Vesa Halava | Tero Harju | Mika Hirvensalo

Undecidability Bounds for Integer Matrices using Claus Instances

Turku Centre *for* Computer Science

TUCS Technical Report
No 766, April 2006

Undecidability Bounds for Integer Matrices using Claus Instances

Vesa Halava
Department of Mathematics and
TUCS - Turku Centre for Computer Science
University of Turku FIN-20014 Turku, Finland.
Supported by the Academy of Finland under grant 208414.
vehalava@utu.fi

Tero Harju
Department of Mathematics and
TUCS - Turku Centre for Computer Science
University of Turku, FIN-20014 Turku, Finland.
harju@utu.fi

Mika Hirvensalo
Department of Mathematics and
TUCS - Turku Centre for Computer Science
University of Turku FIN-20014 Turku, Finland.
Supported by the Academy of Finland under grant 208797.
mikhirve@utu.fi

TUCS Technical Report
No 766, April 2006

Abstract

There are several known undecidability problems for 3×3 integer matrices the proof of which uses a reduction from the Post Correspondence Problem (PCP). We establish new lower bounds in the numbers of matrices for the mortality, zero in left upper corner, vector reachability, matrix reachability, scaler reachability and freeness problems. Also, we give a short proof for a strengthened result due to Bell and Potapov stating that the membership problem is undecidable for finitely generated matrix semigroups $R \subseteq \mathbb{Z}^{4\times 4}$ whether or not $kI_4 \in R$ for any given diagonal matrix kI_4 with $|k| > 1$. These bounds are obtained by using Claus instances of the PCP.

Keywords: Undecidability; integer matrices; mortality; vector reachability; membership problem; scalar reachability; Post Correspondence Problem

TUCS Laboratory
Discrete Mathematics for Information Technology Laboratory

1 Introduction

There exist several simply defined decision problems for integer matrices which are undecidable already for matrices of dimension 3. Most of the proofs of these results apply, in one way or another, the coding technique introduced by M.S. Paterson in [13], where he proved that it is undecidable for given 3×3 integer matrices, whether or not the zero matrix belongs to the matrix semigroup generated by them. This problem is known as the *mortality problem*. Paterson's coding maps injectively a pair of words to 3×3 integer matrices. The proofs of undecidability for our problems employ an undecidability problem on pairs words originally defined and proved to be undecidable by E. Post in 1946 [14].

Problem 1 (Post Correspondence Problem (PCP)). *Let $\Gamma = \{a, b\}$ be a binary alphabet. Given a set of n pairs of words over an alphabet Γ,*

$$\{(u_i, v_i) \mid u_i, v_i \in \Gamma^*,\ i = 1, 2, \ldots, n\}, \tag{1.1}$$

does there exist a nonempty sequence $i_1, i_2, \ldots, i_k$ of indices from $\{1, 2, \ldots, n\}$ such that

$$u_{i_1} u_{i_2} \cdots u_{i_k} = v_{i_1} v_{i_2} \cdots v_{i_k}\,? \tag{1.2}$$

The PCP can also be expressed using morphisms of words. For an instance (1.1) of the PCP, let $\Sigma = \{b_1, b_2, \ldots, b_n\}$ be an alphabet and define two morphisms $h, g\colon \Sigma^* \to \Gamma^*$ by

$$h(b_i) = u_i \quad \text{and} \quad g(b_i) = v_i$$

for each $i = 1, 2, \ldots, n$. Now the original form of the PCP is equivalent to the following problem.

Problem 2 (PCP). *Given two morphisms $h, g\colon \Sigma^* \to \Gamma^*$, does there exist a nonempty word $w \in \Sigma^+$ such that*

$$h(w) = g(w)\,? \tag{1.3}$$

A given pair (h, g) of morphisms is an *instance* of the PCP. A word w with $h(w) = g(w)$ is called a *solution* of the instance (h, g). The *size* of an instance (h, g) is the cardinality of the domain alphabet, i.e., the size is equal to $|\Sigma|$, when $h, g\colon \Sigma^* \to \Gamma^*$.

The following theorem was proved by E. Post in 1946 [14].

Theorem 1. *The PCP is undecidable.*

It is known that the PCP is undecidable when $|\Sigma| = 7$. This was proved by Matiyasevich and Sénizergues in [12]. We shall recall the idea of the proof in the next section in order to express the PCP in a more strict form.

Theorem 2. *It is undecidable whether an instance (h, g) of the PCP, where $h, g\colon \{b_1, b_2, \ldots, b_7\}^* \to \Gamma^*$, has a solution $b_1 w b_7$ with $w \in \{b_2, b_3, \ldots, b_6\}^*$.*

We note that already Post's original proof of undecidability in [14] gives undecidability in the above strict form with fixed beginning letter and ending letter of the solution, but for a larger number of letters. Using this form of the PCP, a new undecidability bound for the problem called *common element in the semigroups* was established in [8].

For a finite set $\{M_1, M_2, \ldots, M_k\}$ of $n \times n$ matrices, we let

$$\langle M_1, M_2, \ldots, M_k \rangle = \{M_{i_1} M_{i_2} \ldots M_{i_m} \mid m \geq 1 \text{ and } 1 \leq i_1, i_2, \ldots, i_m \leq k\}$$

denote the semigroup generated by them.

The following matrix problems and some of their special cases are studied here.

Problem 3 (Membership problem). *Given a semigroup* $\mathbf{S} = \langle M_1, M_2, \ldots, M_k \rangle$ *of* $n \times n$ *integer matrices and a matrix* X*. Determine whether or not* $X \in \mathbf{S}$*.*

The membership problem is sometimes called *matrix reachability problem*. Note that the mortality problem is a special case of the membership problem, where X is the zero matrix.

Problem 4 (Vector reachability). *Given a semigroup* $\mathbf{S} = \langle M_1, M_2, \ldots, M_k \rangle$ *of* $n \times n$ *integer matrices and two vectors* $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^n$*. Determine whether or not there exists a matrix* $X \in \mathbf{S}$ *such that* $\mathbf{u} \cdot X = \mathbf{v}$*.*

Problem 5 (Scalar reachability). *Given a semigroup* $\mathbf{S} = \langle M_1, M_2, \ldots, M_k \rangle$ *of* $n \times n$ *integer matrices, vectors* $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^n$ *and a constant* $a \in \mathbb{Z}$*. Determine whether or not there exists a matrix* $N \in \mathbf{S}$ *such that* $\mathbf{v}N \cdot \mathbf{u}^T = a$*.*

The scalar reachability problem is connect to the problems called *zero in the right upper corner* and *zero in the right upper corner*. We define only the first variant since for that we will obtain a new bound on the number of generating matrices.

Problem 6 (Zero in the left upper corner). *Given a semigroup* $\mathbf{S} = \langle M_1, M_2, \ldots, M_k \rangle$ *of* $n \times n$ *integer matrices. Determine whether or not there exists a matrix* $N \in \mathbf{S}$ *such that* $N_{11} = 0$*, i.e., the left upper corner element of* N *is zero.*

Recall that a semigroup S is said to be *free* if there exists a subset X of S such that every element of S has a unique factorization over X, i.e., every element $s \in S$ can be uniquely expressed as a product $s = x_1 x_2 \ldots x_m$ of elements $x_i \in X$.

