The freeness problem over matrix semigroups and bounded languages

Émilie Charlier [a,1,*], Juha Honkala[b,2]

[a]Institut de mathématiques, Université de Liège, Belgium
[b]Department of Mathematics and Statistics, University of Turku, Finland

Abstract

We study the freeness problem for matrix semigroups. We show that the freeness problem is decidable for upper-triangular 2×2 matrices with rational entries when the products are restricted to certain bounded languages. We also show that this problem becomes undecidable for sufficiently large matrices.

Keywords: matrix semigroup, freeness problem, bounded language, representation of rational numbers, decidability.

1. Introduction

In this paper we study the freeness problem over matrix semigroups. In general, if S is a semigroup and X is a subset of S, we say that X is a code if for any integers $m, n \geq 1$ and any elements $x_1, \ldots, x_m, y_1, \ldots, y_n \in X$ the equation

$$x_1 x_2 \ldots x_m = y_1 y_2 \ldots y_n$$

implies that $m = n$ and $x_i = y_i$ for $1 \leq i \leq m$. The freeness problem over S consists of deciding whether a finite subset of S is a code.

The freeness problem over S can also be stated as follows. Suppose Σ is a finite nonempty alphabet and $\mu : \Sigma^+ \to S$ is a morphism. Then the freeness problem over S is to decide whether μ is injective.

For a general introduction to freeness problems over semigroups see [1].

An interesting special case of the freeness problem concerns freeness of matrix semigroups. Let R be a semiring and let $k \geq 1$ be an integer. Then the semiring of $k \times k$ matrices (resp. upper-triangular $k \times k$ matrices) is denoted by $R^{k \times k}$ (resp. $R^{k \times k}_{\text{uptr}}$). The sets $R^{k \times k}$ and $R^{k \times k}_{\text{uptr}}$ are monoids, and the freeness problem over $R^{k \times k}$ is to decide whether a given morphism

$$\mu : \Sigma^* \to R^{k \times k}$$

[*] Corresponding author
[1] Tel: +3243669384, E-mail address: echarlier@ulg.ac.be.
[2] E-mail address: juha.honkala@utu.fi.

is injective. Most cases of this problem are undecidable. In fact, Klarner, Birget and Satterfield [2] proved that the freeness problem over $\mathbb{N}^{3\times 3}$ is undecidable. Cassaigne, Harju and Karhumäki [3] improved this result by showing that the problem remains undecidable for $\mathbb{N}^{3\times 3}_{\text{uptr}}$. Both of these undecidability results use the Post correspondence problem. Cassaigne, Harju and Karhumäki also discuss the freeness problem for 2×2 matrices having rational entries (also see [4]). This problem is still open, even for upper-triangular 2×2 matrices having rational entries. On the other hand, Bell and Potapov [5] have proved that the freeness problem is undecidable for diagonal matrices over quaternions. For some special decidable cases of the freeness problem for 2×2 matrices see [1, 3, 6, 7].

In this paper we discuss the problem whether a given morphism $\mu : \Sigma^* \to \mathbb{Q}^{k\times k}_{\text{uptr}}$ is injective on certain bounded languages. This approach is inspired by the well-known fact that many language-theoretic problems which are undecidable in general become decidable when restricted to bounded languages. Recall that a language $L \subseteq \Sigma^*$ is called bounded if there is an integer s and words $w_1, \ldots, w_s \in \Sigma^*$ such that $L \subseteq w_1^* w_2^* \ldots w_s^*$. Our main result is that we can decide the injectivity of a given morphism $\mu : \{x, z_1, \ldots, z_{t+1}\}^* \to \mathbb{Q}^{2\times 2}_{\text{uptr}}$ on the language $L_t = z_1 x^* z_2 x^* z_3 \ldots z_t x^* z_{t+1}$ for any $t \geq 1$, provided that the matrices $\mu(z_i)$ are nonsingular for $1 \leq i \leq t + 1$. To prove this result we will study the representation of rational numbers in a rational base.

On the other hand, we will show that if we consider sufficiently large matrices, the injectivity problem becomes undecidable, even if restricted to certain very special bounded languages. Hence, contrary to the common situation in language theory, the restriction of the freeness problem over bounded languages remains undecidable. The proof of our undecidability result will use a reduction from Hilbert's tenth problem in a way which is commonly used to obtain various undecidability results for rational power series (see [8]) and which is also used in [9] to prove that the mortality problem is undecidable on a bounded language.

2. Results and examples

As usual, $\mathbb{Z}$ and $\mathbb{Q}$ are the sets of integers and rational numbers. If $k \geq 1$ is an integer, the set of $k \times k$ matrices having integer (resp., rational) entries is denoted by $\mathbb{Z}^{k\times k}$ (resp., $\mathbb{Q}^{k\times k}$) and the set of upper-triangular $k \times k$ matrices is denoted by $\mathbb{Z}^{k\times k}_{\text{uptr}}$ (resp., $\mathbb{Q}^{k\times k}_{\text{uptr}}$).

We will consider two special families of bounded languages. Suppose $t \geq 1$ is a positive integer. Let

$$\Sigma_t = \{x, z_1, \ldots, z_{t+1}\}$$

be an alphabet having $t + 2$ different letters and let

$$\Delta = \{x, y, z_1, z_2\}$$

be an alphabet having four different letters. Define the languages $L_t \subseteq \Sigma_t^*$ and $K_t \subseteq \Delta^*$ by

$$L_t = z_1 x^* z_2 x^* z_3 \cdots z_t x^* z_{t+1}$$

and

$$K_t = z_1(x^*y)^{t-1}x^*z_2.$$

We can now state our results.

Theorem 1. *Let t be a positive integer. It is decidable whether a given morphism*

$$\mu\colon \Sigma_t^* \to \mathbb{Q}_{\mathrm{uptr}}^{2\times 2}$$

such that $\mu(z_i)$ is nonsingular for $i = 1, \ldots, t+1$, is injective on L_t.

Theorem 2. *There exist two positive integers k and t such that there is no algorithm to decide whether a given morphism*

$$\mu\colon \Delta^* \to \mathbb{Z}_{\mathrm{uptr}}^{k\times k}$$

is injective on K_t.

Observe that Theorem 1 still holds if Σ_t and L_t are replaced by Δ and K_t, respectively.

Intuitively, the languages K_t of Theorem 2 are the simplest bounded languages for which we are able to show that the injectivity problem is undecidable, while the languages L_t of Theorem 1 are the most general bounded languages for which we are able to show decidability. The study of the injectivity problem on bounded languages is motivated by the fact that while bounded languages have a simple structure, the induced matrix products already can be used to represent very general sets, as we will see in the proof of Theorem 2.

Our proof of Theorem 2 gives a method to compute the integers k and t in Theorem 2. Indeed, if we are given a polynomial which has the required universality property for Hilbert's tenth problem, the computation of k is a tedious but straightforward task which is left to the interested reader. The resulting value of k is large.

We will continue with examples which illustrate the problem considered in Theorem 1. In the examples we assume that t is a positive integer, and

$$\mu : \Sigma_t^* \to \mathbb{Q}_{\mathrm{uptr}}^{2\times 2}$$

is a morphism such that $\mu(z_i)$ is nonsingular for $i = 1, \ldots, t+1$. We write

$$\mu(x) = M \text{ and } \mu(z_i) = N_i$$

for $i = 1, \ldots, t+1$.

