$, and let $\mathcal{S}^{\pm 1}$ be the semigroup which is generated by all matrices from $F$ with determinant $\pm 1$, that is, $\mathcal{S}^{\pm 1} = \langle F \cap \mathrm{GL}(2, \mathbb{Z}) \rangle$. Then it is not hard to see that $M \in \langle F \rangle$ if and only if $M \in \mathcal{S}^{\pm 1}$ or there is a sequence of indices $i_1, \ldots, i_t \in \{1, \ldots, n\}$ and matrices $A_1, \ldots, A_{t+1}$ from $\mathcal{S}^{\pm 1}$ such that

$$M = A_1 M_{i_1} A_2 M_{i_2} \cdots A_t M_{i_t} A_{t+1}.$$

The key point of the proof is that the value of $t$ is bounded. Indeed, since $|\det(M_{i_s})| \geq 2$, for $s = 1, \ldots, t$, we have that $t \leq \log_2 |\det(M)|$. So to decide whether or not $M \in \langle F \rangle$ we first need to check whether $M \in \mathcal{S}^{\pm 1}$. If $M \notin \mathcal{S}^{\pm 1}$, then we need to go through all sequences $i_1, \ldots, i_t \in \{1, \ldots, n\}$ of length up to $\log_2 |\det(M)|$ and for every such sequence check whether there are matrices $A_1, \ldots, A_{t+1}$ from $\mathcal{S}^{\pm 1}$ such that $M = A_1 M_{i_1} A_2 M_{i_2} \cdots A_t M_{i_t} A_{t+1}$. The rest of the paper is devoted to the proof that these problems are algorithmically decidable.

In Section 3.1 we describe an algorithm that decides whether $M \in \mathcal{S}^{\pm 1}$. In fact, in Proposition 7 we prove a stronger statement that it is decidable whether $M \in \mathcal{S}$, where $\mathcal{S}$ is an arbitrary regular subset of $\mathrm{GL}(2, \mathbb{Z})$, that is, a subset which is defined by a finite automaton. The precise definition of this notion is given in Section 3.1. We will also show there that any semigroup in $\mathrm{GL}(2, \mathbb{Z})$, and in particular $\mathcal{S}^{\pm 1}$, is a regular subset.

Proposition 7 provides an alternative proof for the decidability of the membership in $\mathrm{GL}(2, \mathbb{Z})$ presented in [11]. The difference of our approach is that we do not introduce new symbols in the alphabet, and we explicitly construct an automaton $\mathrm{Can}(\mathcal{A})$ that accepts only canonical words. The construction of $\mathrm{Can}(\mathcal{A})$ will be also used in the next steps of our algorithm.

In Section 3.2 we provide a proof for the decidability of the second problem in the special case when $t = 1$. Again, in Corollary 15 we prove a more general statement that for any two nonsingular matrices $M_1$ and $M_2$ from $\mathbb{Z}^{2 \times 2}$ and regular subsets $\mathcal{S}_1$ and $\mathcal{S}_2$, it is decidable whether there are matrices $A_1 \in \mathcal{S}_1$ and $A_2 \in \mathcal{S}_2$ such that $A_1 M_1 A_2 = M_2$.

Finally, in Section 3.3 we describe an algorithm for the general case. Namely, in Theorem 19 we will prove that for any nonsingular matrices $M_1, \ldots, M_t$ from $\mathbb{Z}^{2 \times 2}$ and for any regular subsets $\mathcal{S}_1, \ldots, \mathcal{S}_t$ of $\mathrm{GL}(2, \mathbb{Z})$, it is decidable whether there are matrices $A_1 \in \mathcal{S}_1, \ldots, A_t \in \mathcal{S}_t$ such that $A_1 M_1 \cdots A_{t-1} M_{t-1} A_t = M_t$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

*Remark.* The complexity of our algorithm is in EXPSPACE. The exponential blow-up in memory usage happens when we translate matrices into words and construct a finite automaton for the semigroup $\mathcal{S}^{\pm 1}$ (see the paragraph before Corollary 8 in Section 3.1). The other steps of the algorithm require only polynomial space. Furthermore, our algorithm can be extended to check the membership not only for semigroups in $\mathbb{Z}^{2 \times 2}$ but for arbitrary regular subsets of nonsingular matrices from $\mathbb{Z}^{2 \times 2}$.

## 3.1 Decidability of the membership problem in $\mathrm{GL}(2, \mathbb{Z})$.

We will use an encoding of matrices from $\mathrm{GL}(2, \mathbb{Z})$ by words in alphabet $\Sigma = \{X, N, S, R\}$. For this we define a mapping $\varphi : \Sigma \to \mathrm{GL}(2, \mathbb{Z})$ as follows:

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

We can extend $\varphi$ to the morphism $\varphi : \Sigma^* \to \mathrm{GL}(2, \mathbb{Z})$ in a natural way. It is a well-known fact that morphism $\varphi$ is surjective, that is, for every $M \in \mathrm{GL}(2, \mathbb{Z})$ there is a word $w \in \Sigma^*$ such that $\varphi(w) = M$.

**Definition 2.** We call two words $w_1$ and $w_2$ from $\Sigma^*$ *equivalent*, denoted $w_1 \sim w_2$, if $\varphi(w_1) = \varphi(w_2)$. Two languages $L_1$ and $L_2$ in the alphabet $\Sigma$ are *equivalent*, denoted $L_1 \sim L_2$, if

(i) for each $w_1 \in L_1$, there exists $w_2 \in L_2$ such that $w_1 \sim w_2$, and

(ii) for each $w_2 \in L_2$, there exists $w_1 \in L_1$ such that $w_2 \sim w_1$.

In other words, $L_1 \sim L_2$ if and only if $\varphi(L_1) = \varphi(L_2)$. Two finite automata $\mathcal{A}_1$ and $\mathcal{A}_2$ with alphabet $\Sigma$ are *equivalent*, denoted $\mathcal{A}_1 \sim \mathcal{A}_2$, if $L(\mathcal{A}_1) \sim L(\mathcal{A}_2)$.

To simplify the notation we will often write $M = w$ instead of $M = \varphi(w)$ when $M \in \mathrm{GL}(2, \mathbb{Z})$ and $w \in \Sigma^*$. Note that in this notation if $M = w_1$ and $M = w_2$, then we have $w_1 \sim w_2$ but not necessarily $w_1 = w_2$.

**Definition 3.** A subset $\mathcal{S} \subseteq \mathrm{GL}(2, \mathbb{Z})$ is called *regular* or *automatic* if there is a regular language $L$ in alphabet $\Sigma$ such that $\mathcal{S} = \varphi(L)$.

Throughout the paper we will use the following abbreviation: if $n$ is a positive integer and $V \in \Sigma$, then $V^n$ denotes a words of length $n$ which contains only letter $V$, and $V^0$ is assumed to be equal to the empty word.

**Definition 4.** A word $w \in \Sigma^*$ is called a *canonical word* if it has the form

$$w = N^\delta X^\gamma S^\beta R^{\alpha_0} S R^{\alpha_1} S R^{\alpha_2} \ldots S R^{\alpha_{n-1}} S R^{\alpha_n},$$

where $\beta, \delta, \gamma \in \{0, 1\}$, $\alpha_0, \ldots, \alpha_{n-1} \in \{1, 2\}$, and $\alpha_n \in \{0, 1, 2\}$. In other words, $w$ is *canonical* if it does not contain subwords $SS$ or $RRR$. Moreover, letter $N$ may appear only once in the first position, and letter $X$ may appear only once either in the first position or after $N$.

We will make use of Corollary 6 below which states that every matrix from $\mathrm{GL}(2, \mathbb{Z})$ can be represented by a unique canonical word.

**Proposition 5** ([22, 23, 29]). *For every matrix $M \in \mathrm{SL}(2, \mathbb{Z})$, there is a unique canonical word $w$ such that $M = w$. Note that $w$ does not contain letter $N$ because $\varphi(N) \notin \mathrm{SL}(2, \mathbb{Z})$.*

**Corollary 6.** *For every matrix $M \in \mathrm{GL}(2, \mathbb{Z})$, there is a unique canonical word $w$ such that $M = w$.*

*Proof.* If $\det(A) = 1$, that is, $M \in \mathrm{SL}(2, \mathbb{Z})$, then by Proposition 5 there is a unique canonical word $w$ such that $M = w$. If $\det(A) = -1$, then $N^{-1}M \in \mathrm{SL}(2, \mathbb{Z})$ and again by Proposition 5 there is a unique canonical word $w$ such that $N^{-1}M = w$ or $M = Nw$. Note that $Nw$ is also a canonical word since $w$ does not contain letter $N$. □

**Proposition 7.** *There is an algorithm that for any regular subset $\mathcal{S} \subseteq \mathrm{GL}(2, \mathbb{Z})$ and a matrix $M \in \mathrm{GL}(2, \mathbb{Z})$ decides whether $M \in \mathcal{S}$.*

*Proof.* Let $L$ be a regular language such that $\mathcal{S} = \varphi(L)$, and let $\mathcal{A}$ be a finite automaton that recognizes $L$, that is, $L = L(\mathcal{A})$. The words in $L$ do not have to be in canonical form. So, we will construct a new automaton $\mathrm{Can}(\mathcal{A})$ whose language contains only canonical words and such that $\mathrm{Can}(\mathcal{A})$ is equivalent to $\mathcal{A}$, that is, $\varphi(L(\mathrm{Can}(\mathcal{A}))) = \varphi(L(\mathcal{A})) = \mathcal{S}$. The construction of $\mathrm{Can}(\mathcal{A})$ consists of a sequence of transformations that insert new paths and $\varepsilon$-transitions into $\mathcal{A}$. The detailed description of this construction is given in Section 4.1 of the Appendix.

Using the automaton $\mathrm{Can}(\mathcal{A})$ we can decide whether $M \in \mathcal{S}$. Indeed, by Corollary 6, there is a unique canonical word $w$ that represents the matrix $M$, i.e., $M = \varphi(w)$. Now we have the following equivalence: $M \in \mathcal{S}$ if and only if $w \in L(\mathrm{Can}(\mathcal{A}))$. Therefore, to decide whether $M \in \mathcal{S}$, we need to check whether $w$ is accepted by $\mathrm{Can}(\mathcal{A})$.

