Vesa Halava | Mika Hirvensalo

Improved Matrix Pair Undecidability Results

Turku Centre *for* Computer Science

TUCS Technical Report
No 799, December 2006

Improved Matrix Pair Undecidability Results

Vesa Halava
TUCS–Turku Centre for Computer Science, and
Department of Mathematics, University of Turku
FIN-20014 Turku, Finland
vehalava@utu.fi
Supported by the Academy of Finland under grant 208414
Mika Hirvensalo
TUCS–Turku Centre for Computer Science, and
Department of Mathematics, University of Turku
FIN-20014 Turku, Finland
mikhirve@utu.fi
Supported by the Academy of Finland under grant 208797

TUCS Technical Report
No 799, December 2006

Abstract

We improve undecidability bounds for problems involving two integer matrices. We prove that *Scalar Reachability*, *Zero in the Right Upper Corner*, *Vector Reachability*, and *Zero in the Left Upper Corner* are undecidable for dimensions of 9, 10, 11, and 13, respectively.

Keywords: Undecidability, Integer Matrices, Reachability

TUCS Laboratory
Discrete Mathematics for Information Technology

1 Preliminaries

1.1 Undecidability

Algorithmic unsolvability, *undecidability* appeared already in the very first article establishing the basic notions of theoretical computer science [13]. After Turing's pioneering article, many variants of undecidable problems have been presented. One of the most useful variant is called the *Post Correspondence Problem* (PCP) [12]. The usefulness of PCP is due to the combinatorial formulation of the problem.

There are many powerful results grasping the boundary of decidability. For instance, an interesting theorem in [10] says that a *semi-Thue system* with only three rules can simulate an arbitrary semi-Thue system. This implies that a universal computing device, no matter how complicated, can be simulated by a semi-Thue system with only three rules. An interesting corollary of this result is that the Post Correspondence Problem is undecidable for only seven pairs of words [5], [8].

By using the method of [11] one can encode PCP into integer matrices. Hence it is possible to establish undecidability results on problems on matrices. There are a number of those problems known before (see [1], [2], [3], [4], [7], [8], and [11] for instance). Especially in [4] and [2], problems involving only two matrices are studied, and the purpose of this article is to prove undecidability results for such problems so that the dimension of matrices is as small as possible.

1.2 Matrix Problems

In all the problems studied in this article, the semigroup $\mathbf{S} = \langle M_1, \ldots, M_k \rangle$ is finitely generated and given simply by presenting all matrices M_1, ..., M_k. Moreover, the main results handle the case where $\mathbf{S} = \langle M_1, M_2 \rangle$ is generated by two matrices.

Problem 1 (Scalar Reachability)**.** Given a semigroup $\mathbf{S}$ of $n \times n$ integer matrices, vectors $\boldsymbol{x}$, $\boldsymbol{y} \in \mathbb{Z}^n$ and a constant $a \in \mathbb{Z}$. Decide if there exists a matrix $N \in \mathbf{S}$ such that $\boldsymbol{x}^T N \boldsymbol{y} = a$.

Remark 1. We prove that if $\mathbf{S}$ is generated by two matrices, this problem is undecidable for $n = 9$.

Problem 2 (Zero in the Right Upper Corner)**.** Given a semigroup $\mathbf{S}$ of $n \times n$ integer matrices, decide if $\mathbf{S}$ contains a matrix N with $N_{1n} = 0$.

Remark 2. In the case that $\mathbf{S}$ is generated by two matrices, this problem was proved undecidable for $n = 24$ in [4], which was subsequently in [7] improved to $n = 23$. In [1] this bound was lowered to $n = 18$. Here we prove that this problem is undecidable for $n = 10$.

As Zero in the Right Upper Corner is a special case of Scalar Reachability, any of the previous bounds is valid also for the Scalar Reachability.

Problem 3 (Vector Reachability)**.** Given a semigroup $\mathbf{S}$ of $n \times n$ integer matrices and two vectors $\boldsymbol{x}$, $\boldsymbol{y} \in \mathbb{Z}^n$. Determine whether or not there exists a matrix $N \in \mathbf{S}$ such that $N\boldsymbol{y} = \boldsymbol{x}$.

Remark 3. If $\mathbf{S}$ is generated by two matrices, this problem was proved undecidable for $n = 16$ in [1]. We show the undecidability for $n = 11$.

Problem 4 (Zero in the Left Upper Corner)**.** Given a semigroup $\mathbf{S}$ 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.

Remark 4. Up to our knowledge, no previous bound for the undecidability for this problem has been introduced for a semigroup $\mathbf{S}$ generated by two matrices. Here we prove the undecidability for $n = 13$.

1.3 Graphs and Automata

The matrix combination techniques in this article are based on representing the matrices and automata as weighted graphs. In this section, we represent the basic notions on graphs and automata needed in this paper.

A (directed) *graph* with n vertices is a pair $G = (V, E)$, where $V = \{1, \ldots, n\}$ is the set of *vertices*, and $E \subseteq V \times V$ is the set of *edges*. Also an arbitrary finite set V can be used as the set of vertices, but then we fix an enumeration $f : V \to \{1, \ldots, |V|\}$ and identify the vertex v with its number $f(v) \in \mathbb{N}$. A *path* in a graph G is a sequence $i_0, i_1, \ldots, i_l$ of vertices satisfying $(i_j, i_{j+1}) \in E$ for each j. The *length* of path $i_0, i_1, \ldots, i_l$ is l.

Let R be a semiring. An *R-weighted graph* is a triplet $G = (V, E, \mathrm{wt})$, where V an E are as before, and wt is a mapping $E \to R$. For any R-weighted graph $G = (V, E, \mathrm{wt})$ with n vertices we define a *matrix representation* $M \in R^{n \times n}$ by $M_{ji} = \mathrm{wt}((i, j))$ if $(i, j) \in E$, and $M_{ji} = 0$ if $(i, j) \notin E$ (Recall that $V = \{1, \ldots, n\}$).

