On Reachability Problems for Low-Dimensional Matrix Semigroups

Thomas Colcombet
IRIF, CNRS, Université Paris Diderot, France
thomas.colcombet@irif.fr

Joël Ouaknine
The Max Planck Institute for Software Systems, Germany
Department of Computer Science, University of Oxford, United Kingdom
joel@mpi-sws.org

Pavel Semukhin
Department of Computer Science, University of Oxford, United Kingdom
pavel.semukhin@cs.ox.ac.uk

James Worrell
Department of Computer Science, University of Oxford, United Kingdom
jbw@cs.ox.ac.uk

Abstract

We consider the Membership and the Half-Space Reachability problems for matrices in dimensions two and three. Our first main result is that the Membership Problem is decidable for finitely generated sub-semigroups of the Heisenberg group over rational numbers. Furthermore, we prove two decidability results for the Half-Space Reachability Problem. Namely, we show that this problem is decidable for sub-semigroups of $\mathrm{GL}(2,\mathbb{Z})$ and of the Heisenberg group over rational numbers.

2012 ACM Subject Classification Theory of computation → Formal languages and automata theory; Computing methodologies → Symbolic and algebraic algorithms

Keywords and phrases Membership Problem, Half-Space Reachability Problem, matrix semigroups, Heisenberg group, general linear group

Digital Object Identifier 10.4230/LIPIcs.ICALP.2019.39

Related Version A full version of the paper is available at `https://arxiv.org/abs/1902.09597`, [11].

Funding *Thomas Colcombet*: Supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No.670624), and by the DeLTA ANR project (ANR-16-CE40-0007).
Joël Ouaknine: Supported by ERC grant AVS-ISS (648701) and by DFG grant 389792660 as part of TRR 248 (see `https://perspicuous-computing.science`).
Pavel Semukhin: Supported by ERC grant AVS-ISS (648701).
James Worrell: Supported by EPSRC Fellowship EP/N008197/1.

1 Introduction

The algorithmic theory of matrix groups and semigroups is a staple of computational algebra [3] with numerous applications to automata theory and program analysis [7, 10, 12, 19, 20, 27] and has been influential in developing the notion of interactive proofs in complexity theory [1].

Two central decision problems on matrix semigroups are the *Membership* and *Half-Space Reachability* (see, e.g., [6]). For the Membership Problem the input is a finite set of generators $A_1, \ldots, A_k$ and a target matrix A, with all matrices being square and of the same dimension. The question is whether A lies in the semigroup generated by $A_1, \ldots, A_k$. We emphasize that

46th International Colloquium on Automata, Languages, and Programming (ICALP 2019).
Editors: Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi;
Article No. 39; pp. 39:1–39:15
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

we consider membership in finitely generated *sub-semigroups*, i.e., we seek to recover A as a non-empty product of generators. In a related *subgroup* membership problem one additionally allows to take inverses of generators. The subgroup membership can clearly be reduced to the sub-semigroup membership and tends to be more tractable (e.g., the subgroup membership for polycyclic groups is well-known to be decidable [38], and the subgroup membership for the modular group $\mathrm{PSL}(2,\mathbb{Z})$ is in PTIME [15]). For the Half-Space Reachability Problem the target matrix is replaced by vectors $\boldsymbol{u}$, $\boldsymbol{v}$ and a scalar λ, and the question is now whether there exists a matrix A in the semigroup generated by $A_1, \ldots, A_k$ such that $\boldsymbol{u}^\top A\boldsymbol{v} \geq \lambda$. Geometrically the question is whether the orbit of $\boldsymbol{v}$ under the action of the semigroup reaches a certain half-space with normal $\boldsymbol{u}$. Closely related to these problems are the Vector Reachability and the Hyperplane Reachability[1] problems, which ask whether there exists a matrix A in the semigroup generated by $A_1, \ldots, A_k$ such that $A\boldsymbol{v} = \boldsymbol{u}$ or such that $\boldsymbol{u}^\top A\boldsymbol{v} = \lambda$, respectively.

Undecidability of the Membership Problem has long been known (indeed, this was one of the earliest undecidability results—see A. Markov [28]). Subsequently a number of positive decidability results were obtained in the case of semigroups generated by commuting matrices over infinite fields [2, 20]. More recently, attention has focussed on integer matrices in dimension two. A classical result of [10] shows decidability of the Membership Problem for sub-semigroups of $\mathrm{GL}(2,\mathbb{Z})$—the group of 2×2 integer matrices with integer inverses (equivalently, with determinants equal to ± 1). Moreover, the semigroup membership for the identity matrix was shown to be NP-complete for $\mathrm{SL}(2,\mathbb{Z})$ [4]. Furthermore, the Membership Problem is decidable for 2×2 integer matrices with nonzero determinant [32] and for 2×2 integer matrices with determinants equal to 0 and ± 1 [33]. However it is still unknown whether the Membership Problem is decidable for all 2×2 integer matrices.

Going beyond dimension two, it has long been known that the Membership Problem is undecidable for general 3×3 integer matrices [31]. However the status of the Membership Problem for $\mathrm{GL}(3,\mathbb{Z})$ is currently an outstanding open problem. Related to this, it was shown in [23] that for a two-element alphabet Σ, the monoid $\Sigma^* \times \Sigma^*$ cannot be embedded in $\mathrm{GL}(3,\mathbb{Z})$. This fact suggests that undecidability proofs of the Membership Problem in other settings (such as [31]), which are based on encodings of the Post Correspondence Problem, are unlikely to carry over to $\mathrm{GL}(3,\mathbb{Z})$. It is classical that the Membership Problem for $\mathrm{GL}(4,\mathbb{Z})$ is undecidable [29, 5, 23]; thus it can reasonably be said that dimension three lies on the borderline between decidability and undecidability.

Our first main result (Theorem 7) concerns the Membership Problem for a simple subgroup of $\mathrm{GL}(3,\mathbb{Z})$: the so-called *Heisenberg group* $\mathrm{H}(3,\mathbb{Z})$, which comprises upper triangular integer matrices with ones along the diagonal. Since the Heisenberg group is polycyclic, the sub*group* membership problem is decidable [38]. It was moreover recently shown in [23] how to decide membership of the identity matrix in finitely generated sub-semigroups of $\mathrm{H}(3,\mathbb{Z})$. Our main theorem strengthens this last result to show decidability of the Membership Problem for $\mathrm{H}(3,\mathbb{Z})$. In fact, like in [23], our argument works for Heisenberg groups of any dimension and even over the field of rational numbers, that is, for $\mathrm{H}(n,\mathbb{Q})$.

Our proof relies on arguments developed in [23] but contains several significant new elements, including the use of linear programming, integer register automata, and matrix logarithms. The following algebraic property of $\mathrm{H}(3,\mathbb{Z})$ is important for our construction: the subgroup generated by commutators of matrices from a given subset $\mathcal{G} \subseteq \mathrm{H}(3,\mathbb{Z})$ is isomorphic to a subgroup of $\mathbb{Z}$. Such property does not hold for the direct product of two

[1] In the literature the Hyperplane Reachability Problem is also called the Scalar Reachability Problem.

Heisenberg groups $\mathrm{H}(3,\mathbb{Z})^2$ or for the group of 4×4 upper unitriangular matrices $\mathrm{UT}(4,\mathbb{Z})$. This makes it challenging to generalize our argument to show decidability of the Membership Problem for $\mathrm{H}(3,\mathbb{Z})^2$, $\mathrm{UT}(4,\mathbb{Z})$ or other similar matrix groups.

In [24] a related problem was studied, called the Knapsack Problem. Namely, it was proved that the Knapsack Problem is decidable for $\mathrm{H}(3,\mathbb{Z})$, that is, given matrices $A_1, \ldots, A_k$ and A from $\mathrm{H}(3,\mathbb{Z})$ one can decide whether there are non-negative integers $n_1, \ldots, n_k$ such that $A_1^{n_1} \cdots A_k^{n_k} = A$. Decidability of the Knapsack Problem is shown by reduction to the problem of solving a single quadratic equation in integer numbers (proved to be decidable in [13, 14]). By contrast, our decision procedure for the Membership Problem relies only on linear programming and integer linear arithmetic. As far as we can tell, there is no straightforward reduction in either direction between the Membership and Knapsack Problems for $\mathrm{H}(3,\mathbb{Z})$.