Example 3. Assume that $t = 2$. Let $\mu(x) = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$ and let $\mu(z_2) = \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$. Then

$$\mu(x^m z_2 x^n) = \begin{pmatrix} 2\cdot 3^{m+n} & 3^m \\ 0 & 3 \end{pmatrix}$$

for all $m, n \in \mathbb{N}$. Hence μ is injective on L_2.

Example 4. Assume that $t = 1$. Let $M = c\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ where $b, c \in \mathbb{Q}$ and $c \neq 0$. Then

$$M^{n} = c^{n}\begin{pmatrix} 1 & nb \\ 0 & 1 \end{pmatrix}$$

for all $n \geq 0$. It follows that there exist distinct integers $m, n \geq 0$ such that

$$M^{m} = M^{n}$$

if and only if $c \in \{-1, 1\}$ and $b = 0$. Hence μ is injective on L_1 if and only if $c \notin \{-1, 1\}$ or $b \neq 0$.

Example 5. Assume that $t = 2$ and let M be as in Example 4. Let

$$N_2 = \begin{pmatrix} A_2 & B_2 \\ 0 & C_2 \end{pmatrix}$$

where $A_2, B_2, C_2 \in \mathbb{Q}$. Then

$$M^{m} N_2 M^{n} = c^{m+n}\begin{pmatrix} A_2 & A_2bn + B_2 + C_2bm \\ 0 & C_2 \end{pmatrix}$$

for all $m, n \geq 0$. This implies that if $c \notin \{-1, 1\}$, then μ is injective if and only if $A_2b \neq C_2b$. If $c \in \{-1, 1\}$, then μ is not injective on L_2.

Example 6. Assume that $t \geq 3$. Let M and N_2 be as in Example 5 and let

$$N_3 = \begin{pmatrix} A_3 & B_3 \\ 0 & C_3 \end{pmatrix}$$

where $A_3, B_3, C_3 \in \mathbb{Q}$. Then we can find two different triples (m_1, m_2, m_3) and (n_1, n_2, n_3) of nonnegative integers such that

$$m_1 + m_2 + m_3 = n_1 + n_2 + n_3$$

and

$$C_2C_3m_1 + A_2C_3m_2 + A_2A_3m_3 = C_2C_3n_1 + A_2C_3n_2 + A_2A_3n_3.$$

This implies that

$$M^{m_1} N_2 M^{m_2} N_3 M^{m_3} = M^{n_1} N_2 M^{n_2} N_3 M^{n_3},$$

which shows that μ is not injective on L_t.

3. Proof of Theorem 1

3.1. From matrices to representations of rational numbers

For any rational number m, we introduce a corresponding letter $\overline{m}$. We regard the elements of the set $\mathbb{Q}_1 = \{\overline{m} \mid m \in \mathbb{Q}\}$ as digits. For any $r \in \mathbb{Q} \setminus \{0\}$ and any word $w = \overline{w_{n-1}} \cdots \overline{w_1}\,\overline{w_0}$, where the $\overline{w_i}$'s belong to $\mathbb{Q}_1$, we define the *value of w with respect to the base r* to be the number

$$\operatorname{val}_r(w) = \sum_{i=0}^{n-1} w_i\, r^i.$$

Observe that $\operatorname{val}_r(\overline{m}) = m$ holds for any $m \in \mathbb{Q}$. If u and v are words over $\mathbb{Q}_1$ and k is a positive integer, then

$$\operatorname{val}_r(uv) = r^{|v|}\operatorname{val}_r(u) + \operatorname{val}_r(v)$$

and

$$\operatorname{val}_r(u^k) = (r^{(k-1)|u|} + \cdots + r^{|u|} + 1)\operatorname{val}_r(u).$$

The following lemma is straightforward.

Lemma 7. *Let $M = c\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $c, a, b \in \mathbb{Q}$. Then*

$$M^n = c^n \begin{pmatrix} a^n & \operatorname{val}_a(\overline{b}^{\,n}) \\ 0 & 1 \end{pmatrix}$$

for any $n \geq 1$.

The following lemma shows that in order to prove Theorem 1 we can study representations of rational numbers in a rational base.

Lemma 8. *Let $s \geq 1$ be a positive integer, let $M = c\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ with $a, b, c \in \mathbb{Q}$ and, for $i = 1, \ldots, s+1$, let $N_i = \begin{pmatrix} A_i & B_i \\ 0 & C_i \end{pmatrix}$ with $A_i, B_i, C_i \in \mathbb{Q}$. Then there exist rational numbers $q_1, \ldots, q_{s+1}, p_1, \ldots, p_s$ such that for all positive integers $m_1, \ldots, m_s$,*

$$N_1 M^{m_1} N_2 \cdots N_s M^{m_s} N_{s+1}$$

$$= c^{m_1+\cdots+m_s} \begin{pmatrix} A_1 \cdots A_{s+1} a^{m_1+\cdots+m_s} & \operatorname{val}_a(\overline{q_1}\,\overline{p_1}^{\,m_s-1}\,\overline{q_2} \cdots \overline{q_s}\,\overline{p_s}^{\,m_1-1}\,\overline{q_{s+1}}) \\ 0 & C_1 \cdots C_{s+1} \end{pmatrix}. \tag{1}$$

PROOF. We proceed by induction on s. Suppose first that $s = 1$. If $m_1 \geq 1$, Lemma 7 implies

$$\begin{aligned}
N_1 M^{m_1} N_2 &= \begin{pmatrix} A_1 & B_1 \\ 0 & C_1 \end{pmatrix} c^{m_1} \begin{pmatrix} a^{m_1} & \mathrm{val}_a(\overline{b}^{m_1}) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A_2 & B_2 \\ 0 & C_2 \end{pmatrix} \\
&= c^{m_1} \begin{pmatrix} A_1 a^{m_1} & A_1 \mathrm{val}_a(\overline{b}^{m_1}) + B_1 \\ 0 & C_1 \end{pmatrix} \begin{pmatrix} A_2 & B_2 \\ 0 & C_2 \end{pmatrix} \\
&= c^{m_1} \begin{pmatrix} A_1 A_2 a^{m_1} & A_1 B_2 a^{m_1} + A_1 C_2 \mathrm{val}_a(\overline{b}^{m_1}) + B_1 C_2 \\ 0 & C_1 C_2 \end{pmatrix} \\
&= c^{m_1} \begin{pmatrix} A_1 A_2 a^{m_1} & \mathrm{val}_a\left(\overline{A_1B_2}\, \overline{A_1C_2b}^{m_1-1}\, \overline{C_2(A_1b+B_1)}\right) \\ 0 & C_1 C_2 \end{pmatrix}.
\end{aligned}$$

This implies the claim for $s = 1$.