Conversely, if $M \in R^{n \times n}$ is a square matrix over a semiring R, its *graph representation* is an R-weighted graph with n vertices defines as follows: Let $V = \{1, \ldots, n\}$, $E = \{(i, j) \mid i, j \in V, M_{ji} \neq 0\}$, and $\mathrm{wt}((i, j)) = M_{ji}$ for each $(i, j) \in E$. It is worth noticing that by fixing the vertex set of a graph in this way, we gain uniqueness: given a matrix $M \in R^{n \times n}$, its graph representation is defined uniquely, and vice versa.

Example 1. In the sequel, we need matrices of form

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

whose each entry is a natural number. The graph representation of $\gamma(u, v)$ is shown in figure 1.

An n-state *R-weighted automaton* (*an R-automaton* for short) over a finite alphabet $\Sigma = \{1, \ldots, k\}$ is a triplet $(\boldsymbol{x}, \{M_a \mid a \in \Sigma\}, \boldsymbol{y})$, where $\boldsymbol{y} \in R^n$ is the *initial vector*, each M_a an $n \times n$ matrix with entries in R, and $\boldsymbol{x} \in R^n$ is the *final vector*. The vectors in R^n are understood as column vectors, and sometimes, though not in this article, the entries of the initial and final vectors are restricted to

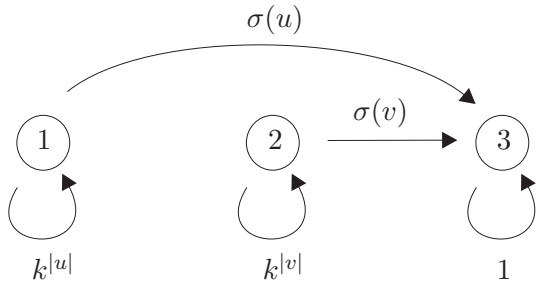

Figure 1: The graph representation of matrix $\gamma(u, v)$.

$\{0, 1\}$. Again, an arbitrary finite set Σ can serve as an alphabet, but in that case we also fix an enumeration $\Sigma \to \{1, \ldots, k\}$ and identify each letter a with its number. The empty word is denoted by ϵ. As usual, we denote $M_{i_1} M_{i_2} \ldots M_{i_n} = M_{i_1 i_2 \ldots i_n}$ for matrices M_{i_j}, where $i_j \in \Sigma$, and a similar notion is used for words: $u_{i_1} \ldots u_{i_n} = u_{i_1 \ldots i_n}$. This is actually just one way to represent a morphism from Σ^* to another semigroup. Equally well we could write $M(i_1 \ldots i_n) = M_{i_1} \ldots M_{i_n}$ or $u(i_1 \ldots i_n) = u_{i_1} \ldots u_{i_n}$, but we do not use such notions in this article.

Let the notations be as above and assume that $G_a = (\{1, \ldots, n\}, E_a, \mathrm{wt}_a)$ is the graph representation of matrix M_a. For convenience, we extend each weight function wt_a by $\mathrm{wt}_a((i, j)) = 0$, if $(i, j) \notin E_a$. The *graph representation* of an n-state R-automaton is a triplet (G, I, F) defined as follows: G is a weighted graph $G = (V, E, \mathrm{wt})$, where $V = \{1, \ldots, n\}$, $E = \cup_{a \in \Sigma} E_a$, and $\mathrm{wt} : E \to R^k$ is the weight function defined by $\mathrm{wt}(e) = (\mathrm{wt}_1(e), \ldots, \mathrm{wt}_k(e))$. I and F are the initial and final state functions defined as $I(j) = \boldsymbol{x}_j$ and $F(j) = \boldsymbol{y}_j$ for each $j \in V$. Hence I and F can be seen as vertex labelling. In figures, it is customary to write $\mathrm{wt}(e)$ as $1 \mid \mathrm{wt}_1(e), \ldots, k \mid \mathrm{wt}_k(e)$ instead of $(\mathrm{wt}_1(e), \ldots, \mathrm{wt}_k(e))$. Also, the vertices are usually called *states* in the graph representation of an automaton.

Example 2. Consider an $\mathbb{N}$-automaton A on alphabet $\Sigma = \{a, b\}$, where a and b are enumerated as 1 and 2, respectively, and $M_a = \gamma(u, v)$ (cf. Equation (1)), and

$$M_b = \begin{pmatrix} 2 & 0 & 0 \\ 3 & 8 & 0 \\ 1 & 2 & 1 \end{pmatrix}.$$

We also define $\boldsymbol{x} = (1, 0, 0)$ and $\boldsymbol{y} = (0, 0, 1)$. Then the graph representation of A is shown in Figure 2. The nonzero values of the initial and final function are customarily indicated by labelled ingoing and outcoming arrows, respectively, as in the figure.

Let A be an R-automaton. Then A defines a function $f_A : \Sigma^* \to R$ by

$$f_A(w) = \boldsymbol{x}^T M_{w^R} \boldsymbol{y},$$

where $M_{w^R} = M_{a_l} \ldots M_{a_2} M_{a_1}$, if $w = a_1 a_2 \ldots a_l \in \Sigma^*$ (w^R stands for the *mirror image of word* w). The following theorem is the core of our matrix composition techniques. The proof is straightforward by induction and can be found in [6].

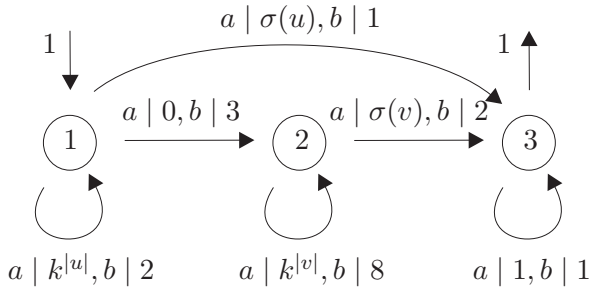

Figure 2: The graph representation of automaton A.

