Membership and Reachability Problems for Row-monomial Transformations

Alexei Lisitsa and Igor Potapov *

Department of Computer Science, University of Liverpool, Chadwick Building, Peach St, Liverpool L69 7ZF, U.K.,
{alexei,igor}@csc.liv.ac.uk

Abstract. In this paper we study the membership and vector reachability problems for labelled transition systems with row-monomial transformations. We show the decidability of these problems for row-monomial martix semigroups over rationals and extend these results to the wider class of matrix semigroups. After that we apply our methods to reachability problems for a class of transition systems which turn out to be equivalent to specific counter machines.

1 Introduction

In this paper we study the membership and vector reachability problems for labelled transition systems with row-monomial transformations.

We started our work on the membership and vector reachability problem for matrix semigroups that have natural and quite broad connections with combinatorics on words [2], the accessibility problem for linear sequential machines [13], the reachability problem in linear maps, verification of broadcasting protocols [9] etc. Then it turns out that these questions also are closely related to verification of counters automata and labelled transition systems.

The membership problem for a semigroup with only one generator ("is a matrix B a power of a matrix A") was known as the "orbit problem" and was shown to be decidable (in polynomial time) by Kannan and Lipton in 1986 [13]. The most natural generalization of the the "orbit problem" is the membership problem for matrix semigroups, given by a list of generators.

Problem 1. **The membership problem.** Let S be a given finitely generated semigroup of $n \times n$ matrices from $\mathbb{Q}^{n \times n}$. Determine whether a matrix M belongs to S. In other words, determine whether there exists a sequence of matrices $M_1, M_2, \ldots, M_k$ in S such that $M_1 \cdot M_2 \cdots M_k = M$

Paterson [15] shown that the problem is undecidable even for 3×3 integral matrices when considered a special case of the membership problem for matrix semigroups - the *mortality problem* (determination whether the zero matrix belongs to a matrix semigroup). It was shown in [4] that the mortality problem is

* Work partially supported by The Nuffield Foundation grant NAL/00684/G.

undecidable even for a case of two generators where the dimension of the matrices is at least 45. This result was improved in [12] by reducing the dimension to 24. Also the mortality problem for a case of 2×2 matrices and the problem of checking whether the identity matrix belongs to a matrix semigroup are still open [2]. At the same time several decidable cases have been discovered. The decidability of the general membership problem for semigroups generated by *commutative matrices* [13], was shown in [3] for a case of two matrix generator and then extended in [1] for the general case of commutative matrices.

We show in this paper that the membership problem is decidable for any finitely generated row-monomial matrix semigroup over $\mathbb{Q}$. The elements of such semigroups are row-monomial matrices, i.e. matrices with exactly one non-zero rational entry in every row. Note that row-monomial matrix semigroups in general are not commutative. Row-monomial matrices appear naturally in the semigroup representations by matrices over groups with zero [8], due to the property that no *addition* operation is needed for the matrix multiplication. It is turned out also to be a crucial property that we use later for the decidability proofs.

Another generalization of the "orbit problem" is the vector reachability problem for a matrix semigroup or reachability in iterative maps.

Problem 2. **The vector reachability problem for matrix semigroups.** Let S be a given finitely generated semigroup of $n \times n$ matrices from $\mathbb{Q}^{n \times n}$ and vectors $\bar{x}$,$\bar{y}$ from $\mathbb{Q}^n$. Decide whether there is a matrix $M \in S$ such that $M \cdot \bar{x} = \bar{y}$.

In other words it is equivalent to the following reachability problem for non-deterministic linear maps: "Given two vectors u and v in n-dimensional vector space over $\mathbb{Q}$ and a set A of linear transformations. Determine whether there exists a sequence of transformations from A such that maps v to u". In algebraic terms the vector reachability problem can be expressed as a problem of determining whether it is possible to get a vector u by an action of matrix semigroup on the initial vector v. This problem is also decidable for a case of semigroups generated by one matrix [13]. In order to show the decidablity for a case of non-deterministic linear row-monomial maps we use a technique similar to that we applied to the membership problem. We show that the vector reachability problem is decidable for any row-monomial semigroup over $\mathbb{Q}$.

An inspection of proofs about decidability results for row-monomial matrix semigroups over rationals reveals that these results can be generalized to the case of row-monomial matrix semigroups over commutative semigroup $\mathcal{S}$ satisfying some natural effectiveness conditions. As an instance of the general result we show the decidability of the membership and vector reachability problems for row-monomial matrix semigroups over $\mathcal{S}$, where $\mathcal{S}$ is an arbitrary finitely generated *commutative* matrix semigroup over an algebraic number field F.

Another natural generalization is considering an arbitrary finite graph structure, instead of a Cayley graph for semigroups, but still with labels from a semigroup $\mathcal{S}$. We show that this class of transition systems have decidable matrix and vector reachability problems, as well.