Problem 7 (Freeness). *Given a semigroup* $\mathbf{S} = \langle M_1, M_2, \ldots, M_k \rangle$ *of* $n \times n$ *integer matrices. Determine whether or not* $\mathbf{S}$ *is free.*

Using the undecidability result of Theorem 2, we can reduce the number of matrices in the proofs for the above stated problems. In Section 7 we consider the following problem which was shown to be undecidable by Bell and Potapov [1] for dimension 4.

Problem 8 (Special diagonal membership). *Given a semigroup* $\mathbf{S} = \langle M_1, M_2, \ldots, M_k \rangle$ *of* $n \times n$ *integer matrices and a diagonal matrix* kI_n *for an integer* $|k| > 1$*. Determine whether or not* $kI_n \in \mathbf{S}$*.*

We give a short proof of this result and improve the bound needed for the generators down to 12.

2 Proof of Theorem 2

A *semi–Thue system* $T = (\Sigma, R)$ consists of an alphabet Σ and a relation $R \subseteq \Sigma^* \times \Sigma^*$, the elements of which are called the *rules* of T. For two words $u, v \in \Sigma^*$, we write $u \to_T v$, if there are words u_1 and u_2 such that

$$u = u_1 x u_2 \quad \text{and} \quad v = u_1 y u_2 \quad \text{where} \quad (x, y) \in R.$$

Let $\rightarrow_T^*$ be the reflexive and transitive closure of the relation $\rightarrow$. Therefore, we have $u \rightarrow_T^* v$ if and only if either $u = v$ or there exists a finite sequence of words $u = v_1, v_2, \ldots, v_n = v$ such that $v_i \rightarrow_T v_{i+1}$ for each $i = 1, 2, \ldots, n-1$.

In the *individual word problem* we are given a semi-Thue system T and a fixed word w_0 and we ask, for input words w, whether or not $w \rightarrow_T^* w_0$ holds. It is known that there exist a 3-rule semi-Thue system and a fixed w_0 such that the individual word problem is undecidable, see [12].

The following result is due to Matiyasevich and Sénizergues in [12].

Theorem 3. *There exists a 3-rule semi-Thue system with undecidable individual word problem.*

The reduction from semi-Thue systems to the PCP is due to Claus [5].

Consider an instance (h, g) of the PCP, where $h, g\colon \Sigma^* \rightarrow \Gamma^*$ for $\Gamma = \{a_1, a_2, \ldots, a_m\}$. The morphism $\varphi\colon \Gamma^* \rightarrow \{a, b\}^*$ defined by $\varphi(a_i) = ab^{i+1}a$ is injective, and hence in the instance $(\varphi h, \varphi g)$ the morphisms are from Σ^* to $\{a, b\}^*$ such that the images do not have a substring aba. Accordingly, the PCP is undecidable for such instances.

Let $\Gamma = \{a, b\}$, and let

$$d = aba \quad \text{and} \quad A = ab^2b^*a.$$

An instance (h, g) with $h, g\colon \Sigma^* \rightarrow (abb^*a)^*$ of the PCP is called a *Claus instance*, if $\Sigma = \{b_1, b_2, \ldots, b_n\}$ and

$$h(b_i) \in (dA)^* \text{ with } h(b_n) = dd,$$
$$g(b_i) \in (Ad)^* \text{ with } g(b_1) = d \text{ and } g(b_n) \in (Ad)^+d.$$

The following lemma is straightforward, see, e.g., [5, 9].

Lemma 1. *Let (h, g) be a Claus instance, where $h, g\colon \{b_1, b_2, \ldots, b_n\}^* \rightarrow \Gamma^*$. Then the set of all nonempty solutions of (h, g) is*

$$\left\{b_1wb_n \mid w \in \{b_2, \ldots, b_{n-1}\}^*,\ h(b_1wb_n) = g(b_1wb_n)\right\}^+.$$

Theorem 4. *If there is a semi-Thue system with n rules having an undecidable individual word problem, then the PCP is undecidable for Claus instances of size $n + 4$.*

We shortly recall Claus's construction. Let $T = (\Gamma, R)$ be a semi–Thue system, where $\Gamma = \{a, b\}$ and the set of rules is $R = \{t_1, t_2, \ldots, t_k\}$ with $t_i = (u_i, v_i)$. We may suppose without restriction that the rules $t_i \in R$ are encoded by φ so that $u_i, v_i \in A^*$. In the following we shall consider R also as an alphabet. Let $f = aa$ be a special word used as a marker. Note that aa is not an image of φ.

Let $w, w_0 \in \{a, b\}^*$ be two given words, w being the input and w_0 fixed. Recall that $d = aba$, and define the *desynchronizing morphisms* $\ell_d, r_d\colon \{a, b\}^* \rightarrow (abb^*a)^*$ by

$$\ell_d(x) = dx \quad \text{and} \quad r_d(x) = xd$$

for both $x \in \{a, b\}$. Next define the morphisms

$$h, g\colon (\{a, b, c, e\} \cup R)^* \rightarrow \{a, b\}^*,$$

where c and e are now new letters, by

$$\begin{array}{llll} h(x) = \ell_d(x), & g(x) = r_d(x), & \text{for } x \in \{a, b\}, \\ h(t_i) = \ell_d(v_i), & g(t_i) = r_d(u_i), & \text{for } t_i \in R, \\ h(c) = \ell_d(wf), & g(c) = d, & \\ h(e) = dd, & g(e) = r_d(fw_0)d, & \end{array} \tag{2.1}$$

Clearly (h, g) is a Claus instance with $b_1 = c$ and $b_n = e$ for a suitable n.

By Lemma 1, and the proofs given in [5, 9], the solutions (if they exist) of (h, g) are necessarily of the form

$$cw_1fw_2f\cdots fw_me,$$

where each w_i has the form

$$w_i = x_{i_0}t_{i_1}x_{i_1}t_{i_2}\cdots t_{p_i}x_{p_i} \tag{2.2}$$

for some words x_{i_j} not containing letters from R. Moreover, we have $w_i \to_T^* w_{i+1}$ for $i = 1, 2, \ldots, m-1$. Note that it is possible that $p_i = 0$, in which case w_i contains no letters from R.

By Lemma 1, the minimal solutions (i.e., those that are not catenation of shorter solutions) of the instance (h, g) are of the form cwe, where $w \in (\{a, b\} \cup R)^*$. For a sake of completeness, we give a short proof for (h, g) defined in (2.1).

It is clear that the number of c's and number of e's are equal in a solution by the occurrences of $\ell_d(f)$ in the image of a solution. Assume contrary that there is a solution $cw'ew''e$ such that $cw'e$ is not a solution. We may assume that $w' \in (\{a, b, c\} \cup R)$, i.e., that w' does not have letter e, in other words, we remove any prefix of $cw'e$ being already a solution. Now $|h(cw')| > |g(cw')|$, $h(cw') \in (dA)^+$ and $g(e)$ end with double d. Only d^2 in $h(cw'e)$ is at the end, implying that $h(cw'e) = g(cw'e)$, and this is contrary to our assumption.