Theorem 1. *Let A be an R-automaton and G_A its graph representation. Then the value $f_A(w)$ for word $w = a_1 \dots a_l$ coincides with the value*

$$\sum_{i \in V} \sum_{P(i,j)} \sum_{j \in V} I(i) \operatorname{wt}(P(i,j), w) F(j), \tag{2}$$

where the middle sum is over all paths in G_A of length l starting at i and ending at j, and $\operatorname{wt}(P(i_0, i_l), w)$ for a path $P = (i_0, i_1, \dots, i_l)$ is defined as

$$\operatorname{wt}(P(i_0, i_l), w) = \operatorname{wt}_{a_1}((i_0, i_1)) \cdot \ldots \cdot \operatorname{wt}_{a_l}((i_{l-1}, i_l)).$$

Example 3. The automaton of Example 2 has $I(i)F(j) \neq 0$ only when $i = 1$ and $j = 3$. Hence, when computing sum (2), we need to find the paths from state 1 to 3. As one can see from Figure 2, there are 6 paths of length 3 leading from 1 to 3: 1333, 1133, 1113, 1223, 1233, and 1123. For word $w = abb$ paths 1233 and 1233 yield zero weight, since they contain an a-transition from state 1 to 2. The remaining paths contribute $\sigma(u) \cdot 1 \cdot 1 + k^{|u|} \cdot 1 \cdot 1 + k^{|u|} \cdot 2 \cdot 1 + k^{|u|} \cdot 3 \cdot 2 = 9k^{|u|} + \sigma(u)$. The same result can be obtained by computing $f_A(abb) = \boldsymbol{x}^T M_b M_b M_a \boldsymbol{y}$.

Another way to express an R-automaton is via the *transition function* $\delta : V \times \Sigma \times V \to R$ defined as

$$\delta(i, a, j) = (M_a)_{ji}. \tag{3}$$

This formulation becomes also convenient later. We will also use the terminology rather flexibly. For instance, as a *path in the automaton* we mean a path in the graph representation of the automaton, and as a transition we mean both transition function and a labelled path of length 1 in an automaton.

1.4 The PCP and Encodings

We prove the undecidability results by showing that for a given instance $\mathcal{I}$ of *Post Correspondence Problem* (PCP) (see [9]), one can construct an automaton that accepts words if and only $\mathcal{I}$ has a solution. Thus our undecidability results are based in the following theorem [10], [8]:

Theorem 2. *For $k \geq 7$, it is undecidable whether an instance $\mathcal{I} = \{(u_1, v_1), \dots, (u_k, v_k)\}$ of PCP has a solution $u_{i_1} u_{i_2} \dots u_{i_n} = v_{i_1} v_{i_2} \dots v_{i_n}$.*

To get improved results, we will also use the following variant of PCP [5], [8]:

Theorem 3. *There are instances $\mathcal{I} = \{(u_1, v_1), \ldots, (u_k, v_k)\}$ of PCP such that all minimal solutions*[1] $u_{i_1}u_{i_2}\ldots u_{i_n} = v_{i_1}v_{i_2}\ldots v_{i_n}$ *are of form $i_1 = 1$, $i_n = k$, and $i_2 \ldots i_{n-1} \in \{2, \ldots, k-1\}^+$. For $k \geq 7$, PCP remains undecidable when restricting to these instances.*

The instances of the above theorem are called *Claus instances*. In fact, all undecidability proofs of PCP known to the authors force the undecidable instances of PCP to be Claus instances, so the question "is a given instance a Claus instance?" is of no importance in this context.

Representing the words over Σ as integers is rather easy. In fact, if $\Sigma = \{1, \ldots, k\}$, we can define $\sigma(i_1 i_2 \ldots i_n) = \sum_{j=1}^{n} i_j k^{n-j}$ and $\sigma(\epsilon) = 0$. It is then easy to see that $\sigma : \Sigma^* \to \mathbb{N} = \{0, 1, 2, \ldots\}$ is a bijection obeying a natural concatenation law $\sigma(uv) = k^{|v|}\sigma(u) + \sigma(v)$. However, $\mathbb{N}$ is commutative, and hence a richer structure is needed to represent algebraic operations on words, or even on pairs of words.

To encode PCP into matrix problems, we use the embedding of [11]. If $|\Sigma| = k$, it is easy to see that $\gamma(u, v)$ of Equation (1) is an injective embedding of $\Sigma^* \times \Sigma^*$ onto $\mathbb{N}^{3\times 3}$, that is, $\gamma(u_1, v_1)\gamma(u_2, v_2) = \gamma(u_1u_2, v_1v_2)$ always, and $\gamma(u_1, v_1) = \gamma(u_2, v_2)$ implies $u_1 = u_2$ and $v_1 = v_2$.

Finally, to encode an alphabet $\Sigma = \{1, \ldots, k\}$ of $k > 2$ symbols into a binary alphabet $\{1, 2\}$, we use an embedding $\psi(i) = 1^{i-1}2$ for $i < k$, and $\psi(k) = 1^{k-1}$. Since $\psi(\Sigma)$ is a prefix code, ψ is clearly injective.

Lemma 1. *Let $w \in \{1, 2\}^*$. Then $w = \psi(w_1)r$, where $w_1 \in \{1, \ldots, k\}^*$ and $r \in \{\epsilon, 1, 11, \ldots, 1^{k-2}\}$.*

Proof. If $w = 1^{l-1}2w'$, where $l < k$, then $w = \psi(l)w'$, and we may apply the same procedure for w'. If $w = 1^{k-1}w'$, then $w = \psi(k)w'$, and again we can proceed recursively on w'. The only case we cannot apply recursion occurs when the remaining word w' consists entirely of 1's and is shorter than $k - 1$. □

2 Scalar Reachability and Zero in the Right Upper Corner

We begin with a sharpening of Eilenberg's result [6].