Let then $s \geq 1$ and assume inductively that we have computed rational numbers $q_1, \ldots, q_{s+1}, p_1, \ldots, p_s$ such that (1) holds for all $m_1, \ldots, m_s \geq 1$. Let $m_{s+1} \geq 1$ and let $N_{s+2} = \begin{pmatrix} A_{s+2} & B_{s+2} \\ 0 & C_{s+2} \end{pmatrix}$. For the sake of brevity, let us denote $d_1 = A_1 \cdots A_{s+1}$, $d_2 = C_1 \cdots C_{s+1}$ and $N_{s+2} = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$. Then

$$\begin{aligned}
&N_1 M^{m_1} N_2 M^{m_2} N_3 \cdots N_{s+1} M^{m_{s+1}} N_{s+2} \\
&= c^{m_1+\cdots+m_s} \begin{pmatrix} d_1 a^{m_1+\cdots+m_s} & T \\ 0 & d_2 \end{pmatrix} c^{m_{s+1}} \begin{pmatrix} a^{m_{s+1}} & \mathrm{val}_a(\overline{b}^{m_{s+1}}) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \\
&= c^{m_1+\cdots+m_{s+1}} \begin{pmatrix} d_1 a^{m_1+\cdots+m_s} & T \\ 0 & d_2 \end{pmatrix} \begin{pmatrix} A a^{m_{s+1}} & B a^{m_{s+1}} + C \mathrm{val}_a(\overline{b}^{m_{s+1}}) \\ 0 & C \end{pmatrix} \\
&= c^{m_1+\cdots+m_{s+1}} \begin{pmatrix} d_1 A a^{m_1+\cdots+m_{s+1}} & d_1 a^{m_1+\cdots+m_s}(B a^{m_{s+1}} + C \mathrm{val}_a(\overline{b}^{m_{s+1}})) + CT \\ 0 & d_2 C \end{pmatrix}
\end{aligned}$$

where $T = \mathrm{val}_a(\overline{q_1}\, \overline{p_1}^{m_s-1}\, \overline{q_2} \cdots \overline{q_s}\, \overline{p_s}^{m_1-1}\, \overline{q_{s+1}})$. We compute $d_1 A = A_1 \cdots A_{s+2}$, $d_2 C = C_1 \cdots C_{s+2}$ and

$$\begin{aligned}
&d_1 a^{m_1+\cdots+m_s}(B a^{m_{s+1}} + C \mathrm{val}_a(\overline{b}^{m_{s+1}})) + CT \\
&\quad = \mathrm{val}_a(\overline{d_1B}\, \overline{d_1Cb}^{m_{s+1}-1}\, \overline{C(d_1b+q_1)}\, \overline{Cp_1}^{m_s-1}\, \overline{Cq_2} \cdots \overline{Cq_s}\, \overline{Cp_s}^{m_1-1}\, \overline{Cq_{s+1}}).
\end{aligned}$$

This concludes the proof.

3.2. Comparison of the representations

If Σ is an alphabet, we let $\hat{\Sigma}$ be the alphabet defined by

$$\hat{\Sigma} = \left\{ \begin{bmatrix} \sigma_1 \\ \sigma_2 \end{bmatrix} : \sigma_1, \sigma_2 \in \Sigma \right\}.$$

A word in $\hat{\Sigma}^*$ given by

$$\left[\begin{array}{c}\sigma_{i_1}\\ \sigma_{j_1}\end{array}\right]\left[\begin{array}{c}\sigma_{i_2}\\ \sigma_{j_2}\end{array}\right]\cdots\left[\begin{array}{c}\sigma_{i_\ell}\\ \sigma_{j_\ell}\end{array}\right]$$

will be written as

$$\left[\begin{array}{c}\sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_\ell}\\ \sigma_{j_1}\sigma_{j_2}\cdots\sigma_{j_\ell}\end{array}\right].$$

In what follows it is important to observe that if we have a word $\left[\begin{array}{c}w_1\\ w_2\end{array}\right]$ in $\hat{\Sigma}^*$ then necessarily the words w_1 and w_2 have equal lengths.

The next lemma shows that in comparing the representations of rational numbers we can use regular languages.

Lemma 9. *Let $S \subseteq \mathbb{Q}$ be a finite nonempty set, let $S_1 = \{\overline{s}\colon s \in S\}$ and let $X = \hat{S_1}$. Let $r \in \mathbb{Q} \setminus \{-1, 0, 1\}$. Then the language*

$$L = \left\{\left[\begin{array}{c}w_1\\ w_2\end{array}\right] \in X^* : \mathrm{val}_r(w_1) = \mathrm{val}_r(w_2)\right\}$$

is effectively regular.

Proof. First, observe that

$$\mathrm{val}_r(x_n \cdots x_1 x_0) = \mathrm{val}_r(y_n \cdots y_1 y_0)$$

holds if and only if

$$\mathrm{val}_{r^{-1}}(x_0 x_1 \cdots x_n) = \mathrm{val}_{r^{-1}}(y_0 y_1 \cdots y_n)$$

holds (here, the x_i's and y_i's are digits). Indeed, we have

$$x_n r^n + \cdots + x_1 r + x_0 = y_n r^n + \cdots + y_1 r + y_0$$

if and only if

$$x_0 r^{-n} + x_1 r^{-n+1} + \cdots + x_n = y_0 r^{-n} + y_1 r^{-n+1} + \cdots + y_n.$$

Because the class of effectively regular languages is closed under reversal, we may assume $|r| > 1$ without loss of generality.

Next, we assume without loss of generality that

$$S = \{-m+1, -m+2, \ldots, -1, 0, 1, \ldots, m-2, m-1\}$$

where m is a positive integer. In other words, we will assume that

$$X = \left\{\left[\begin{array}{c}\overline{a}\\ \overline{b}\end{array}\right] : a, b \in \{-m+1, -m+2, \ldots, -1, 0, 1, \ldots, m-2, m-1\}\right\}.$$

Let $r = \frac{u}{v}$, where $u, v \in \mathbb{Z}$ do not have any nontrivial common factor. Let $d = \frac{2m-2}{|r|-1}$. We define the nondeterministic automaton $\mathcal{A} = (Q, X, \delta, \{q_0\}, \{q_0\})$ as follows:

$$Q = \{q_i \colon i \in [-d, d] \cap \mathbb{Z}\}$$

and

$$\delta\big(q_i, \left[\begin{array}{c} \overline{a} \\ b \end{array}\right]\big) = \begin{cases} q_j, & \text{if } i + a - b = rj; \\ \emptyset, & \text{if } \frac{i+a-b}{r} \notin [-d, d] \cap \mathbb{Z}. \end{cases}$$

We will prove $L(\mathcal{A}) = L^T$. (Here L^T is the reversal of L.)

Assume first that

$$\left[\begin{array}{c} \overline{a_0} \\ b_0 \end{array}\right]\left[\begin{array}{c} \overline{a_1} \\ b_1 \end{array}\right]\cdots\left[\begin{array}{c} \overline{a_n} \\ b_n \end{array}\right] \in L^T,$$

or, equivalently,

$$a_0 + a_1 r + \cdots + a_n r^n = b_0 + b_1 r + \cdots + b_n r^n. \tag{2}$$

We claim that there exist states $q_{\gamma_1}, q_{\gamma_2}, \ldots, q_{\gamma_{n+1}} \in Q$ such that

$$\delta\big(q_0, \left[\begin{array}{c} \overline{a_0} \\ b_0 \end{array}\right]\left[\begin{array}{c} \overline{a_1} \\ b_1 \end{array}\right]\cdots\left[\begin{array}{c} \overline{a_i} \\ b_i \end{array}\right]\big) = q_{\gamma_{i+1}} \tag{3}$$

and

$$\gamma_{i+1} + a_{i+1} + \cdots + a_n r^{n-i-1} = b_{i+1} + \cdots + b_n r^{n-i-1} \tag{4}$$

hold for all $i = 0, \ldots, n$.