Also we found that subclass of such systems can be translated to counter machine model with guards of the form $x'_i = x_j \cdot c_{i,j}$, where $c_{i,j} \in \mathbb{Q}$, x'_i or x_i the value, respectively, after or before the transition or equivalent counter machine with additive quards of the form $x'_i = x_j + c_{i,j}$ where $c_{i,j} \in \mathbb{Z}$. So we also have decidability of the reachability problem for these classes of counter machines.

This paper is organised as follows. Next section contains preliminaries. In the third section we give a technical background for row-monomial matrices and semigroups, that we use in Section 4 to prove the decidability results. The Section 5 contains a number of generalizations of systems with row-monomial transformations. The paper ends with some conclusions and directions for further research.

2 Preliminaries

In what follows we use traditional denotations $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ and $\mathbb{Q}^+$ for the sets of naturals (non-negative integers), integers, rationals and non-negative rationals, respectively. By $[n]$ we denote the initial segment $\{1, \ldots, n\}$ of positive integers. For any vectors $\bar{x}, \bar{y} \in \mathbb{Q}^n$ denote by $\bar{x} \cdot \bar{y}$ their component-wise multiplication, that is $(x_1, \ldots, x_n) \cdot (y_1, \ldots y_n) = (x_1 \cdot y_1, \ldots, x_n \cdot y_n)$. Further, let $\bar{x}^n = \underbrace{\bar{x} \cdot \ldots \bar{x}}_{n}$.

Semigroups. A *semigroup* is a pair $(S, \cdot)$, where S is a set and $\cdot$ is an associative binary operation on S. A semigroup $(S, \cdot)$ is generated by a set A of its elements iff every element of S is a finite product $a_{i_1} \cdot a_{i_2} \cdot \ldots \cdot a_{i_k}$ where $a_{i_j} \in A$.

Definition 1. *Let S is a semigroup generated by A. The (right) Cayley graph for a semigroup S with respect to A is a directed labelled graph defined as follows: V is the set of vertices, where $V = S$; $E = \cup_{a \in A} E_a$ is the set of labelled arcs, where $E_a = \{\langle s, sa\rangle | s \in S, a \in A\}$ is a set of arcs labelled by a. The left Cayley graph is defined analogously, with $E_a = \{\langle s, a \cdot s\rangle | s \in S, a \in A\}$*

Multiplicative subgroups of $\mathbb{Q}^+$ and additive groups $\mathbb{Z}^r$. Let P be a finite set of prime numbers $\{p_1, \ldots, p_r\}$. Denote by Q_P multiplicative group of rationals, generated by P, that is the set $\{p_1^{m_1} \cdot \ldots \cdot p_1^{m_r} \mid m_1, \ldots, m_r \in \mathbb{Z}\}$ together with multiplication as the group operation. Notice that Q_P is a finitely generated subgroup of $(\mathbb{Q}^+, \cdot)$.

It follows from the properties of multiplication, in particular from fundamental theorem of arithmetics that the mapping $\rho_P : \mathbb{Q}_P \to \mathbb{Z}^r$, $\rho(p_1^{m_1} \cdot \ldots \cdot p^{m_r}) = (m_1, \ldots m_r)$ is isomorphism between $(\mathbb{Q}_P, \cdot)$ and $(\mathbb{Z}_r, +)$.

Let $\mathbb{Z}_2$ be two-elements cyclic group $(\{0, 1\}, +^{\mathrm{mod}\ 2})$. The mapping *sign* : $\mathbb{Q} - \{0\} \to \mathbb{Z}_2$, $sign(q) = 0$ if $q > 0$ and $sign(q) = 1$ if $q < 0$ is homomorphism from $(\mathbb{Q} - \{0\}, \cdot)$ to $\mathbb{Z}_2$.

Linear and semilinear sets. A subset S of $\mathbb{N}^k$ is a *linear set* iff there exists vectors $v_0, v_1, \cdots, v_t$ in $\mathbb{N}^k$ such that $S = \{v | v = v_0 + a_1 v_1 + \cdots + a_t v_t, a_i \in \mathbb{N}\}$. The vectors v_0 (referred to as the constant vector) and $v_1, \cdots, v_t$ (referred to as the periods) are called the generators of the linear set S. The set $S \subseteq \mathbb{N}^k$ is *s*emilinear if it is a finite union of linear sets.

Theorem 1. *([11]) The problem of emptiness of the intersection of two effectively definable semilinear sets is decidable.*

Parikh maps. Let $\Sigma = \{a_1, a_2, ..., a_n\}$ be an alphabet. For each word w in Σ^*, define the *Parikh map* of w to be $\psi(w) = (|w|_{a_1}, |w|_{a_2}, \ldots, |w|_{a_n})$. For a language $L \subseteq \Sigma^*$, the *Parikh map* of L is $\psi(L) = \{\psi(w)|w \in L\}$. The language L is semilinear if $\psi(L)$ is a semilinear set. The following theorem gives an effective characterization of the Parikh maps of *regular* languages.