The Vector Reachability, Hyperlane Reachability, and Half-Space Reachabilty Problems are all known to be undecidable in general (see [9, 16, 17]). The Vector and Hyperplane Reachability problems are known to be decidable for $\mathrm{GL}(2,\mathbb{Z})$, as shown in [34]. For matrix semigroups with a single generator, the Half-Space Reachability Problem is equivalent to the *Positivity Problem* for linear recurrence sequences: a longstanding and apparently difficult open problem [30, 36]. Our second main result is that the Half-Space Reachability Problem is decidable for both $\mathrm{GL}(2,\mathbb{Z})$ (Theorem 17) and $\mathrm{H}(n,\mathbb{Q})$ (Theorem 20). For $\mathrm{GL}(2,\mathbb{Z})$ we build on automata-theoretic techniques developed in [10], with the key insight being that the set of matrices in $\mathrm{GL}(2,\mathbb{Z})$ with a positive value in a given entry can be represented as a regular language over the generators of $\mathrm{GL}(2,\mathbb{Z})$. For $\mathrm{H}(n,\mathbb{Q})$ we rely on a nontrivial result about the nonnegativity of quadratic forms over the integers from [13, 14] (related to the result used in [24] to solve the Knapsack Problem).

2 Preliminaries

The Heisenberg Group.

We use notations I_n and 0_n for the identity matrix and for the zero matrix of size $n \times n$, respectively. For $n \geq 3$, the *Heisenberg group* of dimension n is the group $\mathrm{H}(n,\mathbb{R})$ of $n \times n$ real matrices of the form

$$A = \begin{pmatrix} 1 & \boldsymbol{a}^\top & c \\ 0 & I_{n-2} & \boldsymbol{b} \\ 0 & 0 & 1 \end{pmatrix}, \tag{1}$$

where $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^{n-2}$, $c \in \mathbb{R}$. For brevity, we will often denote a matrix A as in (1) by the triple $(\boldsymbol{a}, \boldsymbol{b}, c) \in \mathbb{R}^{n-2} \times \mathbb{R}^{n-2} \times \mathbb{R}$. It is easy to check that the product operation is given by

$$(\boldsymbol{a}, \boldsymbol{b}, c) \cdot (\boldsymbol{a}', \boldsymbol{b}', c') = (\boldsymbol{a} + \boldsymbol{a}', \boldsymbol{b} + \boldsymbol{b}', c + c' + \boldsymbol{a}^\top \boldsymbol{b}') \,.$$

We use ψ to denote the group homomorphism $\psi : \mathrm{H}(n,\mathbb{R}) \to \mathbb{R}^{2n-4}$ given by $\psi(\boldsymbol{a}, \boldsymbol{b}, c) = (\boldsymbol{a}, \boldsymbol{b})$.

The Heisenberg group $\mathrm{H}(n,\mathbb{R})$ is a Lie group whose corresponding Lie algebra $\mathfrak{h}(n,\mathbb{R})$ comprises the vector space of $n \times n$ real matrices of the form

$$B = \begin{pmatrix} 0 & \boldsymbol{a}^\top & c \\ 0 & 0_{n-2} & \boldsymbol{b} \\ 0 & 0 & 0 \end{pmatrix}, \tag{2}$$

where $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^{n-2}$ and $c \in \mathbb{R}$, together with the binary *Lie bracket* operation $[A, B] := AB - BA$ for $A, B \in \mathfrak{h}(n, \mathbb{R})$. Note that $[A, B]$ has only zero entries except for the $(1, n)$-entry. From this it is easy to check that $[[A, B], C] = 0_n$ for all $A, B, C \in \mathfrak{h}(n, \mathbb{R})$.

Given $A \in \mathrm{H}(n, \mathbb{R})$, as shown in (1), we define its logarithm $\log(A) \in \mathfrak{h}(n, \mathbb{R})$ to be

$$\log(A) := (A - I) - \frac{(A - I)^2}{2} = \begin{pmatrix} 0 & \boldsymbol{a}^\top & c - \frac{1}{2}\boldsymbol{a}^\top \boldsymbol{b} \\ 0 & 0_{n-2} & \boldsymbol{b} \\ 0 & 0 & 0 \end{pmatrix}.$$

Conversely, given $B \in \mathfrak{h}(n, \mathbb{R})$, as shown in (2), we define its exponential $\exp(B) \in \mathrm{H}(n, \mathbb{R})$ to be $\exp(B) := I + B + \frac{B^2}{2} = (\boldsymbol{a}, \boldsymbol{b}, c + \frac{1}{2}\boldsymbol{a}^\top \boldsymbol{b})$. It is easy to verify that log and exp are mutually inverse and together induce a bijection between $\mathrm{H}(n, \mathbb{R})$ and $\mathfrak{h}(n, \mathbb{R})$.

The following is a specialisation to $\mathrm{H}(n, \mathbb{R})$ of the Baker-Campbell-Hausdorff product formula (see [18, Chapter 5] for a details). Given a sequence of matrices $B_1, \ldots, B_m \in \mathrm{H}(n, \mathbb{R})$, we have

$$\log(B_1 \cdots B_m) = \sum_{i=1}^{m} \log(B_i) + \frac{1}{2} \sum_{1 \le i < j \le m} [\log(B_i), \log(B_j)]\,. \tag{3}$$

Regular subsets of $\mathrm{GL}(2, \mathbb{Z})$.

We will use the notation $\mathrm{GL}(2, \mathbb{Z})$ for the general linear group of 2×2 integer matrices, that is, $\mathrm{GL}(2, \mathbb{Z}) = \{M \in \mathbb{Z}^{2\times 2} : \det(M) = \pm 1\}$. A matrix is called *singular* if its determinant is zero and *nonsingular* otherwise.

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

$$\varphi(X) = -I_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \ \varphi(N) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ \varphi(S) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ \varphi(R) = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

We can extend φ to a morphism $\varphi : \Sigma^* \to \mathrm{GL}(2, \mathbb{Z})$ in a natural way. It is a well-known fact that morphism φ is surjective, that is, for every $M \in \mathrm{GL}(2, \mathbb{Z})$ there is a word $w \in \Sigma^*$ such that $\varphi(w) = M$. This presentation is not unique because of identities such as $\varphi(SS) = \varphi(RRR) = \varphi(X)$. However, as explained below, every matrix $M \in \mathrm{GL}(2, \mathbb{Z})$ is represented by a unique word in the *canonical* form.

In the following definition, for n a positive integer and $V \in \Sigma$, V^n is the word consisting of n copies of V, while V^0 denotes the empty word.

▶ **Definition 1.** *A word $w \in \Sigma^*$ is called* canonical *if it has the form*

$$w = N^\delta X^\gamma S^\beta R^{\alpha_1} S R^{\alpha_2} \cdots S R^{\alpha_n} S^\varepsilon,$$

where $\beta, \gamma, \delta, \varepsilon \in \{0, 1\}$ and $\alpha_i \in \{1, 2\}$ for $i = 1, \ldots, n$. 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.*

The next proposition is a well-known fact.

▶ **Proposition 2** ([25, 26, 32, 35])**.** *For every matrix $M \in \mathrm{GL}(2, \mathbb{Z})$, there is a unique canonical word w such that $M = \varphi(w)$.*

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

▶ **Definition 4.** *Two words w_1 and w_2 from Σ^* are* equivalent*, denoted $w_1 \sim w_2$, if $\varphi(w_1) = \varphi(w_2)$. Two languages L_1 and L_2 in the alphabet Σ 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 Σ are equivalent*, denoted $\mathcal{A}_1 \sim \mathcal{A}_2$, if $L(\mathcal{A}_1) \sim L(\mathcal{A}_2)$.*

The following theorem is a crucial ingredient of our decidability results.

▶ **Theorem 5** ([32]). *For any automaton $\mathcal{A}$ over the alphabet $\Sigma = \{X, N, S, R\}$, there exists an automaton $\mathrm{Can}(\mathcal{A})$ such that $\mathrm{Can}(\mathcal{A})$ is equivalent to $\mathcal{A}$ and $\mathrm{Can}(\mathcal{A})$ accepts only canonical words. Furthermore, $\mathrm{Can}(\mathcal{A})$ can be constructed from $\mathcal{A}$ in polynomial time.*

The proof of the following corollary is given in the full version [11].

▶ **Corollary 6.** *Regular subsets of $\mathrm{GL}(2, \mathbb{Z})$ are effectively closed under Boolean operations. Namely, given two regular languages $L, L' \subseteq \Sigma^*$, we can algorithmically construct in polynomial time regular languages $L^{\cup}$, $L^{\cap}$ and L^c such that $\varphi(L^{\cup}) = \varphi(L) \cup \varphi(L')$, $\varphi(L^{\cap}) = \varphi(L) \cap \varphi(L')$, and $\varphi(L^c) = \mathrm{GL}(2, \mathbb{Z}) \setminus \varphi(L)$.*

Decision problems for matrix semigroups.