For Claus instances we have the following consequence of Theorem 3. This result also proves Theorem 2.

Theorem 5. *The PCP is undecidable for Claus instances of size $n = 7$.*

Note that, we always can find an equivalent instance of the PCP such that the range alphabet Γ is binary, for example, by using a variant of the encoding φ.

When the construction in (2.1) is applied to the given semi-Thue system T of Theorem 3 with undecidable individual problem, we obtain the following strong version of Theorem 5 where there is only one variable word u_1 as an input. Indeed, in (2.1) only the image $h(c)$ contains a word (w) that is not fixed by T and the individual word problem.

Theorem 6. *Let $\Gamma = \{a, b\}$. There exist a word $v_1 \in \Gamma^*$ and six pairs $(u_2, v_2), (u_3, v_3), \ldots, (u_7, v_7) \in \Gamma^* \times \Gamma^*$ such that it is undecidable whether for a given word $u_1 \in \Gamma^*$,*

$$u_1u_{i_2}u_{i_3}\ldots u_{i_m}u_7 = v_1v_{i_2}v_{i_3}\ldots v_{i_m}v_7$$

for some indices $i_2, i_3, \ldots, i_m \in \{2, 3, \ldots, 6\}$. Moreover, the instance (h, g), where $h(b_i) = u_i$ and $g(b_i) = v_i$ for $i = 1, 2, \ldots, 7$, is a Claus instance.

Finally, we remark that the Claus's construction also yields a nice corollary for the *generalized PCP* (GPCP, for short).

Problem 9 (GPCP). *Given a pair of morphisms (h, g), where $h, g\colon \Sigma^* \to \Gamma^*$, and words $p_1, p_2, s_1, s_2 \in \Gamma^*$, and it is asked to determine whether or not there exists a word $w \in \Sigma^*$ such that*

$$p_1h(w)s_1 = p_2g(w)s_2?$$

As a general reference for the GPCP we give [9]. The following theorem gives a new undecidability bound for the GPCP, the old bound being $|\Sigma| = 7$.

Theorem 7. *The GPCP is undecidable for instances having $|\Sigma| = 5$. Moreover, there exists a fixed pair (h, g) of morphisms and fixed words p_2, s_1, s_2 such that it is undecidable for a word p whether or not a there exists a word w such that $ph(w)s_1 = p_2g(w)s_2$.*

3 Zero in the left upper corner and the scalar reachability

In this section we give new proofs for undecidability of the zero in the left upper corner and for the scalar reachability problem. We begin with some definitions needed throughout this paper. In the following let ε denote the empty word.

For any alphabet $\Delta = \{a_1, a_2, ..., a_n\}$, define a mapping $\sigma\colon \Delta^* \to \mathbb{N}$ by

$$\sigma(a_{i_1}a_{i_2}\cdots a_{i_k}) = \sum_{j=1}^{k} i_j n^{k-j} \quad \text{and} \quad \sigma(\varepsilon) = 0. \tag{3.1}$$

Notice that σ is injective, and

$$\sigma(uv) = n^{|v|}\sigma(u) + \sigma(v). \tag{3.2}$$

Define a monoid morphism $\gamma\colon \Delta^* \times \Delta^* \to \mathbb{N}^{3\times 3}$, originally defined by Paterson in [13], by

$$\gamma(u, v) = \begin{pmatrix} n^{|u|} & 0 & 0 \\ 0 & n^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{pmatrix}. \tag{3.3}$$

The following lemma is easy to prove, see e.g. [9].

Lemma 2. *The function $\gamma\colon \Delta^* \times \Delta^* \to \mathbb{N}^{n\times n}$ is an injective morphism satisfying*

$$\gamma(u_1u_2, v_1v_2) = \gamma(u_1, v_1)\gamma_1(u_2, v_2).$$

Actually the morphism γ is *doubly injective* meaning that if $\gamma(u_1, v_1)_{31} = \gamma(u_2, v_2)_{31}$, then $u_1 = u_2$, and if $\gamma(u_1, v_1)_{32} = \gamma(u_2, v_2)_{32}$, then $v_1 = v_2$. Notice that for the empty word ε, we have $\gamma(\varepsilon, \varepsilon) = I_3$, the identity matrix.

Let now $\Delta = \{a_1, a_2, a_3\}$ and $\Gamma = \{a_2, a_3\}$ be fixed alphabets. We use the morphism $\gamma\colon \Delta^* \times \Delta^* \to \mathbb{N}^{3\times 3}$ defined in (3.3) to represent pairs of words by nonnegative integer matrices:

$$\gamma(u, v) = \begin{pmatrix} 3^{|u|} & 0 & 0 \\ 0 & 3^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{pmatrix}. \tag{3.4}$$

Consider the following special matrix A and its inverse A^{-1},

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad A^{-1} = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

and define $\gamma'\colon \Delta^* \times \Delta^* \to \mathbb{N}^{3\times 3}$ by

$$\gamma'(u, v) = A\gamma(u, v)A^{-1} = \begin{pmatrix} 3^{|u|} + \sigma(u) - \sigma(v) & \sigma(v) & -3^{|u|} - \sigma(u) + \sigma(v) + 1 \\ 3^{|u|} - 3^{|v|} & 3^{|v|} & -3^{|u|} + 3^{|v|} \\ \sigma(u) - \sigma(v) & \sigma(v) & -\sigma(u) + \sigma(v) + 1 \end{pmatrix}.$$

Since the matrices $\gamma'(u,v)$ and $\gamma(u,v)$ are similar, γ' is an injective morphism. Indeed, $\gamma'(u_1,v_1)\gamma'(u_2,v_2) = \gamma'(u_1u_2, v_1v_2)$.

Furthermore, by above, for all words $u, v \in \Delta^*$, we have

$$(\gamma'(u,v))_{11} = 3^{|u|} + \sigma(u) - \sigma(v). \tag{3.5}$$

It was proved in [7] that it is undecidable whether or not a finitely generated semigroup $\mathbf{S}$ of 3×3 integer matrices contains a matrix M with $M_{11} = 0$. In [7] the number of generating matrices was not directly mentioned, but the construction there gives 14 generators. Applying a trick used in the proof of the undecidability of mortality problem in [7], one can show that a better bound of 8 matrices can be achieved. We now improve this bound to 7, and strengthen the claim according to Theorem 6.

Theorem 8. *There is a semigroup $\mathbf{S}$ generated by six 3×3 integer matrices $M_2, M_3, \ldots, M_7$ such that it is undecidable for a matrix $M_1 \in \mathbb{Z}^{3\times 3}$ whether $\mathbf{S}$ contains a matrix M with $(M_1M)_{11} = 0$.*

In particular, it is undecidable for matrix semigroups $\mathbf{M}$ generated by seven 3×3 integer matrices whether $\mathbf{M}$ contains a matrix M with $M_{11} = 0$.