□

Note that any finitely generated semigroup $\langle M_1, \ldots, M_n \rangle$ in $\mathrm{GL}(2, \mathbb{Z})$ is a regular subset. Indeed, let $w_1, \ldots, w_n$ be canonical words that represent the matrices $M_1, \ldots, M_n$, respectively, and consider a regular language $L = (w_1 + \cdots + w_n)^*$. Clearly $\varphi(L) = \langle M_1, \ldots, M_n \rangle$, and hence the semigroup $\langle M_1, \ldots, M_n \rangle$ is regular. So as a corollary from Proposition 7 we obtain the decidability of the membership problem for semigroups in $\mathrm{GL}(2, \mathbb{Z})$.

**Corollary 8.** *The membership problem for $\mathrm{GL}(2, \mathbb{Z})$ is decidable. That is, there is an algorithm that for a given finite collection of matrices $M_1, \ldots, M_n$ and $M$ from $\mathrm{GL}(2, \mathbb{Z})$, decides whether $M \in \langle M_1, \ldots, M_n \rangle$.*

## 3.2 Special case: $A_1 M_1 A_2 = M_2$

In this section we show that for any two nonsingular matrices $M_1$ and $M_2$ from $\mathbb{Z}^{2 \times 2}$ and regular subsets $\mathcal{S}_1$ and $\mathcal{S}_2$, it is decidable whether there exist matrices $A_1 \in \mathcal{S}_1$ and $A_2 \in \mathcal{S}_2$ such that $A_1 M_1 A_2 = M_2$ (Corollary 15). First, we prove this statement in the case when $M_1 = M_2 = D$, where $D$ is a diagonal matrix in the Smith normal form (Proposition 14).

For the proof of this result we will use a few algebraical facts and results that are explained below. The most important of them is the following theorem about the Smith normal form of a matrix.

**Theorem 9** (Smith normal form [19])**.** *For any matrix $A \in \mathbb{Z}^{2 \times 2}$, there are matrices $E, F$ from $\mathrm{GL}(2, \mathbb{Z})$ such that*

$$A = E \begin{bmatrix} t_1 & 0 \\ 0 & t_2 \end{bmatrix} F$$

*for some $t_1, t_2 \in \mathbb{Z}$ such that $t_1 \mid t_2$. The diagonal matrix $\begin{bmatrix} t_1 & 0 \\ 0 & t_2 \end{bmatrix}$, which is unique up to the signs of $t_1$ and $t_2$, is called the* Smith normal form *of $A$. Moreover, $E$, $F$, $t_1$, and $t_2$ can be computed in polynomial time.*

**Definition 10.** If $H$ is a subgroup of $G$, then the sets $gH = \{gh : h \in H\}$ and $Hg = \{hg : h \in H\}$, for $g \in G$, are called the *left* and *right cosets* of $H$ in $G$, respectively. An element $g$ is called a *representative* of the left coset $gH$ (respectively, of the right coset $Hg$).

The collection of left cosets or right cosets of $H$ form a disjoint partition of $G$. Moreover, the number of left cosets is equal to the number of right cosets, and this number is called the *index* of $H$ in $G$, denoted $|G : H|$.

For every natural $n \geq 1$, let us define the following subgroups of $\mathrm{GL}(2, \mathbb{Z})$:

$$H(n) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathrm{GL}(2, \mathbb{Z}) \ : \ n \text{ divides } a_{21} \right\},$$

$$F(n) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathrm{GL}(2, \mathbb{Z}) \ : \ n \text{ divides } a_{12} \right\}.$$

Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ be any matrix from $\mathrm{GL}(2, \mathbb{Z})$ and let $D = \begin{bmatrix} m & 0 \\ 0 & mn \end{bmatrix}$ be a diagonal matrix in the Smith normal form, where $m, n \neq 0$. Then the conjugation of $A$ with $D$ is equal to

$$A^D = D^{-1} A D = \begin{bmatrix} a_{11} & n a_{12} \\ \frac{1}{n} a_{21} & a_{22} \end{bmatrix}.$$

From this formula we see that if $A^D \in \mathrm{GL}(2, \mathbb{Z})$, then $n$ divides $a_{21}$. On the other hand, if $a_{21}$ is divisible by $n$, then $A^D$ is in $\mathrm{GL}(2, \mathbb{Z})$, and in fact in $F(n)$. Thus we have the following criterion.

**Proposition 11.** *Suppose $A$ is in $\mathrm{GL}(2, \mathbb{Z})$ and $D$ is a diagonal matrix of the above form, then $A^D \in \mathrm{GL}(2, \mathbb{Z})$ if and only if $A \in H(n)$. Moreover, if $A \in H(n)$, then $A^D \in F(n)$.*

**Theorem 12.** *The subgroups $H(n)$ and $F(n)$ have finite index in $\mathrm{GL}(2, \mathbb{Z})$. Furthermore, there is an algorithm that for a given $n$ computes representatives of the left and right cosets of $H(n)$ and $F(n)$ in $\mathrm{GL}(2, \mathbb{Z})$.*

*Proof.* We will only show how to compute representatives of the left cosets of $H(n)$ because the other cases are similar. For each pair of indices $i, j$ such that $0 \leq i, j \leq n - 1$, let us define a matrix $W_{i,j}$ as follows. Let $W_{i,0}$ be the identity matrix for $i = 0, \ldots, n - 1$. If $j > 0$, then consider $d = \gcd(i, j)$ and let $i_0$ and $j_0$ be such that $i = i_0 d$ and $j = j_0 d$. Since $i_0, j_0$ are relatively prime, there exist integers $u$ and $v$ such that $u i_0 + v j_0 = 1$. Hence if we let $W_{i,j} = \begin{bmatrix} u & v \\ -j_0 & i_0 \end{bmatrix}$, then $W_{i,j}$ belongs to $\mathrm{GL}(2, \mathbb{Z})$.

Now consider an arbitrary matrix $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ from $\mathrm{GL}(2, \mathbb{Z})$. Let $a_{11} = i + nk$ and $a_{21} = j + nl$, where $0 \leq i, j \leq n-1$. We will show that $W_{i,j} A \in H(n)$. If $j = 0$, then $a_{21} = nl$ is divisible by $n$, and hence $A \in H(n)$. Since we defined $W_{i,0}$ to be the identity matrix, it follows that $W_{i,0} A = A \in H(n)$. If $j > 0$, then let $d = \gcd(i, j)$ and let $i_0, j_0$ be such that $i = i_0 d$ and $j = j_0 d$. In this case

$$W_{i,j} A = \begin{bmatrix} u & v \\ -j_0 & i_0 \end{bmatrix} \begin{bmatrix} di_0 + nk & a_{12} \\ dj_0 + nl & a_{22} \end{bmatrix},$$

and the lower left corner of $W_{i,j} A$ is equal to $-j_0 d i_0 - j_0 nk + i_0 d j_0 + i_0 nl = n(-j_0 k + i_0 l)$, which is divisible by $n$. Thus $W_{i,j} A \in H(n)$.

So we showed that for any matrix $A \in \mathrm{GL}(2, \mathbb{Z})$ there is a pair $i, j$ such that $W_{i,j} A \in H(n)$ or, equivalently, $A \in W_{i,j}^{-1} H(n)$. Therefore, the collection $\{W_{i,j}^{-1} H(n) : 0 \leq i, j \leq n - 1\}$ contains all left cosets of $H(n)$ in $\mathrm{GL}(2, \mathbb{Z})$. In particular, the index of $H(n)$ in $\mathrm{GL}(2, \mathbb{Z})$ is bounded by $n^2$.

Note that some of the cosets in $\{W_{i,j}^{-1} H(n) : 0 \leq i, j \leq n - 1\}$ may be equal to each other. In fact, two cosets $W_{i_1, j_1}^{-1} H(n)$ and $W_{i_2, j_2}^{-1} H(n)$ are equal if and only if $W_{i_1, j_1} W_{i_2, j_2}^{-1} \in H(n)$. Since the domain of the subgroup $H(n)$ is a computable set, the equality of two cosets is a decidable property. Therefore, we can algorithmically choose a collection of pairwise nonequivalent representatives of the left cosets of $H(n)$ in $\mathrm{GL}(2, \mathbb{Z})$. $\qquad \square$

**Lemma 13.** *Let $L_{H(n)}$ and $L_{F(n)}$ be the languages that correspond to the subgroups $H(n)$ and $F(n)$, respectively, that is, $L_{H(n)} = \{w \in \Sigma^* : \varphi(w) \in H(n)\}$ and $L_{F(n)} = \{w \in \Sigma^* : \varphi(w) \in F(n)\}$. Then $L_{H(n)}$ and $L_{F(n)}$ are regular languages.*

*Proof.* We will show that $L_{H(n)}$ is regular by constructing an automaton $\mathcal{A}_{H(n)}$ that recognizes it. The proof for $L_{F(n)}$ is similar.

Let $U_0, U_1, \ldots, U_k$ be pairwise nonequivalent representatives of the right cosets of $H(n)$ in $\mathrm{GL}(2, \mathbb{Z})$, which can be computed by Theorem 12. We will assume that $U_0 = I$ and hence $H(n)U_0 = H(n)$. The automaton $\mathcal{A}_{H(n)}$ will have $k$ states $u_0, u_1, \ldots, u_k$, where $u_0$ is the only initial and the only final state of $\mathcal{A}_{H(n)}$. The transitions of $\mathcal{A}_{H(n)}$ are defined as follows: there is a transition from $u_i$ to $u_j$ labelled by $\sigma \in \Sigma$ if and only if the element $U_i \varphi(\sigma)$ belongs to the coset $H(n)U_j$. Note that since for every $i$ and $\sigma$ there is exactly one $j$ such that $U_i \varphi(\sigma) \in H(n)U_j$, the automaton $\mathcal{A}_{H(n)}$ is deterministic.

