

On Affine Reachability Problems^{*}

Stefan Jaax¹ and Stefan Kiefer²

¹ Technische Universität München, Germany

² University of Oxford, UK

Abstract. We analyze affine reachability problems in dimensions 1 and 2. On the one hand, we show that the reachability problem for 1-register machines over the integers with affine updates is PSPACE-hard, hence PSPACE-complete, strengthening a result by Finkel et al. that required polynomial updates. On the other hand, motivated by tight connections with 1-dimensional affine reachability problems without control states, we study algorithmic problems in finitely generated semigroups of 2-dimensional upper-triangular integer matrices. Building on a variety of techniques from recent years, we obtain a number of complexity results, including NP-completeness of the mortality problem for matrices with determinants +1 and 0.

Keywords: Counter Machines · Matrix Semigroups · Reachability

1 Introduction

Counter machines are abstract models of computation, consisting of a finite control and a set of registers which store numbers. Upon taking a transition, the machine may perform simple arithmetic on the registers. There is a great variety of counter machines, depending on the domain of the registers (rationals, integers, naturals, \dots), whether the content of the registers influences the control flow (e.g., via zero tests), and the types of allowed register updates (changes can only be additive, linear, affine, polynomial, \dots).

As a model of programs with arithmetic, counter machines relate to program analysis and verification. They also provide natural classes of finitely presented systems with infinitely many states, with a regular-shaped transition structure. Minsky [18] showed that counter machines with nonnegative integer registers, additive updates, and zero tests are Turing-powerful. *Vector addition systems with states* (VASS), which are roughly equivalent to *Petri nets*, are a related well-studied model without zero tests. Reachability in this model is decidable, albeit with very high complexity [9].

One of the contributions of this paper is the precise complexity of reachability of *affine register machines*. These are counter machines with a single integer register (two registers already lead to undecidability [26, Chapter 2.5]), no zero tests, and affine register updates; i.e., the transitions are labelled with updates of the

^{*} Stefan Jaax is supported by an ERC Advanced Grant (787367: PaVeS). Stefan Kiefer is supported by a Royal Society University Research Fellowship.

form $x := ax + b$, where x stands for the register and a, b are integer coefficients. Finkel et al. [11] considered a more general model, *polynomial register machines*, with the difference that the updates consist of arbitrary integer polynomials, not just affine polynomials $ax + b$. The main result of [11] is that reachability in polynomial register machines is PSPACE-complete. We show that reachability in affine register machines is also PSPACE-hard, hence PSPACE-complete. Niskanen [20] strengthened the lower bound from [11] in an orthogonal direction, by showing PSPACE-hardness in the case with polynomial updates but without control states. As we explain in the following (see also Proposition 1 below), the stateless case is intimately connected with finitely generated monoids over two-dimensional upper-triangular integer matrices. This leads us to investigate several natural reachability problems in such monoids.

Matrix monoids. A finite set of matrices $\mathcal{M} \subset \mathbb{Q}^{d \times d}$ generates a monoid $\langle \mathcal{M} \rangle$ under matrix multiplication, i.e., $\langle \mathcal{M} \rangle$ is the set of products of matrices from \mathcal{M} , including the identity matrix, which we view as the empty product. Algorithmic problems about such monoids are hard, often undecidable. For example, Pater-son [23] showed in 1970 that the *mortality* problem, i.e., deciding whether the zero matrix is in the generated monoid, is undecidable, even for integer matrices with $d = 3$. It remains undecidable for $d = 3$ with $|\mathcal{M}| = 6$ and for $d = 18$ with $|\mathcal{M}| = 2$; see [19]. Mortality for two-dimensional matrices is known to be NP-hard [1], but decidability remains a longstanding open problem; see, e.g., [25].

Mortality is a special case of the *membership* problem: given \mathcal{M} and a matrix T , is $T \in \langle \mathcal{M} \rangle$? Two other natural problems consider certain linear projections of the matrices in $\langle \mathcal{M} \rangle$: The *vector reachability* problem asks, given \mathcal{M} and two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Q}^d$, if there is a matrix $M \in \langle \mathcal{M} \rangle$ such that $M\mathbf{x} = \mathbf{y}$. Similarly, the *scalar reachability* problem asks if there is a matrix $M \in \langle \mathcal{M} \rangle$ such that $\mathbf{y}^T M \mathbf{x} = \lambda$ holds for given vectors \mathbf{x}, \mathbf{y} and a given scalar $\lambda \in \mathbb{Q}$. For $d = 2$ none of these problems are known to be decidable, not even for integer matrices. In the case $d = 2$, mortality is known to be decidable when $|\mathcal{M}| = 2$ holds [5], and for integer matrices whose determinants are in $\{-1, 0, +1\}$ (see [21]).

Even the case of a single matrix, i.e., $|\mathcal{M}| = 1$, is very difficult; see [22] for a survey. This case is closely related to the algorithmic analysis of *linear recurrence sequences*, which are sequences u_0, u_1, \dots of numbers such that there are constants a_1, \dots, a_d such that $u_{n+d} = a_1 u_{n+d-1} + a_2 u_{n+d-2} + \dots + a_d u_n$ holds for all $n \in \mathbb{N}$. In the case $|\mathcal{M}| = 1$ the vector reachability problem is referred to as the *orbit* problem, and the scalar reachability problem as *Skolem* problem. The orbit problem is decidable in polynomial time [16], but the Skolem problem is only known to be decidable for $d \leq 4$ (this requires Baker's Theorem) [22, 8].

In the following we do not restrict $|\mathcal{M}|$ but focus on integer matrices in $d = 2$. Recently, there has been steady progress for certain special cases. It was shown by Potapov and Semukhin [25] that the membership problem for two-dimensional integer matrices is decidable for non-singular matrices. This result builds on automata-theoretic techniques developed, e.g., in [7], where it was shown that the problem of deciding whether $\langle \mathcal{M} \rangle$ is a group is decidable. At its heart, this technique exploits the special structure of the group of matrices with determi-

nants ± 1 and its subgroups. For matrices with determinant 1, further results are known, namely decidability of vector reachability [24] and NP-completeness of the membership problem [2]. If all matrices in \mathcal{M} have determinant 1 and \mathcal{M} is closed under inverses, then $\langle \mathcal{M} \rangle$ is a group. In this case, one can decide in polynomial time for a given matrix M whether M or $-M$ is in $\langle \mathcal{M} \rangle$ [14].

We focus on *upper-triangular* integer matrices, i.e., integer matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$. Curiously, decidability of the membership, vector reachability, and scalar reachability problems are still challenging, and indeed open, despite the severe restriction on the matrix shape and dimension. This class of reachability problems is motivated by its tight connection to (stateless) affine reachability. For instance, *affine reachability over \mathbb{Q}* reduces to scalar reachability for upper-triangular two-dimensional integer matrices; see Proposition 1. Affine reachability over \mathbb{Q} asks, given a set of affine rational functions in one variable and two rational numbers $x, y \in \mathbb{Q}$, whether x can be transformed into y using one or more applications of the given functions, chosen nondeterministically.

Whereas affine reachability over \mathbb{Z} is in PSPACE by [11], decidability of affine reachability over \mathbb{Q} is open. This problem can be viewed as a “nondeterministic” variant of the reachability problem with a single, but only piecewise affine, function, so-called *piecewise affine maps*; this problem is not known to be decidable either; see [17,6]. Variants of piecewise affine reachability, also over \mathbb{Z} , are studied in [3].

Contribution and organization of the paper. The paper centres around reachability problems in monoids over two-dimensional upper-triangular integer matrices. In Section 2 we state tight (perhaps folklore) connections of these problems to reachability problems of affine functions.

In Section 3 we study the case with ± 1 on the diagonal. Establishing a connection with so-called \mathbb{Z} -VASS [15] allows us to prove NP-completeness, although we show that the case where all generator matrices have determinant -1 is in P by a reduction to a linear system of Diophantine equations over the integers.

In Section 4 we study vector reachability. We show that the problem is hard for affine reachability over \mathbb{Q} , hence decidability requires a breakthrough, but the case where the bottom-right entries are non-zero reduces to reachability in polynomial register machines, hence is in PSPACE.

In Section 5 we study the membership problem. If both diagonal entries are non-zero, we show that the problem is NP-complete, which in turn shows NP-completeness of the following problem: given $n + 1$ non-constant affine functions over \mathbb{Z} in one variable, can the $n + 1$ st function be represented as a composition of the other n functions? The case where only one of the diagonal entries is restricted to be non-zero is decidable in PSPACE. Finally, for the case where both diagonal entries may be 0, we establish reductions between membership and scalar reachability, suggesting that decidability of membership would also require a breakthrough.

In Section 6 we turn to the mortality problem. We show that mortality is NP-hard even when the non-singular matrices are upper-triangular with 1s on the

diagonal. This strengthens the main result of [1] and simplifies its proof. Leveraging recent results from [24,2], we show that mortality of two-dimensional integer matrices (not necessarily triangular) with determinants $\pm 1, 0$ is NP-complete.

In Section 7 we show that reachability in affine register machines is PSPACE-hard, hence PSPACE-complete. We conclude in Section 8.

2 Preliminaries

We write \mathbb{Z} for the set of integer numbers, $\mathbb{N} = \{0, 1, 2, \dots\}$ for the set of non-negative integers, and \mathbb{Q} for the set of rationals. We write UT for the set (and the monoid under matrix multiplication) of two-dimensional upper-triangular integer matrices:

$$\text{UT} := \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x, y, z \in \mathbb{Z} \right\}$$

We may drop the 0 in the bottom-left corner and write $\begin{pmatrix} x & y \\ & z \end{pmatrix}$ for matrices in UT. Let $\Phi(A)$ be a constraint for $A \in \text{UT}$. We write $\text{UT}[\Phi(A)] := \{A \in \text{UT} \mid \Phi(A)\}$, e.g., $\text{UT}[A_{22} = 1]$ denotes the set of all upper-triangular matrices whose bottom-right coefficient equals 1.