Proof. Let (h, g) be a Claus instance of the PCP provided by Theorem 6 such that $h, g\colon \Sigma^* \to \Gamma^*$ where $\Sigma = \{b_1, b_2, \ldots, b_7\}$ and $\Gamma = \{a_2, a_3\}$ $(= \{a, b\})$. Let a_1 be a new symbol, and denote $\Delta = \{a_1, a_2, a_3\}$. Then the minimal solutions of (h, g) are of the form b_1wb_7, where w does not contain the letters b_1 and b_7. Define the matrices

$$M_1 = \gamma'(h(b_1), a_1g(b_1)) \quad \text{and} \quad M_i = \gamma'(h(b_i), g(b_i)) \tag{3.6}$$

for $2 \le i \le 7$, and let $\mathbf{M} = \langle M_1, M_2, \ldots, M_7\rangle$. Then $\mathbf{S} = \langle M_2, \ldots, M_7\rangle$. Notice that the matrices $M_2, \ldots, M_7$ are fixed for all instances in Theorem 6, and thus only M_1 varies.

Let $N = M_{j_1}M_{j_2}\cdots M_{j_n} \in \mathbf{M}$ for some $w = b_{j_1}b_{j_2}\ldots b_{j_n}$. By (3.5) and (3.2),

$$N_{11} = 3^{|u|} + \sigma(u) - \sigma(v) = \sigma(a_1u) - \sigma(v)$$

for $u = h(w) \in \Gamma^*$ and for a word $v \in \Delta^*$. Therefore, since σ is injective, $N_{11} = 0$ if and only if $v = a_1u$. In order for a_1 to be a prefix of v, we must have $j_1 = 1$, since a_1 appear only in the matrix M_1. Hence $N = M_1M_{j_2}\cdots M_{j_n}$. Finally, $N_{11} = 0$ if and only if $v = a_1g(w) = a_1h(w)$ and $w = b_1b_{j_2}\cdots b_{j_n}$ and $h(w) = g(w)$. Since the solutions of (h, g) are of the form b_1xb_7, this holds if and only there exists a minimal i with $2 \le i \le n$ such that $i = 7$, $w' = b_{j_2}\cdots b_{j_{i-1}} \in \{b_2, \ldots, b_6\}^*$ and $h(b_1w'b_7) = g(b_1w'b_7)$. Then obviously,

$$(M_1M_{j_2}\cdots M_{j_{i-1}}M_7)_{11} = 0.$$

The claim now follows from Theorem 2. □

In the above we were able to decrease the number of the matrices needed in the proof by one. For the scalar reachability we can do better, since the old bound is seven matrices, see [9]. Note that the claim follows for semigroups generated by seven integer matrices by Theorem 8 by using vector vectors $\mathbf{u} = \mathbf{v} = (1, 0, \ldots, 0)$.

Theorem 9. *The scalar reachability problem is undecidable for semigroups $\mathbf{S}$ generated by five integer matrices of dimension 3.*

Proof. Let (h, g) be a Claus instance, where $h, g\colon \{b_1, \ldots, b_6\}^* \to \Gamma^*$. It is clear that the PCP for Claus instance is undecidable also in the form where it is asked whether not there exist $w \in \{b_2, \ldots, b_6\}^+$ (i.e., w is non-empty) such that $h(b_1 w b_7) = g(b_1 w b_7)$. We need this stricter form in the following.

Let $\mathbf{S}$ be the semigroup attached to a Claus instance (h, g) as in the proof of Theorem 8 according to which there is a matrix product having 0 in the left upper corner if and only if for some $2 \leq j_2, \ldots, j_{i-1} \leq 6$ with $i > 2$ (since w' for (h, g) is non-empty),

$$(M_1 M_{j_2} \cdots M_{j_{i-1}} M_7)_{11} = 0.$$

This is equivalent to the condition

$$(1, 0, 0) M_1 M_{j_2} \cdots M_{j_{i-1}} M_7 (1, 0, 0)^T = 0. \tag{3.7}$$

Let then $\mathbf{x} = (1, 0, 0) M_{b_1}$ and $\mathbf{y} = M_7 (1, 0, 0)^T$. Now (3.7) is equivalent to

$$\mathbf{x} M_{j_2} \cdots M_{j_{i-1}} \mathbf{y} = 0.$$

Therefore, zero in the left upper corner problem is equivalent to scalar reachability problem for semigroups generated by 5 matrices $M_2, M_3, \ldots, M_6$, together with the vectors $\mathbf{x}$, $\mathbf{y}$ and scalar 0. This proves the claim. □

Note that for the zero in the right upper corner, the bound of numbers of matrices is 7. This is achieved by a direct reduction from the PCP, see [5] or [9]. This bound cannot be decreased by the above Claus instances.

4 The mortality problem and the matrix reachability problem

Next prove that the mortality problem is undecidable for semigroups generated by seven 3×3 integer matrices. The proof is a modification of the proof in [7] where it was proved that the mortality problem is undecidable in 3×3 case for eight generators.

Theorem 10. *There is a semigroup $\mathbf{S}$ generated by six 3×3 integer matrices such that it is undecidable for a matrix A whether $AM = 0$ for some $M \in \mathbf{S}$.*

In particular, the mortality problem is undecidable for semigroups generated by seven 3×3 integer matrices.

Proof. Let $\mathbf{M}$ be the semigroup of 3×3 integer matrices generated by the matrices $M_1, M_2, \ldots, M_7$ as defined in the proof of Theorem 8 for a Claus instance (h, g) of the PCP. Again, the matrices $M_2, \ldots, M_7$ are fixed for all instances in Theorem 6, and thus only M_1 varies.

Let $\mathbf{R}$ be the semigroup generated by $M_1, M_2, \ldots, M_7$ together with the idempotent matrix B for which $B_{11} = 1$ and otherwise $B_{ij} = 0$. Then, for any matrix $M \in \mathbf{M}$,

$$BMB = \begin{pmatrix} M_{11} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Therefore, if there exists a matrix $M \in \mathbf{M}$ with $M_{11} = 0$, then $0 \in \mathbf{R}$. On the other hand, assume that $0 \in \mathbf{R}$. Without restriction we can assume that

$0 = BN_1BN_2 \cdots N_nB$, for some $n \geq 1$ and $N_i \in \mathbf{M}$ for all $i = 1, 2, \ldots, n$. Since B is idempotent, we have

$$\begin{aligned} 0 =& (BN_1BN_2 \cdots N_tB)_{11} = (BN_1B \cdot BN_2B \cdots BN_nB)_{11} \\ =& (N_1)_{11}(N_2)_{11} \cdots (N_n)_{11}, \end{aligned}$$

and therefore $(N_i)_{11} = 0$ for some index i. We conclude that $0 \in \mathbf{R}$ if and only if $N_{11} = 0$ for some $N \in \mathbf{M}$. Now $N_{11} = 0$ for a matrix $N \in \mathbf{M}$ if and only if

$$N = M_1 M_{j_1} \cdots M_{j_i} M_7$$

and $h(b_1 b_{j_1} \cdots b_{j_i} b_7) = g(b_1 b_{j_1} \cdots b_{j_i} b_7)$ where $2 \leq j_1, \ldots, j_i \leq 6$. Therefore, the zero matrix belongs to $\mathbf{R}$ if and only if it is in the semigroup $\mathbf{S}'$ generated by the following seven matrices: $BM_1, M_2, M_3, \ldots, M_6, M_7B$. The first claim follows by choosing $\mathbf{S} = \langle M_2, M_3, \ldots, M_6, M_7B \rangle$ and $A = BM_1$. □

On the other hand, the case where the dimension of the matrices is two remains problematic, see [15].