If $\mathcal{G}$ is a finite collection of matrices, then $\langle \mathcal{G} \rangle$ denotes the semigroup generated by $\mathcal{G}$, that is, $A \in \langle \mathcal{G} \rangle$ if and only if there are matrices $A_1, \ldots, A_t \in \mathcal{G}$ such that $A = A_1 \cdots A_t$.

In this paper we will consider the following decision problems for matrix semigroups:

- **The Membership Problem:** Given a finite collection of matrices $\mathcal{G}$ and a "target" matrix A, decide whether A belongs to $\langle \mathcal{G} \rangle$.
- **The Half-Space Reachability Problem:** Given a finite collection of matrices $\mathcal{G}$, two vectors $\boldsymbol{u}, \boldsymbol{v}$ and a scalar λ, decide whether there exists a matrix $A \in \langle \mathcal{G} \rangle$ such that $\boldsymbol{u}^\top A \boldsymbol{v} \geq \lambda$. In other words, decide whether it is possible to reach the half-space $\mathcal{H} = \{\boldsymbol{x} : \boldsymbol{u}^\top \boldsymbol{x} \geq \lambda\}$ using matrices from $\mathcal{G}$ starting from an initial vector $\boldsymbol{v}$.

When we talk about *the Membership Problem for* $\mathrm{GL}(2, \mathbb{Z})$ *or for the Heisenberg group* $\mathrm{H}(n, \mathbb{Q})$, we mean that A and the matrices from $\mathcal{G}$ belong to $\mathrm{GL}(2, \mathbb{Z})$ or $\mathrm{H}(n, \mathbb{Q})$, respectively. Similarly, in *the Half-Space Reachability Problem for* $\mathrm{GL}(2, \mathbb{Z})$ *or* $\mathrm{H}(n, \mathbb{Q})$ we assume that $\mathcal{G}$ is a finite subset of $\mathrm{GL}(2, \mathbb{Z})$ or $\mathrm{H}(n, \mathbb{Q})$, respectively, and furthermore we assume that the vectors $\boldsymbol{u}, \boldsymbol{v}$ have rational coefficients and λ is a rational number.

3 The Membership Problem for the Heisenberg Group

Let $\mathrm{H}(n, \mathbb{Z})$ and $\mathrm{H}(n, \mathbb{Q})$ be subgroups of $\mathrm{H}(n, \mathbb{R})$ comprising all matrices with integer and rational entries, respectively. In this section we will prove our first main result.

▶ **Theorem 7.** *The Membership Problem for $\mathrm{H}(n, \mathbb{Z})$ is decidable.*

We first give an overview of our decision procedure. Let $\mathcal{G} = \{A_1, \ldots, A_k\}$ be a finite set of generators from $\mathrm{H}(n, \mathbb{Z})$ and $A \in \mathrm{H}(n, \mathbb{Z})$ be a target matrix. The idea is to partition the set of generators $\mathcal{G}$ into two sets $\mathcal{G}_+$ and $\mathcal{G}_0$. The definition of $\mathcal{G}_+$ is such that there is a computable upper bound on the number of occurrences of a matrix from $\mathcal{G}_+$ in any string of generators whose product equals the target matrix A. The definition of $\mathcal{G}_0$ is such that the image of the semigroup generated by $\mathcal{G}_0$ under the homomorphism ψ is a sub*group* of $\mathbb{R}^{2n-4}$ (i.e., the image is closed under inverses). We then proceed by a case analysis according to whether or not $\mathcal{G}_0$ is a commutative set of matrices. If $\mathcal{G}_0$ is commutative then the Membership Problem can be reduced to solving a system of linear equations over non-negative integer variables. If $\mathcal{G}_0$ is not commutative then we reduce the Membership Problem to a reachability query in an integer register automaton.

Partitioning the Set of Generators.

In the rest of this section we work with an instance of the Membership Problem in which the generators are $A_i = (\boldsymbol{a}_i, \boldsymbol{b}_i, c_i)$, for $i = 1, \ldots, k$, and the target matrix is $A = (\boldsymbol{a}, \boldsymbol{b}, c)$. Recalling the homomorphism $\psi : \mathrm{H}(n, \mathbb{Z}) \to \mathbb{Z}^{2n-4}$, let us define $\boldsymbol{v}_i := \psi(A_i) = (\boldsymbol{a}_i, \boldsymbol{b}_i)$, for $i = 1, \ldots, k$, and $\boldsymbol{v} := \psi(A) = (\boldsymbol{a}, \boldsymbol{b})$.

A set $C \subseteq \mathbb{R}^n$ is called a *cone* if $\sum_{i=1}^{k} r_i \boldsymbol{u}_i \in C$ for all $r_1, \ldots, r_k \in \mathbb{R}_{\geq 0}$ and $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \in C$. The *dual* of a cone $C \subseteq \mathbb{R}^n$ is the cone defined as

$$C^* := \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{x}^\top \boldsymbol{y} \geq 0 \text{ for all } \boldsymbol{y} \in C\}.$$

We will use the fact that $C = C^{**}$, i.e., a cone is equal to its double dual [8, Chapter 2.6.1].

We write $\mathrm{Cone}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ for the cone generated by the vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$. We now partition the set of generators $\mathcal{G}$ into two disjoint sets $\mathcal{G}_0, \mathcal{G}_+$, where

$$\begin{aligned} \mathcal{G}_0 &:= \left\{A_i : \forall \boldsymbol{u} \in \mathrm{Cone}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)^* \quad \boldsymbol{v}_i^\top \boldsymbol{u} = 0\right\} \\ \mathcal{G}_+ &:= \left\{A_i : \exists \boldsymbol{u} \in \mathrm{Cone}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)^* \quad \boldsymbol{v}_i^\top \boldsymbol{u} > 0\right\}. \end{aligned}$$

We can determine the sets $\mathcal{G}_0$ and $\mathcal{G}_+$ using linear programming [37]. Without loss of generality we can assume that $\mathcal{G}_0 = \{A_1, \ldots, A_\ell\}$ for some $\ell \geq 0$.

We show how to compute a bound $\beta > 0$ such that for every sequence $\mathcal{S} = B_1, \ldots, B_m$ of elements of $\mathcal{G}$ whose product is equal to the target matrix A, the number of indices i such that $B_i \in \mathcal{G}_+$ is at most β. By definition of $\mathcal{G}_+$, for each $i \in \{1, \ldots, \ell\}$, there exists $\boldsymbol{u}_i \in \mathrm{Cone}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)^*$ such that $\boldsymbol{v}_i^\top \boldsymbol{u}_i > 0$. Since $\boldsymbol{v}_j^\top \boldsymbol{u}_i \geq 0$ for all $j \neq i$, $\mathcal{S}$ contains at most $\frac{\boldsymbol{v}^\top \boldsymbol{u}_i}{\boldsymbol{v}_i^\top \boldsymbol{u}_i}$ occurrences of matrix A_i (or no occurrences if $\boldsymbol{v}^\top \boldsymbol{u}_i \leq 0$). Thus we may define $\beta := \sum_i \frac{\boldsymbol{v}^\top \boldsymbol{u}_i}{\boldsymbol{v}_i^\top \boldsymbol{u}_i}$ where the sum is take over the indices $i = 1, \ldots, \ell$ such that $\boldsymbol{v}^\top \boldsymbol{u}_i > 0$

We now consider two cases according to whether $\mathcal{G}_0$ is a commutative set of matrices.

Case I: $\mathcal{G}_0$ is commutative

Consider a sequence $\mathcal{S} = B_1, \ldots, B_m$ of elements of $\mathcal{G}$. Let $B_{i_1}, \ldots, B_{i_s}$ be the subsequence of $\mathcal{S}$ containing all occurrences of elements of $\mathcal{G}_+$ in $\mathcal{S}$, where $0 = i_0 < i_1 < \ldots < i_s < i_{s+1} = m + 1$. For $i \in \{1, \ldots, \ell\}$ and $j \in \{1, \ldots, s+1\}$, write $n_{i,j}$ for the number of occurrences of $A_i \in \mathcal{G}_0$ in the subsequence of $\mathcal{S}$ lying strictly between $B_{i_{j-1}}$ and B_{i_j} (where B_0 is interpreted as the beginning of $\mathcal{S}$ and B_{m+1} as the end of $\mathcal{S}$). The idea is to write a formula for $\log(B_1 \cdots B_m)$ that is a linear form in the variables $n_{i,j}$.