For a finite set \mathcal{M} of matrices, we write $\langle \mathcal{M} \rangle$ for the monoid generated by \mathcal{M} under matrix multiplication. In this paper we consider mainly the following reachability problems:

- **Membership:** Given a finite set $\mathcal{M} \subseteq \text{UT}$, and a matrix $T \in \text{UT}$, is $T \in \langle \mathcal{M} \rangle$?
- **Vector reachability:** Given a finite set $\mathcal{M} \subseteq \text{UT}$, and vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^2$, is there a matrix $M \in \langle \mathcal{M} \rangle$ such that $M\mathbf{x} = \mathbf{y}$?
- **Scalar reachability:** Given a finite set $\mathcal{M} \subseteq \text{UT}$, vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^2$, and a scalar $\lambda \in \mathbb{Z}$, is there a matrix $M \in \langle \mathcal{M} \rangle$ such that $\mathbf{y}^T M \mathbf{x} = \lambda$? We refer to the special case with $\lambda = 0$ as the *0-reachability* problem.

We write $\text{Aff}(\mathbb{Z})$ for the set (and the monoid under function composition) of affine functions:

$$\text{Aff}(\mathbb{Z}) := \{x \mapsto ax + b \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}^{\mathbb{Z}} \quad (\text{where } \mathbb{Z}^{\mathbb{Z}} = \{f : \mathbb{Z} \rightarrow \mathbb{Z}\})$$

Define $\text{Aff}(\mathbb{Q})$ similarly, with \mathbb{Z} replaced by \mathbb{Q} . For a finite set \mathcal{A} of affine functions, we write $\langle \mathcal{A} \rangle$ for the monoid (i.e., including the identity function $x \mapsto x$) generated by \mathcal{A} under function composition. The motivation to study the matrix reachability problems above is their relationship to the following one-dimensional affine reachability problems:

- **Affine membership over \mathbb{Z} :** Given a finite set $\mathcal{A} \subseteq \text{Aff}(\mathbb{Z})$, and a function $f \in \text{Aff}(\mathbb{Z})$, is $f \in \langle \mathcal{A} \rangle$?
- **Affine reachability over \mathbb{Z} :** Given a finite set $\mathcal{A} \subseteq \text{Aff}(\mathbb{Z})$, and numbers $x, y \in \mathbb{Z}$, is there a function $f \in \langle \mathcal{A} \rangle$ such that $f(x) = y$?

– **Affine reachability over \mathbb{Q} :** The same problem with \mathbb{Z} replaced by \mathbb{Q} .

The following proposition links these problems (recall from the definitions above that the matrices need to be two-dimensional upper-triangular integer matrices):

Proposition 1.

1. *Affine membership over \mathbb{Z} is equivalent to (matrix) membership restricted to matrices with 1 in the bottom-right corner.*
2. *Affine reachability over \mathbb{Z} is equivalent to vector reachability restricted to matrices with 1 in the bottom-right corner.*
3. *Affine reachability over \mathbb{Q} is equivalent to 0-reachability restricted to matrices with non-zero entries in the bottom-right corner and vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^2$ such that the bottom entry of \mathbf{x} and the top entry of \mathbf{y} are non-zero.*

Proof. Items 1 and 2 follow from the isomorphism $\varphi : \text{Aff}(\mathbb{Z}) \rightarrow \text{UT}[A_{22} = 1]$ with $\varphi(x \mapsto ax+b) = \begin{pmatrix} a & b \\ & 1 \end{pmatrix}$, and the injection $\varphi' : \mathbb{Z} \rightarrow \mathbb{Z}^2$ with $\varphi'(x) = (x \ 1)^T$. More specifically, we have $\varphi(f_2 \circ f_1) = \varphi(f_2)\varphi(f_1)$ and $\varphi'(f(x)) = \varphi(f)\varphi'(x)$.

For item 3 consider the quotient UT/\sim of UT by the equivalence \sim with $\begin{pmatrix} a_1 & b_1 \\ & c_1 \end{pmatrix} \sim \begin{pmatrix} a_2 & b_2 \\ & c_2 \end{pmatrix}$ if and only if there is $\lambda \in \mathbb{Q} \setminus \{0\}$ with $\begin{pmatrix} a_1 & b_1 \\ & c_1 \end{pmatrix} = \lambda \begin{pmatrix} a_2 & b_2 \\ & c_2 \end{pmatrix}$. We define a similar injection $\varphi : \text{Aff}(\mathbb{Q}) \rightarrow \text{UT}/\sim$ as above such that $\varphi(x \mapsto \frac{ax+b}{c}) = \begin{pmatrix} a & b \\ & c \end{pmatrix}$ where $a, b, c \in \mathbb{Z}$ and $c \neq 0$. It is an isomorphism, as

$$\varphi\left(x \mapsto \frac{a_2 \frac{a_1 x + b_1}{c_1} + b_2}{c_2}\right) = \varphi\left(x \mapsto \frac{a_2 a_1 x + a_2 b_1 + b_2 c_1}{c_2 c_1}\right) = \begin{pmatrix} a_2 & b_2 \\ & c_2 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ & c_1 \end{pmatrix}.$$

Define also the equivalence \sim' such that $(p_1 \ q_1)^T \sim' (p_2 \ q_2)^T$ holds if and only if there is $\lambda \in \mathbb{Q} \setminus \{0\}$ such that $(p_1 \ q_1)^T = \lambda (p_2 \ q_2)^T$. Finally, define the injection $\varphi' : \mathbb{Q} \rightarrow \mathbb{Z}^2/\sim'$ with $\varphi\left(\frac{p}{q}\right) = (p \ q)^T$, for $p, q \in \mathbb{Z}$ and $q \neq 0$. Then we have, similarly as in items 1 and 2:

$$\varphi'\left(\frac{a \frac{p}{q} + b}{c}\right) = \begin{pmatrix} a & b \\ & c \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix} = \varphi\left(x \mapsto \frac{ax+b}{c}\right) \varphi'\left(\frac{p}{q}\right)$$

It follows that we have $\frac{a \frac{x_1}{x_2} + b}{c} = \frac{y_1}{y_2}$ if and only if $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \sim' \begin{pmatrix} a & b \\ & c \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, which in turn is equivalent to $(y_2 - y_1) \begin{pmatrix} a & b \\ & c \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0$. Item 3 follows. \square

Simple reductions show that these problems are all NP-hard:

Proposition 2. *Membership, vector reachability and 0-reachability are all NP-hard, even for matrices with only 1s on the diagonal, and for $\mathbf{x} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and for $\mathbf{y} = \begin{pmatrix} t \\ 1 \end{pmatrix}$ (for vector reachability) resp. $\mathbf{y}^T = (1 - t)$ (for 0-reachability).*

Proof. The following problem, *multi-subset-sum*, is known to be NP-complete; see the comment under “[MP10] Integer Knapsack” in [12]: given a finite set $\{a_1, \dots, a_k\} \subseteq \mathbb{N}$ and a value $t \in \mathbb{N}$, decide whether there exist coefficients $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ such that $\sum_{i=1}^k \alpha_i a_i = t$. Given an instance of multi-subset-sum, construct

$$\mathcal{M} := \left\{ \begin{pmatrix} 1 & a_i \\ & 1 \end{pmatrix} \mid i \in \{1, \dots, k\} \right\} \quad \text{and} \quad T := \begin{pmatrix} 1 & t \\ & 1 \end{pmatrix}.$$

Using the observation that $\begin{pmatrix} 1 & a \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ & 1 \end{pmatrix}$ and that, hence, $\langle \mathcal{M} \rangle$ is commutative, it is straightforward to verify that the instance of multi-subset-sum is positive if and only if $T \in \langle \mathcal{M} \rangle$. The proofs for vector reachability and 0-reachability are similar. \square

On various occasions, we make use of the notion of *polynomial register machine*: Let $\mathbb{Z}[x]$ denote the set of polynomials over x with integer coefficients. A *polynomial register machine (PRM)* is a tuple $R = (Q, \Delta, \lambda)$ where Q is a finite set of *states*, $\Delta \subseteq Q \times Q$ is the *transition relation*, and $\lambda: \Delta \rightarrow \mathbb{Z}[x]$ is the *transition labelling function*, labelling each transition with an *update polynomial*. We write $q \xrightarrow{p(x)} q'$ whenever $(q, q') \in \Delta$ and $\lambda((q, q')) = p(x)$. The set $\mathcal{C}(R)$ of *configurations* of R is $\mathcal{C}(R) := Q \times \mathbb{Z}$. By $(\rightarrow_R) \subseteq \mathcal{C}(R) \times \mathcal{C}(R)$ we denote the *one-step relation* given by

$$(q, a) \rightarrow_R (q', b) \iff q \xrightarrow{p(x)} q' \text{ and } b = p(a).$$

Let \rightarrow_R^* be the reflexive-transitive closure of \rightarrow_R . The following theorem is the main result of [11]:

Theorem 1 ([11]). *The following problem is PSPACE-complete: given a PRM R and two configurations $(q, a), (q', b) \in \mathcal{C}_R$, does $(q, a) \rightarrow_R^* (q', b)$ hold?*

3 Determinant ± 1

In this section we study the case where the monoid $\langle \mathcal{M} \rangle$ is restricted to matrices with determinants ± 1 , i.e., with ± 1 on the diagonal. In this case, the matrices $M \in \langle \mathcal{M} \rangle$ are characterized by the sign pattern on the diagonal and the top-right entry. Our problems become NP-complete under this restriction, but are in P if the determinants are -1 . First we prove the following lemma:

Lemma 1. *Let $\mathcal{M} \subseteq \text{UT}$ be with $\det(M) \in \{1, -1\}$ for all $M \in \mathcal{M}$. There exists an existential Presburger formula $\varphi(s, a, t)$ that can be constructed in time polynomial in the description of \mathcal{M} such that $\varphi(s, a, t)$ holds if and only if $\begin{pmatrix} s & a \\ t \end{pmatrix} \in \langle \mathcal{M} \rangle$.*

Proof. Note that $\mathcal{M} \subseteq \text{UT}[|A_{11}| = |A_{22}| = 1]$. We reduce the problem whether $\begin{pmatrix} s & a \\ t \end{pmatrix} \in \langle \mathcal{M} \rangle$ holds for some $s, t \in \{1, -1\}$ and $a \in \mathbb{Z}$ to a reachability problem on one-dimensional \mathbb{Z} -VASS (integer vector addition systems with states) [15]. The reachability relation of one-dimensional \mathbb{Z} -VASS is known to be effectively definable by an existential Presburger formula of polynomial length; see, e.g., [15], which then entails the claim to be shown.