We first show the existence of q_{γ_1}. Since (2) implies

$$a_0 v^n + a_1 u v^{n-1} + \cdots + a_n u^n = b_0 v^n + b_1 u v^{n-1} + \cdots + b_n u^n,$$

we have $a_0 \equiv b_0 \pmod{u}$. Hence

$$\gamma_1 = \frac{a_0 - b_0}{r} = \frac{(a_0 - b_0)v}{u}$$

is an integer. Then since $|a_0| \leq m - 1$ and $|b_0| \leq m - 1$, we have

$$|\gamma_1| = \frac{|a_0 - b_0|}{|r|} \leq d,$$

and hence the state q_{γ_1} exists.

Further, we have

$$\delta\big(q_0, \left[\begin{array}{c} \overline{a_0} \\ b_0 \end{array}\right]\big) = q_{\gamma_1}$$

and

$$\gamma_1 + a_1 + a_2 r + \cdots + a_n r^{n-1} = b_1 + b_2 r + \cdots + b_n r^{n-1}.$$

This proves the claim for $i = 0$.

Assume then $j \in \{1, \ldots, n\}$ and assume that there exist $q_{\gamma_1}, \ldots, q_{\gamma_j} \in Q$ such that (3) and (4) hold for $i = 0, \ldots, j-1$. From (4) it follows

$$\gamma_j + a_j \equiv b_j \pmod{u}.$$

Hence

$$\gamma_{j+1} = \frac{\gamma_j + a_j - b_j}{r} = \frac{(\gamma_j + a_j - b_j)v}{u}$$

is an integer. Because we have

$$|\gamma_{j+1}| = \frac{|\gamma_j + a_j - b_j|}{|r|} \leq \frac{|\gamma_j| + |a_j - b_j|}{|r|} \leq \frac{d + 2m - 2}{|r|} = \frac{d + d(|r| - 1)}{|r|} = d,$$

the state $q_{\gamma_{j+1}}$ exists. Further, we have

$$\delta\big(q_0, \left[\, \frac{\overline{a_0}}{b_0} \,\right]\left[\, \frac{\overline{a_1}}{b_1} \,\right] \cdots \left[\, \frac{\overline{a_j}}{b_j} \,\right]\big) = \delta\big(q_{\gamma_j}, \left[\, \frac{\overline{a_j}}{b_j} \,\right]\big) = q_{\gamma_{j+1}}$$

and

$$\gamma_{j+1} + a_{j+1} + a_{j+2}r + \cdots + a_n r^{n-j-1} = b_{j+1} + b_{j+2}r + \cdots + b_n r^{n-j-1}.$$

This concludes the proof of the claim.

From the claim it follows

$$\delta\big(q_0, \left[\, \frac{\overline{a_0}}{b_0} \,\right]\left[\, \frac{\overline{a_1}}{b_1} \,\right] \cdots \left[\, \frac{\overline{a_n}}{b_n} \,\right]\big) = q_{\gamma_{n+1}}$$

and

$$\gamma_{n+1} = 0.$$

Therefore

$$\left[\, \frac{\overline{a_0}}{b_0} \,\right]\left[\, \frac{\overline{a_1}}{b_1} \,\right] \cdots \left[\, \frac{\overline{a_n}}{b_n} \,\right] \in L(\mathcal{A}).$$

Hence $L^T \subseteq L(\mathcal{A})$.

Suppose now that

$$\left[\, \frac{\overline{a_0}}{b_0} \,\right]\left[\, \frac{\overline{a_1}}{b_1} \,\right] \cdots \left[\, \frac{\overline{a_n}}{b_n} \,\right] \in L(\mathcal{A}).$$

Then there exist states $q_{\gamma_0}, q_{\gamma_1}, \ldots, q_{\gamma_{n+1}} \in Q$ such that

$$\delta\big(q_{\gamma_i}, \left[\, \frac{\overline{a_i}}{b_i} \,\right]\big) = q_{\gamma_{i+1}}$$

for $i = 0, \ldots, n$ and $\gamma_0 = \gamma_{n+1} = 0$. By the definition of $\mathcal{A}$ we have

$$\gamma_i + a_i - b_i = r\gamma_{i+1}$$

for $i = 0, \ldots, n$. This implies

$$a_0 + a_1 r + \cdots + a_n r^n = b_0 + b_1 r + \cdots + b_n r^n.$$

Hence

$$\left[\, \frac{\overline{a_0}}{b_0} \,\right]\left[\, \frac{\overline{a_1}}{b_1} \,\right] \cdots \left[\, \frac{\overline{a_n}}{b_n} \,\right] \in L^T.$$

Therefore $L(\mathcal{A}) \subseteq L^T$.

3.3. A decidability method for Theorem 1

We are now ready for the proof of Theorem 1.

Let t be a positive integer and assume that

$$\mu\colon \Sigma_t^* \to \mathbb{Q}_{\mathrm{uptr}}^{2\times 2}$$

is a morphism such that $\mu(z_i)$ is nonsingular for $i = 1, \ldots, t+1$.

First, we consider the particular case where $\mu(x)$ is singular. Suppose $\mu(x) = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, the case $\mu(x) = \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix}$ being symmetric. Then $\mu(x^n) = a^{n-1}\mu(x)$ for all $n \geq 1$. If $t = 1$, then μ in injective on L_1 if and only if $a \notin \{-1, 0, 1\}$. If $t \geq 2$, then the equation $\mu(x^2 z_2 x) = \mu(x z_2 x^2)$ implies that μ is not injective on L_t.

For the rest of the proof we suppose that $\mu(x)$ is not singular. Let

$$\mu(x) = M = c \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

and, for $i = 1, \ldots, t+1$, let

$$\mu(z_i) = N_i = \begin{pmatrix} A_i & B_i \\ 0 & C_i \end{pmatrix},$$

where $a, b, c, A_i, B_i, C_i \in \mathbb{Q}$ for $i = 1, \ldots, t+1$. Because M and N_i are nonsingular, a, c, A_i, C_i are nonzero for $i = 1, \ldots, t+1$.

If $a = -1$, then $M^2 = c^2 I$. If $t \geq 2$, then μ is not injective on L_t because we have $N_1 M^2 N_2 = N_1 N_2 M^2$. If $t = 1$ and $c \in \{-1, 1\}$, then μ is not injective on L_t because $N_1 N_2 = N_1 M^2 N_2$. If $t = 1$ and $c \notin \{-1, 1\}$, it follows from the equation $\det(M^n) = (-c)^n$ that μ is injective on L_t.

For the rest of the proof we suppose in addition that $a \neq -1$. We also suppose that $a \neq 1$. In fact, we have already proved Theorem 1 if $a = 1$ in Examples 4, 5 and 6.

For each subset $K \subseteq \{1, \ldots, t\}$, let

$$L_t(K) = \{z_1 x^{m_1} z_2 x^{m_2} z_3 \cdots z_t x^{m_t} z_{t+1} \colon m_i = 0 \text{ for } i \in K,\ m_i \geq 1 \text{ for } i \notin K\}.$$

Now L_t is the union of the disjoint languages $L_t(K)$ where K runs over all the subsets of $\{1, \ldots, t\}$. This implies the following lemma.

Lemma 10. *With the notation explained above, the morphism μ is injective on L_t if and only if*

(i) for each $K \subseteq \{1, \ldots, t\}$, μ is injective on $L_t(K)$; and

(ii) if $K_1, K_2 \subseteq \{1, \ldots, t\}$ with $K_1 \neq K_2$, then there does not exist two words $w_1 \in L_t(K_1)$ and $w_2 \in L_t(K_2)$ such that $\mu(w_1) = \mu(w_2)$.