Problem 10 (Open). *Is the mortality problem decidable for semigroups of* 2×2 *integer matrices?*

Since the mortality problem is a special case of the membership problem, we have

Corollary 1. *The membership problem is undecidable for semigroups generated by seven* 3×3 *integer matrix.*

We shall return to the membership problem for diagonal matrices in Section 7.

It is known that the mortality problem is undecidable for semigroups generated by two matrices of dimension nk, where n is the bound for the dimension of undecidable cases of the mortality problem for k matrices; see [4] and [2]. Therefore, Theorem 10 has the following corollary.

Theorem 11. *The mortality problem is undecidable for two matrices of dimension 21.*

5 Vector reachability

In this section we study the vector reachability problem. In the special case of this problem, the *vector mortality problem* the given vector is $\mathbf{v} = (0, \ldots, 0)$. We prove that this problem is undecidable for six 3×3 integer matrix. The previous best bound was eight proved in [6].

Here we use the morphisms γ defined in (3.4), namely

$$\gamma(u, v) = \begin{pmatrix} 3^{|u|} & 0 & 0 \\ 0 & 3^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{pmatrix}.$$

We define a special matrix

$$A = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Theorem 12. *The vector reachability problem (and the vector mortality problem) is undecidable for semigroups generated by six 3×3 integer matrix.*

Proof. Let (h, g) be a Claus instance of the PCP, where $h, g\colon \{b_1, b_2, \ldots, b_7\}^* \to \Delta^*$ for $\Delta = \{a_1, a_2, a_3\}$ (where again $\{a, b\} = \{a_2, a_3\}$). Let the first vector $\mathbf{u}$ be defined by

$$\mathbf{u} = (\sigma(h(b_1)), \sigma(g(b_1)), 1),$$

where σ is given in (3.1). Define the matrices

$$M_i = \gamma(h(b_i), g(b_i)),$$

for $i = 2, 3, \ldots, 7$, and let $\mathbf{S}$ be the semigroup generated by the six matrices $M_2, \ldots, M_6, M_7A$. Note that

$$(\sigma(u_1), \sigma(v_1), 1)\gamma(u_2, v_2) = (\sigma(u_1u_2), \sigma(v_1v_2), 1),$$

for all $u_1, u_2, v_1, v_2 \in \Delta^*$. It follows that for a word $w = b_{j_1} \cdots b_{j_k} \in \{b_2, \ldots, b_6\}^*$

$$\begin{aligned} &\mathbf{u}M_{j_1} \cdots M_{j_k} M_7 A = \\ &(\sigma(h(b_1 w b_7)) - \sigma(g(b_1 w b_7)), \sigma(g(b_1 w b_7)) - \sigma(h(b_1 w b_7)), 0). \end{aligned} \tag{5.1}$$

We prove that (h, g) has a solution if and only if there exists $M \in \mathbf{S}$ such that $\mathbf{u} \cdot M = (0, 0, 0)$.

The "$\Longrightarrow$" direction is clear by (5.1). Conversely assume that there exists a matrix $M \in \mathbf{S}$ such that $\mathbf{u}M = (0, 0, 0)$. Assume that M has the minimum number factors in the factorization of M into generators of $\mathbf{S}$, say

$$M = M_{j_{11}} \cdots M_{j_{1k_1}} (M_7A) M_{j_{21}} \cdots M_{j_{2k_2}} (M_7A) \cdots (M_7A) M_{j_{m1}} \cdots M_{j_{mk_m}}.$$

Since the matrices M_i are invertible, and

$$A \begin{pmatrix} p & 0 & 0 \\ 0 & s & 0 \\ r & t & 1 \end{pmatrix} A = (p + s)A,$$

and $A^2 = 2A$, it is clear by the minimality of M that it is of the form

$$M = M_{j_{11}} \cdots M_{j_{1k_1}} (M_7A).$$

Now, let $w = b_{j_{11}} \cdots b_{j_{1k_1}} \in \{b_2, \ldots, b_6\}^*$. Then

$$\mathbf{u}M = (\sigma(h(b_1 w b_7)) - \sigma(g(b_1 w b_7)), \sigma(g(b_1 w b_7)) - \sigma(h(b_1 w b_7)), 0) = (0, 0, 0).$$

By the injectivity of σ, $h(b_1 w b_7) = g(b_1 w b_7)$. This proves our claim. □

Often the vector reachability problem is stated in the following form: Given a semigroup S of matrices and two vectors $\mathbf{u}$ and $\mathbf{v}$, determine whether or not there exists $M \in \mathbf{S}$ such that $M \cdot \mathbf{u}^T = \mathbf{v}^T$. The above can be modified for this version by transpositions.

6 Freeness problem

In this section we concentrate on the freeness property of matrix semigroups. This problem is one of the most fundamental properties of semigroups.

Recall that a semigroup $\mathbf{S}$ is said to be free if there exists a subset X of $\mathbf{S}$ such that every element of $\mathbf{S}$ has a unique factorization over X.

We prove that the freeness problem is undecidable for 3×3 matrices. This result was first proved by Klarner, Birget and Satterfield [10] in 1990, but we will present the proof developed by Cassaigne, Harju and Karhumäki [3]. Their proof is shorter and also gives the bound 18 for the number of matrices.

The proof uses the same technique as the previous proofs, but instead of an instance of PCP we will reduce an instance of *mixed PCP* to this problem.

Problem 11 (Mixed PCP). *Given two morphisms $h, g\colon \Sigma^* \to \Delta^*$ determine whether there exists a word $w = a_1 \dots a_k$ with $a_i \in \Sigma$ and $k \geq 1$, such that*

$$h_1(a_1)h_2(a_2)\dots h_k(a_k) = g_1(a_1)g_2(a_2)\dots g_k(a_k), \tag{6.1}$$

where, for each i, h_i and g_i are in $\{h, g\}$ and, for some j, $h_j \neq g_j$.

The word w satisfying the equation (6.1) is called a *solution* of the instance (h, g) of the Mixed PCP.

The freeness problem is know to be undecidable for 18 matrices in the generator set. This follows from the fact that the Mixed PCP is undecidable for instances of 9 letters. We obtain a decreased bound of 14 for number of matrices by proving that the Mixed PCP is undecidable for the Claus instances of the PCP, which gives the undecidability for instances of size 7.

Theorem 13. *The Mixed PCP is undecidable for Claus instances of size 7.*

Proof. Let (h, g) be a Claus instance of the PCP and assume that $h, g\colon \Sigma^* \to \Gamma^*$ for $\Gamma = \{a, b\}$. Recall that $d = aba$, and that $h(x), g(x) \in (ab^2b^*)^*$ for all letters a. By Lemma 1, the minimal solutions of (h, g) are necessarily of the form $b_1 w b_n$ for some $w \in \{b_2, \dots, b_{n-1}\}^*$.