A (one-dimensional) \mathbb{Z} -VASS can be described as a triple (Q, Σ, δ) where Q is a finite set of states, $\Sigma \subset \mathbb{Z}$ is a finite set of integer numbers, and $\delta \subseteq Q \times \Sigma \times Q$ is a finite transition relation. A *run from $q_0 \in Q$ to $q_n \in Q$ of length n* is a sequence $q_0 a_1 q_1 a_2 q_2 \cdots a_n q_n$ such that $(q_{i-1}, a_i, q_i) \in \delta$ holds for all $i \in \{1, \dots, n\}$. The *value* of such a run is defined as $\sum_{i=1}^n a_i$. The \mathbb{Z} -VASS *reachability* problem is to decide, given a \mathbb{Z} -VASS, two states $q, q' \in Q$, and a number $t \in \mathbb{Z}$, whether there is a run from q to q' with value t .

We give a polynomial reduction from the membership problem to the reachability problem for \mathbb{Z} -VASS: Define $Q := \{(+1, +1), (+1, -1), (-1, +1), (-1, -1)\}$, each state reflecting the diagonal. A transition $(q, a, q') \in \delta$ corresponds to a multiplication with a matrix $M \in \mathcal{M}$.

More precisely, for each state (s, t) and each $\begin{pmatrix} s' & a' \\ t' \end{pmatrix} \in \mathcal{M}$ we add a transition $((s, t), stt'a', (ss', tt'))$. We claim that there exists a run from $(+1, +1)$ to (s_n, t_n) of length n and value $a \in \mathbb{Z}$ if and only if there are matrices $M_1, \dots, M_n \in \mathcal{M}$ such that $M_1 \cdots M_n = \begin{pmatrix} s_n & t_n a \\ t_n \end{pmatrix}$. The claim can be proven by a straightforward induction on n (see Appendix A for the proof). The claim implies that there is $\begin{pmatrix} s & a \\ t \end{pmatrix} \in \langle \mathcal{M} \rangle$ if and only if there is a run from $(+1, +1)$ to (s, t) of value $t_n a$. Recall that the reachability relation of the \mathbb{Z} -VASS is definable in an existential Presburger formula of polynomial size, and thus so is the query $\begin{pmatrix} s & a \\ t \end{pmatrix} \in \langle \mathcal{M} \rangle$. The statement follows. \square

Theorem 2. *Let $\mathcal{M} \subseteq \text{UT}$ be with $\det(M) \in \{1, -1\}$ for all $M \in \mathcal{M}$.*

1. *Membership, vector reachability and scalar reachability are NP-complete.*
2. *They are NP-hard even for $\mathcal{M} \subseteq \text{UT}[A_{11} = A_{22} = 1]$ and for $\mathcal{M} \subseteq \text{UT}[A_{11} = A_{22} = -1]$.*
3. *They are in P if $\det(M) = -1$ for all $M \in \mathcal{M}$.*

Proof. For item 1 the lower bound follows from Proposition 2. The upper bound for membership follows from Lemma 1 and the folklore result that existential

Presburger arithmetic is in NP [4,13]. Vector and scalar reachability are easily reduced to membership, as there are only four choices in total for the diagonal entries s, t , and this choice together with the input determines the top-right entry uniquely. This completes the proof of item 1.

Towards item 2, NP-hardness of the case $\text{UT}[A_{11} = A_{22} = 1]$ follows from the proof of Proposition 2. For the case $\text{UT}[A_{11} = A_{22} = -1]$ we adapt this reduction by constructing

$$\mathcal{M} := \left\{ \begin{pmatrix} -1 & -a_i \\ & -1 \end{pmatrix} \mid i \in \{1, \dots, k\} \right\} \cup \left\{ \begin{pmatrix} -1 & 0 \\ & -1 \end{pmatrix} \right\} \quad \text{and} \quad T := \begin{pmatrix} 1 & t \\ & 1 \end{pmatrix}.$$

Note that $\begin{pmatrix} -1 & -a \\ & -1 \end{pmatrix} \begin{pmatrix} -1 & -b \\ & -1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ & 1 \end{pmatrix}$. The additional (negative identity) matrix ensures that an even number of matrices from \mathcal{M} can be used to form the product T . NP-hardness for vector reachability and 0-reachability are similar. This completes the proof of item 2.

Towards item 3, we will give an explicit description of $\langle \mathcal{M} \rangle$, such that membership can be checked in polynomial time. We focus on matrix products of even length $M_1 \cdots M_{2n} \in \langle \mathcal{M} \rangle$. These are exactly the matrices in $\langle \mathcal{M} \rangle$ with determinant 1. The extension to odd-length products (which have determinant -1) will be straightforward, as such products simply arise from even-length products multiplied with a single element of \mathcal{M} . The even-length products also form a monoid, finitely generated by $\mathcal{M}' := \{M_1 M_2 \mid M_1 \in \mathcal{M}, M_2 \in \mathcal{M}\}$, and all matrices in \mathcal{M}' have $(+1, +1)$ or $(-1, -1)$ on the diagonal. Clearly, \mathcal{M}' can be computed in polynomial time. Let \mathcal{M}'_+ and \mathcal{M}'_- be such that $\mathcal{M}' = \mathcal{M}'_+ \cup \mathcal{M}'_-$, and \mathcal{M}'_+ is the set of matrices from \mathcal{M}' that have $(+1, +1)$ on the diagonal, and \mathcal{M}'_- is defined analogously. For all $\begin{pmatrix} -1 & c \\ & -1 \end{pmatrix} \in \mathcal{M}'_-$, the matrix $\begin{pmatrix} -1 & -c \\ & -1 \end{pmatrix}$ is also in \mathcal{M}'_- , as

$$\begin{pmatrix} +1 & a \\ & -1 \end{pmatrix} \begin{pmatrix} -1 & b \\ & +1 \end{pmatrix} = \begin{pmatrix} -1 & a+b \\ & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & b \\ & +1 \end{pmatrix} \begin{pmatrix} +1 & a \\ & -1 \end{pmatrix} = \begin{pmatrix} -1 & -a-b \\ & -1 \end{pmatrix}.$$

The analogous statement for \mathcal{M}'_+ holds as well.

Let $g \in \mathbb{N}$ denote the gcd of all top-right entries in \mathcal{M}'_+ , with $g = 0$ in case all those entries are 0. By the observation at the end of the previous paragraph, $\langle \mathcal{M}'_+ \rangle = \begin{pmatrix} 1 & g\mathbb{Z} \\ & 1 \end{pmatrix}$, where here and later in this proof we write $\begin{pmatrix} a & B \\ & c \end{pmatrix}$ with $B \subseteq \mathbb{Z}$ to denote the set $\left\{ \begin{pmatrix} a & b \\ & c \end{pmatrix} \mid b \in B \right\}$, and $g\mathbb{Z}$ are the integer multiples of g . Given two sets of matrices $\mathcal{A}_1, \mathcal{A}_2$, we write $\mathcal{A}_1 \mathcal{A}_2$ to denote the set $\{A_1 A_2 \mid A_1 \in \mathcal{A}_1, A_2 \in \mathcal{A}_2\}$. For $k \in \mathbb{N}$, let \mathcal{P}_k denote the products of \mathcal{M}' where exactly k factors are from \mathcal{M}'_- . We have $\mathcal{P}_0 = \begin{pmatrix} 1 & g\mathbb{Z} \\ & 1 \end{pmatrix}$. Let $S \subset \mathbb{Z}$ such that

$\mathcal{M}'_- = \begin{pmatrix} -1 & S \\ & -1 \end{pmatrix}$ and define $S^{\oplus k} := \left\{ \sum_{i=1}^k s_i \mid s_i \in S \right\}$. We have:

$$\begin{aligned} \mathcal{P}_1 &= \begin{pmatrix} 1 & g\mathbb{Z} \\ & 1 \end{pmatrix} \begin{pmatrix} -1 & S \\ & -1 \end{pmatrix} \begin{pmatrix} 1 & g\mathbb{Z} \\ & 1 \end{pmatrix} = \begin{pmatrix} -1 & S + g\mathbb{Z} \\ & -1 \end{pmatrix} \quad \text{and} \\ \mathcal{P}_2 &= \mathcal{P}_1 \mathcal{P}_1 = \begin{pmatrix} -1 & S + g\mathbb{Z} \\ & -1 \end{pmatrix} \begin{pmatrix} -1 & S + g\mathbb{Z} \\ & -1 \end{pmatrix} = \begin{pmatrix} 1 & S^{\oplus 2} + g\mathbb{Z} \\ & 1 \end{pmatrix} \\ \mathcal{P}_3 &= \mathcal{P}_2 \mathcal{P}_1 = \begin{pmatrix} 1 & S^{\oplus 2} + g\mathbb{Z} \\ & 1 \end{pmatrix} \begin{pmatrix} -1 & S + g\mathbb{Z} \\ & -1 \end{pmatrix} = \begin{pmatrix} -1 & S^{\oplus 3} + g\mathbb{Z} \\ & -1 \end{pmatrix} \end{aligned}$$

Continuing this pattern, we see that the set of matrices from $\langle \mathcal{M} \rangle$ with $(+1, +1)$ on the diagonal is

$$\bigcup_{k \in \mathbb{N}} \mathcal{P}_{2k} = \bigcup_{k \in \mathbb{N}} \begin{pmatrix} 1 & S^{\oplus 2k} + g\mathbb{Z} \\ & 1 \end{pmatrix},$$

and the set with $(-1, -1)$ on the diagonal is

$$\bigcup_{k \in \mathbb{N}} \mathcal{P}_{2k+1} = \bigcup_{k \in \mathbb{N}} \begin{pmatrix} -1 & S^{\oplus 2k+1} + g\mathbb{Z} \\ & -1 \end{pmatrix}.$$

It remains to show that we can efficiently check membership in such sets. Let $S = \{s_1, \dots, s_m\}$. Recall that $S = \{-s_1, \dots, -s_m\}$. Suppose $T = \begin{pmatrix} -1 & t \\ & -1 \end{pmatrix}$ and we want to check whether $T \in \bigcup_{k \in \mathbb{N}} \mathcal{P}_{2k+1}$. This holds if and only if the linear system given by the two equalities

$$t = \sum_{i=1}^m s_i x_i + gy \qquad 2k+1 = \sum_{i=1}^m x_i$$

has an integer solution in the variables x_i, y, k . It is known that affine Diophantine equations can be solved in polynomial time [27, Chapter 5]. The case where the diagonal entries of T are $(+1, +1)$ is similar. As remarked above, the extension to odd-length products, which have diagonals $(+1, -1)$ or $(-1, +1)$, is straightforward. The vector reachability and scalar reachability problems (with the restriction on determinants in place) easily reduce to the membership problem, hence are also in P. \square

4 Vector Reachability

We show:

Theorem 3. *The vector reachability problem for $\text{UT}[A_{22} \neq 0]$ is in PSPACE.*

Proof. We construct a nondeterministic Turing machine \mathcal{T} that decides the reachability problem for $\text{UT}[A_{22} \neq 0]$ in polynomial space. Let $\mathcal{M} \subseteq \text{UT}[A_{22} \neq 0]$ and $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^2$ be an instance of the reachability problem, that is, \mathcal{T} has to check whether $M \cdot \mathbf{x} = \mathbf{y}$ holds for some $M \in \langle \mathcal{M} \rangle$.