Theorem 2. *[14] Let F be a one-way nondeterministic finite automaton. Then the Parikh map of the regular language $L(F)$ of words accepted by F is a semilinear set effectively computable from F.*

3 Row-monomial Matrices and Semigroups

In this section we give a technical background for row-monomial matrices and semigroups, that we use to prove the decidability results.

Definition 2. *A matrix $M \in \mathbb{Q}^{n\times n}$ is said to be monomial if it has exactly one non-zero entry in each row and in each column. If the matrix has exactly one no-zero entry in each row it is said to be row-monomial.*

Simple check shows that if $M_1, M_2 \in \mathbb{Q}^{n\times n}$ are row-monomial then $M_1 \times M_2$ is also row-monomial and thus all such matrices form a semigroup with matrix multiplication as its binary operation. Denote by S^n_{row} a semigroup of all row-monomial matrices from $\mathbb{Q}^{n\times n}$.

Definition 3. *A matrix semigroup of the dimension n is called row-monomial iff it is subsemigroup of S^n_{row}.*

With any row-monomial matrix $M = (a_{ij}) \in S^n_{row}$ we associate two mappings: *Position mapping* $p_M : [n] \to [n]$ defined as $p_M(i) = j$ iff $a_{ij} \neq 0$, and *Value mapping* $v_M : [n] \to \mathbb{Q}$ defined as $v_M(i) = a_{i\,p_M(i)}$, i.e. $v_M(i) = a_{ij}$ where $a_{ij} \neq 0$ Note that any row-monomial matrix M is determined uniquely by pair $\langle p_M, v_M\rangle$.

Let T_n be a transformation semigroup over finite set $[n] = \{1, \ldots, n\}$, that is the set of all functions from $[n]$ to $[n]$ with a binary operation $*$ defined via composition of functions: $f * g = g \circ f$, i.e. $(f * g)(i) = g(f(i))$.

Proposition 1. *The mapping $\tau : M \mapsto p_M$ is a homomorphism from S^n_{row} to T_n*

Proposition 2. *For row-monomial matrices M_1 and M_2 we have $v_{M_1\times M_2} = v_{M_2}(p_{M_1}) \cdot v_{M_1}$*

The row-monomial matrices (and corresponding linear mappings) and their multiplication (composition) have a natural graph representation. Although it is not used in the proofs, it is placed here to reveal an intuition of the "dynamics", which is hidden behind the matrix multiplication.

Definition 4. *For a row-monomial matrix $M = (a_{ij}) \in \mathbb{Q}^{n\times n}$ define its graph representation as a labelled bipartite graph g_M with the set of vertices $I \cup O$, where $I = \{i_1, \ldots, i_n\}$ are* input *vertices and $O = \{o_1, \ldots, o_n\}$ are* output *vertices. The vertices i_k and o_l are connected by an arc labelled by a rational m iff $a_{lk} = m \neq 0$.*

3.1 Graphs Associated with Row-monomial Semigroups

Let S be row-monomial semigroup of the dimension n generated by set $A = \{M_1, \ldots, M_k\}$. We associate with S a directed labelled graph $G_S = (V, E)$ as follows: $V = \{p_M \mid M \in S\} \cup \{e\}$ is the set of vertices, where $e : [n] \to [n]$ is an identity mapping; $E = \cup_{M \in A} E_M$ is the set of arcs, where $E_M = \{\langle s, s * p_M \rangle \mid s \in V, M \in A\}$ is the set of arcs labelled by M. We call such labels *primary*.

Note 1. The graph G_S is very closely related to the right Cayley graph of $\tau(S) \cup e$ (see Proposition 1 for definition of τ) and has the same vertices. The difference is that the edges are labelled by the elements of $A \subset S$ and not by elements of $\tau(S) \cup e$. Thus, G_S represents the action of S on $\tau(S) \cup e$.

Extended labelled graph EG_S of a row-monomial semigroup S is an extension of G_S with the *secondary*, or *arithmetical* labels, which are n-tuples of rationals, i.e. the elements of $\mathbb{Q}^n$. For an arc $\langle s, s * p_M \rangle$ with the primary label M define its secondary label $l \in \mathbb{Q}^n$ as follows: $l = \langle v_M(s(1)), \ldots v_M(s(n)) \rangle$. Remember, that v_M is the value mapping of M and s is a function from $[n]$ to $[n]$.