Theorem 4. *It is undecidable for 3-state $\mathbb{Z}$-automata A over an alphabet Σ of 5 symbols, if $f_A(w) = 0$ for some word $w \in \Sigma^*$.*

Proof. Let $\mathcal{I} = \{(u_1, v_1), \ldots, (u_7, v_7)\}$ be an instance of PCP, and define $A_i = \gamma(u_i, v_i)$ for $i \in \{1, \ldots, 7\}$. Let also $\boldsymbol{x}_1 = (0, 0, 1)^T$ and $\boldsymbol{y}_1 = (1, -1, 0)^T$. Because γ is a morphism, it is easy to see that for $w = i_1 \ldots i_n \in \{1, \ldots, 7\}^*$,

$$\begin{aligned} \boldsymbol{x}_1^T A_w \boldsymbol{y}_1 &= \boldsymbol{x}_1^T \gamma(u_{i_1}, v_{i_1}) \ldots \gamma(u_{i_n}, v_{i_n}) \boldsymbol{y}_1 \\ &= \boldsymbol{x}_1^T \gamma(u_{i_1} \ldots u_{i_n}, v_{i_1} \ldots v_{i_n}) \boldsymbol{y}_1 \\ &= \sigma(u_{i_1} \ldots u_{i_n}) - \sigma(v_{i_1} \ldots v_{i_n}). \end{aligned}$$

[1] A solution to PCP is *minimal* if it is not a concatenation of two solutions.

Since σ is injective, we have $\boldsymbol{x}_1^T A_w \boldsymbol{y}_1 = 0$ if and only $u_{i_1} \dots u_{i_n} = v_{i_1} \dots v_{i_n}$. Hence, $\boldsymbol{x}_1^T A_w \boldsymbol{y}_1 = 0$ for some word $w \in \{1, \dots, 7\}^+$ if and only if $\mathcal{I}$ has a solution. This problem is undecidable by Theorem 2.

To reduce the number of matrices, and to remove the property $\boldsymbol{x}_1^T \boldsymbol{y}_1 = 0$ we notice that by Theorem 3 we can assume that $\mathcal{I}$ is a Claus instance. Hence we can assume that if $u_{i_1} \dots u_{i_n} = v_{i_1} \dots v_{i_n}$, then $w = i_1, \dots, i_n \in 1\{2, \dots, 6\}^+7$. Let then $\boldsymbol{x}_2 = (\boldsymbol{x}_1^T A_1)^T$, $\boldsymbol{y}_2 = A_7 \boldsymbol{y}_1$, and $B_1 = A_2$, …, $B_5 = A_6$. Then $\boldsymbol{x}_2^T \boldsymbol{y}_2 = \boldsymbol{x}_1^T A_1 A_7 \boldsymbol{y} \neq 0$, since otherwise we would have $u_1 u_7 = v_1 v_7$, which contradicts Theorem 3. Now $\boldsymbol{x}_2^T B_w \boldsymbol{y}_2 = 0$ for some $w \in \{1, \dots, 5\}^+$ if and only if $\boldsymbol{x}_1^T A_{w'} \boldsymbol{y}_1 = 0$ for some $w' \in 1\{2, \dots, 6\}^+7$. The $\mathbb{Z}$-automaton required is thus $B = (\boldsymbol{x}_2, \{B_1, \dots, B_5\}, \boldsymbol{y}_2)$. Notice that since we are looking for *any* word w with the aforementioned property, we can ignore the mapping $w \mapsto w^R$ in the definition of function f_A. For later use, we find out that $\boldsymbol{x}_2 = (\sigma(u_1), \sigma(v_1), 1)^T$ and $\boldsymbol{y}_2 = (2^{|u_7|}, -2^{|v_7|}, \sigma(u_7) - (v_7))^T$. □

To combine the 5 matrices of the above theorem into two matrices with the same undecidability property, we use Theorem 1 together with the graph representations of the matrices.

Theorem 5. *It is undecidable for 9-state $\mathbb{Z}$-automata A over a binary alphabet, if $f_A(w) = 0$ for some word $w \in \{1, 2\}^*$.*

Proof. Recall that the graph representations of all matrices B_1, …, B_5 of the above theorem are of a special form shown in Figure 1. We will use encoding $\psi(1) = 2$, $\psi(2) = 12$, $\psi(3) = 112$, $\psi(4) = 1112$, and $\psi(5) = 1111$. Then we augment the graph of Figure 1 with extra vertices, which will decode ψ in the new automaton. It is important to notice that the state 3 of the new automaton does not need any decoder since the transition from 3 is unambiguous: Any transition from 3 will enter again 3 with weight 1.

We define the new transition function δ' so that when reading a sequence of 1's, the automaton will move from a state of form (i, j) into the state $(i, j + 1)$ (case $j = 4$ is an exception), thus counting how many 1's have been read so far. In all these transitions, a weight of 1 is introduced. When the first 2 or the 4th 1 occurs, the automaton moves to the state of form $(r, 1)$ introducing the weight corresponding to $\delta(i, a, r)$ of the original automaton, where $a \in \{1, \dots, 5\}$ is the letter whose encoding $\psi(a)$ equals to the string $1 \dots 12$ or (1^4) that was recently read.

More precisely: Let δ be the transition function of automaton B of Theorem 4 (recall Equation (3)). The state set V' of the new automaton C consists of states (i, j), where $i \in \{1, 2\}$, and $j \in \{1, \dots 4\}$, plus a state $(3, 1)$, altogether 9 states. The new transition function δ' is defined as (for $(i, r) \neq (3, 3)$)

$$\delta'((i,j),1,(r,s)) = \begin{cases} \delta(i,5,r), & \text{if } j = 4, \text{ and } s = 1, \\ 1, & \text{if } i = r \leq 2 \text{ and } j + 1 = s \leq 4, \\ 0 & \text{otherwise.} \end{cases}$$

$$\delta'((i,j),2,(r,s)) = \begin{cases} \delta(i,j,r) & \text{if } s = 1, \\ 0 & \text{otherwise,} \end{cases}$$

$\delta'((3,1),c,(3,1)) = 1$ for $c \in \{1,2\}$, and $\delta'((i,j),c,(r,s)) = 0$ for the cases not defined before. See Figure 3 for a graphical representation of the automaton C. Let C_1 and C_2 be the matrices of automaton C (recall equation 3).