Assume that $M^{(1)} \cdot \dots \cdot M^{(k)} \cdot x = y$ holds for some $M^{(1)}, \dots, M^{(k)} \in \mathcal{M}$. Observe that for all $A \in \mathcal{M}$ and all $z_1, z_2, z'_1, z'_2 \in \mathbb{Z}$ such that $A \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}^T = \begin{pmatrix} z'_1 \\ z'_2 \end{pmatrix}^T$, we have $z'_2 = A_{22}z_2$. From this observation we conclude:

1. If $x_2 \neq 0$, then $y_2 \neq 0$, too, and the number of indices $1 \leq i \leq k$ where $|M_{22}^{(i)}| > 1$ is bounded by a function in $\mathcal{O}(\log(|y_2|))$.
2. If $x_2 = 0$ or $y_2 = 0$, then $x_2 = y_2 = 0$ and $y_1 = M_{11}^{(1)} \cdot \dots \cdot M_{11}^{(k)} \cdot x_1$.

Let us first consider the case where $x_2 = 0$ or $y_2 = 0$ holds. In this case, \mathcal{T} rejects the input if $x_2 \neq 0$ or $y_2 \neq 0$. Otherwise, \mathcal{T} needs to check whether y_1 can be written as a product $M_{11}^{(1)} \cdot \dots \cdot M_{11}^{(k)} \cdot x_1$ for some indices $1, \dots, k$, which can be done in polynomial space (even in NP), since k can be bounded by $\mathcal{O}(\log(|y_1|))$.

Now consider the case where $|x_2| > 0$ and $|y_2| > 0$ holds. By the above observation, if the reachability problem has a solution, it can be given by

$$\mathbf{y} = A^{(l+1)} \cdot B^{(l)} \cdot A^{(l)} \cdot \dots \cdot B^{(2)} \cdot A^{(2)} \cdot B^{(1)} \cdot A^{(1)} \cdot \mathbf{x}, \quad (1)$$

- where the length of $l \in \mathbb{N}$ is polynomially bounded in the size of the input,
- $B^{(i)} \in \text{UT}[|A_{22}| > 1] \cap \mathcal{M}$ for every i ,
- $A^{(i)}$ can be written as product of matrices from $\text{UT}[|A_{22}| = 1] \cap \mathcal{M}$.

Notice that the matrices from $\text{UT}[|A_{22}| = 1]$ behave like affine update polynomials in a PRM, with the register value stored in the first component of the vector. This suggests the following approach: \mathcal{T} guesses the sequence of matrices $B = B^{(1)}, \dots, B^{(l)}$ and constructs a PRM R_B , whose size is polynomially bounded in the size of the input, such that $(q, x_1) \rightarrow_{R_B}^* (q', y_1)$ holds for some fixed states q, q' if the reachability problem has a solution of the form given in (1). The register machine only needs to store in its finite states how many of the B -matrices have already been applied, plus the current sign of the second vector component reached thus far, and is thus of size polynomial in the input. The claim then follows by applying Theorem 1.

More formally, fix some guess $B = B^{(1)}, \dots, B^{(l)}$ by \mathcal{T} . For a given matrix $M \in \text{UT}$ and a given integer α , let $f_{M,\alpha}$ be the affine function given by

$$f_{M,\alpha}(a) := M_{11} \cdot a + M_{12} \cdot \alpha.$$

Assume (1) holds for the guessed B and some $A^{(1)}, \dots, A^{(l+1)}$. Let $m \in \mathbb{N}$ and $M^{(i)} \in \mathcal{M}$, $1 \leq i \leq m$ be such that

$$M^{(m)} \cdot M^{(m-1)} \cdot \dots \cdot M^{(1)} = A^{(l+1)} \cdot B^{(l)} \cdot A^{(l)} \cdot \dots \cdot B^{(2)} \cdot A^{(2)} \cdot B^{(1)} \cdot A^{(1)}.$$

For $0 \leq i \leq m$, set $\alpha(i) := x_2 \cdot \prod_{j=1}^{i-1} M_{22}^{(j)}$. Then it is easy to verify that the following holds:

$$\begin{aligned} y_1 &= (f_{M^{(m)}, \alpha(m)} \circ f_{M^{(m-1)}, \alpha(m-1)} \cdots \circ f_{M^{(2)}, \alpha(2)} \circ f_{M^{(1)}, \alpha(1)}) (x_1) \\ y_2 &= M_{22}^{(m)} \cdot \alpha(m) \\ \alpha(i) &\in \left\{ \pm x_2 \cdot \prod_{j=1}^k B_{22}^{(j)} \mid k \in \{0, \dots, l\} \right\} \text{ for every } 1 \leq i \leq m. \end{aligned}$$

The PRM $R_B = (Q, \Delta, \lambda)$ can then be defined as $Q := \{\pm x_2 \cdot \prod_{j=1}^k B_{22}^{(j)} \mid k \in \{0, \dots, l\}\}$, $\Delta := Q \times Q$, and the labelling function λ is uniquely defined by the following constraints:

$$\lambda((\alpha, \alpha')) \subseteq \{f_{M, \alpha} \mid M \in \mathcal{M}\} \text{ for every } (\alpha, \alpha') \in Q \times Q, \quad (2)$$

$$f_{M, \alpha} \in \lambda((\alpha, \alpha')) \iff \alpha' = M_{22} \cdot \alpha \text{ for every } (\alpha, \alpha') \in Q \times Q, M \in \mathcal{M}. \quad (3)$$

By construction, $(x_2, x_1) \rightarrow_{R_B}^* (y_2, y_1)$ holds if (1) holds for some matrices $A^{(i)}$, $1 \leq i \leq l + 1$. Conversely, if $(x_2, x_1) \xrightarrow{f_{M_1, \alpha_1}}_{R_B} \circ \xrightarrow{f_{M_2, \alpha_2}}_{R_B} \circ \dots \circ \xrightarrow{f_{M_k, \alpha_k}}_{R_B} (y_2, y_1)$ holds for some $M_1, \dots, M_k \in \mathcal{M}$, then $\mathbf{y} = M_k \cdot \dots \cdot M_1 \cdot \mathbf{x}$ is a witness for reachability. Notice that R_B is polynomial in the size of the input, and thus by Theorem 1, \mathcal{T} can verify in polynomial space whether matrices $A^{(i)}$ exist such that (1) holds for the guess B , or a permuted subsequence of B . \square

Without the restriction on $\text{UT}[A_{22} \neq 0]$ the vector reachability problem becomes hard for affine reachability over \mathbb{Q} :

Theorem 4. *There is a polynomial-time Turing reduction from affine reachability over \mathbb{Q} to vector reachability.*

Proof. Let an instance of affine reachability over \mathbb{Q} be given. We first assume that all input functions are non-constant. Then we use the reduction from Proposition 1.3 to obtain an instance of the 0-reachability problem: $\mathcal{M} \subseteq \text{UT}[A_{11} \neq 0, A_{22} \neq 0]$ and $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ and $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ with $x_2 \neq 0$ and $y_1 \neq 0$. Define $T := \begin{pmatrix} y_1 & y_2 \\ 0 & 0 \end{pmatrix}$ and $\mathcal{M}' := \mathcal{M} \cup \{T\}$. We show that the instance of the 0-reachability problem is positive if and only if the vector reachability for \mathcal{M}' and \mathbf{x} and $\mathbf{0}$ is positive. Suppose the instance of the 0-reachability problem is positive. Then there is $M \in \langle \mathcal{M} \rangle$ such that $\begin{pmatrix} y_1 & y_2 \end{pmatrix} M \mathbf{x} = \mathbf{0}$, thus $TM \mathbf{x} = \mathbf{0}$, so $\mathbf{0}$ is reachable from \mathbf{x} . Conversely, suppose the instance of the 0-reachability problem is negative. Let $M \in \langle \mathcal{M} \rangle$. Then $M \mathbf{x} \neq \mathbf{0}$, as the bottom component of $M \mathbf{x}$ is non-zero. Since the instance of the 0-reachability problem is negative, we have $TM \mathbf{x} = \begin{pmatrix} t \\ 0 \end{pmatrix}$ for some $t \neq 0$. Since the top-left component of all matrices in \mathcal{M}' is non-zero, it follows that $M' TM \mathbf{x} \neq \mathbf{0}$ holds for all $M' \in \langle \mathcal{M}' \rangle$. Thus, $M'' \mathbf{x} \neq \mathbf{0}$ holds for all $M'' \in \langle \mathcal{M}' \rangle$, and so the instance of the vector reachability problem is negative.

Now we allow input functions of affine reachability to be constant. Suppose the constant functions are $f_i : x \mapsto 0x + c_i$ for $i \in \{1, \dots, n\}$ for some $n \in \mathbb{N}$. It is easy to see that then the affine reachability problem can be solved by removing all f_i from the set of functions and checking affine reachability starting from c_i , where $i \in \{1, \dots, n\}$, one by one. These instances can be reduced to vector reachability, as described before. \square

5 Membership

In this section we study the membership problem. As we will see, the difficulty depends on how many 0s are allowed on the diagonal. Any product of upper-

triangular matrices is non-zero on the top-left (bottom-right, respectively) if and only if all factors are non-zero on the top-left (bottom-right, respectively). So when we speak of the membership problem for, say, $\text{UT}[A_{11} \neq 0]$, the restriction refers both to \mathcal{M} and the target matrix T .