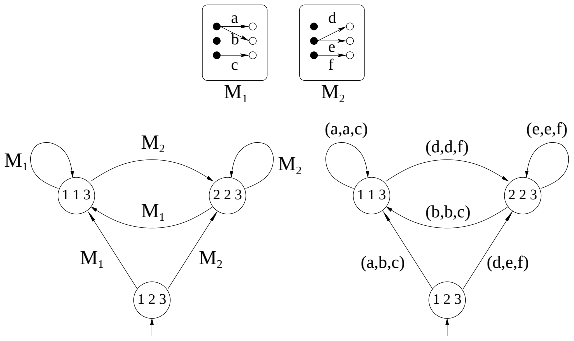

Fig. 1. Graphs associated with a row-monomial semigroup: G_S (left) and EG_S (right, primary labelling omitted)

Example 1. The figure 1 shows G_S and EG_S for the row-monomial semigroup generated by matrices $M_1 = \begin{pmatrix} a & 0 & 0 \\ b & 0 & 0 \\ 0 & 0 & c \end{pmatrix}$ and $M_2 = \begin{pmatrix} 0 & d & 0 \\ 0 & e & 0 \\ 0 & 0 & f \end{pmatrix}$.

Proposition 3. *Let S be a row-monomial semigroup generated by A. Then for any vertex s of the graph G_S and any sequence $D = M_{i_1}, \ldots M_{i_j}$ of elements from A there is a path in G_S outgoing from a vertex s with a sequence of primary labels D.*

Proof By definition of G_S for every vertex s and label $M \in A$ there is an arc outgoing from s and labelled by M $\square$.

Now we have a key lemma connecting the properties of pathes in EG_S with the properties of multiplication in S.

Lemma 1. *For a row-monomial semigroup S let $M_{i_1}, \ldots, M_{i_j}$ be the sequence of primary labels, and $l_1 = \langle l_{11}, \ldots, l_{1n} \rangle, \ldots, l_j = \langle l_{j1}, \ldots, l_{jn} \rangle$ be the sequence of secondary labels along a path (of non-zero finite length) from e to some vertex s in the graph EG_S. Then we have $p_{M_{i_1} \times \ldots \times M_{i_j}} = s$ and for any $t \in [n]$ $v_{M_{i_1} \times \ldots \times M_{i_j}}(t) = \prod\limits_{1 \leq k \leq j} l_{kt}$.*

Proof Easy induction on the length of a path based on two observations: for an arc with the label M going from v to v' we have $v' = v * p_M = p_M \circ v$ (definition of G_S), and $p_{M_{i_1} \times \ldots \times M_{i_j}} = p_{M_{i_1}} * \ldots * p_{M_{i_j}} = p_{M_{i_j}} \circ \ldots \circ p_{M_{i_1}}$ (corollary of Proposition 1). The proof proceeds by induction on the length of a path. Let us fix some $t \in [n]$. For a path of length 1 having a primary label M_{i_1}, which starts from e we have a secondary label (by definition of secondary labels) $l_1 = \langle v_{M_{i_1}}(e(1)), \ldots, v_{M_{i_1}}(e(n)) \rangle = \langle v_{M_{i_1}}(1), \ldots, v_{M_{i_1}}(n) \rangle$. It follows $v_{M_{i_1}}(t) = l_{1t} = \prod\limits_{1 \leq k \leq 1} l_{kt}$. Consider now a path $s_0 = e \stackrel{M_{i_1}}{\to} s_1 \stackrel{M_{i_2}}{\to} \ldots \stackrel{M_{i_{j-1}}}{\to} s_{j-1} \stackrel{M_{i_j}}{\to} s_j$ of length $j > 1$. Then we have $v_{M_{i_1} \times \ldots \times M_{i_j}}(t) = = v_{M_{i_j}}(p_{M_{i_1} \times \ldots \times M_{i_{j-1}}}(t)) \cdot v_{M_{i_1} \times \ldots \times M_{i_{j-1}}}(t)$ (by Proposition 2) $= v_{M_{i_j}}(s_{j-1}(t)) \cdot v_{M_{i_1} \times \ldots \times M_{i_{j-1}}}(t)$ (by part 1 of the Lemma) $= l_{jt} \cdot v_{M_{i_1} \times \ldots \times M_{i_{j-1}}}(t)$ (by definition of secondary labels) $= l_{jt} \cdot \prod\limits_{1 \leq k \leq j-1} l_{kt}$ (by induction assumption) $= \prod\limits_{1 \leq k \leq j} l_{kt}$ $\square$.

4 Decidability of the Membership and the Vector Reachability Problems

In this section we show that the membership and reachability problems are decidable for row-monomial matrix semigroups over $\mathbb{Q}$.