We show that the instance (h, g), as an instance of the PCP, has a solution if and only if it has a solution as an instance of the Mixed PCP.

If (h, g) has a solution $b_1 w b_n$ as an instance of PCP, then this is also a solution of the Mixed PCP, therefore the implication in one direction is trivial. So assume that the pair (h, g) has a solution as an instance of the Mixed PCP and let $w = a_1 a_2 \cdots a_k$ be a solution of minimal length. We claim that also $h(w) = g(w)$, i.e., w is a solution of instance (h, g) of PCP, and $a_1 = b_1$, $a_k = b_n$.

In notation of (6.1), the minimality of w implies that $h_1 \neq g_1$ and $h_k \neq g_k$, and so by the definitions of h and g, $a_1 = b_1$ and $a_k = b_n$. We see also that $a_i \neq b_1$ and $a_i \neq b_n$ if each $i = 2, \dots, k-1$, because otherwise there would be a shorter solution than $b_1 w b_n$. We may assume, by symmetry, that $h_1 = h$ and $g_1 = g$ and we will show that $h_i = h$ and $g_i = g$ for all $i = 1, \dots, k$.

Assume that $h_i = h$ for $i \leq p$ and $g_i = g$ for $i \leq q$. If $h(a_1 a_2 \cdots a_p)$ is a prefix of $g(a_1 a_2 \cdots a_q)$ then $g(a_1 a_2 \cdots a_q) = h(a_1 a_2 \cdots a_p)z$, where, by the form of g and h, the overflow z begins with a word from dA, since the images of h end in the word from A. Therefore also $h_{p+1} = h$. Similarly, we deduce that if $g(a_1 a_2 \cdots a_q)$ is a prefix of $h(a_1 a_2 \cdots a_p)$, then also $g_{q+1} = g$, and this proves the claim. □

We present a proof for the next theorem for the sake of completeness, the proof is from [3].

Theorem 14. *It is undecidable whether a semigroup* **S** *generated by fourteen 3×3 matrices of non-negative integer entries is free.*

Proof. Let (h, g) be an instance of the Mixed PCP. We may assume that h and g are morphism from Σ^* into Σ^*, i.e., they are endomorphisms. Let

$$X = \{\gamma(a, h(a)), \gamma(a, g(a)) \mid a \in \Sigma\}$$

and let $\mathbf{S}$ be the semigroup generated by X.

Let $M_1, \ldots, M_p$, $N_1, \ldots, N_q$ be in X, where $M_t = \gamma(a_{i_t}, h_{i_t}(a_{i_t}))$ and $N_s = \gamma(b_{j_s}, g_{j_s}(b_{j_s}))$ with $h_{i_t}, g_{j_s} \in \{h, g\}$ and $a_{i_t}, b_{j_s} \in \Sigma$, for $t = 1, 2, \ldots, p$ and $s = 1, 2, \ldots, q$. Then, by the definition of γ, we have:

$$M_1 \ldots M_p = N_1 \ldots N_q \text{ in } \mathbf{S}$$

if and only if

$$(M_1 \ldots M_p)_{3,1} = (N_1 \ldots N_q)_{3,1} \quad \text{and} \quad (M_1 \ldots M_p)_{3,2} = (N_1 \ldots N_q)_{3,2}.$$

But this is equivalent to

$$a_{i_1} \ldots a_{i_p} = b_{j_1} \ldots b_{j_q} \quad \text{and} \quad h_{i_1}(a_{i_1}) \ldots h_{i_p}(a_{i_p}) = g_{j_1}(b_{j_1}) \ldots g_{j_q}(b_{j_q})$$

by the injectivity of σ.

Therefore, $\mathbf{S}$ is not free if and only if the instance (h, g) of the Mixed PCP has a solution. Hence the freeness is an undecidable property for finitely generated matrix semigroups of the required kind. □

The next corollary is clear by extending the matrices in the above proof in an obvious way.

Corollary 2. *The freeness problem is undecidable for $n \times n$ upper triangular matrices with non-negative integer entries for any $n \geq 3$.*

7 Membership for the diagonal matrices

In this section we prove that the membership problem for a diagonal matrix is undecidable for finitely generated semigroups of 4×4 integer matrices. This result was original proved by Bell and Potapov in [1]. Their proof gives semigroups generated by 30 matrices. We use their clever coding of the PCP to this problem but by using Claus instances of the PCP, we are able to reduce the number of generators to 14. Also, our proof is shorter than the original proof, since we employ free groups in our proof.

Consider

$$G_n = \{0, 1, \ldots, n-1\}$$

as an alphabet, and let $\mathbb{F}_n$ denote the free group generated by G_n. For the inverse elements, instead of i^{-1} we use the notation $\bar{i}$ for clarity. Let thus $\bar{G}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ be the set of the inverses of the elements of G_n. Recall that two words u and v over $G_n \cup \bar{G}_n$ are equal in the free group $\mathbb{F}_n$ (i.e., $u = v$ in $\mathbb{F}_n$) if and only if they have the same reduced word obtained by removing all factors $i\bar{i}$ and $\bar{i}i$ from them. The empty word ε is the identity element of the group $\mathbb{F}_n$.

Our main tool here is the group morphism $\varphi\colon \mathbb{F}_2 \to G$, where G is a group of 2×2 integer matrices (generated by the images $\varphi(0)$ and $\varphi(1)$). Let

$$\varphi(0) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad \varphi(1) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

for which we have

$$\varphi(\bar{0}) = \varphi(0)^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \quad \text{and} \qquad \varphi(\bar{1}) = \varphi(1)^{-1} = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}.$$

It was shown by Sanov, see e.g. Lyndon and Schupp [11], that the matrix group generated by $\varphi(0)$ and $\varphi(1)$ is free, and hence the mapping φ is a group isomorphism. First we study the free group $\mathbb{F}_2$ and then using the isomorphism φ, we can use the useful properties in the matrix group.

Two words $u, v \in (G_n \cup G_n^{-1})^*$ are *conjugates* if $u = u_1 v_1$ and $v = v_1 u_1$ for some words u_1 and v_1. It is clear that if u and v are conjugates and $u = \varepsilon$ in $\mathbb{F}_n$, then also $v = \varepsilon$ in $\mathbb{F}_n$.

To simplify the proofs, we begin with the free group $\mathbb{F}_8$, and then use a group embedding of $\mathbb{F}_8$ to $\mathbb{F}_2$. Consider the set

$$X = \{1, 2, \ldots, 7, \bar{7}0, \bar{0}\bar{1}\} \cup \{\bar{0}\bar{i}0 \mid i = 2, \ldots, 6\} \subset \mathbb{F}_8.$$

Lemma 3. *All elements $x \in X^+$ which contain exactly one occurrence of the generator $\bar{7}0$ such that $x = \varepsilon$ in $\mathbb{F}_8$ are conjugates (in terms of X) of the elements*

$$1i_1 \cdots i_k 7(\bar{7}0)(\bar{0}\bar{i}_k 0) \cdots (\bar{0}\bar{i}_1 0)\bar{0}\bar{1},$$

for some $k \geq 0$ and $2 \leq i_j \leq 6$.