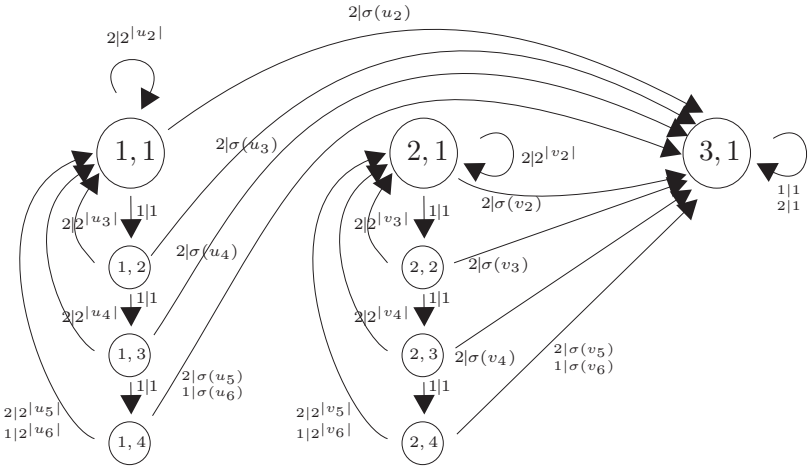

Figure 3: The binary automaton C.

We will then fix an enumeration $g : (1,1) \to 1, \ldots, (1,4) \to 4, (2,1) \to 5, \ldots, (2,4) \to 8, (3,1) \to 9$, and define vector $\boldsymbol{x}_3 \in \mathbb{Z}^9$ such that $(\boldsymbol{x}_3)_{g(i,1)} = (\boldsymbol{x}_2)_i$ for $i \in \{1,2,3\}$, and $(\boldsymbol{x}_3)_{g(i,j)} = 0$ for $j \neq 1$. Vector $\boldsymbol{y}_3$ is defined similarly. Finally, let C_1 and $C_2 \in \mathbb{Z}^{9\times 9}$ be the matrices of C corresponding to the transition function δ'.

We will then show that $\boldsymbol{x}_3^T C_{\psi(w)^R} \boldsymbol{y}_3 = \boldsymbol{x}_2^T B_{w^R} \boldsymbol{y}_2$ for each $w \in \{1,\ldots,5\}^*$. Moreover, we will see that $\boldsymbol{x}_3^T C_w \boldsymbol{y}_3 \neq 0$ for each $w \in \{1,2\}^*$ which is not in the image of ψ.

To prove the first assertion, we use Theorem 1. Since now $I((i,j))F((r,s)) \neq 0$ only if $j = s = 1$, it is enough to show that for any word $w \in \{1,\ldots,5\}^*$ $\mathrm{wt}(P(i,j),w) = \mathrm{wt}(P((i,1),(j,1)),\psi(w))$ for any path $P(i,j)$ in the original automaton. But this is straightforward by the definition of δ': For each transition in automaton B there is a path P' in automaton C beginning at $(i_k,1)$ and ending at $(i_{k+1},1)$ so that all weights along P' are 1, except the last one, which equals to the weight B associates to the original transition. The claim follows, since this holds for each transition in path $P(i,j)$.

To see that the latter claim holds, we assume that w is not in the image of ψ, and use Lemma 1 to write w as $w = \psi(w_1)r$, where $r \in \{1, 11, 111\}$ and $w_1 \in \{1,\ldots,5\}^*$. Recall that $\boldsymbol{y}_2 = A_7\boldsymbol{y}_1 = (2^{|u_7|}, -2^{|v_7|}, \sigma(u_7) - \sigma(v_7))^T$, and as well, $B_{w_1{}^R}\boldsymbol{y}_2 = B_{w_1{}^R}A_7\boldsymbol{y}_1 = A_{w'}\boldsymbol{y}_1 = (2^{|u_{w'}|}, -2^{|v_{w'}|}, \sigma(u_{w'}) - \sigma(v_{w'}))$ is of the same form (here $w' = w_1^R 7 \in \{2,\ldots,6\}^*7$). By the definition,

$$\boldsymbol{y}_3 = (2^{|u_7|}, 0, 0, 0, -2^{|v_7|}, 0, 0, 0, \sigma(u_7) - \sigma(v_7))^T,$$

and according to the previous part of the proof, $C_{\psi(w_1)^R}\boldsymbol{y}_3$ is of form

$$C_{\psi(w_1)^R}\boldsymbol{y}_3 = (2^{|u_{w'}|}, 0, 0, 0, -2^{|v_{w'}|}, 0, 0, 0, \sigma(u_{w'}) - \sigma(v_{w'}))^T. \qquad (4)$$

At the same time, $\boldsymbol{x}_2 = (\sigma(u_1), \sigma(u_2), 1)^T$, and hence

$$\boldsymbol{x}_3 = (\sigma(u_1), 0, 0, 0, \sigma(u_2), 0, 0, 0, 1)^T. \tag{5}$$