We now show that the language of $\mathcal{A}_{H(n)}$ is equal to $L_{H(n)}$. Take any word $w = \sigma_1 \sigma_2 \ldots \sigma_t \in \Sigma^*$ and consider a run $\rho = u_{i_0} u_{i_1} \ldots u_{i_t}$ of $\mathcal{A}_{H(n)}$ on $w$. Note that $i_0 = 0$, and $u_{i_0} = u_0$ is the initial state. Since $\mathcal{A}_{H(n)}$ has transitions $u_{i_{s-1}} \xrightarrow{\sigma_s} u_{i_s}$, for $s = 1, \ldots, t$, we have that $U_{i_{s-1}} \varphi(\sigma_s) \in H(n)U_{i_s}$ and hence $U_{i_{s-1}} \varphi(\sigma_s) U_{i_s}^{-1} \in H(n)$. Since $U_{i_0} = U_0 = I$, we can rewrite $\varphi(w) = \varphi(\sigma_1)\varphi(\sigma_2) \ldots \varphi(\sigma_t)$ as

$$\varphi(w) = (U_{i_0} \varphi(\sigma_1) U_{i_1}^{-1})(U_{i_1} \varphi(\sigma_2) U_{i_2}^{-1}) \cdots (U_{i_{t-1}} \varphi(\sigma_t) U_{i_t}^{-1}) U_{i_t}.$$

If $u_{i_t} = u_0$, that is, if $w$ is accepted by $\mathcal{A}_{H(n)}$, then $i_t = 0$ and $U_{i_t} = U_0 = I \in H(n)$. This implies that $\varphi(w) \in H(n)$ because for all $s = 1, \ldots, t$ we have $U_{i_{s-1}} \varphi(\sigma_s) U_{i_s}^{-1} \in H(n)$. On the other hand, if

7

$\varphi(w) \in H(n)$, then it must be that $U_{i_t} \in H(n)$, which can only happen if $i_t = 0$ and hence $u_{i_t} = u_0$. This means that $w$ is accepted by $\mathcal{A}_{H(n)}$. Therefore, we proved that $L(\mathcal{A}_{H(n)}) = L_{H(n)}$.

$\square$

Now for any automaton $\mathcal{A}$ with alphabet $\Sigma$ we construct two automata $\mathrm{Inv}(\mathcal{A})$ and $\mathcal{F}_D(\mathcal{A})$, where $D$ is a diagonal matrix in the Smith normal form. The automaton $\mathrm{Inv}(\mathcal{A})$ recognizes inverses to the words from $L(\mathcal{A})$, that is:

(1) For every $w \in L(\mathcal{A})$, there exists $w' \in L(\mathrm{Inv}(\mathcal{A}))$ such that $\varphi(w') = \varphi(w)^{-1}$.

(2) For every $w' \in L(\mathrm{Inv}(\mathcal{A}))$, there exists $w \in L(\mathcal{A})$ such that $\varphi(w) = \varphi(w')^{-1}$.

In other words, for any matrix $A \in \mathrm{GL}(2, \mathbb{Z})$, $A \in \varphi(L(\mathcal{A}))$ if and only if $A^{-1} \in \varphi(L(\mathrm{Inv}(\mathcal{A})))$.

**Construction of the automaton** $\mathrm{Inv}(\mathcal{A})$. We will make use of the following equivalences, which are easy to check: $X^{-1} \sim X$, $N^{-1} \sim N$, $S^{-1} \sim S^3$, and $R^{-1} \sim R^5$. Informally speaking, to construct $\mathrm{Inv}(\mathcal{A})$ we want to reverse the transitions in $\mathcal{A}$ and replace the labels by their inverses. More formally, $\mathrm{Inv}(\mathcal{A})$ will have the same states as $\mathcal{A}$ plus some newly added states as explained below. The initial states of $\mathrm{Inv}(\mathcal{A})$ are the final states of $\mathcal{A}$, and the final states of $\mathrm{Inv}(\mathcal{A})$ are the initial states of $\mathcal{A}$. For every transitions of the form $q \xrightarrow{X} q'$ and $q \xrightarrow{N} q'$ in $\mathcal{A}$ we add the transitions $q' \xrightarrow{X} q$ and $q' \xrightarrow{N} q$ to $\mathrm{Inv}(\mathcal{A})$, respectively. Furthermore, for every transitions of the form $q \xrightarrow{S} q'$ and $q \xrightarrow{R} q'$ in $\mathcal{A}$ we add the paths $q' \xrightarrow{S} p_1 \xrightarrow{S} p_2 \xrightarrow{S} q$ and $q' \xrightarrow{R} p_3 \xrightarrow{R} p_4 \xrightarrow{R} p_5 \xrightarrow{R} p_6 \xrightarrow{R} q$ to $\mathrm{Inv}(\mathcal{A})$, respectively, where $p_1, p_2, \ldots, p_6$ are newly added states. It is not hard to verify that $\mathrm{Inv}(\mathcal{A})$ has the desired properties.

The purpose of the automaton $\mathcal{F}_D(\mathcal{A})$ is to recognize conjugations of the words from $L(\mathcal{A})$ with matrix $D$. To explain formally what this means, let $D = \begin{bmatrix} m & 0 \\ 0 & mn \end{bmatrix}$ be a diagonal matrix in the Smith normal form, where $m, n \neq 0$. Recall that by Proposition 11, for any matrix $A \in \mathrm{GL}(2, \mathbb{Z})$, $A^D \in \mathrm{GL}(2, \mathbb{Z})$ if and only if $A \in H(n)$. The automaton $\mathcal{F}_D(\mathcal{A})$ will have the following properties:

(1) For every $w \in L(\mathcal{A}) \cap L_{H(n)}$, there exists $w' \in L(\mathcal{F}_D(\mathcal{A}))$ such that $\varphi(w') = \varphi(w)^D$.

(2) For every $w' \in L(\mathcal{F}_D(\mathcal{A}))$, there exists $w \in L(\mathcal{A}) \cap L_{H(n)}$ such that $\varphi(w)^D = \varphi(w')$.

In other words, we will have

$$\varphi(L(\mathcal{F}_D(\mathcal{A}))) = \{\varphi(w)^D \; : \; \text{where } w \in L(\mathcal{A}) \text{ and } \varphi(w) \in H(n)\}.$$

**Construction of the automaton** $\mathcal{F}_D(\mathcal{A})$. Let $\mathcal{A}$ be a finite automaton in alphabet $\Sigma$ and let $D = \begin{bmatrix} m & 0 \\ 0 & mn \end{bmatrix}$ be a diagonal matrix in the Smith normal form, where $m, n \neq 0$.

Suppose that $\mathcal{A}$ has the states $q_0, q_1, \ldots, q_t$. Recall from the proof of Lemma 13 that the automaton $\mathcal{A}_{H(n)}$, which recognizes $L_{H(n)}$, has the states $u_0, u_1, \ldots, u_k$, where $u_0$ is the only initial and also the only final state. First, we construct an automaton $\mathcal{A}'$ for the language $L(\mathcal{A}) \cap L_{H(n)}$ by taking the direct product of $\mathcal{A}$ and $\mathcal{A}_{H(n)}$. Namely, $\mathcal{A}'$ has the states $(q_i, u_j)$, for $i = 0, \ldots, t$ and $j = 0, \ldots, k$. The initial states of $\mathcal{A}'$ are of the form $(q_i, u_0)$, where $q_i$ is an initial state of $\mathcal{A}$, and the final states of $\mathcal{A}'$ are of the form $(q_i, u_0)$, where $q_i$ is a final state of $\mathcal{A}$. Furthermore, there is a transition from $(q_i, u_j)$ to $(q_{i'}, u_{j'})$ labelled by $\sigma$ if and only if there are transitions $q_i \xrightarrow{\sigma} q_{i'}$ and $u_j \xrightarrow{\sigma} u_{j'}$ in $\mathcal{A}$ and $\mathcal{A}_{H(n)}$, respectively.

Next we replace every transition in $\mathcal{A}'$ by a new path as follows. Let $(q_{i_1}, u_{j_1}) \xrightarrow{\sigma} (q_{i_2}, u_{j_2})$ be a transition in $\mathcal{A}'$. So there must be a transition of the form $u_{j_1} \xrightarrow{\sigma} u_{j_2}$ in $\mathcal{A}_{H(n)}$. By construction of

$\mathcal{A}_{H(n)}$ as described in Lemma 13, we have $U_{j_1}\varphi(\sigma) \in H(n)U_{j_2}$ or, equivalently, $U_{j_1}\varphi(\sigma)U_{j_2}^{-1} \in H(n)$, where $U_0,\ldots,U_k$ are pairwise nonequivalent representatives of the right cosets of $H(n)$ in $\mathrm{GL}(2,\mathbb{Z})$, such that $U_0 = I$. Hence $(U_{j_1}\varphi(\sigma)U_{j_2}^{-1})^D$ is a matrix with integer coefficients, that is, it belongs to $\mathrm{GL}(2,\mathbb{Z})$. Let $w = \sigma_1\ldots\sigma_s \in \Sigma^*$ be a canonical word[1] such that $\varphi(w) = (U_{j_1}\varphi(\sigma)U_{j_2}^{-1})^D$. Then we replace the transition $(q_{i_1}, u_{j_1}) \xrightarrow{\sigma} (q_{i_2}, u_{j_2})$ by a path of the form

$$(q_{i_1}, u_{j_1}) \xrightarrow{\sigma_1} p_1 \xrightarrow{\sigma_2} \cdots \xrightarrow{\sigma_{s-1}} p_{s-1} \xrightarrow{\sigma_s} (q_{i_2}, u_{j_2}),$$

where $p_1,\ldots,p_{s-1}$ are new states added to $\mathcal{A}'$. Let $\mathcal{F}_D(\mathcal{A})$ be an automaton that we obtain after applying the above procedure to $\mathcal{A}'$.