The case with no 0s on the diagonal is NP-complete:

Theorem 5. *The membership problem for $\text{UT}[A_{11} \neq 0 \wedge A_{22} \neq 0]$ is NP-complete.*

Proof. The lower bound was shown in Proposition 2. For the upper bound, we construct an NP Turing machine. Fix \mathcal{M} and T . Assume for the moment that T can be written as a product $T = M^{(k)} \cdot \dots \cdot M^{(1)}$ of matrices from \mathcal{M} . Let l be the number of indices $i > 1$ where $M^{(i)} \in \text{UT}[|A_{11}| > 1 \vee |A_{22}| > 1]$ holds. Since $T_{ii} = \prod_{j=1}^k M_{ii}^{(j)}$ holds for both $i \in \{1, 2\}$, the number l can be bounded by $\mathcal{O}(\log(|T_{11}|) + \log(|T_{22}|))$, and T can be written as

$$T = A^{(l+1)} B^{(l)} A^{(l)} \cdot \dots \cdot B^{(1)} \cdot A^{(1)} M^{(1)} \quad (4)$$

such that $B^{(j)} \in \text{UT}[|A_{11}| > 1 \vee |A_{22}| > 1] \cap \mathcal{M}$ and $A^{(j)} \in \langle \text{UT}[|A_{11}| = |A_{22}| = 1] \cap \mathcal{M} \rangle \cup \{I\}$ for every j .

The Turing machine guesses matrices $B^{(1)}, \dots, B^{(l)}$ and the matrix $M^{(1)}$ and constructs in polynomial time an existential Presburger formula $\varphi(t_1, t_2, t_3)$ that satisfies $t_1 = T_{11}$, $t_2 = T_{12}$, $t_3 = T_{22}$ if and only if T can be written as a product of the form given in (4) for the guessed $B^{(i)}$ and $M^{(1)}$. By Lemma 1, such a formula $\varphi(t_1, t_2, t_3)$ exists and can be efficiently constructed. The claim then follows from the fact that $\varphi(t_1, t_2, t_3)$ is existential Presburger of size polynomial in the input, and that the existential Presburger fragment is in NP [4,13]. \square

The proof of Proposition 1.1 with the isomorphism between affine functions over \mathbb{Z} and upper-triangular matrices with 1 on the bottom-right shows that non-constant functions correspond to matrices that do not have 0s on the diagonal. Hence we have:

Corollary 1. *Affine membership over \mathbb{Z} with non-constant functions is NP-complete.*

The case where 0s are allowed at one of the diagonal positions can be reduced to vector reachability:

Theorem 6. *The membership problems for $\text{UT}[A_{11} \neq 0]$ and for $\text{UT}[A_{22} \neq 0]$ are in PSPACE.*

Proof. We give a proof sketch for $\text{UT}[A_{22} \neq 0]$; the detailed proof can be found in the appendix. If $T_{11} \neq 0$, then a PSPACE decision procedure follows from Theorem 5. If $T_{11} = 0$, then the problem reduces to a reachability problem with the additional restriction that $\text{UT}[A_{11} = 0]$ must be included in the matrix product. This problem in turn is decidable in PSPACE via a straightforward modification of the PRM R_B in the proof of Theorem 3. \square

The general membership problem, without restrictions on the position of 0s, is related to (variants of) scalar reachability. Theorems 7 and 8 provide reductions in both ways.

Theorem 7. *Let s be an oracle for the scalar reachability problem. The membership problem is in PSPACE^s .*

Proof. Fix some finite $\mathcal{M} \subseteq \text{UT}$ and $T \in \text{UT}$. We give a PSPACE^s procedure that decides whether $T \in \langle \mathcal{M} \rangle$ holds. We make the following case distinction:

1. $T = \mathbf{0}$
2. $T \in \text{UT}[A_{11} \neq 0 \vee A_{22} \neq 0]$
3. $T \in \text{UT}[A_{11} = A_{22} = 0 \wedge A_{12} \neq 0]$

In the first case, the membership problem is easy: if $T = \mathbf{0} \in \langle \mathcal{M} \rangle$, then there must exist matrices $M_1 \in \text{UT}[A_{11} = 0] \cap \mathcal{M}$ and $M_2 \in \text{UT}[A_{22} = 0] \cap \mathcal{M}$, but then $T = \mathbf{0} = M_1 \cdot M_2$. The existence of such M_1, M_2 is trivial to check. In the second case, the problem reduces to $T \in \langle \text{UT}[A_{11} \neq 0] \cap \mathcal{M} \rangle$ or $T \in \langle \text{UT}[A_{22} \neq 0] \cap \mathcal{M} \rangle$, which is decidable in PSPACE by Theorem 6.

Let us now consider the last case and assume for the moment that $T \in \langle \mathcal{M} \rangle$, that is, $T = M_1 \dots M_k$ for some matrices $M_i \in \langle \mathcal{M} \rangle$. Since the product of any two matrices from $\text{UT}[A_{11} = A_{22} = 0 \wedge A_{12} \neq 0]$ equals the zero matrix, we know that there is at most one index i such that $M_i \in \text{UT}[A_{11} = A_{22} = 0 \wedge A_{12} \neq 0]$. Moreover, if no such index i exists, it is easy to verify that there must be some indices $1 \leq i < j \leq k$ such that $M_i \in \text{UT}[A_{22} = 0]$ and $M_j \in \text{UT}[A_{11} = 0]$. Moreover, observe that for every $M \in \text{UT}$, we have $A \cdot M = M_{22} \cdot A$ and $M \cdot A = M_{11} \cdot A$ for every $A \in \text{UT}[A_{11} = 0]$ and every $A \in \text{UT}[A_{22} = 0]$, respectively. From these observations, we conclude that $T \in \langle \mathcal{M} \rangle$ if and only if one of the following equalities is satisfied for some $M, M', M'' \in \langle \mathcal{M} \rangle$:

$$T = M_{11} \cdot A \cdot M'_{22} \quad \text{for some } A \in \mathcal{M} \cap \text{UT}[A_{11} = A_{22} = 0], \quad (5)$$

$$T = M_{11} \cdot A \cdot M'' \cdot B \cdot M'_{22} \quad \text{for some } A, B \in \mathcal{M} \cap \text{UT}[A_{11} = 0 \vee A_{22} = 0]. \quad (6)$$

Note that the absolute values of M_{11} and M'_{22} in (5) and (6) are bounded by $|T_{12}|$. Moreover, for a product of upper triangular matrices $M = M^{(1)} \dots M^{(k)}$, we have the identity $M_{11} = M_{11}^{(1)} \dots M_{11}^{(k)}$, and thus we may assume without loss of generality that M can be written as a product of matrices from \mathcal{M} whose length is bounded by $\mathcal{O}(\log(|T_{12}|))$, and similarly for M' . Now, in order to decide the membership problem, a nondeterministic Turing machine can first guess whether (5) or (6) holds. If it guesses (5), it proceeds to guess the $|T_{12}|$ -bounded scalars M_{11} and M'_{22} and the matrix A , verifies the existence of M and M' in polynomial space via guessing the corresponding products of length $\mathcal{O}(\log(|T_{12}|))$, and tests for equality. If the machine guesses (6), it proceeds to guess $\alpha = M_{11}$ and $\beta = M'_{22}$ and the matrices A and B in polynomial space, tests in polynomial space whether $\alpha A \in \langle \mathcal{M} \rangle$ and $\beta B \in \langle \mathcal{M} \rangle$ holds by Theorem 6, and then use the oracle s to verify the existence of $M'' \in \langle \mathcal{M} \rangle$ such that $T_{12} = \alpha (A_{11} \ A_{12}) M'' \begin{pmatrix} B_{12} \\ B_{22} \end{pmatrix} \beta$. \square

Theorem 8. *The following sign-invariant version of the scalar-reachability problem is polynomial-time Turing-reducible to the membership problem: given $\mathcal{M} \subseteq \text{UT}$ and column vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^2$, does $\mathbf{y}^T M \mathbf{x} \in \{-1, 1\}$ hold for some $M \in \langle \mathcal{M} \rangle$?*

Proof. Fix $\mathcal{M}, \mathbf{x}, \mathbf{y}$. Let I be the identity, $\mathcal{A} := \mathcal{M} \cap \text{UT}[A_{22} = 0]$, $\mathcal{B} := \mathcal{M} \cap \text{UT}[A_{11} = 0]$, $\mathcal{C} := (\mathcal{M} \setminus (\mathcal{A} \cup \mathcal{B}))$, $Y := \begin{pmatrix} y_1 & y_2 \\ 0 & 0 \end{pmatrix}$, and $X := \begin{pmatrix} 0 & x_1 \\ 0 & x_2 \end{pmatrix}$. Set $\mathcal{A}' := \mathcal{A}$, if $|y_1| = 1$, otherwise set $\mathcal{A}' := \emptyset$; further set $\mathcal{B}' := \mathcal{B}$, if $|x_2| = 1$, otherwise set $\mathcal{B}' := \emptyset$.