By the definition of C_1, it is easy to see that

$$\begin{aligned} & C_{(\psi(w_1)1)^R}\boldsymbol{y}_3 = C_1 C_{\psi(w_1)^R}\boldsymbol{y}_3 \\ = \quad & (0, 2^{|u_{w'}|}, 0, 0, 0, -2^{|v_{w'}|}, 0, 0, \sigma(u_{w'}) - \sigma(v_{w'}))^T, \end{aligned}$$

as well as

$$C_{(\psi(w_1)11)^R}\boldsymbol{y}_3 = (0, 0, 2^{|u_{w'}|}, 0, 0, 0, -2^{|v_{w'}|}, 0, \sigma(u_{w'}) - \sigma(v_{w'}))^T,$$

and

$$C_{(\psi(w_1)111)^R}\boldsymbol{y}_3 = (0, 0, 0, 2^{|u_{w'}|}, 0, 0, 0, -2^{|v_{w'}|}, \sigma(u_{w'}) - \sigma(v_{w'}))^T,$$

Hence for each $r \in \{1, 11, 111\}$ we have (recall Equation 5) $\boldsymbol{x}_3^T C_{(\psi(w_1)r)^R}\boldsymbol{y}_3 = \sigma(u_{w'}) - \sigma(v_{w'})$. Thus $\boldsymbol{x}_3^T C_{(\psi(w_1)r)^R}\boldsymbol{y}_3 = 0$ implies $u_{w'} = v_{w'}$, which is impossible by Theorem 3, since $w' \in \{2, \ldots, 6\}^*$7. □

Corollary 1. *The Scalar Reachability is undecidable for two integer matrices of size* 9×9.

Proof. Choose the matrices, vectors, and scalar as C_1, C_2, $\boldsymbol{x}_3$, $\boldsymbol{y}_3$, and 0. □

Corollary 2. *Zero in the Right Upper Corner is undecidable for two matrices of size* 11×11.

Proof. Let C_1, C_2, $\boldsymbol{x}_3$, and $\boldsymbol{y}_3$ be as before, and define

$$D_i = \begin{pmatrix} 0 & \boldsymbol{x}_3^T C_i & \boldsymbol{x}_3^T C_i \boldsymbol{y}_3 \\ 0 & C_i & C_i \boldsymbol{y}_3 \\ 0 & 0 & 0 \end{pmatrix}.$$

Now D_1 and D_2 are the required matrices. □

We can improve the above corollary slightly by noticing that matrix A_1 in the initial part of the proof of Theorem 4 can be "wrapped around" the other matrices.

Theorem 6. *Zero in the Right Upper Corner is undecidable for two matrices of size* 10×10.

Proof. Let

$$\beta(u, v) = \begin{pmatrix} k^{|v|} & 0 & 0 \\ 0 & k^{|u|} & 0 \\ -k^{|v|}\sigma(u) & -k^{|u|}\sigma(v) & k^{|uv|} \end{pmatrix}$$

and notice that $\gamma(u, v)\beta(u, v) = \beta(u, v)\gamma(u, v) = k^{|uv|}I$, that is, $\beta(u, v) = k^{|uv|}\gamma(u, v)^{-1}$. We choose then $A_i = \gamma(u_1, v_1)\gamma(u_i, v_i)\beta(u_1, v_1)$ for $2 \leq i \leq 6$,

$\boldsymbol{y} = \gamma(u_1, v_1)\gamma(u_7, v_7)(1, -1, 0)^T$, and $\boldsymbol{x} = (0, 0, 1)^T$. Then, for any $w = i_1 \dots i_l \in \{2, \dots, 6\}^*$,

$$\begin{aligned}
\boldsymbol{x}^T A_w \boldsymbol{y} &= \boldsymbol{x}^T A_{i_1} A_{i_2} \dots A_{i_l} \boldsymbol{y} \\
&= \boldsymbol{x}^T \gamma(u_1, v_1)\gamma(u_{i_1}, v_{i_1})\beta(u_1, v_1)\gamma(u_1, v_1)\gamma(u_{i_2}, v_{i_2})\beta(u_1, v_1) \cdot \dots \\
&\quad \cdot\gamma(u_1, v_1)\gamma(u_{i_l}, v_{i_l})\beta(u_1, v_1) \cdot \gamma(u_1, v_1)\gamma(u_7, v_7)(1, -1, 0)^T \\
&= (k^{|u_1 v_1|})^l \boldsymbol{x}^T \gamma(u_1, v_1)\gamma(u_w, v_w)\gamma(u_7, v_7)(1, -1, 0)^T \\
&= k^{|u_1 v_1| l}(0, 0, 1)\gamma(u_{1w7}, v_{1w7})(1, -1, 0)^T \\
&= k^{|u_1 v_1| l}(\sigma(u_{1w7}) - \sigma(v_{1w7})).
\end{aligned}$$

Hence $\boldsymbol{x}^T A_w \boldsymbol{y} = 0$ for some $w \in \{2, \dots, 6\}^+$ if and only if the Claus instance $\mathcal{I} = \{(u_1, v_1), \dots, (u_7, v_7)\}$ has a solution $w \in 1\{2, \dots, 6\}^+7$. Letting $B_1 = A_2$, …, $B_5 = A_6$ it is therefore undecidable for $\mathbb{Z}$-automaton $B = (\boldsymbol{x}, \{B_1, \dots, B_5\}, \boldsymbol{y})$ whether $f_B(w) = 0$ for some word $w \in \{1, \dots, 5\}^+$ (as in Theorem 4, it is easy to verify that $f_B(\epsilon) \neq 0$).