To prove the first property of $\mathcal{F}_D(\mathcal{A})$, take any $w = \sigma_1\ldots\sigma_s \in L(\mathcal{A}) \cap L_{H(n)}$. Then there must be an accepting run $\rho = (q_{i_0}, u_{j_0})(q_{i_1}, u_{j_1})\ldots(q_{i_s}, u_{j_s})$ of $\mathcal{A}'$ on $w$. For every transition $(q_{i_{r-1}}, u_{j_{r-1}}) \xrightarrow{\sigma_r} (q_{i_r}, u_{j_r})$ in the run $\rho$, there is a path in $\mathcal{F}_D(\mathcal{A})$ from $(q_{i_{r-1}}, u_{j_{r-1}})$ to $(q_{i_r}, u_{j_r})$ labelled by a word $w_r$ such that $\varphi(w_r) = (U_{j_{r-1}}\varphi(\sigma_r)U_{j_r}^{-1})^D$, where $U_{j_{r-1}}\varphi(\sigma_r)U_{j_r}^{-1} \in H(n)$. If we let $w' = w_1\ldots w_s$, then $w'$ is accepted by $\mathcal{F}_D(\mathcal{A})$. To prove that $\varphi(w') = \varphi(w)^D$, we first note that since $w \in L_{H(n)}$, the run $u_{j_0}u_{j_1}\ldots u_{j_s}$ is an accepting run of $\mathcal{A}_{H(n)}$ on $w$, and in particular $j_0 = j_s = 0$. Since $U_{j_0} = U_{j_s} = U_0 = I$, we can rewrite $\varphi(w)$ as

$$\varphi(w) = U_{j_0}^{-1}(U_{j_0}\varphi(\sigma_1)U_{j_1}^{-1})(U_{j_1}\varphi(\sigma_2)U_{j_2}^{-1})\cdots(U_{j_{s-1}}\varphi(\sigma_s)U_{j_s}^{-1})U_{j_s}$$
$$= (U_{j_0}\varphi(\sigma_1)U_{j_1}^{-1})(U_{j_1}\varphi(\sigma_2)U_{j_2}^{-1})\cdots(U_{j_{s-1}}\varphi(\sigma_s)U_{j_s}^{-1}) \quad \text{(here we used that } U_{j_0} = U_{j_s} = I\text{)}.$$

Recall that for each $r = 1,\ldots,s$, we have $\varphi(w_r) = (U_{j_{r-1}}\varphi(\sigma_r)U_{j_r}^{-1})^D$. Therefore,

$$\varphi(w)^D = (U_{j_0}\varphi(\sigma_1)U_{j_1}^{-1})^D(U_{j_1}\varphi(\sigma_2)U_{j_2}^{-1})^D\cdots(U_{j_{s-1}}\varphi(\sigma_s)U_{j_s}^{-1})^D$$
$$= \varphi(w_1)\varphi(w_2)\cdots\varphi(w_s) = \varphi(w').$$

This proves the first property of $\mathcal{F}_D(\mathcal{A})$.

To prove the second property of $\mathcal{F}_D(\mathcal{A})$, take any $w' \in L(\mathcal{F}_D(\mathcal{A}))$ and consider an accepting run of $\mathcal{F}_D(\mathcal{A})$ on $w'$. This run passes through some states of the form $(q_i, u_j)$, that are present in both $\mathcal{F}_D(\mathcal{A})$ and $\mathcal{A}'$, and some new states that exist only in $\mathcal{F}_D(\mathcal{A})$. Let $(q_{i_0}, u_{j_0}), (q_{i_1}, u_{j_1}),\ldots,(q_{i_s}, u_{j_s})$ be the subsequence of the states of the first type which appear in the accepting run of $\mathcal{F}_D(\mathcal{A})$. They naturally divide $w'$ into subwords $w' = w_1w_2\ldots w_s$, where $w_r$ is a label of the path from $(q_{i_{r-1}}, u_{j_{r-1}})$ to $(q_{i_r}, u_{j_r})$ for $r = 1,\ldots,s$. By construction of $\mathcal{F}_D(\mathcal{A})$, for each $r = 1,\ldots,s$, there exists a symbol $\sigma_r \in \Sigma$ for which there is a transition $(q_{i_{r-1}}, u_{j_{r-1}}) \xrightarrow{\sigma_r} (q_{i_r}, u_{j_r})$ in $\mathcal{A}'$ and, moreover, $U_{j_{r-1}}\varphi(\sigma_r)U_{j_r}^{-1} \in H(n)$ and $\varphi(w_r) = (U_{j_{r-1}}\varphi(\sigma_r)U_{j_r}^{-1})^D$.

Let $w = \sigma_1\sigma_2\ldots\sigma_s$, then $q_{i_0}q_{i_1}\ldots q_{i_s}$ will be an accepting run of $\mathcal{A}$ on $w$ and $u_{j_0}u_{j_1}\ldots u_{j_s}$ will be an accepting run of $\mathcal{A}_{H(n)}$ on $w$. Thus $w \in L(\mathcal{A}) \cap L_{H(n)}$. Furthermore, we have $u_{j_0} = u_{j_s} = u_0$ and hence $U_{j_0} = U_{j_s} = I$. So we can rewrite $\varphi(w)$ as

$$\varphi(w) = U_{j_0}^{-1}(U_{j_0}\varphi(\sigma_1)U_{j_1}^{-1})(U_{j_1}\varphi(\sigma_2)U_{j_2}^{-1})\cdots(U_{j_{s-1}}\varphi(\sigma_s)U_{j_s}^{-1})U_{j_s}$$
$$= (U_{j_0}\varphi(\sigma_1)U_{j_1}^{-1})(U_{j_1}\varphi(\sigma_2)U_{j_2}^{-1})\cdots(U_{j_{s-1}}\varphi(\sigma_s)U_{j_s}^{-1}).$$

From this we obtain the following equalities

$$\varphi(w)^D = (U_{j_0}\varphi(\sigma_1)U_{j_1}^{-1})^D(U_{j_1}\varphi(\sigma_2)U_{j_2}^{-1})^D\cdots(U_{j_{s-1}}\varphi(\sigma_s)U_{j_s}^{-1})^D$$
$$= \varphi(w_1)\varphi(w_2)\cdots\varphi(w_s) = \varphi(w').$$

This proves the second property of $\mathcal{F}_D(\mathcal{A})$.

---

[1] Actually, we can take $w$ to be any word that represents $(U_{j_1}\varphi(\sigma)U_{j_2}^{-1})^D$. The fact that it is canonical is not important for our construction.

**Proposition 14.** *Let $D$ be a diagonal matrix in the Smith normal form and let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two regular subsets of $\mathrm{GL}(2, \mathbb{Z})$. Then it is decidable whether there exist matrices $A_1 \in \mathcal{S}_1$ and $A_2 \in \mathcal{S}_2$ such that $A_1 D A_2 = D$.*

*Proof.* Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be finite automata such that $\mathcal{S}_1 = L(\mathcal{A}_1)$ and $\mathcal{S}_2 = L(\mathcal{A}_2)$, respectively. We will show that the equation $A_1 D A_2 = D$ has a solution for some $A_1 \in \mathcal{S}_1$ and $A_2 \in \mathcal{S}_2$ if and only if $L(\mathrm{Can}(\mathcal{F}_D(\mathcal{A}_1))) \cap L(\mathrm{Can}(\mathrm{Inv}(\mathcal{A}_2))) \neq \emptyset^2$.

First, suppose there exist matrices $A_1 \in \mathcal{S}_1$ and $A_2 \in \mathcal{S}_2$ such that $A_1 D A_2 = D$. Let $w_1 \in L(\mathcal{A}_1)$ and $w_2 \in L(\mathcal{A}_2)$ be such that $\varphi(w_1) = A_1$ and $\varphi(w_2) = A_2$, respectively. Also let $D = \begin{bmatrix} m & 0 \\ 0 & mn \end{bmatrix}$ for some $m, n \neq 0$. We can rewrite the equation $A_1 D A_2 = D$ as $A_2^{-1} = A_1^D$. From this we can see that the matrix $A_1^D$ must have integer coefficients. Hence, by Proposition 11, $A_1 \in H(n)$ and $w_1 \in L_{H(n)}$. Since $w_1 \in L(\mathcal{A}_1) \cap L_{H(n)}$, there exists $w_1' \in L(\mathcal{F}_D(\mathcal{A}_1))$ such that $\varphi(w_1') = \varphi(w_1)^D = A_1^D$. Also there is $w_2' \in L(\mathrm{Inv}(\mathcal{A}_2))$ such that $\varphi(w_2') = \varphi(w_2)^{-1} = A_2^{-1}$. Since $A_2^{-1} = A_1^D$, we have $\varphi(w_1') = \varphi(w_2')$. In other words, $w_1'$ and $w_2'$ are equivalent. Let $w$ be a canonical word such that $w \sim w_1' \sim w_2'$, then $w \in L(\mathrm{Can}(\mathcal{F}_D(\mathcal{A}_1))) \cap L(\mathrm{Can}(\mathrm{Inv}(\mathcal{A}_2)))$.

Now suppose there is a word $w$ that belongs to $L(\mathrm{Can}(\mathcal{F}_D(\mathcal{A}_1))) \cap L(\mathrm{Can}(\mathrm{Inv}(\mathcal{A}_2)))$. Hence there are words $w_1'$ and $w_2'$ such that $w \sim w_1' \sim w_2'$ and $w_1' \in L(\mathcal{F}_D(\mathcal{A}_1))$ and $w_2' \in L(\mathrm{Inv}(\mathcal{A}_2))$. Therefore, there exists $w_1 \in L(\mathcal{A}_1) \cap L_{H(n)}$ such that $\varphi(w_1)^D = \varphi(w_1')$. Also there exists $w_2 \in L(\mathcal{A}_2)$ such that $\varphi(w_2)^{-1} = \varphi(w_2')$. Let $A_1 = \varphi(w_1)$ and $A_2 = \varphi(w_2)$. Then we have $A_1^D = \varphi(w_1)^D = \varphi(w_1') = \varphi(w_2') = \varphi(w_2)^{-1} = A_2^{-1}$, which is equivalent to $A_1 D A_2 = D$. Moreover, since $w_1 \in L(\mathcal{A}_1)$ and $w_2 \in L(\mathcal{A}_2)$, we have that $A_1 \in \mathcal{S}_1$ and $A_2 \in \mathcal{S}_2$.

The proof of the proposition now follows from the facts that the intersection of two regular languages is regular and that the emptiness problem for regular languages is decidable. $\square$

**Corollary 15.** *Let $M_1$ and $M_2$ be nonsingular matrices from $\mathbb{Z}^{2 \times 2}$ and let $\mathcal{S}_1$ and $\mathcal{S}_2$ be regular subsets of $\mathrm{GL}(2, \mathbb{Z})$. Then it is decidable whether there exist matrices $A_1 \in \mathcal{S}_1$ and $A_2 \in \mathcal{S}_2$ such that $A_1 M_1 A_2 = M_2$.*

*Proof.* Let $D_1$ and $D_2$ be the Smith normal forms of $M_1$ and $M_2$, respectively, that is, $M_1 = E_1 D_1 F_1$ and $M_2 = E_2 D_2 F_2$ for some $E_1, F_1, E_2, F_2 \in \mathrm{GL}(2, \mathbb{Z})$. Without loss of generality, we can assume that $D_1$ and $D_2$ have strictly positive diagonal coefficients. Note that if the equation $A_1 M_1 A_2 = M_2$ has a solution for some $A_1, A_2 \in \mathrm{GL}(2, \mathbb{Z})$, then, by Theorem 9, $M_1$ and $M_2$ must have the same Smith normal form. Therefore, if $D_1 \neq D_2$, then the equation does not have a solution.