We obtain the following equivalences:

$$\exists M \in \langle \mathcal{M} \rangle : \mathbf{y}^T M \mathbf{x} \in \{\pm 1\} \quad \Leftrightarrow \quad (7)$$

$$\exists A \in \mathcal{A} \cup \{I\}, B \in \mathcal{B} \cup \{I\}, C \in \langle \mathcal{C} \rangle : \mathbf{y}^T \cdot (A \cdot C \cdot B) \cdot \mathbf{x} \in \{\pm 1\} \quad \Leftrightarrow \quad (8)$$

$$\begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix} \in \bigcup_{A \in \mathcal{A}' \cup \{Y\}, B \in \mathcal{B}' \cup \{X\}} \langle \mathcal{C} \cup \{A, B\} \rangle. \quad (9)$$

We provide detailed derivations of these equivalences in Appendix C. Deciding (9) requires polynomially many queries to a membership oracle where input sizes are polynomial in the description of $\mathcal{M}, \mathbf{x}, \mathbf{y}$. This entails the theorem. \square

6 Mortality

In this section we consider the *mortality* problem: given a finite set $\mathcal{M} \subseteq \mathbb{Z}^{2 \times 2}$ of integer matrices (not necessarily triangular), is the zero matrix $\mathbf{0}$ in $\langle \mathcal{M} \rangle$? In the upper-triangular case the problem is almost trivial: if there is $M \in \langle \mathcal{M} \rangle$ with only zeros on the diagonal, there must be $M_1, M_2 \in \mathcal{M}$ with $M_1 = \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix}$ and $M_2 = \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix}$ —but then $M_1 M_2 = \mathbf{0}$. Hence, we consider mortality for matrices with determinants $\pm 1, 0$ and prove:

Theorem 9. *The mortality problem for two-dimensional integer matrices (not necessarily triangular) with determinants ± 1 or 0 is NP-complete. It is NP-hard even if there is one singular matrix and the non-singular matrices are of the form $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$.*

Both for the lower and the upper bound we need the following lemma from [5]:

Lemma 2 ([5, Lemma 2]). *Let $\mathcal{M} \subseteq \mathbb{R}^{2 \times 2}$ be a finite set of matrices. We have $\mathbf{0} \in \langle \mathcal{M} \rangle$ if and only if there are $M_1, \dots, M_n \in \mathcal{M}$ with $M_1 \cdots M_n = \mathbf{0}$ and $\text{rank}(M_1) = \text{rank}(M_n) < 2$ and $\text{rank}(M_i) = 2$ for all $i \in \{2, \dots, n-1\}$.*

First we prove NP-hardness:

Proof (of the NP-hardness part of Theorem 9). Concerning NP-hardness, the reduction from Proposition 2 for 0-reachability constructs, given an instance of multi-subset-sum, a set \mathcal{M} of matrices of the form $\begin{pmatrix} 1 & a \\ & 1 \end{pmatrix}$ and a number $t \in \mathbb{N}$ such that the instance of multi-subset-sum is positive if and only if there is $M \in \mathcal{M}$ with $(1-t) M \begin{pmatrix} 0 & 1 \end{pmatrix}^T = 0$. Define the rank-1 matrix

$$T := \begin{pmatrix} 0 \\ 1 \end{pmatrix} (1-t) = \begin{pmatrix} 0 & 0 \\ 1 & -t \end{pmatrix}$$

and set $\mathcal{M}' := \mathcal{M} \cup \{T\}$. If there is $M \in \mathcal{M}$ with $(1-t) M \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$, then $\mathbf{0} = TMT \in \langle \mathcal{M}' \rangle$. Conversely, if there is $\mathbf{0} \in \langle \mathcal{M}' \rangle$, then, by Lemma 2, there is $M \in \mathcal{M}$ with $TMT = \mathbf{0}$, hence $(1-t) M \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$. \square

For the upper bound we use results from [24, 2]. In accordance with the literature, we define $\text{SL}(2, \mathbb{Z}) := \{M \in \mathbb{Z}^{2 \times 2} \mid \det(M) = 1\}$.

Lemma 3 ([24, Lemma 4]). *Let $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{Z}^2$ and $\mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in \mathbb{Z}^2$ and $M \in \text{SL}(2, \mathbb{Z})$. If $M\mathbf{x} = \mathbf{y}$ then $\gcd(x_1, x_2) = \gcd(y_1, y_2)$.*

Theorem 10 ([24, Theorem 8, Corollary 9]). *Let $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^2$ with $\mathbf{x} \neq \mathbf{0}$. Then one can compute in polynomial time matrices $B, C \in \text{SL}(2, \mathbb{Z})$ such that for every $M \in \text{SL}(2, \mathbb{Z})$ the following equivalence holds:*

$$M\mathbf{x} = \mathbf{y} \iff \text{there is } k \in \mathbb{Z} \text{ with } M = B \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k C$$

In the following theorem, a *regular expression* describes a set of matrices, so that the atomic expressions describe singleton sets, the operator \cup is set union, and the operator \cdot is elementwise multiplication:

Theorem 11 ([2, Corollary 5.1]). *Given a regular expression over matrices in $\text{SL}(2, \mathbb{Z})$, one can decide in NP whether the identity matrix is in the set described by the regular expression.*

Now we can complete the proof of Theorem 9:

Proof (of the upper bound in Theorem 9). We give an NP procedure. We guess the matrices M_1, M_n from Lemma 2. Define $\mathcal{M}' := \mathcal{M} \cap \text{SL}(2, \mathbb{Z})$. We have to verify that there is a matrix $M \in \langle \mathcal{M}' \rangle$ such that $M_1 M M_n = \mathbf{0}$. Let $\mathbf{x} = (x_1 \ x_2)^T \in \mathbb{Z}^2$ be a non-zero multiple of a non-zero column of M_n (if M_n does not have a non-zero column, the problem is trivial) such that $\gcd(x_1, x_2) = 1$. This defines \mathbf{x} uniquely up to a sign. Similarly, let $\mathbf{y} = (y_1 \ y_2)^T \in \mathbb{Z}^2$ be a non-zero multiple of a non-zero row of M_1 such that $\gcd(y_1, y_2) = 1$. Now it suffices to check whether there is $M \in \langle \mathcal{M}' \rangle$ such that $(y_1 \ y_2) M \mathbf{x} = 0$. By Lemma 3 the

latter equation is equivalent to $M\mathbf{x} = (-y_2 \ y_1)^T$. Compute the matrices B, C from Theorem 10. Now it suffices to check whether there are $M \in \langle \mathcal{M}' \rangle$ and $k \in \mathbb{Z}$ with $M = B \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k C$. Equivalently, one may check whether the identity matrix is in the set described by the regular expression

$$B \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cup \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \right)^* C (A_1^{-1} \cup \dots \cup A_m^{-1})^* \quad \text{where } \mathcal{M}' = \{A_1, \dots, A_m\}.$$

(Note that $A_i^{-1} \in \text{SL}(2, \mathbb{Z})$.) By Theorem 11 this can be checked in NP. \square

7 Reachability in Affine Register Machines

In this section, we show that the reachability problem for PRMs is PSPACE-complete even when the register updates are restricted to affine functions. We call such PRMs *affine register machines*. For our proof, we need the notion of a bounded one-counter automaton.

Definition 1. A bounded one-counter automaton is a tuple (L, b, Δ) where

- L is a finite set of locations,
- $b \in \mathbb{N}$ is a global counter bound,
- Δ is the transition relation containing tuples of the form (l, p, l') where
 - $l, l' \in L$ are predecessor/successor locations,
 - $p \in [-b, b]$ specifies how the counter should be modified.

Each state of the automaton consists of a location $l \in L$ and counter value c . We define the set of states to be $S = L \times [0, b]$. For two states $(l, c), (l', c')$ we write $(l, c) \rightarrow (l', c')$ whenever $(l, p, l') \in \Delta$ for some $p \in \mathbb{Z}$ such that $c' = c + p \in [0, b]$.

Let \rightarrow^* denote the reflexive-transitive closure of the relation \rightarrow . The reachability problem for bounded one-counter automata is PSPACE-complete [10]. This is the following problem: given a bounded one-counter automaton (L, b, Δ) , a location l_0 , and a state $(l, c) \in S$, does $(l_0, 0) \xrightarrow{*} (l, c)$ hold?

We show that reachability in affine register machines is PSPACE-complete via reduction from the reachability problem for bounded one-counter automata.

Theorem 12. The following problem is PSPACE-complete: Given an affine register machine, and configurations $(q, x), (r, y)$, does $(q, x) \xrightarrow{*} (r, y)$ hold?

Proof. Membership in PSPACE follows from Theorem 1. It remains to show that the problem is PSPACE-hard.

Fix a bounded one-counter automaton $\mathcal{A} = (L, b, \Delta)$. We give a polynomial-time construction of affine register machine R such that $(l_0, 0) \xrightarrow{*}_{\mathcal{A}} (l, c_{\text{tgt}})$ holds for some configurations $(l_0, 0), (l, c_{\text{tgt}})$ of \mathcal{A} if and only if $(q_0, 0) \xrightarrow{*}_R (q, c_{\text{tgt}})$ holds for some distinct states q_0 and q of R .

Let $i \in [0, b]$ and $c \in \mathbb{Z}$, and define:

$$K := 2b + 1 \quad K(i, c) := (K + 1)c - i \cdot K.$$

Before we construct R, we establish the following implications:

$$i \neq c \implies K(i, c) \notin [-b, 2b] \quad (10)$$

$$i = c \implies K(i, c) = i = c \in [0, b] \quad (11)$$

Let us show these implications. Let us first show (10). Assume $i \neq c$. We make the following case distinction:

1. $c < i$: Then $i = c + \delta$ for some $\delta > 0$. We thus obtain

$$\begin{aligned} K(i, c) &= (K + 1)c - i \cdot K && \text{by definition of } K(i, c), \\ &= (K + 1)c - (c + \delta)K && \text{by substituting } i = c + \delta, \\ &= c - K \cdot \delta \\ &= c - (2b + 1) \cdot \delta && \text{by definition of } K, \\ &\leq c - (2b + 1) && \text{since } \delta > 0 \text{ by assumption,} \\ &\leq -b - 1 && \text{since } c < i \leq b. \end{aligned}$$

Hence $K(i, c) \notin [-b, 2b]$ if $c < i$.

2. $c > i$:

$$\begin{aligned} K(i, c) &= (K + 1)c - i \cdot K && \text{by definition of } K(i, c), \\ &\geq (K + 1)c - (c - 1) \cdot K && \text{since } c > i \geq 0, \\ &= c + K \\ &> 2b && \text{since } c > 0 \text{ and } K = 2b + 1. \end{aligned}$$

Hence $K(i, c) \notin [-b, 2b]$ if $c > i$.

This completes the proof of (10). Now, for (11), observe that setting $i = c$ satisfies $K(i, c) = i = c$. This completes the proof of (11).