Indeed by Equation (3), writing $C_{i_j} := \log(B_{i_j})$ for $j = 1, \ldots, s$ and $D_i := \log(A_i)$ for $i = 1, \ldots, \ell$, we have

$$\begin{aligned} \log(B_1 \cdots B_m) = \sum_{j=1}^{s} C_{i_j} + \sum_{i=1}^{\ell} \sum_{j=1}^{s+1} n_{i,j} D_i + \sum_{1 \leq j < j' \leq s} [C_{i_j}, C_{i_{j'}}] \\ + \sum_{i=1}^{\ell} \sum_{1 \leq j \leq j' \leq s} n_{i,j} [D_i, C_{i_{j'}}] + \sum_{i=1}^{\ell} \sum_{1 \leq j < j' \leq s+1} n_{i,j'} [C_{i_j}, D_i] \end{aligned} \tag{4}$$

An important observation is that the above formula has no quadratic terms due to commutativity of $\mathcal{G}_0$. Now $B_1 \cdots B_m = A$ if and only if $\log(B_1 \cdots B_m) = \log(A)$. Setting the right-hand-side of (4) equal to $\log(A)$ yields a linear Diophantine equation in variables $n_{i,j}$. The form of this equation is determined by the subsequence of matrices $B_{i_1}, \ldots, B_{i_s}$ lying in $\mathcal{G}_+$. Recall that we can without loss of generality restrict attention to the case that $s \le \beta$ and thus we reduce the question of whether A lies in the semigroup generated by $\mathcal{G}$ to the solubility of finitely many linear equations in nonnegative integers.

Case II: $\mathcal{G}_0$ is not commutative

Let $\mathcal{G}_0 = \{A_1, \ldots, A_\ell\}$ for some $\ell \ge 2$ such that A_1 and A_2 do not commute. Recall that by definition of $\mathcal{G}_0$ it holds that $\boldsymbol{v}_i^\top \boldsymbol{u} = 0$ for all $\boldsymbol{u} \in \mathrm{Cone}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)^*$ and $i = 1, \ldots, \ell$. Therefore,

$$\mathrm{Span}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell) \subseteq \mathrm{Cone}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)^{**} = \mathrm{Cone}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)\,. \tag{5}$$

Following ideas from [23], we will show that there exist integers $p > 0$ and $q < 0$ such that $M_+ = (\mathbf{0}, \mathbf{0}, p)$ and $M_- = (\mathbf{0}, \mathbf{0}, q)$ and both lie in the semigroup generated by $\mathcal{G}$.

Indeed, from Equation (5) it follows that $-(\boldsymbol{v}_1 + \boldsymbol{v}_2)$ lies in $\mathrm{Cone}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$. Thus there exist $r_1, \ldots, r_k \in \mathbb{R}_{\ge 0}$ with r_1, r_2 strictly positive such that $\sum_{i=1}^k r_i \boldsymbol{v}_i = \mathbf{0}$. But since the vectors $\boldsymbol{v}_i$ have integer coefficients we can solve the above equation in natural numbers $r_1, \ldots, r_k$ with $r_1, r_2 > 0$. Taking a sequence of matrices $B_1, \ldots, B_m$, drawn from $\mathcal{G}$, such that $B_1 = A_1$, $B_2 = A_2$ and such that matrix A_i appears r_i times in the sequence for $i \in \{1, \ldots, k\}$, we obtain $\psi(B_1 \cdots B_m) = \mathbf{0}$. Since ψ is a homomorphism to a commutative group we have that $\psi(B^t_{\sigma(1)} \cdots B^t_{\sigma(m)}) = \mathbf{0}$ for all $t \ge 1$ and permutations $\sigma \in S_m$.

Write $C_i = \log(B_i)$ for $i = 1, \ldots, m$. Applying the Baker-Campbell-Hausdorff Formula (3), we have that for any positive integer t and permutation $\sigma \in S_m$

$$\log(B^t_{\sigma(1)} \cdots B^t_{\sigma(m)}) = t \sum_{i=1}^m C_{\sigma(i)} + \frac{t^2}{2} \sum_{i<j} [C_{\sigma(i)}, C_{\sigma(j)}]. \tag{6}$$

We show that we can obtain the desired matrices M_+ and M_- as $M_+ := B^t_{\sigma(1)} \cdots B^t_{\sigma(m)}$ and $M_- := B^t_{\sigma(m)} \cdots B^t_{\sigma(1)}$ for some permutation $\sigma \in S_m$ and large enough t.

Let $\sigma_0 \in S_m$ be the permutation that transposes 1 and 2. Write also $\mathrm{id} \in S_m$ for the identity permutation. Defining $\delta_\sigma := \sum_{i<j} [C_{\sigma(i)}, C_{\sigma(j)}]_{1,n}$, we have $\delta_{\mathrm{id}} - \delta_{\sigma_0} = 2[C_1, C_2]_{1,n} \neq 0$ since B_1, B_2 do not commute. Hence there exists $\sigma \in \{\mathrm{id}, \sigma_0\}$ with $\delta_\sigma \neq 0$. Defining the reverse permutation $\sigma' \in S_m$ by $\sigma'(i) = \sigma(m + 1 - i)$ for $i = 1, \ldots, m$, we moreover have $\delta_{\sigma'} = -\delta_\sigma$, and thus we may suppose that $\delta_\sigma > 0$ and $\delta_{\sigma'} < 0$. It remains to note, by inspection of (6), that for t sufficiently large, if $\delta_\sigma \neq 0$ then the sign of the $(1, n)$-entry of $\log(B^t_{\sigma(1)} \cdots B^t_{\sigma(m)})$ is equal to the sign of δ_σ. But since $\log(B^t_{\sigma(1)} \cdots B^t_{\sigma(m)})$ has zeros in all entries, except for the $(1, n)$-entry, this entry is in fact equal to the $(1, n)$-entry of $B^t_{\sigma(1)} \cdots B^t_{\sigma(m)}$.

So, under the assumption that $\mathcal{G}_0$ is not commutative we have shown that one can compute integers $p > 0$ and $q < 0$ such that $M_+ = (\mathbf{0}, \mathbf{0}, p)$ and $M_- = (\mathbf{0}, \mathbf{0}, q)$ are in $\mathcal{G}$. It follows that $\langle \mathcal{G} \rangle$ contains the group $\mathcal{N} = \{(\mathbf{0}, \mathbf{0}, c) \in \mathrm{H}(n, \mathbb{Z}) : c \equiv 0 \pmod{m}\}$, where $m = \gcd(p, q)$. Since

$$(\boldsymbol{a}, \boldsymbol{b}, c) \cdot (\mathbf{0}, \mathbf{0}, c') = (\mathbf{0}, \mathbf{0}, c') \cdot (\boldsymbol{a}, \boldsymbol{b}, c) = (\boldsymbol{a}, \boldsymbol{b}, c + c'),$$

we have the following equivalence for the target matrix $A = (\boldsymbol{a}, \boldsymbol{b}, c)$:

$$\begin{aligned} A = (\boldsymbol{a}, \boldsymbol{b}, c) \in \langle \mathcal{G} \rangle \quad & \text{iff} \quad \exists B \in \langle \mathcal{G} \rangle \text{ such that } AB^{-1} \in \mathcal{N} \\ & \text{iff} \quad \exists B \in \langle \mathcal{G} \rangle \text{ such that } B = (\boldsymbol{a}, \boldsymbol{b}, c') \text{ and } c' \equiv c \pmod{m}\,. \end{aligned}$$

To decide whether $\langle\mathcal{G}\rangle$ contains a matrix $B = (\boldsymbol{a}, \boldsymbol{b}, c')$ with $c' \equiv c \pmod{m}$, we will use register automata. Let $d = n - 2$ and consider the following finite automaton with $2d$ registers:

$$\mathbf{Q} = (\{A_1, \dots, A_k\}, S, R_1, \dots, R_d, T_1, \dots, T_d, s_0, \delta, F),$$

where the alphabet of $\mathbf{Q}$ is equal to the set of generator matrices $\mathcal{G} = \{A_1, \dots, A_k\}$, and the set of states S is equal to

$$S = \{(s_1, \dots, s_d, t_1, \dots, t_d, u) \ : \ s_i, t_i, u \in \{0, \dots, m-1\} \text{ for } i = 1, \dots, d\}.$$

Intuitively, $(2d+1)$-tuples from S store the values of a vector $(\boldsymbol{a}, \boldsymbol{b}, c)$ modulo m, and the registers $R_1, \dots, R_d$ and $T_1, \dots, T_d$ store the values of $\boldsymbol{a}$ and $\boldsymbol{b}$, respectively.