So suppose that $D = D_1 = D_2$ is the Smith normal form of $M_1$ and $M_2$. Then $A_1 M_1 A_2 = M_2$ is equivalent to $A_1(E_1 D F_1) A_2 = E_2 D F_2$, which we can rewrite as $(E_2^{-1} A_1 E_1) D (F_1 A_2 F_2^{-1}) = D$. Let $\mathcal{S}_1' = \{E_2^{-1} A E_1 : A \in \mathcal{S}_1\}$ and $\mathcal{S}_2' = \{F_1 A F_2^{-1} : A \in \mathcal{S}_2\}$. Then $\mathcal{S}_1'$ and $\mathcal{S}_2'$ are regular subsets of $\mathrm{GL}(2, \mathbb{Z})$ because $E_1, F_1, E_2$, and $F_2$ are some fixed matrices. Now it is not hard to see that the equation $A_1 M_1 A_2 = M_2$ has a solution $A_1, A_2$ such that $A_1 \in \mathcal{S}_1$ and $A_1 \in \mathcal{S}_2$ if and only if the equation $A_1' D A_2' = D$ has a solution $A_1', A_2'$ such that $A_1' \in \mathcal{S}_1'$ and $A_2' \in \mathcal{S}_2'$. By Proposition 14, this problem is decidable. $\square$

### 3.3 General case: $A_1 M_1 \ldots A_{t-1} M_{t-1} A_t = M_t$

To prove an analog of Corollary 15 in the general case, we will extend the construction of the automaton $\mathcal{F}_D(\mathcal{A})$ to build an automaton $\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t)$ (where $\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}$ are finite automata in alphabet $\Sigma$ and $M_1, \ldots, M_{t-1}, M_t$ are nonsingular matrices from $\mathbb{Z}^{2 \times 2}$) which will have the following properties:

---
[2]We remind that the construction of the automaton $\mathrm{Can}(\mathcal{A})$ is described in Section 4.1 of the Appendix.

(1) If $w_1 \in L(\mathcal{A}_1), \ldots, w_{t-1} \in L(\mathcal{A}_{t-1})$ and there is a matrix $A \in \mathrm{GL}(2, \mathbb{Z})$ which satisfies the equation $\varphi(w_1)M_1 \ldots \varphi(w_{t-1})M_{t-1}A = M_t$, then there is $w \in L(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t))$ such that $\varphi(w_1)M_1 \ldots \varphi(w_{t-1})M_{t-1}\varphi(w)^{-1} = M_t$ (and hence $A = \varphi(w)^{-1}$).

(2) If $w \in L(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t))$, then there are $w_1 \in L(\mathcal{A}_1), \ldots, w_{t-1} \in L(\mathcal{A}_{t-1})$ such that $\varphi(w_1)M_1 \ldots \varphi(w_{t-1})M_{t-1}\varphi(w)^{-1} = M_t$.

**Construction of $\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t)$.** The construction will be done by induction on $t$. We will use the following notations: If $\mathcal{A}_1$ and $\mathcal{A}_2$ are finite automata in alphabet $\Sigma$, then $\mathcal{A}_1 \cdot \mathcal{A}_2$ denotes the concatenation of $\mathcal{A}_1$ and $\mathcal{A}_2$. If $\mathcal{A}$ is an automaton and $w \in \Sigma^*$, then $\mathcal{A} \cdot w$ denotes an automaton that recognizes the language $L(\mathcal{A}) \cdot \{w\} = \{uw : u \in L(\mathcal{A})\}$. Similarly, $w \cdot \mathcal{A}$ is an automaton that recognizes $\{w\} \cdot L(\mathcal{A}) = \{wu : u \in L(\mathcal{A})\}$.

First, we construct an automaton $\mathcal{F}(\mathcal{A}_1, M_1; M_2)$, which will serve as a base for induction. Let $D_1$ and $D_2$ be diagonal matrices with nonnegative coefficients which are equal to the Smith normal forms of $M_1$ and $M_2$, respectively. If $D_1 \neq D_2$, then define $\mathcal{F}(\mathcal{A}_1, M_1; M_2)$ to be an automaton that accepts the empty language. Otherwise, let $D = D_1 = D_2$ be the common Smith normal form of $M_1$ and $M_2$, and suppose $M_1 = E_1 D F_1$ and $M_2 = E_2 D F_2$ for some matrices $E_1, F_1, E_2, F_2 \in \mathrm{GL}(2, \mathbb{Z})$. Let $w(E_1)$, $w(F_1)$, $w(E_2^{-1})$ and $w(F_2^{-1})$ be canonical words that represent the matrices $E_1, F_1, E_2^{-1}$ and $F_2^{-1}$, respectively, and define $\mathcal{F}(\mathcal{A}_1, M_1; M_2)$ to be the following automaton

$$\mathcal{F}(\mathcal{A}_1, M_1; M_2) = w(F_2^{-1}) \cdot \mathcal{F}_D\big(w(E_2^{-1}) \cdot \mathcal{A}_1 \cdot w(E_1)\big) \cdot w(F_1).$$

The following proposition states that the automaton $\mathcal{F}(\mathcal{A}_1, M_1; M_2)$ indeed satisfies the desired properties.

**Proposition 16.** *Let $\mathcal{A}_1$ be a finite automaton in alphabet $\Sigma$, and let $M_1$ and $M_2$ be nonsingular matrices from $\mathbb{Z}^{2\times 2}$. Then the automaton $\mathcal{F}(\mathcal{A}_1, M_1; M_2)$ has the following properties:*

*(1) If $w_1 \in L(\mathcal{A}_1)$ and there is a matrix $A \in \mathrm{GL}(2, \mathbb{Z})$ which satisfies the equation $\varphi(w_1)M_1 A = M_2$, then there is $w \in L(\mathcal{F}(\mathcal{A}_1, M_1; M_2))$ such that $\varphi(w_1)M_1\varphi(w)^{-1} = M_2$ (and hence $A = \varphi(w)^{-1}$).*

*(2) If $w \in L(\mathcal{F}(\mathcal{A}_1, M_1; M_2))$, then there is $w_1 \in L(\mathcal{A}_1)$ such that $\varphi(w_1)M_1\varphi(w)^{-1} = M_2$.*

*Proof.* Note that if $M_1$ and $M_2$ have different Smith normal forms, then by the uniqueness part of Theorem 9 the equation $A_1 M_1 A_2 = M_2$ cannot have a solution $A_1, A_2 \in \mathrm{GL}(2, \mathbb{Z})$. Therefore, in this case both properties of $\mathcal{F}(\mathcal{A}_1, M_1; M_2)$ are trivially satisfied. Now suppose that $D = \begin{bmatrix} m & 0 \\ 0 & mn \end{bmatrix}$ is the common Smith normal form of $M_1$ and $M_2$ and let $E_1, F_1, E_2, F_2$ be matrices form $\mathrm{GL}(2, \mathbb{Z})$ such that $M_1 = E_1 D F_1$ and $M_2 = E_2 D F_2$.

To see that the first property of $\mathcal{F}(\mathcal{A}_1, M_1; M_2)$ holds, let's take any $w_1 \in L(\mathcal{A}_1)$ for which there is a matrix $A \in \mathrm{GL}(2, \mathbb{Z})$ that satisfies the equation $\varphi(w_1)M_1 A = M_2$. Hence we have that $\varphi(w_1)E_1 D F_1 A = E_2 D F_2$, which is equivalent to $F_2^{-1}(E_2^{-1}\varphi(w_1)E_1)^D F_1 = A^{-1}$. Because $F_2^{-1}$, $F_1$, and $A^{-1}$ are matrices from $\mathrm{GL}(2, \mathbb{Z})$, we conclude that $(E_2^{-1}\varphi(w_1)E_1)^D$ is in $\mathrm{GL}(2, \mathbb{Z})$. Then, by Proposition 11, we have $E_2^{-1}\varphi(w_1)E_1 \in H(n)$ or, equivalently, $w(E_2^{-1}) \cdot w_1 \cdot w(E_1) \in L_{H(n)}$. By the first property of the construction $\mathcal{F}_D$, there exists $w' \in L\big(\mathcal{F}_D\big(w(E_2^{-1}) \cdot \mathcal{A}_1 \cdot w(E_1)\big)\big)$ such that $\varphi(w') = \varphi\big(w(E_2^{-1}) \cdot w_1 \cdot w(E_1)\big)^D = (E_2^{-1}\varphi(w_1)E_1)^D$. Let $w = w(F_2^{-1}) \cdot w' \cdot w(F_1)$. Then $w$ is in $L(\mathcal{F}(\mathcal{A}_1, M_1; M_2))$. Moreover, $\varphi(w) = F_2^{-1}\varphi(w')F_1 = F_2^{-1}(E_2^{-1}\varphi(w_1)E_1)^D F_1$. The last equation is equivalent to $\varphi(w_1)E_1 D F_1\varphi(w)^{-1} = E_2 D F_2$, which is the same as $\varphi(w_1)M_1\varphi(w)^{-1} = M_2$. Hence the first property holds.

Now we prove the second property of $\mathcal{F}(\mathcal{A}_1, M_1; M_2)$. Let's take any $w \in L(\mathcal{F}(\mathcal{A}_1, M_1; M_2))$. Then there exists $w' \in L\big(\mathcal{F}_D\big(w(E_2^{-1}) \cdot \mathcal{A}_1 \cdot w(E_1)\big)\big)$ such that $w = w(F_2^{-1}) \cdot w' \cdot w(F_1)$. By the second

property of the construction $\mathcal{F}_D$, there exists $w_1 \in L(\mathcal{A}_1)$ such that $w(E_2^{-1}) \cdot w_1 \cdot w(E_1) \in L_{H(n)}$ and $\varphi(w') = \varphi\big(w(E_2^{-1}) \cdot w_1 \cdot w(E_1)\big)^D$. The last two conditions are equivalent to the facts that $E_2^{-1}\varphi(w_1)E_1 \in H(n)$ and $\varphi(w') = (E_2^{-1}\varphi(w_1)E_1)^D$. From the equation $w = w(F_2^{-1}) \cdot w' \cdot w(F_1)$ we have that $\varphi(w) = F_2^{-1}\varphi(w')F_1$. Therefore, $\varphi(w) = F_2^{-1}(E_2^{-1}\varphi(w_1)E_1)^D F_1$. The last equation is equivalent to $\varphi(w_1)E_1DF_1\varphi(w)^{-1} = E_2DF_2$, which is the same as $\varphi(w_1)M_1\varphi(w)^{-1} = M_2$. This proves the second property.