Theorem 3. *Any finitely generated row-monomial matrix semigroup over $\mathbb{Q}^+$ has decidable membership problem.*

Proof Let S be a row-monomial semigroup generated by finite set of matrices of the dimension n $A = \{M_1, \ldots M_k\}$. Given an arbitrary row-monomial matrix M we have to decide whether $M \in S$, that is whether there is a sequence $M_{i_1}, \ldots, M_{i_j}$ of elements of A such that $M = M_{i_1} \times \ldots \times M_{i_j}$. By Lemma 1 and Proposition 3 this problem is equivalent to the following problem in terms of a graph EG_S:

Problem 3. **Given:** A matrix M. **Question:** Is there any path $s_0 = e \stackrel{l_1}{\to} s_1 \stackrel{l_2}{\to} \ldots \stackrel{l_{j-1}}{\to} s_{j-1} \stackrel{l_j}{\to} s_j = s$ in EG_S, with secondary labels $l_k = \langle l_{k1}, \ldots l_{kn} \rangle$, $k = 1, \ldots j$, such that

- $p_M = s$ *(Condition 1)*;
- $v_M(t) = \prod\limits_{1 \leq k \leq j} l_{kt}$ for all $t \in [n]$ *(Condition 2)*.

Notice that for any $M \in S^n_{row}$ there is at most one vertex s in EG_S such that $s = p_M$. Since EG_S has only finitely many vertices, obtained constructively from

A, there is a simple decision procedure which determines whether such s exists. If there is no such a vertex then answer to the membership problem is negative: $M \notin S$. Otherwise, we have to check further whether there is a path from e to such s which satisfies the arithmetical constraints of the Condition 2.

Let $L = \{L_1 = \langle L_{11}, \ldots, L_{1n}\rangle \ldots L_m = \langle L_{m1}, \ldots, L_{mn}\rangle\}$ be the *finite* set of *all* secondary labels in EG_S. Let $x_1, \ldots, x_m$ be the multiplicities of labels $L_1, \ldots, L_m$, respectively, on some path from e to $s = P_M$. Then that path satisfies the Condition 2 if and only if these multiplicities satisfy the following equation:

$$L_1^{x_1} \cdot \ldots \cdot L_m^{x_m} = v_M \tag{1}$$

which is compact vector form of the following system of equations:

$$\begin{cases} (L_{11})^{x_1} \cdot (L_{21})^{x_2} \cdot \ldots \cdot (L_{m1})^{x_m} = v_M(1) \\ \vdots \\ (L_{1n})^{x_1} \cdot (L_{2n})^{x_2} \cdot \ldots \cdot (L_{mn})^{x_m} = v_M(n) \end{cases} \tag{2}$$

We transform now every *equation* of the system (2) into the equivalent *system* of linear Diophantine equations by using isomorphism ρ defined in Subsection 2. Let $P = \{p_1, \ldots, p_r\}$ be the set of all prime numbers in the factorizations of all rationals L_{ij} and $v_M(i)$ in (2). Then we replace every equation

$$(L_{1i})^{x_1} \cdot (L_{2i})^{x_2} \cdot \ldots \cdot (L_{mi})^{x_m} = v_M(i)$$

of the system (2) with the equivalent linear equation

$$x_1 \cdot \rho_P(L_{1i}) + x_2 \cdot \rho_P(L_{2i}) + \ldots + x_k \cdot \rho_P(L_{mi}) = \rho_P(v_M(i)) \tag{3}$$

which is a vector representation of a Diophantine system of linear equations:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1m}x_m = b_1 \\ \vdots \\ a_{r1}x_1 + a_{r2}x_2 + \ldots + a_{rm}x_m = b_r \end{cases} \tag{4}$$

where $\langle a_{1j}, a_{2j}, \ldots a_{rj}\rangle = \rho_P(L_{ji})$ and $b_i = \rho_P(v_M(i))$.

When all equations in (2) are replaced we get a system of Diophantine $r \cdot n$ linear equations with integer coefficients in m unknowns $x_1, \ldots, x_m$ which is equivalent to (2) and (1).

Theorem 4. *(see e.g. [7, 6]) The problem whether a Diophantine system of linear equations has a solution, is decidable and all its solutions form an effectively definable semilinear set.*

Then, by Theorem 4 a set of solutions for the equation (1) can be represented by an effectively computable semilinear set which we denote by $\mathcal{S}^{ar}$.

Further, all words in the alphabet L which one can read along the paths from e to s form a regular language which we denote by $\mathcal{L}_s$. By Theorem 2 Parikh map $\psi(\mathcal{L}_s)$ of $\mathcal{L}_s$ is effectively computable semilinear set and we have by that an effective characterization of possible multiplicities of labels on all possible paths form e to s. It follows that there is a path from e to s satisfying Condition 2 iff $\mathcal{S}^{ar} \cap \psi(\mathcal{L}_s) \neq \emptyset$.

Since the problem of emptiness of intersection of two effectively definable semilinear sets is decidable (by Theorem 1), the problem of existence of such a path is decidable and, therefore, we get decidability of membership problem for finitely generated row-monomial semigroups over $\mathbb{Q}^+$. $\square$

Now we extend the result of Theorem 3 to the general case of row-monomial matrices over $\mathbb{Q}$.