The initial state of $\mathbf{Q}$ is $s_0 = (0, \dots, 0)$, and the initial values of all the registers are zeros. The transition function δ is defined as follows. Suppose $\mathbf{Q}$ is in a state $(s_1, \dots, s_d, t_1, \dots, t_d, u)$, and the current values of R_i and T_i are r_i and t_i, respectively, for $i = 1, \dots, d$. If $\mathbf{Q}$ reads a letter $A_\ell = (a_1^\ell, \dots, a_d^\ell, b_1^\ell, \dots, b_d^\ell, c^\ell)$, then it moves to the state $(s_1', \dots, s_d', t_1', \dots, t_d', u')$, where for each $i = 1, \dots, d$:

$$s_i' \equiv s_i + a_i^\ell \pmod{m} \text{ and } t_i' \equiv t_i + b_i^\ell \pmod{m},$$
$$u' \equiv u + c^\ell + s_1 b_1^\ell + \dots + s_d b_d^\ell \pmod{m}.$$

Also, the new value of R_i is $r_i + a_i^\ell$ and the new value of T_i is $t_i + b_i^\ell$.

The set F of final states consists of one state that corresponds to the values of the target matrix $A = (\boldsymbol{a}, \boldsymbol{b}, c) = (a_1, \dots, a_d, b_1, \dots, b_d, c)$ modulo m, that is

$$F = \{(s_1, \dots, s_d, t_1, \dots, t_d, u) \ : \ s_i \equiv a_i, \ t_i \equiv b_i, \ u \equiv c \pmod{m} \ \text{ for } i = 1, \dots, d\}.$$

The automaton $\mathbf{Q}$ accepts a word $w \in \{A_1, \cdots, A_k\}^*$ if after reading w it reaches the final state from F and the values of the registers $R_1, \dots, R_d$ and $T_1, \dots, T_d$ are equal to $a_1, \dots, a_d$ and $b_1, \dots, b_d$, respectively. By construction, the language of $\mathbf{Q}$ in non-empty if and only if $\langle\mathcal{G}\rangle$ contains a matrix $B = (\boldsymbol{a}, \boldsymbol{b}, c')$ with $c' \equiv c \pmod{m}$.

Note that after reading any letter the registers of $\mathbf{Q}$ are changed by constant values, and the transitions have no guards or zero checks. Let $\mathcal{S}$ be the set of values that the registers of $\mathbf{Q}$ can have when it reaches the final state. It is well-known that for a register automaton of this type the set $\mathcal{S}$ is effectively semilinear (see [22, 21] for details). In particular, we can decide whether $\mathcal{S}$ contains the vector $(\boldsymbol{a}, \boldsymbol{b})$, and so the emptiness problem for $\mathbf{Q}$ is decidable. Hence, in the case when $\mathcal{G}_0$ is not commutative the Membership Problem for $\mathrm{H}(n, \mathbb{Z})$ is decidable.

▶ **Corollary 8.** *The Membership Problem for* $\mathrm{H}(n, \mathbb{Q})$ *is decidable.*

Proof. Let $A_i = (\boldsymbol{a}_i, \boldsymbol{b}_i, c_i)$, for $i = 1, \dots, k$, and $A = (\boldsymbol{a}, \boldsymbol{b}, c)$ be the given generators and the target matrix from $\mathrm{H}(n, \mathbb{Q})$. Let N be a natural number such that $A_i = (\frac{1}{N}\boldsymbol{a}_i', \frac{1}{N}\boldsymbol{b}_i', \frac{1}{N^2}c_i')$, for $i = 1, \dots, k$, and $A = (\frac{1}{N}\boldsymbol{a}', \frac{1}{N}\boldsymbol{b}', \frac{1}{N^2}c')$, where $\boldsymbol{a}_i', \boldsymbol{b}_i', c_i'$, for $i = 1, \dots, k$, and $\boldsymbol{a}', \boldsymbol{b}', c'$ are integer vectors and numbers. It is easy to check that

$$(\tfrac{1}{N}\boldsymbol{x}, \tfrac{1}{N}\boldsymbol{y}, \tfrac{1}{N^2}c) \cdot (\tfrac{1}{N}\boldsymbol{x}', \tfrac{1}{N}\boldsymbol{y}', \tfrac{1}{N^2}c') = (\tfrac{1}{N}(\boldsymbol{x} + \boldsymbol{x}'), \tfrac{1}{N}(\boldsymbol{y} + \boldsymbol{y}'), \tfrac{1}{N^2}(c + c' + \boldsymbol{x}^\top \boldsymbol{y}')) .$$

Hence $A \in \langle A_1, \dots, A_k\rangle$ iff $A' \in \langle A_1', \dots, A_k'\rangle$, where $A' = (\boldsymbol{a}', \boldsymbol{b}', c')$ and $A_i' = (\boldsymbol{a}_i', \boldsymbol{b}_i', c_i')$, for $i = 1, \dots, k$, are matrices with integer entries, that is, from $\mathrm{H}(n, \mathbb{Z})$. By Theorem 7 we can decide whether $A' \in \langle A_1', \dots, A_k'\rangle$. ◀

4 The Half-Space Reachability Problem for $\mathrm{GL}(2,\mathbb{Z})$

In this section we will show that the Half-Space Reachability Problem for $\mathrm{GL}(2,\mathbb{Z})$ is decidable (Theorem 17).

▶ **Definition 9.** *For an integer n, the sign of n as follows:* $\mathrm{sg}(n) = 1$ *if* $n > 0$, $\mathrm{sg}(n) = -1$ *if* $n < 0$, *and* $\mathrm{sg}(n) = *$ *if* $n = 0$.

For a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2}$, *define* $\mathrm{sg}(A) := \begin{pmatrix} \mathrm{sg}(a) & \mathrm{sg}(b) \\ \mathrm{sg}(c) & \mathrm{sg}(d) \end{pmatrix}$.

If A and B are two expressions whose values are in the set $\{1, -1, *\}$, then the notation $A \simeq B$ means that $A = B$ or $A = *$ or $B = *$.

▶ **Proposition 10.** *Suppose w is a canonical word of the form $w = SR^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}$, where $\alpha_i \in \{1,2\}$ for $i = 1,\dots,n$. Then* $\mathrm{sg}(\varphi(w)) \simeq \begin{pmatrix} (-1)^n & (-1)^n \\ (-1)^n & (-1)^n \end{pmatrix}$.

Proof. The proof is by induction on n. For $n = 1$, we have

$$\mathrm{sg}(\varphi(SR)) = \mathrm{sg}\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \mathrm{sg}(-1) & \mathrm{sg}(-1) \\ \mathrm{sg}(0) & \mathrm{sg}(-1) \end{pmatrix} \simeq \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix} \quad \text{and}$$

$$\mathrm{sg}(\varphi(SR^2)) = \mathrm{sg}\begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} \mathrm{sg}(-1) & \mathrm{sg}(0) \\ \mathrm{sg}(-1) & \mathrm{sg}(-1) \end{pmatrix} \simeq \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$$

Suppose the statement of the proposition is true for $w = SR^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}$ and consider the words wSR and wSR^2. Assume that $\varphi(w) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\mathrm{sg}(\varphi(w)) = \begin{pmatrix} \mathrm{sg}(a) & \mathrm{sg}(b) \\ \mathrm{sg}(c) & \mathrm{sg}(d) \end{pmatrix} \simeq \begin{pmatrix} (-1)^n & (-1)^n \\ (-1)^n & (-1)^n \end{pmatrix}$. Then we have

$$\varphi(wSR) = \varphi(w)\varphi(SR) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -a & -a-b \\ -c & -c-d \end{pmatrix} \quad \text{and}$$

$$\varphi(wSR^2) = \varphi(w)\varphi(SR^2) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -a-b & -b \\ -c-d & -d \end{pmatrix}.$$

From these formulas it not hard to see that $\mathrm{sg}(\varphi(wSR)) \simeq \begin{pmatrix} (-1)^{n+1} & (-1)^{n+1} \\ (-1)^{n+1} & (-1)^{n+1} \end{pmatrix}$ and $\mathrm{sg}(\varphi(wSR^2)) \simeq \begin{pmatrix} (-1)^{n+1} & (-1)^{n+1} \\ (-1)^{n+1} & (-1)^{n+1} \end{pmatrix}$. ◀

▶ **Proposition 11.** *Let w be a canonical word of the form $w = S^{\beta}R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}S^{\varepsilon}$, where $\beta, \varepsilon \in \{0,1\}$ and $\alpha_i \in \{1,2\}$, $i = 1,\dots,n$. Then* $\mathrm{sg}(\varphi(w)) \simeq \begin{pmatrix} (-1)^n & (-1)^{n+\varepsilon} \\ (-1)^{n-1+\beta} & (-1)^{n-1+\beta+\varepsilon} \end{pmatrix}$.