To conclude the proof of Theorem 1 we have to show that conditions (i) and (ii) in Lemma 10 are decidable. We first prove that (ii) is decidable.

Lemma 11. *Condition (ii) of Lemma 10 is decidable.*

Proof. For $w_1 \in L_t(K_1)$ and $w_2 \in L_t(K_2)$, we have

$$\mu(w_1) = N'_1 M^{k_1} N'_2 M^{k_2} N'_3 \cdots N'_{s_1} M^{k_{s_1}} N'_{s_1+1}$$

and

$$\mu(w_2) = N''_1 M^{\ell_1} N''_2 M^{\ell_2} N''_3 \cdots N''_{s_2} M^{\ell_{s_2}} N''_{s_2+1}$$

where $s_1 = t - |K_1|$, $s_2 = t - |K_2|$, $k_i \geq 1$ for $i = 1, \ldots, s_1$, $\ell_j \geq 1$ for $j = 1, \ldots, s_2$ and

$$N_1 N_2 \cdots N_{t+1} = N'_1 N'_2 \cdots N'_{s_1+1} = N''_1 N''_2 \cdots N''_{s_2+1}.$$

In view of Lemma 8, deciding (ii) is equivalent to deciding the following two problems:

A : Given positive integers s_1, s_2 and rational numbers $p_1, \ldots, p_{s_1}$, $q_1, \ldots, q_{s_1+1}$, $\alpha_1, \ldots, \alpha_{s_2}$, $\beta_1, \ldots, \beta_{s_2+1}$, decide whether there exist positive integers $k_1, \ldots, k_{s_1}$, $\ell_1, \ldots, \ell_{s_2}$ such that the two matrices

$$c^{k_1+\cdots+k_{s_1}} \begin{pmatrix} A_1 \cdots A_{t+1} a^{k_1+\cdots+k_{s_1}} & \mathrm{val}_a(\overline{q_1}\, \overline{p_1}^{k_{s_1}-1}\, \overline{q_2} \cdots \overline{q_{s_1}}\, \overline{p_{s_1}}^{k_1-1}\, \overline{q_{s_1+1}}) \\ 0 & C_1 \cdots C_{t+1} \end{pmatrix} \tag{5}$$

and

$$c^{\ell_1+\cdots+\ell_{s_2}} \begin{pmatrix} A_1 \cdots A_{t+1} a^{\ell_1+\cdots+\ell_{s_2}} & \mathrm{val}_a(\overline{\beta_1}\, \overline{\alpha_1}^{\ell_{s_2}-1}\, \overline{\beta_2} \cdots \overline{\beta_{s_2}}\, \overline{\alpha_{s_2}}^{\ell_1-1}\, \overline{\beta_{s_2+1}}) \\ 0 & C_1 \cdots C_{t+1} \end{pmatrix} \tag{6}$$

are equal.

B : Given a positive integer s and rational numbers $q, p_1, \ldots, p_s, q_1, \ldots, q_{s+1}$, decide whether there exist positive integers $k_1, \ldots, k_s$ such that the two matrices

$$c^{k_1+\cdots+k_s} \begin{pmatrix} A_1 \cdots A_{t+1} a^{k_1+\cdots+k_s} & \mathrm{val}_a(\overline{q_1}\, \overline{p_1}^{k_s-1}\, \overline{q_2} \cdots \overline{q_s}\, \overline{p_s}^{k_1-1}\, \overline{q_{s+1}}) \\ 0 & C_1 \cdots C_{t+1} \end{pmatrix} \tag{7}$$

and

$$\begin{pmatrix} A_1 \cdots A_{t+1} & q \\ 0 & C_1 \cdots C_{t+1} \end{pmatrix} \tag{8}$$

are equal.

Problem B corresponds to the case where one of the subsets K_1 and K_2 is equal to $\{1, \ldots, t\}$. Because the products ac, $A_1 \cdots A_{t+1}$ and $C_1 \cdots C_{t+1}$ are nonzero, a necessary condition for the equality of (7) and (8) is

$$a^{k_1+\cdots+k_s} = 1.$$

Because $a \notin \{-1, 1\}$ this condition never holds and Problem B has no solutions.

We now turn to Problem A. Because the products ac, $A_1 \cdots A_{t+1}$ and $C_1 \cdots C_{t+1}$ are nonzero, (5) and (6) are equal if and only if

$$a^{k_1+\cdots+k_{s_1}} = a^{\ell_1+\cdots+\ell_{s_2}}, \tag{9}$$

$$c^{k_1+\cdots+k_{s_1}} = c^{\ell_1+\cdots+\ell_{s_2}} \tag{10}$$

and

$$\mathrm{val}_a(\overline{q_1}\,\overline{p_1}^{k_{s_1}-1}\,\overline{q_2}\cdots\overline{q_{s_1}}\,\overline{p_{s_1}}^{k_1-1}\,\overline{q_{s_1+1}}) = \mathrm{val}_a(\overline{\beta_1}\,\overline{\alpha_1}^{\ell_{s_2}-1}\,\overline{\beta_2}\cdots\overline{\beta_{s_2}}\,\overline{\alpha_{s_2}}^{\ell_1-1}\,\overline{\beta_{s_2+1}}). \tag{11}$$

Because $a \notin \{-1, 0, 1\}$ (9) and (10) hold if and only if

$$k_1 + \cdots + k_{s_1} = \ell_1 + \cdots + \ell_{s_2}. \tag{12}$$

Let now $S = \{q_1, \ldots, q_{s_1+1}, p_1, \ldots, p_{s_1}, \beta_1, \ldots, \beta_{s_2+1}, \alpha_1, \ldots, \alpha_{s_2}\}$, let $S_1 = \{\overline{s}\colon s \in S\}$ and let $X = \hat{S_1}$. Let

$$L = \left\{ \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \in X^* : \mathrm{val}_a(u_1) = \mathrm{val}_a(u_2) \right\}$$

and let

$$T_1 = \left\{ \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \in X^* : u_1 \in \overline{q_1}\,\overline{p_1}^*\,\overline{q_2}\cdots\overline{q_{s_1}}\,\overline{p_{s_1}}^*\,\overline{q_{s_1+1}}, \right.$$
$$\left. u_2 \in \overline{\beta_1}\,\overline{\alpha_1}^*\,\overline{\beta_2}\cdots\overline{\beta_{s_2}}\,\overline{\alpha_{s_2}}^*\,\overline{\beta_{s_2+1}} \right\}.$$

By Lemma 9, L is effectively regular. Clearly, so is T_1. In fact, it is easy to construct a finite automaton which accepts T_1. Now we can decide (ii) by checking whether

$$L \cap T_1 = \emptyset.$$

Indeed, suppose a word $\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \in X^*$ belongs to $L \cap T_1$. Then there exist positive integers $k_1, \ldots, k_{s_1}, \ell_1, \ldots, \ell_{s_2}$ such that

$$u_1 = \overline{q_1}\,\overline{p_1}^{k_{s_1}-1}\,\overline{q_2}\cdots\overline{q_{s_1}}\,\overline{p_{s_1}}^{k_1-1}\,\overline{q_{s_1+1}}$$

and

$$u_2 = \overline{\beta_1}\,\overline{\alpha_1}^{\ell_{s_2}-1}\,\overline{\beta_2}\cdots\overline{\beta_{s_2}}\,\overline{\alpha_{s_2}}^{\ell_1-1}\,\overline{\beta_{s_2+1}}.$$