$\square$

We now explain how to construct an automaton $\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t)$. For convenience the description of this construction is enclosed in the following proposition.

**Proposition 17.** *Let $\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}$ be finite automata in alphabet $\Sigma$, and let $M_1, \ldots, M_{t-1}, M_t$ be nonsingular matrices from $\mathbb{Z}^{2\times 2}$. Then there is an automaton $\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t)$ which has the following properties:*

(1) *If $w_1 \in L(\mathcal{A}_1), \ldots, w_{t-1} \in L(\mathcal{A}_{t-1})$ and there is a matrix $A \in \mathrm{GL}(2, \mathbb{Z})$ which satisfies the equation $\varphi(w_1)M_1 \ldots \varphi(w_{t-1})M_{t-1}A = M_t$, then there is $w \in L(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t))$ such that $\varphi(w_1)M_1 \ldots \varphi(w_{t-1})M_{t-1}\varphi(w)^{-1} = M_t$ (and hence $A = \varphi(w)^{-1}$).*

(2) *If $w \in L(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t))$, then there are $w_1 \in L(\mathcal{A}_1), \ldots, w_{t-1} \in L(\mathcal{A}_{t-1})$ such that $\varphi(w_1)M_1 \ldots \varphi(w_{t-1})M_{t-1}\varphi(w)^{-1} = M_t$.*

The following lemma will play an important role in the proof of the inductive step in Proposition 17. Informally speaking, it states that when we consider all possible Smith normal forms $UDV$ for a fixed $D$, we can assume that $U$ comes from a finite set of matrices.

**Lemma 18.** *Let $D = \begin{bmatrix} m & 0 \\ 0 & mn \end{bmatrix}$ be a diagonal matrix in the Smith normal form and let $U_0, \ldots, U_k$ be representatives of the right cosets of $H(n)$ in $\mathrm{GL}(2, \mathbb{Z})$. Then*

$$\{UDV \; : \; U, V \in \mathrm{GL}(2, \mathbb{Z})\} = \bigcup_{i=0}^{k} \{U_iDV \; : \; V \in \mathrm{GL}(2, \mathbb{Z})\}.$$

*Proof.* Consider a matrix $M = UDV$ for some $U, V \in \mathrm{GL}(2, \mathbb{Z})$ and choose $i$ such that $U \in U_iH(n)$. In this case we have that $U_i^{-1}U \in H(n)$, and thus $(U_i^{-1}U)^D$ belongs to $\mathrm{GL}(2, \mathbb{Z})$ by Proposition 11. Let $V' = (U_i^{-1}U)^D V \in \mathrm{GL}(2, \mathbb{Z})$. Then we have an equality $M = UDV = U_iDV'$, and hence $M \in \{U_iDV \; : \; V \in \mathrm{GL}(2, \mathbb{Z})\}$. The inclusion in the other direction is obvious.

$\square$

*Proof of Proposition 17.* The proof will be done by induction of $t$. The base case when $t = 2$ follows from Proposition 16. Now suppose the proposition holds for $t - 1$, and thus we have a construction for the automata of the form $\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-2}, M_1, \ldots, M_{t-2}; M_{t-1})$ which satisfy the properties (1) and (2) above. Using these automata, we will show how to construct an automaton $\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t)$.

Let $D_{t-1} = \begin{bmatrix} m & 0 \\ 0 & mn \end{bmatrix}$ be equal to the Smith normal form of the matrix $M_{t-1}$ and let $U_0, \ldots, U_k$ be representatives of the right cosets of $H(n)$, which can be computed by Theorem 12. Then we define $\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t)$ to be an automaton that recognizes the following union of regular languages

$$\bigcup_{i=0}^{k} L\Big(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-3}, \mathcal{A}_{t-2}, M_1, \ldots, M_{t-3}, M_{t-2}U_iD_{t-1}; M_t) \cdot \mathcal{F}(\mathcal{A}_{t-1}, M_{t-1}; U_iD_{t-1})\Big).$$

To see that the first property holds for $\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t)$, let's take $w_1 \in L(\mathcal{A}_1), \ldots, w_{t-1} \in L(\mathcal{A}_{t-1})$, and suppose there is a matrix $A \in \mathrm{GL}(2, \mathbb{Z})$ which satisfies the equation

$$\varphi(w_1)M_1 \ldots \varphi(w_{t-1})M_{t-1}A = M_t.$$

By Lemma 18, there is $i \in \{0, \ldots, k\}$ and $V \in \mathrm{GL}(2, \mathbb{Z})$ such that $\varphi(w_{t-1})M_{t-1}A = U_i D_{t-1} V$. So the above equation is equivalent to the following system of equations

$$\varphi(w_1)M_1 \ldots \varphi(w_{t-2})M_{t-2}U_i D_{t-1}V = M_t,$$
$$\varphi(w_{t-1})M_{t-1}AV^{-1} = U_i D_{t-1}.$$

Since $V \in \mathrm{GL}(2, \mathbb{Z})$, by the inductive hypothesis there is a word $u$ such that

$$u \in L\Big(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-3}, \mathcal{A}_{t-2}, M_1, \ldots, M_{t-3}, M_{t-2}U_i D_{t-1}; M_t)\Big)$$

and

$$\varphi(w_1)M_1 \ldots \varphi(w_{t-2})M_{t-2}U_i D_{t-1}\varphi(u)^{-1} = M_t.$$

Moreover, since $AV^{-1} \in \mathrm{GL}(2, \mathbb{Z})$, by Proposition 16, there is a word $v \in L(\mathcal{F}(\mathcal{A}_{t-1}, M_{t-1}; U_i D_{t-1}))$ such that $\varphi(w_{t-1})M_{t-1}\varphi(v)^{-1} = U_i D_{t-1}$. Combining the last two equations together we obtain that

$$\varphi(w_1)M_1 \ldots \varphi(w_{t-1})M_{t-1}\varphi(v)^{-1}\varphi(u)^{-1} = M_t$$

or, equivalently,

$$\varphi(w_1)M_1 \ldots \varphi(w_{t-1})M_{t-1}\varphi(uv)^{-1} = M_t.$$

Note that

$$uv \in L\Big(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-3}, \mathcal{A}_{t-2}, M_1, \ldots, M_{t-3}, M_{t-2}U_i D_{t-1}; M_t) \cdot \mathcal{F}(\mathcal{A}_{t-1}, M_{t-1}; U_i D_{t-1})\Big)$$

and hence $uv \in L(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t))$. Therefore, property (1) holds.

To show the second property, let's take $w \in L(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t))$. Then there is $i \in \{0, \ldots, k\}$ such that

$$w \in L\Big(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-3}, \mathcal{A}_{t-2}, M_1, \ldots, M_{t-3}, M_{t-2}U_i D_{t-1}; M_t) \cdot \mathcal{F}(\mathcal{A}_{t-1}, M_{t-1}; U_i D_{t-1})\Big).$$

Therefore, there are words $u$ and $v$ such that

$$u \in L\Big(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-3}, \mathcal{A}_{t-2}, M_1, \ldots, M_{t-3}, M_{t-2}U_i D_{t-1}; M_t)\Big).$$

and $v \in L(\mathcal{F}(\mathcal{A}_{t-1}, M_{t-1}; U_i D_{t-1}))$. By Proposition 16, there is $w_{t-1} \in L(\mathcal{A}_{t-1})$ such that

$$\varphi(w_{t-1})M_{t-1}\varphi(v)^{-1} = U_i D_{t-1}.$$

Furthermore, by the inductive hypothesis, there are $w_1 \in L(\mathcal{A}_1), \ldots, w_{t-2} \in L(\mathcal{A}_{t-2})$ such that

$$\varphi(w_1)M_1 \ldots \varphi(w_{t-2})M_{t-2}U_i D_{t-1}\varphi(u)^{-1} = M_t.$$

Combining the last two equation together we obtain

$$\varphi(w_1)M_1 \ldots \varphi(w_{t-1})M_{t-1}\varphi(v)^{-1}\varphi(u)^{-1} = M_t.$$

Note that $\varphi(w)^{-1} = \varphi(v)^{-1}\varphi(u)^{-1}$, and hence we have $\varphi(w_1)M_1 \ldots \varphi(w_{t-1})M_{t-1}\varphi(w)^{-1} = M_t$. Therefore, property (2) holds.

$\square$

**Theorem 19.** *Let $M_1, \ldots, M_t$ be nonsingular matrices from $\mathbb{Z}^{2\times2}$ and let $\mathcal{S}_1, \ldots, \mathcal{S}_t$ be regular subsets of $\mathrm{GL}(2,\mathbb{Z})$. Then it is decidable whether there exist matrices $A_1 \in \mathcal{S}_1, \ldots, A_t \in \mathcal{S}_t$ such that $A_1 M_1 \ldots A_{t-1} M_{t-1} A_t = M_t$.*

*Proof.* Let $\mathcal{A}_1, \ldots, \mathcal{A}_t$ be finite automata such that $\mathcal{S}_i = \varphi(L(\mathcal{A}_i))$, for each $i = 1, \ldots, t$. Now consider an automaton $\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t)$ which was constructed in the proof of Proposition 17. We will show the following equivalence: there exist matrices $A_1 \in \mathcal{S}_1, \ldots, A_t \in \mathcal{S}_t$ that satisfy the equation $A_1 M_1 \ldots A_{t-1} M_{t-1} A_t = M_t$ if and only if

$$L\big(\mathrm{Can}(\mathrm{Inv}(\mathcal{A}_t))\big) \ \cap \ L\big(\mathrm{Can}(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t))\big) \neq \emptyset.$$

The statement of the theorem then follows from the decidability of the emptiness problem for regular languages.

