The freeness problem for products of matrices defined on bounded languages

Émilie Charlier[*] Juha Honkala[†]

April 2014

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 large enough matrices.

The full version of this work was accepted for publication in Information and Computation. It is available online 12 March 2014.

1 Introduction

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 [5].

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. $R^{k \times k}_{\mathrm{uptr}}$). The sets $R^{k \times k}$ and $R^{k \times k}_{\mathrm{uptr}}$ are monoids and the freeness problem over $R^{k \times k}$ is to decide whether a given morphism

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

is injective. Most cases of this problem are undecidable. In fact, Klarner, Birget and Satterfield [8] proved that the freeness problem over $\mathbb{N}^{3 \times 3}$ is undecidable. Cassaigne, Harju and Karhumäki [4] improved this result by showing that the problem remains undecidable for $\mathbb{N}^{3 \times 3}_{\mathrm{uptr}}$. Both of these undecidability results use the Post correspondence problem. Cassaigne, Harju and

[*] Corresponding author, Department of Mathematics, University of Liege

[†] Department of Mathematics and Statistics, University of Turku

Karhumäki also discuss the freeness problem for 2×2 matrices having rational entries (also see [3]). This problem is still open even for upper-triangular 2×2 matrices having rational entries. On the other hand, Bell and Potapov [2] 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 [5], [4], [6] and [7].

In this paper we discuss the problem whether a given morphism $\mu : \Sigma^* \to \mathbb{Q}_{\mathrm{uptr}}^{k\times k}$ 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 $w_1, \dots, w_s \in \Sigma^*$ such that $L \subseteq w_1^* w_2^* \dots w_s^*$. Our main result is that we can decide the injectivity of a given morphism $\mu : \{x, z_1, \dots, z_{t+1}\}^* \to \mathbb{Q}_{\mathrm{uptr}}^{2\times 2}$ on the language $L_t = z_1 x^* z_2 x^* z_3 \dots z_t x^* z_{t+1}$ 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 study the representation of rational numbers in a rational base.

On the other hand, we show that if we consider large enough 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 uses a reduction from Hilbert's tenth problem in a way which is commonly used to obtain various undecidability results for rational power series (see [9]) and which is also used in [1] 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 $\mathbb{Z}_{\mathrm{uptr}}^{k\times k}$ (resp. $\mathbb{Q}_{\mathrm{uptr}}^{k\times k}$).

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

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

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 $i = 1, \dots, t+1$, 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 holds true 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,

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

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

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

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 different 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

$$M^{m_1}N_2M^{m_2}N_3M^{m_3} = M^{n_1}N_2M^{n_2}N_3M^{n_3}$$

which shows that μ is not injective on L_t.

In the proof of our undecidability result we use 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 $\mu(z_i)$, $1 \leq i \leq t+1$, 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 7. Let $t \geq 2$ and assume that there is an integer i, $1 \leq i \leq t-1$, such that N_i is of the form $\begin{pmatrix} 0 & B \\ 0 & C \end{pmatrix}$, where $B, C \in \mathbb{Q}$. Then

$$N_iMN_{i+1} = N_iN_{i+1}M,$$

which implies that μ is not injective on L_t.

Example 8. Let $t \geq 2$ and assume that there is an integer i, $3 \leq i \leq t+1$, such that N_i is of the form $\begin{pmatrix} A & B \\ 0 & 0 \end{pmatrix}$, where $A, B \in \mathbb{Q}$. Then

$$MN_{i-1}N_i = N_{i-1}MN_i,$$

which implies that μ is not injective on L_t.

Example 9. Let $t \geq 1$ 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 $m_1, \ldots, m_t \geq 0$ we have

$$N_1M^{m_1}N_2M^{m_2}N_3 \ldots N_tM^{m_t}N_{t+1} = \begin{pmatrix} 0 & E \\ 0 & 1 \end{pmatrix}$$

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.

3 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.

References

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

[2] Paul Bell and Igor Potapov. Reachability problems in quaternion matrix and rotation semigroups. In *Mathematical foundations of computer science 2007*, volume 4708 of *Lecture Notes in Comput. Sci.*, pages 346–358. Springer, Berlin, 2007.

[3] V.D. Blondel, J. Cassaigne, and J. Karhumäki. Freeness of multiplicative matrix semigroups. In *Unsolved problems in mathematical systems and control theory*, pages 309–314. Princeton University Press, 2004.

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

[5] J. Cassaigne and F. Nicolas. On the decidability of semigroup freeness. *RAIRO Theor. Inform. Appl.*, 46(3):355–399, 2012.

[6] Paweł Gawrychowski, Marin Gutan, and Andrzej Kisielewicz. On the problem of freeness of multiplicative matrix semigroups. *Theoret. Comput. Sci.*, 411(7-9):1115–1120, 2010.

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

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

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