The difference between this construction and that of Theorem 4 is that now vector $\boldsymbol{x}$ is of a very clear form $\boldsymbol{x} = (0, 0, 1)^T$; otherwise we proceed as in the proof or Theorem 4: The matrices of automaton B are of form

$$\begin{aligned}
B_{i-1} &= A_i = \gamma(u_1, v_1)\gamma(u_i, v_i)\beta(u_1, v_1) = \gamma(u_1 u_i, v_1 v_i)\beta(u_1, v_1) \\
&= \begin{pmatrix} k^{|u_1 u_i v_1|} & 0 & 0 \\ 0 & k^{|v_1 v_i u_1|} & 0 \\ k^{|v_1|}(\sigma(u_1 u_i) - \sigma(u_1)) & k^{|u_1|}(\sigma(v_1 v_i) - \sigma(v_1)) & k^{|u_1 v_1|} \end{pmatrix},
\end{aligned}$$

and we see that in each matrix B_i, the transition from state 3 to 3 has a constant weight $k^{|u_1 v_1|}$. Therefore we can construct, as in the proof of Theorem 4, an automaton $C = (\boldsymbol{x}_1, \{C_1, C_2\}, \boldsymbol{y}_1)$ with 9 states so that $\boldsymbol{x}_1^T \boldsymbol{y}_1 \neq 0$, $\boldsymbol{x}_1^T C_{\psi(w)^R} \boldsymbol{y}_1 = \boldsymbol{x}^T B_{w^R} \boldsymbol{y}$ for each $w \in \{1, \dots, 5\}^*$, and $\boldsymbol{x}_1^T C_{w_1^R} \boldsymbol{y}_1 \neq 0$ for each $w_1 \in \{1, 2\}^*$ not in the image of ψ.

Equally importantly, we can choose the enumeration so that $\boldsymbol{x}_1$ has a special form $\boldsymbol{x}_1 = (1, 0, \dots, 0)^T$. This is to say that $\mathcal{I}$ has a solution if and only if the topmost coordinate of $C_w \boldsymbol{y}_1$ is zero for some $w \in \{1, 2\}^*$. Hence, choosing

$$D_i = \begin{pmatrix} C_i & C_i \boldsymbol{y}_1 \\ 0 & 0 \end{pmatrix}$$

we have the required matrices. □

3 Vector Reachability

We need first some auxiliary results. In this section, $\gamma(u, v)$ will be as in Definition 1 with the choice $k = 2$.

Lemma 2. *The set S consisting of all matrices over $\mathbb{Z}$ of form* $\begin{pmatrix} a & b & 0 \\ a & b & 0 \\ c & d & 1 \end{pmatrix}$ *is closed under multiplication.*

Proof. By a direct matrix multiplication. □

Lemma 3. *Let* $M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *and* $\gamma(u,v)$ *as in Definition 1. Then* $M\gamma(u,v)$ *belongs to the set* S *of the previous lemma.*

Proof. By a direct matrix multiplication. □

Theorem 7. *Let* $\mathcal{I} = \{(u_1,v_1),\ldots,(u_7,v_7)\}$ *be a Claus instance of PCP, and the matrices* A_i *and vector* $\boldsymbol{y}$ *defined as* $A_1 = M\gamma(u_1,v_1)$, $A_i = \gamma(u_i,v_i)$ *for* $2 \leq i \leq 6$, *and* $\boldsymbol{y} = \gamma(u_7,v_7)(1,-1,0)^T$. *Then* $A_w\boldsymbol{y} = \mathbf{0}$ *for some* $w \in \{1,\ldots,6\}^*$ *if and only if* $\mathcal{I}$ *has a solution.*

Proof. Notice first that A_w is a product of matrices $\gamma(u_i,v_i)$ and M so that M always occurs in the product in the front of $\gamma(u_1,v_1)$, but nowhere else. Especially, no consecutive M's occur in the product. If w does not contain any 1, then $A_w\boldsymbol{y} = \gamma(u_w,v_w)\boldsymbol{y} = (2^{|u_w|}, -2^{|v_w|}, \sigma(u_w) - \sigma(v_w))^T$. Because of the first and the second coordinate, $A_w\boldsymbol{y} \neq \mathbf{0}$ in this case always.

Assume then that $w = w_1 1 w_2$, where the suffix w_2 belongs to $\{2,\ldots,6\}^*$, i.e., w_2 does not contain any 1's. Now w_1 may contain some number of 1's, so w_1 can be written as $w_1 = x_1 1 x_2 1 \ldots 1 x_n$ ($x_i \in \{2,\ldots,6\}^*$ for each i). Assume first that w_1 actually contains some number of 1's. Since $A_{x_i} = \gamma(u_{x_i}, v_{x_i})$, we know by Lemma 3 that $A_{1x_i} \in S$, and by Lemma 2 we can write $A_{w_1} = \gamma(u_{x_1}, v_{x_1})B$, where $B = \begin{pmatrix} a & b & 0 \\ a & b & 0 \\ c & d & 1 \end{pmatrix}$ is a matrix in set S of Lemma 2. It is important to notice that because of the forms of matrices $\gamma(u_i,v_i)$, we have necessarily $a+b > 0$. If w_1 does not contain any 1's, then B is the identity matrix, and the proof is even easier. We handle here only the former case.

A direct computation shows that

$$\begin{aligned} A_w\boldsymbol{y} &= A_{w_1}A_{1w_2}\boldsymbol{y} = \gamma(u_{x_1},v_{x_1})BA_{1w_27}(1,-1,0)^T \\ &= \begin{pmatrix} 2^{|u_{x_1}|}(a+b)(2^{|u_{1w_27}|} - 2^{|v_{1w_27}|}) \\ 2^{|v_{x_1}|}(a+b)(2^{|u_{1w_27}|} - 2^{|v_{1w_27}|}) \\ ((a+b)(\sigma(u_{x_1}) + \sigma(v_{x_1})) + c + d)(2^{|u_{1w_27}|} - 2^{|v_{1w_27}|}) \\ +\sigma(u_{1w_27}) - \sigma(v_{1w_27}) \end{pmatrix} \end{aligned}$$

(the third coordinate is extended to two rows due to typographical reasons).

Assume now that $A_w\boldsymbol{y} = \mathbf{0}$. Since $a+b > 0$, we have necessarily $2^{|u_{1w_27}|} - 2^{|v_{1w_27}|} = 0$, which implies that $\sigma(u_{1w_27}) - \sigma(v_{1w_27}) = 0$, and since σ is an injection, $u_{1w_27} = v_{1w_27}$ is a solution to $\mathcal{I}$.