Theorem 5. *Any finitely generated row-monomial matrix semigroup over $\mathbb{Q}$ has decidable membership problem.*

Proof Let S be row-monomial semigroup of the dimension n over $\mathbb{Q}$, generated by finite set of matrices $A = \{M_1, \dots M_k\}$. We need to construct an extended version of EG_S which incorporates the information on algebraic signs. The signs of rational values will be represented by the elements of the group $\underbrace{\mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_{n} = \mathbb{Z}_2^n$. Now we construct the graph $EG_S^* = (V, E)$ containing all information on how S acts on $(\tau(S) \cup e) \times \mathbb{Z}_2^n$.

- The set of vertices $V = \{\langle p_M, b\rangle \mid M \in S, b \in \mathbb{Z}_2^n\} \cup \{\langle e, \bar{0}\rangle\}$, where $e : [n] \to [n]$ is an identity mapping and $\bar{0}$ is the zero element in the group $\mathbb{Z}_2^n$;
- The set of arcs $E = \cup_{M \in A} E_M$, where $E_M = \{\langle (s, b)(s * p_M, b + sign(l))\rangle \mid (s, b) \in V, M \in A$ and l is the secondary (arithmetical) label of $\langle s, s * p_M\rangle$ in EG_S $\}$ is the set of arcs labelled by M. Here $sign(l)$ is a homomorphic image of $l \in \mathbb{Q}^n$ in $\mathbb{Z}_2^n$.

Similarly to the proof of Theorem 3, the question whether some matrix M belong to the finitely generated row-monomial semigroup S is equivalent now to the following problem of existence of suitable paths in the graph EG_G^*.

Problem 4. **Given:** A matrix M. **Question:** Is there any path $s_0 = (e, \bar{0}) \xrightarrow{l_1} s_1 \xrightarrow{l_2} \dots \xrightarrow{l_{j-1}} s_{j-1} \xrightarrow{l_j} s_j = s$ in EG_S^*, with secondary labels $l_k = \langle l_{k1}, \dots l_{kn}\rangle$, $k = 1, \dots j$, such that

- $(p_M, (sign(v_M(1)), \dots, sign(v_M(n)))) = s$ *(Condition 1')*;
- $|v_M(t)| = |\prod_{1 \leq k \leq j} l_{kt}|$ for all $t \in [n]$ *(Condition 2')*.

The rest of the proof repeats all arguments of the proof of Theorem 3. $\square$.

Theorem 6. *Any finitely generated row-monomial matrix semigroup over $\mathbb{Q}$ has decidable vector reachability problem.*

Proof. Fix some finitely generated row-monomial semigroup S of the dimension n. Reduce the vector reachability problem for S to the finite set of problems, whose questions are "Is there any matrix $M \in S$ with a given p_M such that $\bar{y} = M \cdot \bar{x}$?". Notice that there is only finitely many different p_M for the elements of semigroup S.

Further, for $\bar{x} = (x_1, \ldots, x_n)$ and $\bar{y} = (y_1, \ldots, y_n) = M \cdot \bar{x}$ we have $y_i = v_M(i) \cdot x_{p_M(i)}$, $i = 1 \ldots n$. Thus, for given $\bar{x}, \bar{y}$ and fixed p_M we get the system SE of linear equations with n unknowns $v_M(i)$. If such a system is inconsistent (e.g. if $y_i \neq 0$ and $x_{p_{M(i)}} = 0$) then there is no matrix M with position mapping p_M satisfying $\bar{y} = M \cdot \bar{x}$. If the system is consistent, then we reduce our problem to the question on whether the semigroup S contains a matrix M with given p_M and v_M (solution the of SE). If $v_M(i)$ is defined for all i then by Theorem 5 this problem is decidable. If some $v_M(i)$ are undefined (e.g. if $y_i = 0$ and $x_{p_M(i)} = 0$) then we reduce the problem to the finitely many modified variants of Problem 4 from the proof of Theorem 5 as follows. Consider all possible variants of Condition 1' which are consistent with the obtained solution $(v_M(1), \ldots, v_M(n))$ of the system SE and with Condition 2' applied only to those t for which $v_M(t)$ is defined. It is easy to see that initial reachability problem has positive answer iff at least one of these variants has a positive solution. □

If all matrices $\{M_1, \ldots M_k\}$ in the generating set of some row-monomial semigroup S are in fact *monomial*, then one may consider group structure on the elements of S. The following theorem is an easy corollary of Theorems 5 and 6.