Proof. First, consider the case when $\varepsilon = 0$. Suppose $\varphi(SR^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then by Proposition 10 we have

$$\mathrm{sg}(\varphi(SR^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n})) = \begin{pmatrix} \mathrm{sg}(a) & \mathrm{sg}(b) \\ \mathrm{sg}(c) & \mathrm{sg}(d) \end{pmatrix} \simeq \begin{pmatrix} (-1)^n & (-1)^n \\ (-1)^n & (-1)^n \end{pmatrix}.$$

On the other hand, $\varphi(R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}) =$

$$= -\varphi(S)\varphi(SR^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix}.$$

Hence $\mathrm{sg}(\varphi(R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n})) = \begin{pmatrix} \mathrm{sg}(c) & \mathrm{sg}(d) \\ \mathrm{sg}(-a) & \mathrm{sg}(-b) \end{pmatrix} \simeq \begin{pmatrix} (-1)^n & (-1)^n \\ (-1)^{n-1} & (-1)^{n-1} \end{pmatrix}$. Thus, for $\beta \in \{0,1\}$, we showed that

$$\mathrm{sg}(\varphi(S^\beta R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n})) \simeq \begin{pmatrix} (-1)^n & (-1)^n \\ (-1)^{n-1+\beta} & (-1)^{n-1+\beta} \end{pmatrix}. \tag{7}$$

Now assume $\varepsilon = 1$ and let $\varphi(S^\beta R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then

$$\begin{aligned} \varphi(S^\beta R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}S) &= \varphi(S^\beta R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n})\varphi(S) \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}. \end{aligned} \tag{8}$$

From equations (7) and (8) we obtain

$$\mathrm{sg}(\varphi(S^\beta R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}S)) = \begin{pmatrix} \mathrm{sg}(b) & \mathrm{sg}(-a) \\ \mathrm{sg}(d) & \mathrm{sg}(-c) \end{pmatrix} \simeq \begin{pmatrix} (-1)^n & (-1)^{n+1} \\ (-1)^{n-1+\beta} & (-1)^{n-1+\beta+1} \end{pmatrix}. \tag{9}$$

Equations (7) and (9) imply that for any $\beta, \varepsilon \in \{0,1\}$ $\mathrm{sg}(\varphi(S^\beta R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}S^\varepsilon)) \simeq \begin{pmatrix} (-1)^n & (-1)^{n+\varepsilon} \\ (-1)^{n-1+\beta} & (-1)^{n-1+\beta+\varepsilon} \end{pmatrix}$. ◀

From Proposition 11 and the equalities

$$\varphi(X)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} \quad \text{and} \quad \varphi(N)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ -c & -d \end{pmatrix}$$

we obtain the following proposition.

▶ **Proposition 12.** *Let w be a canonical word of the form $w = N^\delta X^\gamma S^\beta R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}S^\varepsilon$, where $\beta, \gamma, \delta, \varepsilon \in \{0,1\}$ and $\alpha_i \in \{1,2\}$ for $i = 1, \ldots, n$. Then*

$$\mathrm{sg}(\varphi(w)) \simeq \begin{pmatrix} (-1)^{n+\gamma} & (-1)^{n+\gamma+\varepsilon} \\ (-1)^{n-1+\beta+\gamma+\delta} & (-1)^{n-1+\beta+\gamma+\delta+\varepsilon} \end{pmatrix}.$$

▶ **Theorem 13.** *The set of matrices in $\mathrm{GL}(2,\mathbb{Z})$ whose particular entry is nonnegative forms a regular subset. In other words, for all $i, j \in \{1,2\}$, the following subset of $\mathrm{GL}(2,\mathbb{Z})$ is regular:*

$$\mathrm{Pos}_{ij} = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z}) \ : \ a_{ij} \geq 0 \right\}.$$

Proof. Suppose $i = j = 2$ as other cases are similar. Let A be a matrix from $\mathrm{GL}(2,\mathbb{Z})$ and let $w = N^\delta X^\gamma S^\beta R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}S^\varepsilon$, where $\beta, \gamma, \delta, \varepsilon \in \{0,1\}$ and $\alpha_i \in \{1,2\}$ for $i = 1, \ldots, n$, be a canonical word that represents A, that is, $A = \varphi(w)$. From Proposition 12 we see that $\mathrm{sg}(a_{22}) \simeq (-1)^{n-1+\beta+\gamma+\delta+\varepsilon}$. Hence

$$a_{22} \geq 0 \quad \text{if and only if} \quad n - 1 + \beta + \gamma + \delta + \varepsilon \equiv 0 \pmod 2. \tag{10}$$

To finish the proof, we note that the set of all canonical words is regular. Furthermore, given a canonical word of the form $w = N^{\delta}X^{\gamma}S^{\beta}R^{\alpha_1}SR^{\alpha_2}\cdots SR^{\alpha_n}S^{\varepsilon}$, a finite automaton can read off the values of $\beta, \gamma, \delta, \varepsilon$ and determine the parity of number n. From this data an automaton can decide whether $a_{22} \geq 0$ by the above mentioned equivalence (10). Hence the set of canonical words w such that $\varphi(w) \in \mathrm{Pos}_{22}$ can be recognised by a finite automaton. ◀

Next theorem was proved in [33].

▶ **Theorem 14.** *For every $k \in \mathbb{Z}$, the following subset of* $\mathrm{GL}(2,\mathbb{Z})$ *is regular:*

$$\mathrm{S}_{ij}(k) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z}) \ : \ a_{ij} = k \right\}.$$

As a corollary from Theorems 13 and 14 we obtain:

▶ **Theorem 15.** *For every $k \in \mathbb{Z}$, the following subsets of* $\mathrm{GL}(2,\mathbb{Z})$ *are regular:*

$$\mathrm{S}_{ij}(\geq k) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z}) \ : \ a_{ij} \geq k \right\} \quad \textit{and}$$
$$\mathrm{S}_{ij}(\leq k) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z}) \ : \ a_{ij} \leq k \right\}.$$

Proof. Since $\mathrm{S}_{ij}(\leq k)$ is the complement of $\mathrm{S}_{ij}(\geq k+1)$, it suffices to prove that the sets $\mathrm{S}_{ij}(\geq k)$ are regular.

If $k = 0$, then it follows from Theorem 13 that $\mathrm{S}_{ij}(\geq 0) = \mathrm{Pos}_{ij}$ is regular. Furthermore,

$$\mathrm{S}_{ij}(\geq k) = \mathrm{Pos}_{ij} \ \setminus \ \bigcup_{n=0}^{k-1} M_{ij}(n) \text{ if } k > 0 \quad \text{and} \quad \mathrm{S}_{ij}(\geq k) = \mathrm{Pos}_{ij} \ \cup \ \bigcup_{n=k}^{-1} M_{ij}(n) \text{ if } k < 0.$$

Since by Corollary 6 regular subsets of $\mathrm{GL}(2,\mathbb{Z})$ are closed under Boolean operations, we conclude that $\mathrm{S}_{ij}(\geq k)$ is a regular set for any $k \in \mathbb{Z}$. ◀

▶ **Theorem 16.** *Let $\lambda \in \mathbb{Q}$ and $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Q} \times \mathbb{Q}$. Then the set $\mathcal{S}(\boldsymbol{u}, \boldsymbol{v}, \lambda) = \{ M \in \mathrm{GL}(2,\mathbb{Z}) \ : \ \boldsymbol{u}^{\top} M \boldsymbol{v} \geq \lambda \}$ is a regular subset of* $\mathrm{GL}(2,\mathbb{Z})$.