Implications (10) and (11) suggest the following (tentative) construction of the PRM R with affine updates: R stores the counter value of the bounded one-counter automaton \mathcal{A} in its register x , and it stores the locations of \mathcal{A} in its states. When R simulates a transition $(l, c) \rightarrow (l', c')$ due to $(l, p, l') \in \Delta$, it does the following: It guesses $i \in [0, b]$ from (10), and performs the updates $x \leftarrow (K + 1) \cdot x$, followed by the update $x \leftarrow x - i \cdot K$. If the guess was correct and $x \in [0, b]$, then by (11) the register value remains unchanged in the interval $[0, b]$; otherwise the updates result in a value outside the interval $[-b, 2b]$ by (10). Finally, R performs the update $x \leftarrow x + p$ and transitions to state l' . Since $p \in [-b, b]$, our sequence of updates maintains the following invariant: once the register value x lies outside the interval $[0, b]$, it remains so forever. Moreover, if the target state (l, c_{tgt}) is reachable from $(l_0, 0)$ in the counter machine, then we have a corresponding sequence in the affine register machine, and vice versa.

There is one caveat: representing all possible guesses of $i = 0, 1, \dots, b$ directly in the transition relation of R would not be polynomial. However, these nondeterministic updates can be represented more succinctly with a slight modification: Let $j = \lceil \log b \rceil + 1$. We first transform the counter machine \mathcal{A} into an equivalent machine \mathcal{A}' with counter bound $B = 2^j - 1 \geq b$ as follows: We replace every transition $(l, p, l') \in \Delta$ by the following transitions:

$$(l, p, l'_1) \quad (l'_1, (B - b), l'_2) \quad (l'_2, -(B - b), l') ,$$

where l'_1 and l'_2 are auxiliary intermediate locations. Observe that by construction of \mathcal{A}' , $(l_0, 0) \xrightarrow{*}_{\mathcal{A}} (l, c)$ holds if and only if $(l_0, 0) \xrightarrow{*}_{\mathcal{A}'} (l, c)$. Moreover, the size of \mathcal{A}' is polynomial in the size of \mathcal{A} . In order to prove our hardness result, it thus suffices to construct a PRM R of size polynomial in the size of \mathcal{A}' , such that $(l_0, 0) \xrightarrow{*}_{\mathcal{A}'} (l, c)$ holds if and only if $(l_0, 0) \xrightarrow{*}_R (l, c)$ holds. To this end, apply the previous construction of the PRM to \mathcal{A}' , but instead of guessing $i \in [0, B]$ directly and computing $x \leftarrow x - i \cdot K$, the PRM uses intermediate auxiliary states q_0, \dots, q_{j+1} , and transitions

$$\begin{aligned} q_k &\xrightarrow{x \leftarrow x - 2^k \cdot K} q_{k+1} && \text{(decrement)} \\ q_k &\xrightarrow{x \leftarrow x} q_{k+1} && \text{(no update)} \end{aligned}$$

for every $k \in [0, j]$. Thus, instead of guessing i and subsequent decrementation of x by $i \cdot K$, the machine guesses the $(j+1)$ binary digits of i in increasing order, and after each guess updates the register accordingly. These non-deterministic choices of binary digits represent all updates for values of i in the range $[0, B] = [0, 2^j - 1]$. Furthermore, the number of states of the resulting PRM is polynomial in the size of the reachability query for \mathcal{A}' . This completes the proof. \square

8 Conclusion

Motivated by their connections to affine reachability, we have studied membership, vector reachability, and scalar reachability for two-dimensional upper-triangular integer matrices. To gauge the (relative) difficulty of these problems, we have established several complexity results and reductions. Concerning upper complexity bounds, we have employed a variety of techniques, including existential Presburger arithmetic, \mathbb{Z} -VASS, PRMs, solving linear Diophantine equations over the integers, and special properties of $\text{SL}(2, \mathbb{Z})$. We have also established lower bounds, including hardness of vector reachability for affine reachability over \mathbb{Q} , a connection between membership and scalar reachability, a simpler proof for NP-hardness of the mortality problem, and PSPACE-completeness of reachability in affine register machines. As open problem we highlight the precise complexity (between NP and PSPACE) of (stateless) affine reachability over \mathbb{Z} .

References

1. Bell, P., Hirvensalo, M., Potapov, I.: Mortality for 2×2 matrices is NP-hard. In: Proceedings of MFCS. pp. 148–159 (2012)

2. Bell, P., Hirvensalo, M., Potapov, I.: The identity problem for matrix semigroups in $SL_2(\mathbb{Z})$ is NP-complete. In: Proceedings of SODA. pp. 187–206 (2017)
3. Ben-Amram, A.: Mortality of iterated piecewise affine functions over the integers: Decidability and complexity. *Computability* **4**(1), 19–56 (2015)
4. Borosh, I., Treybig, L.: Bounds on positive integral solutions of linear Diophantine equations. *Proceedings of the American Mathematical Society* **55**, 299–304 (1976)
5. Bournez, O., Branicky, M.: The mortality problem for matrices of low dimensions. *Theory of Computing Systems* **35**(4), 433–448 (2002)
6. Bournez, O., Kurgansky, O., Potapov, I.: Reachability problems for one-dimensional piecewise affine maps. *International Journal of Foundations of Computer Science* **29**(4), 529–549 (2018)
7. Choffrut, C., Karhumäki, J.: Some decision problems on integer matrices. *RAIRO - Theoretical Informatics and Applications* **39**(1), 125–131 (2005)
8. Chonev, V., Ouaknine, J., Worrell, J.: On the complexity of the orbit problem. *Journal of the ACM* **63**(3), 23:1–23:18 (2016)
9. Czerwiński, W., Lasota, S., Lazić, R., Leroux, J., Mazowiecki, F.: The reachability problem for Petri nets is not elementary. In: Proceedings of STOC. pp. 24–33 (2019)
10. Fearnley, J., Jurdziński, M.: Reachability in two-clock timed automata is PSPACE-complete. *Information and Computation* **243**, 26–36 (2015)
11. Finkel, A., Göller, S., Haase, C.: Reachability in register machines with polynomial updates. In: Proceedings of MFCS. pp. 409–420 (2013)
12. Garey, M., Johnson, D.: *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W.H. Freeman & Co., New York, NY, USA (1979)
13. von zur Gathen, J., Sieveking, M.: A bound on solutions of linear integer equalities and inequalities. *Proceedings of the American Mathematical Society* **72**, 155–158 (1978)
14. Gurevich, Y., Schupp, P.: Membership problem for the modular group. *SIAM Journal on Computing* **37**(2), 425–459 (2007)
15. Haase, C., Halfon, S.: Integer vector addition systems with states. In: *Reachability Problems*. pp. 112–124 (2014)
16. Kannan, R., Lipton, R.: The orbit problem is decidable. In: Proceedings of STOC. pp. 252–261 (1980)
17. Kurgansky, O., Potapov, I., Caparrini, F.S.: Reachability problems in low-dimensional iterative maps. *International Journal of Foundations of Computer Science* **19**(4), 935–951 (2008)
18. Minsky, M.: Recursive unsolvability of Post’s problem of “tag” and other topics in theory of Turing machines. *Annals of Mathematics* **74**(3), 437–455 (1961)
19. Neary, T.: Undecidability in binary tag systems and the Post correspondence problem for five pairs of words. In: Proceedings of STACS. pp. 649–661 (2015)
20. Niskanen, R.: Reachability problem for polynomial iteration is PSPACE-complete. In: Proceedings of RP. pp. 132–143 (2017)
21. Nuccio, C., Rodaro, E.: Mortality problem for 2×2 integer matrices. In: *Proceedings of SOFSEM*. pp. 400–405. Springer (2008)
22. Ouaknine, J., Worrell, J.: Decision problems for linear recurrence sequences. In: *Reachability Problems*. pp. 21–28 (2012)
23. Paterson, M.: Unsolvability in 3×3 matrices. *Studies in Applied Mathematics* **49**(1), 105–107 (1970)
24. Potapov, I., Semukhin, P.: Vector reachability problem in $SL(2, \mathbb{Z})$. In: Proceedings of MFCS. LIPIcs, vol. 58, pp. 84:1–84:14 (2016)

- 25. Potapov, I., Semukhin, P.: Decidability of the membership problem for 2×2 integer matrices. In: Proceedings of SODA. pp. 170–186 (2017)
- 26. Reichert, J.: Reachability Games with Counters: Decidability and Algorithms. Ph.D. thesis, ENS Cachan (2015)
- 27. Schrijver, A.: Theory of linear and integer programming. John Wiley & Sons (1986)

A Proof of the Claim in the Proof for Lemma 1

In this section, we provide the omitted proof for the claim in the proof of Lemma 1.

Let the \mathbb{Z} -VASS (Q, Σ, δ) be defined as in the proof for Lemma 1: $Q := \{(+1, +1), (+1, -1), (-1, +1), (-1, -1)\}$, and for each state (s, t) and each $\begin{pmatrix} s' & a' \\ t' \end{pmatrix} \in \mathcal{M}$ we add a transition $((s, t), stt'a', (ss', tt'))$.