Theorem 7. *Let S be a matrix group generated by a finite set A of monomial matrices. Then the membership and reachability problems are decidable for S.*

5 More General Result for Matrix Semigroups

An inspection of the proofs of Theorems 3 and 6 reveals that only a few properties of rational numbers were actually used. Because of that one can generalize these theorems to the following

Theorem 8. *Let $\mathcal{S}$ be any countable commutative semigroup with the following properties: semigroup operation (multiplication) is effectively computable and the set of positive integer solutions of an equation $a_1^{x_1} \cdot \ldots \cdot a_k^{x_k} = a_t$ with $a_1, \ldots, a_k, a_t \in \mathcal{S}$ is effectively computable from the equation semilinear set. Then any finitely-generated row-monomial matrix semigroup over $\mathcal{S}$ has decidable membership and vector reachability problems.*

Proof. The proof repeats the proofs of Theorem 3 and 6, except two parts. First we assume everywhere the elements of $\mathcal{S}$ instead of elements of $\mathbb{Q}^+$ or $\mathbb{Q}$. Second we go directly from the equation (1) to its set of solutions $\mathcal{S}^{ar}$ using the second assumption of the theorem. We again use the fact that the intersection of two semilinear sets is effectively constructible semilinear set and the emptiness problem for a semilinear set is decidable [11]. Finally note that the requirement of commutativity is essential, because otherwise one can not reduce Condition 2 to the equation (1) (see the proof of Theorem 3). □

As an instance of the general result consider the case when $\mathcal{S}$ is an arbitrary finitely generated *commutative* matrix semigroup of the dimension n over an algebraic number field F. It has been shown in [1] that for any multiplicative equation of the above form, the set of its solutions is an effectively computable semilinear set. Then from Theorem 8 we have

Proposition 4. *Let $\mathcal{K} \subseteq (F^{n\times n})^{m\times m}$ be a finitely generated row-monomial matrix semigroup of the dimension m over $\mathcal{S}$. Then K has decidable membership and vector reachability problems.*

Notice, that row-monomial $m \times m$-matrices over $\mathcal{S}$, i.e. block matrices with the entries being themselves $n \times n$-matrices (elements of $\mathcal{S}$) are *not necessarily* row-monomial if considered as *$(n \cdot m \times n \cdot m)$-matrices over F*.

As an interesting application of Proposition 4 consider the membership and vector reachability problems for matrices over complex numbers. It is well-known that the multiplicative (semi-)group of complex numbers is isomorphic to a multiplicative (semi-)group of two-dimensional matrices with the mapping $a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ being an isomorphism. The proposition 4 implies now

Proposition 5. *Any finitely generated row-monomial matrix semigroup over* rational complex *numbers has decidable membrship and vector reachability problems.*

The row-monomial transformations on counter machines. Now we consider another generalization of the decision algorithms which are represented in Sections 4 and 5. This generalization is based on the idea of changing structural constraints of matrix semigroups towards the analysis of row-monomial transformations on arbitrary graph structure. The class of graphs associated with matrix semigroups (Subsection 3.1) is quite limited. The natural extension of such matrix multiplication system is an arbitrary labelled directed graph G where each label is a row-monomial matrix over $\mathcal{S}$. Similarly to the membership problem in matrix semigroups for a matrix M we can define the "matrix reachability problem" in the more general system with an arbitrary labelled directed graph.

Problem 5. **The matrix reachability problem.** Given a row-monomial matrix M over $\mathcal{S}$ and an arbitrary labelled directed finite graph G where each label is a row-monomial matrix over $\mathcal{S}$. Determine whether there exists a sequence of labels $M_1, M_2, \ldots, M_k$ on the finite connecting path in a graph G starting from an initial node, such that $M_1 \times M_2 \times \ldots \times M_k = M$.

Theorem 9. *Let G be an arbitrary directed graph labelled by row-monomial matrices with elements from a commutative semigroup $\mathcal{S}$ satisfying the conditions from Theorem 8. The matrix reachability and vector reachability problems for G are decidable.*

It is not difficult to translate the model of directed graph labelled by row-monomial matrices over $\mathbb{Q}$ to closely related model of counter machine in which a transition can be fired only if the values of counters satisfy some guards [5]. Actually the "row-monomial transformations" on counters correspond to the guards of the form $x'_i = x_j \cdot c_{i,j}$, where x'_i or x_i the value of counter i respectively after or before the transition. According to isomorphism ρ between $(Q_P, \cdot)$ and $(Z_r, +)$

(defined in Subsection 2) we can convert each guard of the form $x'_i = x_j \cdot c_{i,j}$ to the set of guards of the form $x'_i = x_j + c_{i,j}$ and getting to an equivalent additive system. This translation shows that the vector reachability problem for a graph G can be formulated as a reachability problem for a class of counter machine. The reachability problem for multi counter machine is defined as follows: "Given initial state and set of counter values $C_{initial}$ for a counter machine A. Determine whether there is a reachable final state with the set of counter values C_{final}".

Proposition 6. *Let A be a counter machine*

i. *The reachability problem for a counter machine with guards of the form $x'_i = x_j \cdot c_{i,j}$, where $c_{i,j} \in \mathbb{Q}$ is decidable.*

ii. *The reachability problem for a counter machine with guards of the form $x'_i = x_j + c_{i,j}$, where $c_{i,j} \in \mathbb{Z}$ is decidable.*

The decidability results from Theorem 9 and Proposition 6 follow from the existence of decision algorithms for matrix semigroups. The only difference is that the new algorithms should take into account the structure of the graph. But this can be incorporated into existing methods in a straightforward way.