Proof. First consider any product of elements y of the $Y = \{\bar{0}\bar{i}0 \mid i = 2, \ldots, 6\}$. Then $y = \bar{0}w0$ in $\mathbb{F}_8$, where $w \in \{\bar{2}, \bar{3}, \ldots, \bar{6}\}^+$. Also, each word of $(Y \cup \{\bar{0}\bar{1}\})^+$ contains in the reduced form at least one occurrence of $\bar{0}$. Therefore, in $L = (X \setminus \{\bar{7}0\})^+$ there is no element x such that $x = \varepsilon$ in $\mathbb{F}_8$, since each of these words have at least one $\bar{0}$ in its reduced form.

Assume that $x \in X^+$, $x = \varepsilon$ in $\mathbb{F}_8$, and that x contains exactly one occurrence of $\bar{7}0$. Then $x = y_1 \cdots y_k \bar{7}0 x_1 \cdots x_n$ for some $y_i, x_j \in X \setminus \{\bar{7}0\}$ for $1 \leq i \leq k$ and $1 \leq j \leq n$.

Since all conjugates of x reduce to ε, we may assume that the occurrence of $\bar{0}$ cancelling the specified occurrence of 0 is on the right of it, i.e., $x_i = \bar{0}\bar{t}_i 0$ or $x_i = \bar{0}\bar{1}$ for some $i \geq 1$. If $i > 1$, then $\varepsilon = x_1 \cdots x_{i-1}$ in $\mathbb{F}_8$ is in L; a contradiction. Therefore, $i = 1$. Assume that $x_1 = \bar{0}\bar{t}_1 0$. Then

$$y_1 \cdots y_k \bar{7}0\bar{0}\bar{t}_1 0 x_2 \cdots x_n = y_1 \cdots y_k \bar{7}\bar{t}_1 0 x_2 \cdots x_n = \varepsilon \text{ in } \mathbb{F}_8.$$

Again, as in the above, we may assume that the occurrence of $\bar{0}$ cancelling the specified 0 is on the right of it. Proceeding inductively, we obtain that $x_i = \bar{0}\bar{t}_i 0$ for all $1 \leq i \leq m$ for some maximal index $m < n$. Now there remains one occurrence of 0 which is then cancelled by $x_{m+1} = \bar{0}\bar{1}$. Again, since the conjugates reduce to ε, we may assume that $m + 1 = n$, and we have

$$y_1 \cdots y_k \bar{7}0\bar{0}\bar{t}_1 0 \cdots \bar{0}\bar{t}_m 0\bar{0}\bar{1} = y_1 \cdots y_k \overline{1t_m \cdots t_1 7} = \varepsilon \text{ in } \mathbb{F}_8.$$

Note that this case contains also the case where $x_1 = \bar{0}\bar{1}$ when $m = 0$. In other words $y_1 \cdots y_k = 1t_1 \cdots t_m 7$ in $\mathbb{F}_8$. Recall that $y_j \in X \setminus \{\bar{7}0\}$, and in L all the elements generated by at least one element from $Y \cup \{\bar{0}\bar{1}\}$ contain 0 or $\bar{0}$ in the reduced form. Therefore, $y_j \in \{1, 2, \ldots, 7\}$ for all j and $m = k$, $y_1 = 1$, $y_k = 7$, implying that $y_j = t_j$ for $j = 2, \ldots, k - 1$. □

Note that the claim of Lemma 3 holds also if we assume that in x there is exactly on occurrence of the generator $\bar{0}\bar{1}$. This can be seen from the proof of Lemma 3, there is exactly one occurrence of $\bar{7}0$ if and only if there is exactly one occurrence of $\bar{0}\bar{1}$.

Next we define an embedding $\alpha\colon \mathbb{F}_8 \to \mathbb{F}_2$ by

$$\alpha(i) = \bar{1}^i 01^i, \text{ for } i = 0, 1, \ldots, 7.$$

The set $\{\alpha(i) \mid i = 0, 1, \ldots, 7\}$ generates a subgroup of $\langle 0, 1\rangle$ which is free, since all the subgroups of a free group are free; for details, see e.g. Lyndon and Schupp [11]. Therefore $\mathbb{F}_8$ is isomorphic to the subgroup generated by the elements $\alpha(i)$, for $i = 0, 1, \ldots, 7$, and for $Z = \alpha(X)$ there is a $y \in Z^+$ such that $y = \varepsilon$ in $\mathbb{F}_2$ having exactly one occurrence of $\alpha(\bar{7}0)$ as a generator if and only if $y = \alpha(x)$ where x is of the form of Lemma 3.

Now we are ready to define the matrices for our undecidability proof. Let $h, g\colon \{b_1, b_2, \ldots, b_7\}^* \to \{0, 1\}^*$ be a Claus instance of the PCP. Here $\{0, 1\}$ is alphabet, but we shall consider them also as the generators of the free group $\mathbb{F}_2$.

Recall that the matrices $\varphi(0)$ and $\varphi(1)$ generate a free group of 2×2 integer matrices. For each $i = 1, 2, \ldots, 7$ and $j = 2, 3, \ldots, 6$, define the 4×4 integer matrices in the block form by

$$A_i = \begin{pmatrix} \varphi(h(b_i)) & 0 \\ 0 & \varphi(\alpha(i)) \end{pmatrix}, \quad B_j = \begin{pmatrix} \varphi(\overline{g(b_j)}) & 0 \\ 0 & \varphi(\alpha(\bar{0}\bar{j}0)) \end{pmatrix}.$$

Define the special matrices

$$B_7 = \begin{pmatrix} \varphi(\overline{g(b_7)}) & 0 \\ 0 & \varphi(\alpha(\bar{7}0)) \end{pmatrix}, \quad B_1 = \begin{pmatrix} \varphi(\overline{g(b_1)} & 0 \\ 0 & \varphi(\alpha(\bar{0}\bar{1})) \end{pmatrix}.$$

Theorem 15. *There exist an element $M = M_1 \cdots M_n = I_4$, where $M_j \in \{A_i, B_i \mid 1 \le i \le 7\}$ for $1 \le j \le n$, and, for exactly one j, $M_j = B_7$ if and only if the Claus instance (h, g) has a solution.*

Proof. Consider the lower diagonal block of M first. Clearly, it is of the form $\varphi(\alpha(x_1)) \cdots \alpha(x_n)) = \varphi(\alpha(x_1 \cdots x_n))$, where $x_j \in X$ for each j, and, for exactly one j, $x_j = \bar{7}0$. Now in order for this lower block to be equal to I_2, necessarily, $\alpha(x_1 \cdots x_n) = \varepsilon$ in $\mathbb{F}_2$. By Lemma 3, $x_1 x_2 \cdots x_n$ has a conjugate (in terms of X) of the form

$$1 i_1 \cdots i_k 7(\bar{7}0)(\bar{0}\bar{i}_k 0) \cdots (\bar{0}\bar{i}_1 0)\bar{0}\bar{1},$$

for some $k \ge 0$, $2 \le i_j \le 6$. Also, every conjugate of M is equal to I_4. Therefore, there is a conjugate of M of the form

$$A_1 A_{i_1} \cdots A_{i_k} A_7 B_7 B_{i_k} \cdots B_{i_1} B_1 = I_4. \tag{7.1}$$