Proof. Note that if $\boldsymbol{u} = \boldsymbol{0}$ or $\boldsymbol{v} = \boldsymbol{0}$, then $\boldsymbol{u}^{\top} M \boldsymbol{v} = 0$. In this case $\mathcal{S}(\boldsymbol{u}, \boldsymbol{v}, \lambda)$ equals either the empty set or $\mathrm{GL}(2,\mathbb{Z})$, both of which are regular subsets. Hence we will assume that both $\boldsymbol{u} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$ and $\boldsymbol{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ are nonzero vectors. By multiplying the inequality $\boldsymbol{u}^{\top} M \boldsymbol{v} \geq \lambda$ by the least common multiple of the denominators of u_1, u_2, v_1, v_2, we can assume that $\boldsymbol{u}$ and $\boldsymbol{v}$ have integer coefficients. Furthermore, we can divide $\boldsymbol{u}^{\top} M \boldsymbol{v} \geq \lambda$ by $\gcd(u_1, u_2)$ and $\gcd(v_1, v_2)$ and so assume from now on that $\gcd(u_1, u_2) = \gcd(v_1, v_2) = 1$.

Finally, note that the inequality $\boldsymbol{u}^{\top} M \boldsymbol{v} \geq \lambda$ is equivalent to $\boldsymbol{u}^{\top} M \boldsymbol{v} \geq \lceil \lambda \rceil$, where $\lceil \lambda \rceil = \min\{ n \in \mathbb{Z} \ : \ n \geq \lambda \}$. So, we can assume that λ is also an integer number.

Since $\gcd(u_1, u_2) = \gcd(v_1, v_2) = 1$, there are integers s_1, s_2, t_1, t_2 such that $s_1 u_1 + s_2 u_2 = 1$ and $t_1 v_1 + t_2 v_2 = 1$. Hence the matrices $A = \begin{pmatrix} u_1 & -s_2 \\ u_2 & s_1 \end{pmatrix}$ and $B = \begin{pmatrix} v_1 & -t_2 \\ v_2 & t_1 \end{pmatrix}$ belong to $\mathrm{GL}(2,\mathbb{Z})$, and we have that $\boldsymbol{u} = A\boldsymbol{e}_1$ and $\boldsymbol{v} = B\boldsymbol{e}_1$. Therefore, the inequality $\boldsymbol{u}^{\top} M \boldsymbol{v} \geq \lambda$ is equivalent to $\boldsymbol{e}_1^{\top} A^{\top} M B \boldsymbol{e}_1 \geq \lambda$. In other words,

$$M \in \mathcal{S}(\boldsymbol{u}, \boldsymbol{v}, \lambda) \quad \Longleftrightarrow \quad A^{\top} M B \in \mathrm{S}_{11}(\geq \lambda) \quad \Longleftrightarrow \quad M \in \left(A^{\top}\right)^{-1} \cdot \mathrm{S}_{11}(\geq \lambda) \cdot B^{-1}.$$

By Theorem 15, $\mathrm{S}_{11}(\geq \lambda)$ is a regular subset of $\mathrm{GL}(2,\mathbb{Z})$. Let L be a regular language and let w_1, w_2 be canonical words such that $\varphi(L) = \mathrm{S}_{11}(\geq \lambda)$ and $\varphi(w_1) = (A^\top)^{-1}$ and $\varphi(w_2) = B^{-1}$. Then $\{w_1\} \cdot L \cdot \{w_2\}$ is a regular language such that $\varphi(\{w_1\} \cdot L \cdot \{w_2\}) = (A^\top)^{-1} \cdot \mathrm{S}_{11}(\geq \lambda) \cdot B^{-1} = \mathcal{S}(\boldsymbol{u}, \boldsymbol{v}, \lambda)$. ◀

▶ **Theorem 17.** *The Half-Space Reachability Problem for* $\mathrm{GL}(2,\mathbb{Z})$ *is decidable.*

Proof. Let $\mathcal{G} = \{A_1, \ldots, A_k\}$ be a finite collection of matrices from $\mathrm{GL}(2,\mathbb{Z})$, λ be a rational number and $\boldsymbol{u}, \boldsymbol{v}$ be vectors from $\mathbb{Q}^2$. Define $\mathcal{S}(\boldsymbol{u}, \boldsymbol{v}, \lambda) := \{\, M \in \mathrm{GL}(2,\mathbb{Z}) \;:\; \boldsymbol{u}^\top M \boldsymbol{v} \geq \lambda \,\}$. By Theorem 16, $\mathcal{S}(\boldsymbol{u}, \boldsymbol{v}, \lambda)$ is a regular subset of $\mathrm{GL}(2,\mathbb{Z})$. Let $L_\mathcal{S}$ be a regular language such that $\mathcal{S}(\boldsymbol{u}, \boldsymbol{v}, \lambda) = \varphi(L_\mathcal{S})$. It is not hard to see that the semigroup $\langle \mathcal{G} \rangle$ is also a regular subset. Indeed, consider a regular language $L_\mathcal{G} = (w_1 \cup \cdots \cup w_k)^+$, where $w_1, \ldots, w_k$ are canonical words that correspond to the matrices $A_1, \ldots, A_k$, respectively. Then $\langle \mathcal{G} \rangle = \varphi(L_\mathcal{G})$.

By Corollary 6, we can algorithmically construct a regular language $L^\cap$ such that $\varphi(L^\cap) = \varphi(L_\mathcal{S}) \cap \varphi(L_\mathcal{G}) = \mathcal{S}(\boldsymbol{u}, \boldsymbol{v}, \lambda) \cap \langle \mathcal{G} \rangle$. Now we have the following equivalence:

$$\text{there is } M \in \langle \mathcal{G} \rangle \text{ such that } \boldsymbol{u}^\top M \boldsymbol{v} \geq \lambda \quad \text{iff} \quad \mathcal{S}(\boldsymbol{u}, \boldsymbol{v}, \lambda) \cap \langle \mathcal{G} \rangle = \varphi(L^\cap) \neq \emptyset.$$

The last condition is equivalent to $L^\cap \neq \emptyset$. Therefore, we reduced the Half-Space Reachability Problem for $\mathrm{GL}(2,\mathbb{Z})$ to the emptiness problem for regular languages. ◀

5 The Half-Space Reachability Problem for the Heisenberg Group

▶ **Definition 18.** *Let* $\mathcal{S} := B_1, \ldots, B_m$ *be a sequence in* $\mathrm{H}(n,\mathbb{Q})$ *and* A *a particular matrix in* $\mathrm{H}(n,\mathbb{Q})$. *A pair* $i, j \in \{1 \ldots, m\}$ *with* $i \leq j$ *is called an* A-block *of* $\mathcal{S}$ *if*

1. $B_k = A$ *for all* $k \in \{i, \ldots, j\}$,
2. *either* $i = 1$ *or* $B_{i-1} \neq A$,
3. *either* $j = m$ *or* $B_{j+1} \neq A$.

We say that $\mathcal{S}$ *is* pure *if it has at most one* A*-block for every matrix* A.

Given a sequence $\mathcal{S} = B_1, \ldots, B_m \in \mathrm{H}(n,\mathbb{Q})$, define $C_i := \log(B_i)$ for $i = 1, \ldots, m$, $\Delta(\mathcal{S}) := \sum_{1 \leq i < j \leq m} [C_i, C_j]$, and $\delta(\mathcal{S}) := \Delta(\mathcal{S})_{1,n}$. Recall that using the Baker-Campbell-Hausdorff formula (3) we can express the product of the sequence $\mathcal{S}$ as follows

$$B_1 \cdots B_m = \exp\Big(\sum_{i=1}^{m} C_i + \frac{1}{2} \underbrace{\sum_{1 \leq i < j \leq m} [C_i, C_j]}_{\Delta(\mathcal{S})}\Big) \tag{11}$$

▶ **Proposition 19.** *For any sequence of matrices* $\mathcal{S} = B_1, \ldots, B_m \in \mathrm{H}(n,\mathbb{Q})$, *there is a permutation* $\pi \in S_m$ *such that sequence* $\mathcal{S}' := B_{\pi(1)}, \ldots, B_{\pi(m)}$ *is pure and* $\delta(\mathcal{S}) \leq \delta(\mathcal{S}')$.

The proof of Proposition 19 can be found in the full version [11].

▶ **Theorem 20.** *The Half-Space Reachability Problem for* $\mathrm{H}(n,\mathbb{Q})$ *is decidable.*

Proof. Consider an instance of the Half-Space Reachability Problem, given by a finite set $\mathcal{G} = \{A_1, \ldots, A_k\} \subseteq \mathrm{H}(n,\mathbb{Q})$ of generators, vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Q}^n$ and a scalar $\lambda \in \mathbb{Q}$.