Because $\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \in L \cap T_1$, we have $\mathrm{val}_a(u_1) = \mathrm{val}_a(u_2)$ and $|u_1| = |u_2|$. The latter condition means that

$$k_{s_1} + \cdots + k_1 + 1 = \ell_{s_2} + \cdots + \ell_1 + 1$$

which gives (12). Hence (5) and (6) are equal. Conversely, if there exist positive integers $k_1, \ldots, k_{s_1}, \ell_1, \ldots, \ell_{s_2}$ such that the matrices (5) and (6) are equal, then

$$\begin{bmatrix} \overline{q_1}\,\overline{p_1}^{k_{s_1}-1}\,\overline{q_2} \cdots \overline{q_{s_1}}\,\overline{p_{s_1}}^{k_1-1}\,\overline{q_{s_1+1}} \\ \overline{\beta_1}\,\overline{\alpha_1}^{\ell_{s_2}-1}\,\overline{\beta_2} \cdots \overline{\beta_{s_2}}\,\overline{\alpha_{s_2}}^{\ell_1-1}\,\overline{\beta_{s_2+1}} \end{bmatrix} \in L \cap T_1.$$

Lemma 12. *Condition (i) of Lemma 10 is decidable.*

Proof. We have to decide a variant of Problem A where $s_1 = s_2$, $p_i = \alpha_i$ and $q_j = \beta_j$ for $1 \le i \le s_1$, $1 \le j \le s_1 + 1$ and we have to determine whether there exist two different s_1-tuples $(k_1, \ldots, k_{s_1})$ and $(\ell_1, \ldots, \ell_{s_1})$ of positive integers such that (11) and (12) hold. Before we can proceed as we did above in case (ii), we have to check whether there exist different s_1-tuples $(k_1, \ldots, k_{s_1})$ and $(\ell_1, \ldots, \ell_{s_1})$ of positive integers such that

$$\overline{q_1}\,\overline{p_1}^{k_{s_1}-1}\,\overline{q_2} \cdots \overline{q_{s_1}}\,\overline{p_{s_1}}^{k_1-1}\,\overline{q_{s_1+1}} = \overline{q_1}\,\overline{p_1}^{\ell_{s_1}-1}\,\overline{q_2} \cdots \overline{q_{s_1}}\,\overline{p_{s_1}}^{\ell_1-1}\,\overline{q_{s_1+1}}.$$

Observe that such s_1-tuples may exist; for example, they do exist if $p_1 = q_2 = p_2$. However, it is easy to decide whether there are such s_1-tuples. If there are, μ is not injective on $L_t(K)$. We continue with the assumption that such s_1-tuples do not exist. Then we can decide (i) proceeding as we did above. The only difference is that we replace T_1 by

$$T_2 = \left\{ \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \in T_1 : u_1 \neq u_2 \right\}.$$

This is done because we do not want T_2 to include words $\begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$ such that

$$u_1 = \overline{q_1}\,\overline{p_1}^{k_{s_1}-1}\,\overline{q_2} \cdots \overline{q_{s_1}}\,\overline{p_{s_1}}^{k_1-1}\,\overline{q_{s_1+1}},$$

$$u_2 = \overline{q_1}\,\overline{p_1}^{\ell_{s_1}-1}\,\overline{q_2} \cdots \overline{q_{s_1}}\,\overline{p_{s_1}}^{\ell_1-1}\,\overline{q_{s_1+1}}$$

and

$$(k_1, \ldots, k_{s_1}) = (\ell_1, \ldots, \ell_{s_1}).$$

Observe that we did not have this problem in case (ii) because there the languages $L_t(K_1)$ and $L_t(K_2)$ were disjoint.

4. Proof of Theorem 2

Let us fix some notation first. If $A_1, A_2, \ldots, A_s$ are matrices, then their *direct sum* $A_1 \oplus A_2 \oplus \cdots \oplus A_s$ is

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_s \end{pmatrix}.$$

If $A = (a_{ij})_{m\times n}$ and B are matrices, then their *Kronecker product* $A \otimes B$ is

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}.$$

In both cases, we have used block notation.

The direct sum and the Kronecker product have the following properties: if $A_1, A_2, \ldots, A_s$ are $m \times m$ matrices and $B_1, B_2, \ldots, B_s$ are $n \times n$ matrices, then

$$(A_1 \oplus B_1)(A_2 \oplus B_2)\cdots(A_s \oplus B_s) = (A_1A_2\cdots A_s) \oplus (B_1B_2\cdots B_s)$$

and

$$(A_1 \otimes B_1)(A_2 \otimes B_2)\cdots(A_s \otimes B_s) = (A_1A_2\cdots A_s) \otimes (B_1B_2\cdots B_s).$$

For more details on the Kronecker product, see for example [10, Chapter 12] or [8].

If k is a positive integer, then $E_k = (e_{ij})_{k\times k}$ is the $k \times k$ matrix whose only nonzero entry is $e_{1k} = 1$.

The main idea of our proof of Theorem 2 is to use the undecidability of Hilbert's tenth problem combined with the following result. Suppose that t is a positive integer and that $p(x_1, \ldots, x_t)$ is a polynomial with integer coefficients. We want to find a positive integer k and matrices $A, M, N, B \in \mathbb{Z}^{k\times k}_{\mathrm{uptr}}$ such that

$$AM^{a_1}NM^{a_2}N\cdots NM^{a_t}B = p(a_1, \ldots, a_t)E_k$$

for all nonnegative integers $a_1, \ldots, a_t$.

Fix the value of t.

Lemma 13. *There is a positive integer k and matrices $A, N, B \in \mathbb{Z}^{k\times k}_{\mathrm{uptr}}$ such that for any $i \in \{1, \ldots, t\}$ there is a matrix $M \in \mathbb{Z}^{k\times k}_{\mathrm{uptr}}$ such that*

$$AM^{a_1}NM^{a_2}N\cdots NM^{a_t}B = a_iE_k$$

for all nonnegative integers $a_1, \ldots, a_t$.

PROOF. Let $k = 2t$,

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix},$$

where $A, B \in \mathbb{Z}_{\text{uptr}}^{k\times k}$. Let $E = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Let

$$M = I \oplus \cdots \oplus I \oplus E \oplus I \oplus \cdots \oplus I,$$

where there are t summands of which E is the ith one, and let

$$N = \begin{pmatrix} 0 & I & 0 & \cdots & 0 \\ 0 & 0 & I & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & I \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

be a $k \times k$ matrix where each 0 stands for the 2×2 zero matrix.

Then $A, M, N, B \in \mathbb{Z}_{\text{uptr}}^{k\times k}$ and we have

$$\begin{aligned} M^n &= I \oplus \cdots \oplus I \oplus E^n \oplus I \oplus \cdots \oplus I \\ &= I \oplus \cdots \oplus I \oplus \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \oplus I \oplus \cdots \oplus I \end{aligned}$$

for all $n \in \mathbb{N}$.