First, suppose there are matrices $A_1 \in \mathcal{S}_1, \ldots, A_t \in \mathcal{S}_t$ such that $A_1 M_1 \ldots A_{t-1} M_{t-1} A_t = M_t$. Then there are words $w_1 \in L(\mathcal{A}_1), \ldots, w_t \in L(\mathcal{A}_t)$ such that

$$\varphi(w_1) M_1 \ldots \varphi(w_{t-1}) M_{t-1} \varphi(w_t) = M_t.$$

By property (1) of Proposition 17, there is a word $u \in L(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t))$ such that

$$\varphi(w_1) M_1 \ldots \varphi(w_{t-1}) M_{t-1} \varphi(u)^{-1} = M_t.$$

In particular, we have $\varphi(w_t) = \varphi(u)^{-1}$. Furthermore, by the construction of $\mathrm{Inv}(\mathcal{A}_t)$, there is a word $v \in L(\mathrm{Inv}(\mathcal{A}_t))$ such that $\varphi(v) = \varphi(w_t)^{-1}$. So we have $\varphi(u) = \varphi(w_t)^{-1} = \varphi(v)$, that is, $u \sim v$. Let $w$ be the canonical word that is equivalent to $u$ and $v$. Then

$$w \in L\big(\mathrm{Can}(\mathrm{Inv}(\mathcal{A}_t))\big) \ \cap \ L\big(\mathrm{Can}(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t))\big).$$

On the other hand, suppose there is a word $w$ such that

$$w \in L\big(\mathrm{Can}(\mathrm{Inv}(\mathcal{A}_t))\big) \ \cap \ L\big(\mathrm{Can}(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t))\big).$$

Then there are words $u$ and $v$ such that $u \sim v \sim w$ and $u \in L(\mathcal{F}(\mathcal{A}_1, \ldots, \mathcal{A}_{t-1}, M_1, \ldots, M_{t-1}; M_t))$ and $v \in L(\mathrm{Inv}(\mathcal{A}_t))$. Hence there is $w_t \in L(\mathcal{A}_t)$ such that $\varphi(w_t) = \varphi(v)^{-1}$. Also by property (2) of Proposition 17, there are words $w_1 \in L(\mathcal{A}_1), \ldots, w_{t-1} \in L(\mathcal{A}_{t-1})$ such that

$$\varphi(w_1) M_1 \ldots \varphi(w_{t-1}) M_{t-1} \varphi(u)^{-1} = M_t.$$

Since $v \sim u$, we have that $\varphi(u)^{-1} = \varphi(v)^{-1} = \varphi(w_t)$. Therefore, the above equation is equivalent to

$$\varphi(w_1) M_1 \ldots \varphi(w_{t-1}) M_{t-1} \varphi(w_t) = M_t.$$

Now if we let $A_1 = \varphi(w_1), \ldots, A_t = \varphi(w_t)$, then for each $i = 1, \ldots, t$ the matrix $A_i$ belongs to $\mathcal{S}_i$, and hence we have $A_1 M_1 \ldots A_{t-1} M_{t-1} A_t = M_t$. $\qquad\square$

# 4 Appendix

## 4.1 Construction of the automaton $\mathrm{Can}(\mathcal{A})$

Let $\mathcal{A}$ be a finite automaton with alphabet $\Sigma$. We will construct a new automaton $\mathrm{Can}(\mathcal{A})$ such that the language of $\mathrm{Can}(\mathcal{A})$ contains only canonical words and $\mathrm{Can}(\mathcal{A}) \sim \mathcal{A}$, that is, $\varphi(L(\mathrm{Can}(\mathcal{A}))) = \varphi(L(\mathcal{A}))$. In order to do this, we will define a sequence of transformations called Red, $F_N$ and $F_X$ which will have the following properties:

- $\text{Can}(\mathcal{A}) = F_X \circ \text{Red} \circ F_N(\mathcal{A})$,

- $L(F_N(\mathcal{A})) \subseteq \{X, S, R\}^* \cup N\{X, S, R\}^*$, that is, $F_N(\mathcal{A})$ accepts only those words that have at most one occurrence of $N$ which may appear only in the first position,

- $L(\text{Red} \circ F_N(\mathcal{A})) \subseteq \{X, S, R\}^* \cup N\{X, S, R\}^*$ and, moreover, $\text{Red} \circ F_N(\mathcal{A})$ accepts only those words that do not contain subwords of the form $XX$, $SX^\alpha S$ and $RX^{\alpha_1} R X^{\alpha_2} R$ for any $\alpha, \alpha_1, \alpha_2 \in \{0, 1\}$,

- $F_X \circ \text{Red} \circ F_N(\mathcal{A})$ accepts only canonical words,

- finally, we will have the equivalences $\mathcal{A} \sim F_N(\mathcal{A}) \sim \text{Red} \circ F_N(\mathcal{A}) \sim F_X \circ \text{Red} \circ F_N(\mathcal{A}) = \text{Can}(\mathcal{A})$.

We now describe each of these transformations in detail.

**Transformation $F_N$.** We will make use of the following equivalences which can be easily verified: $X \sim NXN$, $S \sim NXSN$, and $R \sim NSR^2SN$.

First, for every transition $q \xrightarrow{X} q'$ which appears in $\mathcal{A}$, we add new states $p_1$, $p_2$ and a new path of the form $q \xrightarrow{N} p_1 \xrightarrow{X} p_2 \xrightarrow{N} q'$. Note that since $X \sim NXN$, the addition of such paths produces an equivalent automaton. Similarly, for any transition $q \xrightarrow{S} q'$ in $\mathcal{A}$, we add new states $p_1$, $p_2$, $p_3$ and a path $q \xrightarrow{N} p_1 \xrightarrow{X} p_2 \xrightarrow{S} p_3 \xrightarrow{N} q'$. Finally, for any transition $q \xrightarrow{R} q'$ in $\mathcal{A}$, we add new states $p_1$, $p_2$, $p_3$, $p_4$, $p_5$ and a path $q \xrightarrow{N} p_1 \xrightarrow{S} p_2 \xrightarrow{R} p_3 \xrightarrow{R} p_4 \xrightarrow{S} p_5 \xrightarrow{N} q'$. Again, the addition of such paths produces an equivalent automaton. Let us call this automaton $\mathcal{A}_1$.

Now for every pair of states $q$, $q'$ in $\mathcal{A}_1$, which are connected by a path labelled with $NN$, we add an $\varepsilon$-transition $q \xrightarrow{\varepsilon} q'$. We repeat this procedure iteratively until no new $\varepsilon$-transitions of this type can be added. Let $\mathcal{A}_2$ be the resulting automaton. Note that since $NN$ is equivalent to the empty word, which represents the identity matrix $I$, the automaton $\mathcal{A}_2$ is equivalent to $\mathcal{A}_1$ and hence to $\mathcal{A}$.

Let $F_N(\mathcal{A})$ be an automaton that recognizes the intersection $L(\mathcal{A}_2) \cap (\{X, S, R\}^* \cup N\{X, S, R\}^*)$. Obviously, the language of $F_N(\mathcal{A})$ is a subset of $\{X, S, R\}^* \cup N\{X, S, R\}^*$, so we only need to show that $F_N(\mathcal{A}) \sim \mathcal{A}$. Take any $w_1 \in L(F_N(\mathcal{A}))$, then $w_1 \in L(\mathcal{A}_2)$ and since $\mathcal{A}_2 \sim \mathcal{A}$, there is $w_2 \in L(\mathcal{A})$ such that $w_1 \sim w_2$. Next, we need to prove that for any $w_2 \in L(\mathcal{A})$, there is $w_1 \in L(F_N(\mathcal{A}))$ such that $w_2 \sim w_1$.

Let us take any $w_2 \in L(\mathcal{A})$. To construct the required word $w_1$, we first need to find all occurrences of letter $N$ in $w_2$. For example, suppose that $w_2 = u_1 N u_2 N \ldots u_{n-1} N u_n$, where each $u_i \in \{X, S, R\}^*$. If the number of $N$'s is odd, then in each subword $u_i$ with odd $i$ we replace every occurrence of $X$, $S$, and $R$ with $NXN$, $NXSN$, and $NSR^2SN$, respectively, and leave $u_i$'s with even $i$ unchanged. On the other hand, if the number of $N$'s is even, then we apply such substitution to each $u_i$ with even $i$ and leave $u_i$'s with odd $i$ unchanged. Let $w'$ be the resulting word. Then by construction $w' \sim w_2$ and $w' \in L(\mathcal{A}_1)$. Next, we repeatedly remove all occurrences of the subword $NN$ from $w'$. This will give us a word $w_1 \sim w' \sim w_2$ such that $w_1 \in L(\mathcal{A}_2)$ and $w_1$ contains at most one letter $N$, which may appear in the first position. Hence $w_1 \in L(F_N(\mathcal{A}))$. This idea is illustrated by the following example. Let $w_2 = SXNRNRSNS \in L(\mathcal{A})$, so $w_2$ contains an odd number of $N$'s and hence

$$w' = (NXSN)(NXN)NRN(NSR^2SN)(NXSN)NS$$
$$= NXS(NN)X(NN)R(NN)SR^2S(NN)XS(NN)S.$$

In the above formula parentheses are inserted only to visually separated subwords in $w'$. After removing subwords $NN$ from $w'$ we obtain $w_1 = NXSXRSR^2SXSS \in L(F_N(\mathcal{A}))$ such that $w_1 \sim w_2$.

The next example illustrates the same idea for an even number of $N$'s. Let $w_2 = SXNRNRSNSN \in L(\mathcal{A})$, then

$$w' = SXN(NSR^2SN)NRSN(NXSN)N$$
$$= SX(NN)SR^2S(NN)RS(NN)XS(NN).$$

After removing $NN$ from $w'$ we obtain $w_1 = SXSR^2SRSXS \in L(F_N(\mathcal{A}))$ such that $w_1 \sim w_2$. This completes the proof that $F_N(\mathcal{A}) \sim \mathcal{A}$.

**Transformation** Red. To construct $\text{Red} \circ F_N(\mathcal{A})$ from $F_N(\mathcal{A})$ we will make use of the following equivalences $SS \sim X$ and $RRR \sim X$. We will also use the fact that $X$ commutes with $S$, $R$, and $N$, and that $XX$ is equivalent to the empty word.

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

(1) For any pair of states $q$, $q'$ in $F_N(\mathcal{A})$ that are connected by a path labelled with $XX$, we add an $\varepsilon$-transition $q \xrightarrow{\varepsilon} q'$.