Now the top block of this matrix is of the form

$$\varphi(h(b_1)\varphi(h(b_{i_1})) \cdots \varphi(h(b_{i_k}))\varphi(h(b_7))\varphi(\overline{g(b_7)})\varphi(\overline{g(b_{i_k})}) \cdots \varphi(\overline{g(b_{i_1})})\varphi(\overline{g(b_1)}) = I_2$$

implying that in $\langle 0, 1\rangle$

$$h(b_1)h(b_{i_1}) \cdots h(b_{i_k})h(b_7)\overline{g(b_7)}\ \overline{g(b_{i_k})}\ \cdots \overline{g(b_{i_1})}\ \overline{g(b_1)} = \varepsilon,$$

which is equivalent to $h(b_1)h(b_{i_1}) \cdots h(b_{i_k})h(b_7) = g(b_1)g(b_{i_1}) \cdots g(b_{i_k})g(b_7)$, i.e., $b_1 b_{i_1} \cdots b_{i_k} b_7$ is a solution to the Claus instance (h, g). □

Note that there is exactly one j that $M_j = B_7$ if and only if there is exactly one j such that $M_j = B_1$ in Theorem 15.

Now we are ready to prove that main theorem of this section.

Theorem 16. *Let k be an integer with $|k| > 1$. It is undecidable for the matrix kI_4 and a matrix semigroup $\mathbf{R}$ generated by twelve 4×4 integer matrices where $|k| > 1$, whether or not $kI_4 \in \mathbf{R}$.*

Moreover, there is a semigroup $\mathbf{S}$ generated by eleven 4×4 such that it is undecidable whether there for a matrix A, $I_4 = AM$ for some matrix $M \in \mathbf{S}$.

Proof. Let $\mathbf{R} = \langle Y \rangle$, where

$$Y = \{A_i, B_i \mid i = 2, 3, \ldots, 6\} \cup \{kA_7B_7, B_1A_1\}.$$

Now $\det(A_i) = \det(B_1A_1) = 1$ for all $i = 2, 3, \ldots, 6$ and $\det(kA_7B_7) = k^4$. Since for all matrices $\det(AB) = \det(A)\det(B)$, and $\det(kI_4) = k^4$, we have that $kI_4 \in \mathbf{R}$ if and only if the decomposition of kI_4 in terms of Y contains exactly one occurrence of the matrix kA_7B_7. By the proof of Theorem 15 and equation (7.1), $kI_4 \in \mathbf{R}$ if and only if

$$k \cdot A_1A_{i_1} \cdots A_{i_k}(A_7B_7)B_{i_k} \cdots B_{i_1}B_1 = kI_4,$$

and again, since B_1 is invertible, if and only if

$$(B_1A_1)A_{i_1} \cdots A_{i_k}(kA_7B_7)B_{i_k} \cdots B_{i_1} = kI_4,$$

where $b_1b_{i_1} \cdots b_{i_k}b_7$ is a solution of the Claus instance (h, g). The claim follows, since $|Y| = 12$.

For the second claim, notice, once more, that when the Claus instance (h, g) is created from the individual word problem of T from Theorem 3, then the other matrices except for the matrix $A = B_1A_1$ are fixed. Let

$$Y' = \{A_i, B_i \mid i = 2, 3, \ldots, 6\} \cup \{A_7B_7\}$$

and let $\mathbf{S} = \langle Y' \rangle$. Assume that there is $M \in \mathbf{S}$ such that $AM = I_4$. Now the product AM contains exactly one occurrence of the matrix B_1 and therefore, by the remark after the proof of Theorem 15, it contains exactly one occurrence of the matrix B_7. Now the claim follows by Theorem 15, since $|Y'| = 11$. □

The decidability status of following problems remain open.

Problem 12 (Identity matrix). *Given a finitely generated semigroup* $\mathbf{S}$ *of* $n \times n$ *integer matrices, determine whether or not* $I_n \in \mathbf{S}$*?*

Problem 13 (Diagonal matrix). *Given a finitely generated semigroup* $\mathbf{S}$ *of* $n \times n$ *integer matrices, determine whether or not there exists any diagonal matrix in* $\mathbf{S}$*?*

References

[1] P. Bell and I. Potapov, *On the membership of invertible diagonal matrices*, DLT'05, Lecture Notes in Comput. Sci., **3572** (2005), 146–157.

[2] V. D. Blondel and J. N. Tsitsiklis, *When is a pair of matrices mortal?*, Information Processing Lett. **63** (1997), 283–286.

[3] J. Cassaigne, T. Harju, and J. Karhumäki, *On the undecidability of freeness of matrix semigroups*, Internat. J. Algebra Comput. **9** (1999), 295–305.

[4] J. Cassaigne and J. Karhumäki, *Examples of undecidable problems for* 2*-generator matrix semigroups*, Theoret. Comput. Sci. **204** (1998), 29–34.

[5] V. Claus, *Some remarks on PCP(k) and related problems.* Bull. of the EATCS, **12** (1980), 54–61.

[6] S. Gaubert and R. Katz, *Reachability Problems for Products of Matrices in Semirings*, manuscript, http://arxiv.org/abs/math.CO/0310028.

[7] V. Halava and T. Harju, *Mortality in matrix semigroups*, Amer. Math. Monthly **108** (2001), 649–653.

[8] V. Halava and T. Harju, *On Markov's Undecidability Theorem for Integer Matrices*, TUCS Tech. Report **758** (2006), submitted.

[9] T. Harju and J. Karhumäki, Morphisms, In G. Rozenberg and A. Salomaa, editors, *Handbook of Formal Languages*, Vol. 1. pp. 439–510, Springer–Verlag, 1997.

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

[11] R. C. Lyndon and P. E. Schupp, Combinatorial group theory, Springer–Verlag, 1977.

[12] Y. Matiyasevich and G. Sénizergues, *Decision problems for semi-Thue systems with a few rules*, Theoret. Comput. Sci. **330** (2005), 145–169.

[13] M. S. Paterson, *Unsolvability in* 3×3 *matrices*, Stud. Appl. Math. **49** (1970), 105–107.

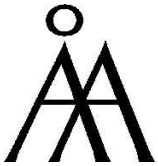
[14] E. Post, *A variant of a recursively unsolvable problem*, Bull. Amer. Math. Soc. **52** (1946), 264–268.

[15] P. Schultz, *Mortality of* 2×2 *matrices*, Amer. Math. Monthly **84** (1977), 463–464.

Turku
Centre *for*
Computer
Science

Lemminkäisenkatu 14 A, 20520 Turku, Finland | www.tucs.fi

University of Turku
- Department of Information Technology
- Department of Mathematics



Åbo Akademi University
- Department of Computer Science
- Institute for Advanced Management Systems Research

Turku School of Economics and Business Administration
- Institute of Information Systems Sciences

ISBN 952-12-1720-0
ISSN 1239-1891