Now, if D is any matrix in $\mathbb{Z}_{\text{uptr}}^{k\times k}$ then the only nonzero entry of ADB is the last entry in the first row, which is equal to D_{1k}. Let us compute this entry for

$$AM^{a_1}NM^{a_2}N\cdots NM^{a_t}B$$

where $a_1, \ldots, a_t$ are nonnegative integers. For this, we regard M and N as $t \times t$ matrices consisting of 2×2 blocks:

$$\begin{aligned} &(M^{a_1}NM^{a_2}N\cdots NM^{a_t})_{1t} \\ &\qquad = (M^{a_1})_{11}N_{12}(M^{a_2})_{22}N_{23}\cdots N_{i-1,i}(M^{a_i})_{ii}N_{i,i+1}\cdots N_{t-1,t}(M^{a_t})_{tt} \\ &\qquad = I \cdot I \cdot I \cdots I \cdot \begin{pmatrix} 1 & a_i \\ 0 & 1 \end{pmatrix} \cdot I \cdots I \\ &\qquad = \begin{pmatrix} 1 & a_i \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

The results follows.

Lemma 14. *Let $p_1(x_1, \ldots, x_t)$ and $p_2(x_1, \ldots, x_t)$ be polynomials with integer coefficients. Suppose there exist $s_1, s_2 \geq 1$, $A_1, M_1, N_1, B_1 \in \mathbb{Z}_{\text{uptr}}^{s_1 \times s_1}$ and $A_2, M_2, N_2, B_2 \in \mathbb{Z}_{\text{uptr}}^{s_2 \times s_2}$ such that*

$$A_1 M_1^{a_1} N_1 M_1^{a_2} N_1 \cdots N_1 M_1^{a_t} B_1 = p_1(a_1, \ldots, a_t) E_{s_1}$$

and

$$A_2 M_2^{a_1} N_2 M_2^{a_2} N_2 \cdots N_2 M_2^{a_t} B_2 = p_2(a_1, \ldots, a_t) E_{s_2}$$

for all $a_1, \ldots, a_t \in \mathbb{N}$. Then

(i) there exist $s_3 \geq 1$ and $A_3, M_3, N_3, B_3 \in \mathbb{Z}_{\text{uptr}}^{s_3 \times s_3}$ such that

$$A_3 M_3^{a_1} N_3 M_3^{a_2} N_3 \cdots N_3 M_3^{a_t} B_3 = (p_1 + p_2)(a_1, \ldots, a_t) E_{s_3}$$

for all $a_1, \ldots, a_t \in \mathbb{N}$;

(ii) there exist $s_4 \geq 1$ and $A_4, M_4, N_4, B_4 \in \mathbb{Z}_{\text{uptr}}^{s_4 \times s_4}$ such that

$$A_4 M_4^{a_1} N_4 M_4^{a_2} N_4 \cdots N_4 M_4^{a_t} B_4 = (p_1 \cdot p_2)(a_1, \ldots, a_t) E_{s_4}$$

for all $a_1, \ldots, a_t \in \mathbb{N}$;

(iii) if $c \in \mathbb{Z}$, then there exists $A_5 \in \mathbb{Z}_{\text{uptr}}^{s_1 \times s_1}$ such that

$$A_5 M_1^{a_1} N_1 M_1^{a_2} N_1 \cdots N_1 M_1^{a_t} B_1 = c \cdot p_1(a_1, \ldots, a_t) E_{s_1}$$

for all $a_1, \ldots, a_t \in \mathbb{N}$.

Proof. To prove (i) we take $M_3 = M_1 \oplus M_2$, $N_3 = N_1 \oplus N_2$,

$$A_3 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \cdot (A_1 \oplus A_2)$$

and

$$B_3 = (B_1 \oplus B_2) \cdot \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & 1 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

To prove (ii), we take $A_4 = A_1 \otimes A_2$, $M_4 = M_1 \otimes M_2$, $N_4 = N_1 \otimes N_2$ and $B_4 = B_1 \otimes B_2$. To prove (iii) it suffices to take $A_5 = cA_1$. Then the claims follow by simple computations which are left to the reader.

Now our goal is achieved and we can state the following lemma.

Lemma 15. *Let t be any positive integer and $p(x_1,\dots,x_t)$ be any polynomial with integer coefficients. Then there effectively exists a positive integer k and matrices $A, M, N, B \in \mathbb{Z}_{\mathrm{uptr}}^{k\times k}$ such that*

$$AM^{a_1}NM^{a_2}N\cdots NM^{a_t}B = \begin{pmatrix} 0 & \cdots & 0 & p(a_1,\dots,a_t) \\ 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}$$

for all $a_1,\dots,a_t \in \mathbb{N}$.

Remark 16. Lemma 15 is closely related to the well-known fact stating that if $p(x_1,\dots,x_t)$ is a polynomial having integer coefficients, then the series

$$\sum_{n_1,\dots,n_t\geq 0} p(n_1,\dots,n_t)\ x^{n_1}yx^{n_2}y\cdots yx^{n_t}$$

is $\mathbb{Z}$-rational; see for example [11]. The purpose of Lemma 15 is to show explicitly that we can get this result using only upper-triangular matrices.

We will use a strong version of the undecidability of Hilbert's tenth problem as stated in the following theorem (see [12, Theorem 3.10]).

Theorem 17. *There exists a polynomial $P(x_1,x_2,\dots,x_m)$ with integer coefficients such that no algorithm exists for the following problem: given a positive integer a, decide whether there exist nonnegative integers $b_2,\dots,b_m$ such that*

$$P(a,b_2,\dots,b_m)=0.$$

For $k=2,3,\dots$, define the Cantor polynomials $C_2, C_3, \dots$ as follows:

$$\begin{aligned} C_2(x_1,x_2) &= \frac{1}{2}(x_1+x_2)(x_1+x_2+1)+x_2, \\ C_{k+1}(x_1,\dots,x_{k+1}) &= C_2(C_k(x_1,\dots,x_k),x_{k+1}). \end{aligned}$$

These polynomials are injective on $\mathbb{N}^k$. In other words, for all nonnegative integers $n_1,\dots,n_k,m_1\dots,m_k$, if $C_k(n_1,\dots,n_k)=C_k(m_1,\dots,m_k)$ then $n_1=m_1,\dots,n_k=m_k$. Note that the C_k's are not injective on $\mathbb{Z}^k$.

Let $P(x_1,\dots,x_m)$ be as in Theorem 17. Take a new indeterminate x_{m+1} and define the polynomial $Q(x_1,\dots,x_m,x_{m+1})$ by

$$Q(x_1,\dots,x_m,x_{m+1}) = e\cdot C_{m+1}(x_1,\dots,x_m,P(x_1,\dots,x_m)^2\cdot x_{m+1}),$$

where e is a positive integer chosen such that Q has integer coefficients.

Lemma 18. *Let a be a positive integer. Then the equation $P(a,x_2,\dots,x_m)=0$ has a solution in nonnegative integers if and only if there exist nonnegative integers $b_2,\dots,b_{m+1},c_2,\dots,c_{m+1}$ such that*

$$Q(a,b_2,\dots,b_{m+1}) = Q(a,c_2,\dots,c_{m+1}) \tag{13}$$

and

$$(b_2,\dots,b_{m+1}) \neq (c_2,\dots,c_{m+1}). \tag{14}$$

Proof. Suppose first that there exist $d_2, \ldots, d_m \in \mathbb{N}$ such that

$$P(a, d_2, \ldots, d_m) = 0.$$

Then we have

$$Q(a, d_2, \ldots, d_m, x) = e \cdot C_{m+1}(a, d_2, \ldots, d_m, 0)$$

for any $x \in \mathbb{N}$. Hence, if we choose

$$(b_2, \ldots, b_{m+1}) = (d_2, \ldots, d_m, 1) \text{ and } (c_2, \ldots, c_{m+1}) = (d_2, \ldots, d_m, 2),$$

then (13) and (14) hold.