Given a sequence $\mathcal{S} = B_1, \ldots, B_m$ of elements of $\mathcal{G}$ and a permutation $\sigma \in \mathrm{Sym}_m$, define $\mathcal{S}_\sigma = B_{\sigma(1)}, \ldots, B_{\sigma(m)}$. It follows from Equation (11) that the entries of the product $B_{\sigma(1)} \cdots B_{\sigma(m)}$ do not depend on the choice of $\sigma \in \mathrm{Sym}_m$, except for the $(1, n)$-entry which is equal to $\frac{1}{2}\Delta(\mathcal{S}_\sigma)_{1,n}$ plus a constant that also does not depend on σ. So, the permutation

σ that maximises $\boldsymbol{u}^\top B_{\sigma(1)} \cdots B_{\sigma(m)} \boldsymbol{v}$ is the same which maximises or minimises $\Delta(\mathcal{S}_\sigma)_{1,n}$ depending on the sign of the coefficient at $\Delta(\mathcal{S}_\sigma)_{1,n}$ in the expression $\boldsymbol{u}^\top \Delta(\mathcal{S}_\sigma)\boldsymbol{v}$, namely, on the sign of $\boldsymbol{u}_1\boldsymbol{v}_n$. By Proposition 19 we may assume without loss of generality that the optimal permutation σ is such that $\mathcal{S}_\sigma$ is pure.

By the reasoning above, to decide the given instance of the Half-Space Reachability Problem it suffices to restrict attention to pure sequences of generators. Equivalently we must decide whether there exist nonnegative integers $n_1, \ldots, n_k$ and a permutation $\sigma \in \mathrm{Sym}_k$ such that $\boldsymbol{u}^\top A^{n_1}_{\sigma(1)} \cdots A^{n_k}_{\sigma(k)} \boldsymbol{v} \geq \lambda$. Write $C_i = \log A_i$ for $i = 1, \ldots, k$. Then

$$\begin{aligned} \boldsymbol{u}^\top A^{n_1}_{\sigma(1)} \cdots A^{n_k}_{\sigma(k)} \boldsymbol{v} &= \boldsymbol{u}^\top \exp\left(\sum_{i=1}^{k} n_i C_{\sigma(i)} + \frac{1}{2} \sum_{i<j} n_i n_j [C_{\sigma(i)}, C_{\sigma(j)}] \right) \boldsymbol{v} \\ &= Q(n_1, \ldots, n_k) \end{aligned}$$

for some quadratic polynomial $Q(x_1, \ldots, x_k)$ with rational coefficients.

In the work of Grunewald and Segal [14] an algorithm is given for solving the following problem: does there exist integers $n_1, \ldots, n_k$ that satisfy a given quadratic equation $Q(n_1, \ldots, n_k) = 0$ (with rational coefficients) and a finite number of linear inequalities on $n_1, \ldots, n_k$ (also with rational coefficients).

By introducing a "dummy" variable we can use the Grunewald and Segal algorithm to decide whether $Q(n_1, \ldots, n_k) \geq \lambda$ for some nonnegative integers $n_1, \ldots, n_k$. Hence the Half-Space Reachability Problem for $\mathrm{H}(n, \mathbb{Q})$ is decidable. ◀

References

1 László Babai. Trading group theory for randomness. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*, pages 421–429, 1985.

2 László Babai, Robert Beals, Jin-yi Cai, Gábor Ivanyos, and Eugene 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.

3 Robert Beals. Algorithms for matrix groups and the Tits alternative. *J. Comput. Syst. Sci.*, 58(2):260–279, 1999.

4 Paul Bell, Mika Hirvensalo, and Igor Potapov. The identity problem for matrix semigroups in $\mathrm{SL}(2, \mathbb{Z})$ is NP-complete. In *Proceedings of the 28th Annual ACM-SIAM Symposium on Discrete Algorithms, SODA*, 2017.

5 Paul C. Bell and Igor 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 Paul C. Bell and Igor Potapov. On the computational complexity of matrix semigroup problems. *Fundam. Inf.*, 116(1-4):1–13, 2012.

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

8 Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

9 Julien Cassaigne, Vesa Halava, Tero Harju, and François Nicolas. Tighter undecidability bounds for matrix mortality, zero-in-the-corner problems, and more. *CoRR*, abs/1404.0644, 2014. URL: `http://arxiv.org/abs/1404.0644`, `arXiv:1404.0644`.

10 Christian Choffrut and Juhani Karhumäki. Some decision problems on integer matrices. *RAIRO-Theor. Inf. Appl.*, 39(1):125–131, 2005.

11 Thomas Colcombet, Joël Ouaknine, Pavel Semukhin, and James Worrell. On reachability problems for low dimensional matrix semigroups. *CoRR*, abs/1902.09597, 2019. URL: `http://arxiv.org/abs/1902.09597`, `arXiv:1902.09597`.

12 H. Derksen, E. Jeandel, and P. Koiran. Quantum automata and algebraic groups. *J. Symb. Comput.*, 39(3-4):357–371, 2005.

13 Fritz J. Grunewald and Daniel Segal. How to solve a quadratic equation in integers. *Mathematical Proceedings of the Cambridge Philosophical Society*, 89(1):1–5, 1981.

14 Fritz J. Grunewald and Daniel Segal. On the integer solutions of quadratic equations. *J. Reine Angew. Math.*, 569:13–45, 2004.

15 Yuri Gurevich and Paul Schupp. Membership problem for the modular group. *SIAM J. Comput.*, 37(2):425–459, May 2007.

16 V. Halava and M. Hirvensalo. Improved matrix pair undecidability results. *Acta Informatica*, 44(3-4):191–205, 2007.

17 Vesa Halava, Tero Harju, and Mika Hirvensalo. Undecidability bounds for integer matrices using Claus instances. *Int. J. Found. Comput. Sci.*, 18(5):931–948, 2007.

18 B. Hall. *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*, volume 222 of *Graduate Texts in Mathematics*. Springer International Publishing, 2015.

19 Ehud Hrushovski, Joël Ouaknine, Amaury Pouly, and James Worrell. Polynomial invariants for affine programs. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*, pages 530–539, 2018.

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

21 Felix Klaedtke and Harald Rueß. Parikh automata and monadic second-order logics with linear cardinality constraints. Technical report, Albert-Ludwigs-Universität Freiburg, 2002.

22 Felix Klaedtke and Harald Rueß. Monadic second-order logics with cardinalities. In *Automata, Languages and Programming, 30th International Colloquium, ICALP*, pages 681–696, 2003.

23 Sang-Ki Ko, Reino Niskanen, and Igor Potapov. On the identity problem for the special linear group and the Heisenberg group. In *45th International Colloquium on Automata, Languages, and Programming, ICALP*, pages 132:1–132:15, 2018.

24 Daniel König, Markus Lohrey, and Georg Zetzsche. Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups. *CoRR*, abs/1507.05145, 2015. URL: `http://arxiv.org/abs/1507.05145`, `arXiv:1507.05145`.

25 Roger C. Lyndon and Paul E. Schupp. *Combinatorial group theory*. Springer-Verlag, Berlin-New York, 1977. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 89.

26 Wilhelm Magnus, Abraham Karrass, and Donald Solitar. *Combinatorial group theory*. Dover Publications, Inc., New York, revised edition, 1976.

27 A. Mandel and I. Simon. On finite semigroups of matrices. *Theor. Comput. Sci.*, 5(2):101–111, 1977.

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

29 K. A. Mihailova. The occurrence problem for a direct product of groups. *Dokl. Akad. Nauk*, 119:1103–1105, 1958.

30 Joël Ouaknine and James Worrell. Positivity problems for low-order linear recurrence sequences. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*, pages 366–379, 2014.

31 Michael S. Paterson. Unsolvability in 3×3 matrices. *Studies in Appl. Math.*, 49:105–107, 1970.

32 Igor Potapov and Pavel 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*, pages 170–186, 2017.

33 Igor Potapov and Pavel Semukhin. Membership problem in GL(2, Z) extended by singular matrices. In *42nd International Symposium on Mathematical Foundations of Computer Science, MFCS 2017, August 21-25, 2017 - Aalborg, Denmark*, pages 44:1–44:13, 2017.

34 Igor Potapov and Pavel Semukhin. Vector and scalar reachability problems in $\mathrm{SL}(2, \mathbb{Z})$. *J. Comput. Syst. Sci.*, 100:30–43, 2019.

35 Robert A. Rankin. *Modular forms and functions*. Cambridge University Press, Cambridge-New York-Melbourne, 1977.

36 Grzegorz Rozenberg and Arto Salomaa. *Cornerstones of undecidability*. Prentice Hall International Series in Computer Science. Prentice Hall, 1994.

37 Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, Inc., New York, NY, USA, 1986.

38 Charles Sims. *Computation with Finitely Presented Groups*. Cambridge University Press, 1994.