We must prove the following proposition:

Proposition 3. *There exists a run from $(+1, +1)$ to (s_n, t_n) of length n and value $a \in \mathbb{Z}$ if and only if there are matrices $M_1, \dots, M_n \in \mathcal{M}$ such that $M_1 \cdots M_n = \begin{pmatrix} s_n & t_n a \\ t_n \end{pmatrix}$.*

Proof. We prove this claim by induction on n . The case $n = 0$ implies $a = 0$ and is easy. For the step, suppose there is a run from $(+1, +1)$ to (s_n, t_n) of length n and value a . By the induction hypothesis, there are matrices $M_1 \cdots M_n = \begin{pmatrix} s_n & t_n a \\ t_n \end{pmatrix}$. Consider the run of length $n + 1$ and value $a + x$ obtained by extending the previous run by a transition $((s_n, t_n), x, (s_{n+1}, t_{n+1})) \in \delta$. The definition of δ implies that there is matrix $M_{n+1} = \begin{pmatrix} s' & a' \\ t' \end{pmatrix} \in \mathcal{M}$ such that $x = s_n t_n t' a'$ and $s_{n+1} = s_n s'$ and $t_{n+1} = t_n t'$. Hence:

$$\begin{aligned} M_1 \cdots M_{n+1} &= \begin{pmatrix} s_n & t_n a \\ t_n \end{pmatrix} \begin{pmatrix} s_n s_{n+1} & s_n t_n t' x \\ t_n t_{n+1} \end{pmatrix} = \begin{pmatrix} s_{n+1} & t_n t' x + t_{n+1} a \\ t_{n+1} \end{pmatrix} \\ &= \begin{pmatrix} s_{n+1} & t_{n+1} (x + a) \\ t_{n+1} \end{pmatrix} \end{aligned}$$

The other direction (from matrix product to run) is similar. This proves the proposition. \square

B Proof of Theorem 6

Theorem 6. *The membership problems for $\text{UT}[A_{11} \neq 0]$ and for $\text{UT}[A_{22} \neq 0]$ are in PSPACE.*

Proof. We only give the proof for $\text{UT}[A_{22} \neq 0]$; the proof for $\text{UT}[A_{11} \neq 0]$ is symmetric. Fix some $T \in \text{UT}$ and $\mathcal{M} \subseteq \text{UT}[A_{22} \neq 0]$. If $T_{11} \neq 0$, then $T \in \langle \text{UT}[A_{11} \neq 0] \cap \mathcal{M} \rangle$ must hold, which by Theorem 5 can be verified in NP, and thus in PSPACE. So let us now assume $T_{11} = 0$. Then we have

$$\begin{aligned} T &= \begin{pmatrix} 0 & T_{12} \\ 0 & T_{22} \end{pmatrix} \in \langle \mathcal{M} \rangle \\ \Leftrightarrow T &= M_1 \cdot A \cdot M_2 \\ \Leftrightarrow \begin{pmatrix} T_{12} \\ T_{22} \end{pmatrix} &= M_1 \cdot A \cdot M_2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{for some } M_1, M_2 \in \langle \mathcal{M} \rangle, A \in \mathcal{M} \cap \text{UT}[A_{11} = 0]. \end{aligned}$$

Thus our problem reduces to the following constrained reachability problem: Is $\mathbf{y} = (T_{12} \ T_{22})^T$ reachable from $\mathbf{x} = (0 \ 1)^T$ via a product of matrices from \mathcal{M} , such that at least one matrix from $\text{UT}[A_{11} = 0]$ occurs in the product? This problem is decidable in PSPACE via a minor modification of the approach outlined in the proof of Theorem 3: The polynomial register machine constructed in the proof of Theorem 3 only needs to additionally track whether a matrix from $\text{UT}[A_{11} = 0]$ has been applied. With $R_B = (Q, \Delta, \lambda)$ from the proof of Theorem 3, this can be realized with the modified polynomial register machine $R'_B = (Q', \Delta', \lambda')$ where $Q' = \{0, 1\} \times Q$, $\Delta' = Q' \times Q'$ and $\lambda': Q' \times Q' \rightarrow \lambda(Q \times Q)$ is defined minimally such that for every $q, q' \in Q$, every $f_{M,\alpha} \in \lambda((q, q'))$, and every $b \in \{0, 1\}$ the following holds:

$$\begin{aligned} (b, q) &\xrightarrow{f_{M,\alpha}} (b, q') \text{ if } M \in \text{UT}[A_{11} \neq 0], \\ (b, q) &\xrightarrow{f_{M,\alpha}} (1, q') \text{ if } M \in \text{UT}[A_{11} = 0]. \end{aligned}$$

After guessing the matrix sequence B as outlined in the proof of Theorem 3, a nondeterministic Turing machine only needs to verify $(0, (0, 1)) \xrightarrow{*}_{R'_B} (1, (T_{22}, T_{21}))$ in order to obtain a positive witness for the constrained reachability problem, which can be done in PSPACE, and the statement follows. \square

C Proof of Equivalences in Section 5

In this section we prove the equivalences $((7) \Leftrightarrow (8))$ and $((8) \Leftrightarrow (9))$ from Section 5. Let us recall the definitions of Section 5:

Fix $\mathcal{M} \subseteq \text{UT}$, \mathbf{x}, \mathbf{y} . Define $\mathcal{A} := \mathcal{M} \cap \text{UT}[A_{22} = 0]$, $\mathcal{B} := \mathcal{M} \cap \text{UT}[A_{11} = 0]$, $\mathcal{C} := (\mathcal{M} \setminus (\mathcal{A} \cup \mathcal{B}))$, $Y := \begin{pmatrix} y_1 & y_2 \\ 0 & 0 \end{pmatrix}$, and $X := \begin{pmatrix} 0 & x_1 \\ 0 & x_2 \end{pmatrix}$.

Further define

$$\begin{aligned} \mathcal{A}' &:= \begin{cases} \mathcal{A} & \text{if } |y_1| = 1, \\ \emptyset & \text{otherwise.} \end{cases} \\ \mathcal{B}' &:= \begin{cases} \mathcal{B} & \text{if } |x_2| = 1, \\ \emptyset & \text{otherwise.} \end{cases} \end{aligned}$$

Then the following equivalences hold:

$$\exists M \in \langle \mathcal{M} \rangle: \mathbf{y}^T M \mathbf{x} \in \{\pm 1\} \quad \Leftrightarrow \quad (7)$$

$$\exists A \in \mathcal{A} \cup \{I\}, B \in \mathcal{B} \cup \{I\}, C \in \langle \mathcal{C} \rangle: \mathbf{y}^T \cdot (A \cdot C \cdot B) \cdot \mathbf{x} \in \{\pm 1\} \quad \Leftrightarrow \quad (8)$$

$$\begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix} \in \bigcup_{A \in \mathcal{A}' \cup \{Y\}, B \in \mathcal{B}' \cup \{X\}} \langle \mathcal{C} \cup \{A, B\} \rangle. \quad (9)$$

Proof of $(7) \Leftrightarrow (8)$. The direction $(8) \Rightarrow (7)$ is immediate. Let us now prove $(7) \Rightarrow (8)$. Assume (7):

$$\exists M \in \langle \mathcal{M} \rangle: \mathbf{y}^T M \mathbf{x} \in \{\pm 1\}.$$

Fix M . If $M \in \langle \mathcal{C} \rangle$, then (8) is directly implied. So let us assume $M \notin \langle \mathcal{C} \rangle$ instead. We only need to consider the case where M can be decomposed into

$$M = M_1 \cdot A \cdot C \cdot B \cdot M_2 \quad (12)$$

such that $M_1 \in \langle \mathcal{M} \rangle$, $A \in \mathcal{A}$, $B \in \mathcal{B}$, $C \in \mathcal{C}$, and $M_2 \in \langle \mathcal{M} \rangle$. The other cases are similar. For every $M \in \mathbf{UT}$ there exist $\alpha, \beta \in \mathbb{Z}$ such that $M \cdot A = \alpha A$ and $B \cdot M = \beta B$, and thus we can rewrite (12) to

$$M = \alpha \cdot A \cdot C \cdot B \cdot \beta \quad (13)$$

for some $\alpha, \beta \in \mathbb{Z}$. Now, by assumption $\mathbf{y}^T M \mathbf{x} \in \{\pm 1\}$ holds, thus we must have $|\alpha| = |\beta| = 1$ in (13). From this we obtain $\mathbf{y}^T (A \cdot C \cdot B) \mathbf{x} \in \{\pm 1\}$. Hence (8) holds. This proves the implication.

Proof of (8) \Leftrightarrow (9). Let us first prove the implication (8) \Rightarrow (9). To this end, assume that (8) holds:

$$\exists A \in \mathcal{A} \cup \{I\}, B \in \mathcal{B} \cup \{I\}, C \in \langle \mathcal{C} \rangle : \mathbf{y}^T \cdot (A \cdot C \cdot B) \cdot \mathbf{x} \in \{\pm 1\}$$

Fix A, B, C . If $A = B = I$, then (9) is immediate via

$$\mathbf{y}^T \cdot C \cdot \mathbf{x} \in \{\pm 1\} \Leftrightarrow (X \cdot C \cdot Y) = \begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix}.$$

So let us consider the most instructive case where $A \in \mathcal{A} \setminus \{I\}$ and $B \in \mathcal{A} \setminus \{I\}$ holds – the remaining cases can be proved by analogous reasoning. In this case, we obtain from (8) the equality:

$$Y \cdot A \cdot C \cdot B \cdot X = y_1 \cdot A \cdot C \cdot B \cdot x_2 = \begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix} \quad (14)$$

From (14) we obtain $|y_1| = |x_2| = 1$, and in particular $\mathcal{A}' = \mathcal{A}$ and $\mathcal{B}' = \mathcal{B}$, and thus:

$$A \cdot C \cdot B = \begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix} \quad (15)$$

where $A \in \mathcal{A}' = \mathcal{A}$ and $B \in \mathcal{B}' = \mathcal{B}$. This implies (9), and we are done showing the implication (8) \Rightarrow (9).

Now let us prove the implication (9) \Rightarrow (8). Assume (9):

$$\begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix} \in \bigcup_{A \in \mathcal{A}' \cup \{Y\}, B \in \mathcal{B}' \cup \{X\}} \langle \mathcal{C} \cup \{A, B\} \rangle.$$

Fix $A \in \mathcal{A}' \cup \{Y\}$, $B \in \mathcal{B}' \cup \{X\}$ such that

$$\begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix} \in \langle \mathcal{C} \cup \{A, B\} \rangle. \quad (16)$$

By the argument given in the proof of (8) \Rightarrow (7), (16) entails:

$$\begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix} = A \cdot C \cdot B \text{ for some } C \in \langle \mathcal{C} \rangle. \quad (17)$$

Now, if $A = Y$ and $B = X$, (8) follows. In the other cases \mathcal{A}' or \mathcal{B}' is non-empty, which by definition of \mathcal{A}' and \mathcal{B}' means that $|y_1| = 1$ or $|x_1| = 1$ must hold, which in turn implies that $Y \cdot A = \pm A$ or $B \cdot X = \pm B$. Let us consider the most instructive case where $A \neq Y$ and $B \neq X$; the other cases are similar. Then by the previous remarks, we have:

$$X \cdot A \cdot C \cdot B \cdot Y = \pm A \cdot C \cdot \pm B = \begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix}.$$

This entails (8), and we are done.