Suppose then that $P(a, d_2, \ldots, d_m) \neq 0$ for all $d_2, \ldots, d_m \in \mathbb{N}$. Suppose that

$$Q(a, b_2, \ldots, b_{m+1}) = Q(a, c_2, \ldots, c_{m+1})$$

where $b_2, \ldots, b_{m+1}, c_2, \ldots, c_{m+1} \in \mathbb{N}$. Hence

$$C_{m+1}(a, b_2, \ldots, b_m, P(a, b_2, \ldots, b_m)^2 b_{m+1})$$
$$= C_{m+1}(a, c_2, \ldots, c_m, P(a, c_2, \ldots, c_m)^2 c_{m+1}).$$

Because C_{m+1} is injective on $\mathbb{N}^{m+1}$ we obtain

$$b_2 = c_2, \ldots, b_m = c_m \tag{15}$$

and

$$P(a, b_2, \ldots, b_m)^2 b_{m+1} = P(a, c_2, \ldots, c_m)^2 c_{m+1}.$$

Using (15) and the assumption

$$P(a, b_2, \ldots, b_m) = P(a, c_2, \ldots, c_m) \neq 0,$$

we obtain $b_{m+1} = c_{m+1}$. Consequently, if $P(a, x_2, \ldots, x_m) = 0$ does not have a solution in nonnegative integers, then there does not exist $b_2, \ldots, b_{m+1}, c_2, \ldots, c_{m+1} \in \mathbb{N}$ such that (13) and (14) hold.

We are now ready for the proof of Theorem 2.

Let $P(x_1, \ldots, x_m)$ and $Q(x_1, \ldots, x_{m+1})$ be as above. By Lemma 15 there is a positive integer k and a morphism $\mu\colon \Delta^* \to \mathbb{Z}_{\text{uptr}}^{k\times k}$ such that

$$\mu(z_1 x^{a_1} y x^{a_2} y \cdots y x^{a_{m+1}} z_2) = Q(a_1, \ldots, a_{m+1}) E_k$$

for all $a_1, \ldots, a_{m+1} \in \mathbb{N}$. For each $a \in \mathbb{N}$ define the morphism $\mu_a\colon \Delta^* \to \mathbb{Z}_{\text{uptr}}^{k\times k}$ by

$$\mu_a(z_1) = \mu(z_1 x^a y),\ \mu_a(x) = \mu(x),\ \mu_a(y) = \mu(y) \text{ and } \mu_a(z_2) = \mu(z_2).$$

Then

$$\mu_a(z_1 x^{a_2} y \cdots y x^{a_{m+1}} z_2) = Q(a, a_2, \ldots, a_{m+1}) E_k$$

for any $a \geq 1$ and $a_2, \ldots, a_{m+1} \in \mathbb{N}$. By Lemma 18, for any $a \geq 1$, the morphism μ_a is injective on K_m if and only if the equation $P(a, x_2 \ldots, x_m) = 0$ does not have a solution in nonnegative integers. Now Theorem 2 follows by Theorem 17.

5. Concluding remarks

In the proof of our undecidability result we used singular matrices. On the other hand, in Theorem 1 we require that $\mu(z_i)$ is nonsingular for $i = 1, \ldots, t+1$. This assumption plays an essential role in our proof of the theorem. At present we do not know how to avoid using this assumption.

The following examples illustrate the situations where some of the matrices $\mu(z_i)$, $1 \le i \le t+1$, are singular. The first two examples show that the singularity of some $\mu(z_i)$ often implies that μ is not injective while the third example shows that this is not always the case. In these examples we use the notations of Section 3.

Example 19. Let $t \ge 2$ and assume that there is an integer i, $1 \le i \le t-1$, such that N_i is of the form $\begin{pmatrix} 0 & B \\ 0 & C \end{pmatrix}$, where $B, C \in \mathbb{Q}$. Then

$$N_i M N_{i+1} = N_i N_{i+1} M,$$

which implies that μ is not injective on L_t.

Example 20. Let $t \ge 2$ and assume that there is an integer i, $3 \le i \le t+1$, such that N_i is of the form $\begin{pmatrix} A & B \\ 0 & 0 \end{pmatrix}$, where $A, B \in \mathbb{Q}$. Then

$$M N_{i-1} N_i = N_{i-1} M N_i,$$

which implies that μ is not injective on L_t.

Example 21. Let $t \ge 1$ and let

$$N_1 = N_2 = \cdots = N_t = \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix}, \; N_{t+1} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \; M = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then for any $m_1, \ldots, m_t \ge 0$ we have

$$N_1 M^{m_1} N_2 M^{m_2} N_3 \ldots N_t M^{m_t} N_{t+1} = \begin{pmatrix} 0 & E \\ 0 & 1 \end{pmatrix}$$

where

$$E = 3^{m_1 + \cdots + m_t + t} + 3^{m_1 + \cdots + m_{t-1} + t - 1} + \cdots + 3^{m_1 + m_2 + 2} + 3^{m_1 + 1} + 1.$$

This implies that μ is injective on L_t.

6. Acknowledgement

The major part of this work was achieved when the first author was a member of the FiDiPro group of the FUNDIM research center at the University of Turku. The authors warmly thank Juhani Karhumäki and Luca Zamboni for their support.

The authors would like to thank the referees for many useful suggestions.

References

[1] J. Cassaigne, F. Nicolas, On the decidability of semigroup freeness, RAIRO Theor. Inform. Appl. 46 (2012) 355–399.

[2] D. A. Klarner, J.-C. Birget, W. Satterfield, On the undecidability of the freeness of integer matrix semigroups, Internat. J. Algebra Comput. 1 (2) (1991) 223–226.

[3] J. Cassaigne, T. Harju, J. Karhumäki, On the undecidability of freeness of matrix semigroups, Internat. J. Algebra Comput. 9 (3-4) (1999) 295–305, dedicated to the memory of Marcel-Paul Schützenberger.

[4] V. Blondel, J. Cassaigne, J. Karhumäki, Freeness of multiplicative matrix semigroups, in: Unsolved problems in mathematical systems and control theory, Princeton University Press, 2004, pp. 309–314.

[5] P. Bell, I. Potapov, Reachability problems in quaternion matrix and rotation semigroups, in: Mathematical foundations of computer science, Vol. 4708 of Lecture Notes in Comput. Sci., Springer, Berlin, 2007, pp. 346–358.

[6] P. Gawrychowski, M. Gutan, A. Kisielewicz, On the problem of freeness of multiplicative matrix semigroups, Theoret. Comput. Sci. 411 (7-9) (2010) 1115–1120.

[7] J. Honkala, Number systems and the injectivity problem for matrix representations of free monoids, Internat. J. Algebra Comput. 19 (2) (2009) 229–233.

[8] W. Kuich, A. Salomaa, Semirings, Automata, Languages, Vol. 5 of EATCS Monographs on Theoretical Computer Science, Springer-Verlag, Berlin, 1986.

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

[10] P. Lancaster, M. Tismenetsky, The Theory of Matrices, 2nd Edition, Computer Science and Applied Mathematics, Academic Press Inc., Orlando, FL, 1985.

[11] A. Salomaa, M. Soittola, Automata-Theoretic Aspects of Formal Power Series, Springer-Verlag, New York, 1978, texts and Monographs in Computer Science.

[12] G. Rozenberg, A. Salomaa, Cornerstones of Undecidability, Prentice Hall, New York, 1994.