Actually the set of reachable states for counter machines from the Proposition 6.ii is definable in Presburger arithmetics. This fact can be extracted from Theorem 4 of Finkel and Leroux in [10]. So the reachability for such class of machines can be determined by checking the formulae in Presburger arithmetics In contrast to their solution we have used more specific methods.

Column-monomial case. The class of column-monomial matrices is a natural counterpart of the class of row-monomial matrices. The matrix transpose A^T of any row-monomial matrix A is a column-monomial and vice versa. All results on decidability of *membership* and *matrix reachability problems* for row-monomial matrices can be easily carried out to the case of column-monomial matrices using classical identity $(A \times B)^T = B^T \times A^T$.

As to the vector reachability problems for column-monomial matrices the situation is more complicated. In order to compute the result of application of a column-monomial linear mapping to a vector, one needs *both multiplication and addition* operations, unlike the row-monomial case, where only multiplication is needed. One may show that vector reachability problems may be reduced in that case to the *parameterized versions* of membership (or, more general, matrix reachability) problems, where a target matrix may include indeterminate entries. We leave the investigation of related decidability and algorithmic issues for the further work.

6 Conclusion

We have shown in this paper that the restriction to the row-monomial matrices makes many algorithmic problems for matrices decidable (unlike the general case). We started with showing decidability of membership and vector reachability problems for row-monomial martix semigroups over rationals. We then carried out these results to the wider class of semigroups of matrices with entries being from any semigroup satisfying some natural effectiveness conditions. Thereby we extend the class of (non-commutative, in general) matrix semigroups where the membership problem is known to be decidable.

Then we have shown that the proposed methods may be extended to show the decidability of more general matrix reachability problems, which in fact are equivalent to the reachability problems for specific counter automata. It is turned out that we get some already known results about automata with integer counters, but using a different and more specific methods.

There are several directions for further work. First, to investigate to what extent the proposed methods can be used to demonstrate decidability of other, not necessarily row-monomial classes of matrix semigroups and related vector reachability problems. Second, to investigate the vector reachability problems for column-monomial matrices. Third, taking counter automata perspective, to investigate whether one can handle more general guards in such automata using the methods we have presented here.

References

1. L. Babai, R. Beals, J. Cai, G. Ivanyos, E. M. Luks Multiplicative equations over commuting matrices. ACM-SIAM symposium on Discrete algorithms, (1996) 28-30
2. J.Bestel and Karhumaki. Combinatorics on Words - A Tutorial, Bulletin of the EATCS, February (2003) 178 - 228
3. Jin-yi Cai, Richard J. Lipton, and Yechezkel Zalcstein. The complexity of the membership problem for 2-generated commutative semigroups of rational matrices. In 35th Annual Symposium on Foundations of Computer Science (1994) 135-142
4. J. Cassaigne and J. Karhumaki. Examples of undecidable problems for 2-generator matrix semigroups. Theoretical Computer Science, 204(1), (1998) 29-34
5. H. Comon and Y. Jurski. Multiple counters automata, safety analysis and Presburger arithmetic. CAV'98, LNCS 1427, (1998) 268-279
6. E. Contejean and H. Devie. An efficient algorithm for solving systems of Diophantine equations. Information and Computation, 113(1), (1994) 143-172
7. E. Contekean, F.Ajil. Complete Solving of Linear Diophantine Equations and Inequations without Adding Variables. CP95, LNCS 976, (1995) 1-17
8. A.H. Clifford and G.B. Preston. The algebraic theory of semigroups, Volume I, American Mathematical Society, Providence, Rhode Island, (1961)
9. J. Esparza, A.Finkel and R. Mayr. On the Verification of Broadacst Protocols. In Proc. LICS'99 (1999) 352-359
10. A. Finkel and J. Leroux. How to compose Presburger-accelerations: Applications to broadcast protocols. FSTTCS02, LNCS 2556, (2002) 145-156
11. S. Ginsburg. The Mathematical Theory of Context-Free Languages. McGraw-Hill, New York, (1966)
12. V.Halava, T.Harju. Mortality in Matrix Semigroups, American Mathematical Monthly, Vol 108 No. 7, (2001) 649-653
13. R. Kannan and R. J. Lipton. Polynomial-time algorithm for the orbit problem, Journal of the ACM (JACM), Volume 33 , Issue 4, (1986) 808 - 821
14. R. Parikh. On context-free languages, J. ACM, 13, (1966), 570-581
15. M. Paterson. Unsolvability in 3×3 matrices. Studies in Applied Mathematics, 49 (1970), 105-107