(2) For any pair of states $q$, $q'$ in $F_N(\mathcal{A})$ that are connected by a path labelled with $SX^\alpha S$, where $\alpha \in \{0,1\}$ (recall that $X^0$ denotes the empty word), we add a new transition $q \xrightarrow{X^\beta} q'$, where $\beta = 1 - \alpha$.

(3) For any pair of states $q$, $q'$ in $F_N(\mathcal{A})$ that are connected by a path labelled with $RX^{\alpha_1}RX^{\alpha_2}R$, 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 $\gamma \equiv \alpha_1 + \alpha_2 + 1 \mod 2$.

We repeat the above steps iteratively until no new transitions can be added.

Let $\mathcal{A}'$ be the resulting automaton. By construction, we have $\mathcal{A}' \sim F_N(\mathcal{A})$. Let $\mathcal{L}_{\text{Red}}$ be the regular language which consists of all words in alphabet $\Sigma$ that do not contain subwords of the form $XX$, $SX^\alpha S$ and $RX^{\alpha_1}RX^{\alpha_2}R$ for any $\alpha, \alpha_1, \alpha_2 \in \{0,1\}$. Define $\text{Red} \circ F_N(\mathcal{A})$ as an automaton that accepts the language $L(\mathcal{A}') \cap \mathcal{L}_{\text{Red}}$. It is not hard to see that the language of $\text{Red} \circ F_N(\mathcal{A})$ is contained in $\mathcal{L}_{\text{Red}} \cap (\{X,S,R\}^* \cup N\{X,S,R\}^*)$.

What is left to show is that $\text{Red} \circ F_N(\mathcal{A}) \sim F_N(\mathcal{A})$. If $w_1 \in L(\text{Red} \circ F_N(\mathcal{A}))$, then $w_1 \in L(\mathcal{A}')$, and hence $w_1 \sim w_2$ for some $w_2 \in L(F_N(\mathcal{A}))$ because $\mathcal{A}' \sim F_N(\mathcal{A})$. On the other hand, if $w_2 \in L(F_N(\mathcal{A}))$, then we can repeatedly remove subwords $XX$ from $w_2$ and replace subwords of the form $SX^\alpha S$ and $RX^{\alpha_1}RX^{\alpha_2}R$, for $\alpha, \alpha_1, \alpha_2 \in \{0,1\}$, with $X^\beta$ and $X^\gamma$, respectively, where $\beta = 1 - \alpha$ and $\gamma \in \{0,1\}$ is such that $\gamma \equiv \alpha_1 + \alpha_2 + 1 \mod 2$. Let $w_1$ be a resulting word that does not contain subwords $XX$, $SX^\alpha S$ and $RX^{\alpha_1}RX^{\alpha_2}R$ for any $\alpha, \alpha_1, \alpha_2 \in \{0,1\}$. Then $w_1 \sim w_2$ and $w_1 \in L(\mathcal{A}') \cap \mathcal{L}_{\text{Red}} = L(\text{Red} \circ F_N(\mathcal{A}))$.

**Transformation** $F_X$. The words accepted by $\text{Red} \circ F_N(\mathcal{A})$ are almost in canonical form with the exception that the letter $X$ may appear in the middle of a word. To get rid of such $X$'s we use a similar idea as in the construction of $F_N(\mathcal{A})$. Namely, we will use the following equivalences: $S \sim XSX$ and $R \sim XRX$. Note that we will not need the equivalence $N \sim XNX$ because the letter $N$ can appear only at the beginning of a word.

To construct $\text{Can}(\mathcal{A}) = F_X \circ \text{Red} \circ F_N(\mathcal{A})$ from $\text{Red} \circ F_N(\mathcal{A})$, we do the following. First, for every transition $q \xrightarrow{S} q'$ which appears in $\text{Red} \circ F_N(\mathcal{A})$, 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 $\text{Red} \circ F_N(\mathcal{A})$, we add new states $p_1$, $p_2$ and a new path of the form $q \xrightarrow{X} p_1 \xrightarrow{R} p_2 \xrightarrow{X} q'$. After that we iteratively add $\varepsilon$ transitions $q \xrightarrow{\varepsilon} q'$ for every pair of states $q$, $q'$ that are connected by a path with label $XX$. We do this until no new $\varepsilon$-transitions can be added.

Let $\mathcal{A}'$ be the resulting automaton, which is by construction equivalent to $\text{Red} \circ F_N(\mathcal{A})$. Let $\mathcal{L}_{\text{Can}}$ be the regular language which consists of all canonical words in alphabet $\Sigma$. Define $\text{Can}(\mathcal{A}) = F_X \circ \text{Red} \circ F_N(\mathcal{A})$ as an automaton that accepts the language $L(\mathcal{A}') \cap \mathcal{L}_{\text{Can}}$. Therefore, $\text{Can}(\mathcal{A})$ accepts only canonical words.

The proof that $\text{Can}(\mathcal{A}) \sim \text{Red} \circ F_N(\mathcal{A})$ is similar to the proof that $F_N(\mathcal{A}) \sim \mathcal{A}$ given above. If $w_1 \in L(\text{Can}(\mathcal{A}))$, then $w_1 \in L(\mathcal{A}')$ and hence $w_1 \sim w_2$ for some $w_2 \in L(\text{Red} \circ F_N(\mathcal{A}))$ because $\mathcal{A}' \sim \text{Red} \circ F_N(\mathcal{A})$. On the other hand, if $w_2 \in L(\text{Red} \circ F_N(\mathcal{A}))$, then to construct $w_1 \in L(\text{Can}(\mathcal{A}))$ such that $w_1 \sim w_2$ we first find all occurrences of the letter $X$ in $w_2$. For example, let $w_2$ has the form $w_2 = Nu_1Xu_2X \ldots u_{n-1}Xu_n$ or the form $w_2 = u_1Xu_2X \ldots u_{n-1}Xu_n$, where each $u_i \in \{S, R\}^*$. If the number of $X$'s is odd, then in each $u_i$ with odd $i$ we replace every occurrence of $R$ and $S$ with $XRX$ and $XSX$, respectively, and leave $u_i$'s with even $i$ unchanged. If the number of $X$'s is even, then we do the same substitution in all $u_i$'s with even $i$ and leave $u_i$'s with odd $i$ unchanged. After that we remove all occurrences of $XX$. If $w_1$ is a resulting word, then $w_1 \sim w_2$ and $w_1 \in L(\mathcal{A}')$. Moreover, since $w_1$ is in canonical form, we also have $w_1 \in L(\text{Can}(\mathcal{A}))$. This idea is illustrated by the following example. Suppose $w_2 = NSRXSXRRX$, then after replacing suitable occurrences of $R$ and $S$ with $XRX$ and $XSX$, respectively, we obtain the word

$$
\begin{aligned}
&N(XSX)(XRX)XSX(XRX)(XRX)X \\
=\,&NXS(XX)R(XX)S(XX)R(XX)R(XX).
\end{aligned}
$$

After removing all occurrences of $XX$ we obtain the word $w_1 = NXSRSRR \sim w_2$ which is in canonical form, and hence $w_1 \in L(\text{Can}(\mathcal{A}))$. This completes the construction of $\text{Can}(\mathcal{A})$.

# References

[1] 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*, SODA '96, pages 498–507, Philadelphia, PA, USA, 1996. Society for Industrial and Applied Mathematics.

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

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

[4] P. C. Bell, M. Hirvensalo, and I. Potapov. Mortality for 2x2 matrices is NP-hard. In B. Rovan, V. Sassone, and P. Widmayer, editors, *Mathematical Foundations of Computer Science 2012*, volume 7464 of *Lecture Notes in Computer Science*, pages 148–159. Springer Berlin Heidelberg, 2012.

[5] P. C. Bell and I. Potapov. On the undecidability of the identity correspondence problem and its applications for word and matrix semigroups. *Int. J. Found. Comput. Sci.*, 21(6):963–978, 2010.

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

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

[8] V. D. Blondel and A. Megretski, editors. *Unsolved problems in mathematical systems and control theory.* Princeton, NJ: Princeton University Press, 2004. http://press.princeton.edu/math/blondel/solutions.html.

[9] J. Cassaigne, V. Halava, T. Harju, and F. Nicolas. Tighter undecidability bounds for matrix mortality, zero-in-the-corner problems, and more. *CoRR*, abs/1404.0644, 2014.

[10] J. Cassaigne, T. Harju, and J. Karhumaki. On the undecidability of freeness of matrix semigroups. *International Journal of Algebra and Computation*, 09(03n04):295–305, 1999. http://www.worldscientific.com/doi/pdf/10.1142/S0218196799000199.

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

[12] V. Chonev, J. Ouaknine, and J. Worrell. The orbit problem in higher dimensions. In *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 941–950, 2013.

[13] V. Chonev, J. Ouaknine, and J. Worrell. On the complexity of the orbit problem. *to apear in JACM*, 2016.

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

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

[16] A. Gerrard and J. M. Burch. *Introduction to matrix methods in optics.* Dover Publications, Inc., New York, 1994. Corrected reprint of the 1975 original.

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

[18] V. Halava, T. Harju, M. Hirvensalo, and J. Karhumaki. Skolem's problem - on the border between decidability and undecidability. Technical Report 683, Turku Centre for Computer Science, 2005.

[19] R. Kannan and A. Bachem. Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. *SIAM J. Comput.*, 8(4):499–507, 1979.

[20] R. Kannan and R. J. Lipton. Polynomial-time algorithm for the orbit problem. *J. ACM*, 33(4):808–821, Aug. 1986.

[21] A. Lisitsa and 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*, pages 623–634, 2004.

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

[23] W. Magnus, A. Karrass, and D. Solitar. *Combinatorial group theory.* Dover Publications, Inc., New York, revised edition, 1976. Presentations of groups in terms of generators and relations.

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

[25] J. Ouaknine, J. a. S. Pinto, and J. Worrell. On termination of integer linear loops. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '15, pages 957–969. SIAM, 2015.

[26] J. Ouaknine and 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*, pages 318–329, 2014.

[27] J. Ouaknine and 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*, pages 330–341, 2014.

[28] I. Potapov and P. Semukhin. Vector reachability problem in SL(2, Z). *CoRR*, abs/1510.03227, 2015. http://arxiv.org/abs/1510.03227.

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