On the other hand, if $u_w = v_w$ is a minimal solution to $\mathcal{I}$, then w is of form $w = 1w_27$, where $w_2 \in \{2,\ldots,6\}^+$, since $\mathcal{I}$ was supposed to be a Claus instance. It is easy to verify that

$$\begin{aligned} A_{1w_2}\boldsymbol{y} &= A_{1w_2}\boldsymbol{y} = A_1A_{w_2}\boldsymbol{y} = A\gamma(u_1,v_1)\gamma(u_{w_2},v_{w_2})\gamma(u_7,v_7)(1,-1,0)^T \\ &= A\gamma(u_{1w_27},v_{1w_27})(1,-1,0)^T = \mathbf{0}. \end{aligned}$$

□

Theorem 8. *Vector Reachability is undecidable for two* 11×11 *matrices with integer entries.*

Proof. Consider a $\mathbb{Z}$-automaton $A = (\boldsymbol{x}, \{A_1, \ldots, A_6\}, \boldsymbol{y})$, where the matrices A_i and $\boldsymbol{y}$ are those of Theorem 7, and $\boldsymbol{x}$ is arbitrary. The form of matrix

$$A_1 = M\gamma(u_1, v_1) = \begin{pmatrix} k^{|u_1|} & k^{|v_1|} & 0 \\ k^{|u_1|} & k^{|v_1|} & 0 \\ \sigma(u_1) & \sigma(v_1) & 1 \end{pmatrix}$$

is a bit different from those of A_2, ..., A_6, but the most important thing remains, namely that the transition from state 3 is unambiguous: There is a transition from state 3 only to itself with a weight of 1. Hence we can produce matrices B_1 and B_2 exactly as we produced 9×9 matrices C_1 and C_2 in theorem 5. we also define $\boldsymbol{y}_1 = (2^{|u_7|}, 0, 0, 0, 0, -2^{|v_7|}, 0, 0, 0, 0, \sigma(u_7) - \sigma(v_7))$. Just like in the proof of Theorem 5, we can see that $B_{\psi(w)^R}\boldsymbol{y}_1 = ((B_{w^R}\boldsymbol{y})_1, 0, 0, 0, 0, (B_{w^R}\boldsymbol{y})_2, 0, 0, 0, 0, (B_{w^R}\boldsymbol{y})_3)$ for any $w \in \{1, \ldots, 6\}$. For $1 \leq k \leq 4$ we have, similarly as in the proof of Theorem 5,

$$B_{(\psi(w)1^k)^R}\boldsymbol{y}_1 = (0, \ldots, (B_{w^R}\boldsymbol{y})_1, 0, 0, 0, 0, (B_{w^R}\boldsymbol{y})_2, 0, \ldots, (B_{w^R}\boldsymbol{y})_3),$$

where $(B_{w^R}\boldsymbol{y})_1$ is at kth position. Thus $B_w\boldsymbol{y} = \mathbf{0}$ if and only if $\mathcal{I}$ has a solution. □

4 Zero in the Left Upper Corner

Theorem 9. *Zero in the Left Upper Corner is undecidable for two integer matrices of size* 13×13.

Proof. We assume that words x_1, ..., x_7, y_1, ..., y_7 are over an alphabet $\Sigma = \{1, 2, 3\}$ and choose $k = 3$ in Equation (1). Consider a 3-state $\mathbb{Z}$-automaton $A = (\boldsymbol{x}, \{A_1, \ldots, A_7\}, \boldsymbol{y})$, where $A_i = \gamma(x_i, y_i)$ for $1 \leq i \leq 7$, and $\boldsymbol{y}$ and $\boldsymbol{x}$ are arbitrary. We call the transition function of this automaton δ.

We encode the alphabet by $\psi : \{1, \ldots, 7\} \to \{1, 2\}^+$ as before: $\psi(1) = 2$, $\psi(2) = 12$, ..., $\psi(6) = 1^52$, $\psi(7) = 1^6$, and construct a $\mathbb{Z}$-automaton $B = (\boldsymbol{x}_1, \{B_1, B_2\}, \boldsymbol{y}_1)$ with $6 + 6 + 1 = 13$ states. The transition function δ' of B defined as in the proof of Theorem 4:

$$\delta'((i,j), 1, (r,s)) = \begin{cases} \delta(i, 7, r), & \text{if } j = 6, \text{ and } s = 1, \\ 1, & \text{if } i = r \leq 2 \text{ and } j + 1 = s \leq 6, \\ 0 & \text{otherwise.} \end{cases}$$

$$\delta'((i,j), 2, (r,s)) = \begin{cases} \delta(i, j, r) & \text{if } s = 1, \\ 0 & \text{otherwise,} \end{cases}$$

$\delta'((3,1), c, (3,1)) = 1$ for $c \in \{1, 2\}$, and $\delta'((i,j), c, (r,s)) = 0$ for the cases not defined before.

As in the proof of Theorem 5, it follows that $\boldsymbol{x}_1^T B_{\psi(w)^R} \boldsymbol{y}_1 = \boldsymbol{x}^T A_{w^R} \boldsymbol{y}$, no matter how $\boldsymbol{x}$ and $\boldsymbol{y}$ were chosen ($\boldsymbol{x}_1$ and $\boldsymbol{y}_1$ are defined in accordance to Theorem 5). By using enumeration $(1,1) \mapsto 1, \ldots (1,6) \mapsto 6, \ldots, (2,1) \mapsto 7, \ldots, (2,6) \mapsto 12$ and $(3,1) \mapsto 13$ we get matrices B_1 and B_2 that are explicitly written in the Appendix. We will use this enumeration in the rest of the proof.

As B_2 depends on words $x_1, \ldots, x_6, y_1, \ldots, y_6$, it also defines a 13×13-matrices over $\mathbb{Z}$ of special kind. We denote these matrices by $B_2(x_1, \ldots, x_6; y_1, \ldots, y_6)$ (see the Appendix for the form of these matrices).

The following facts that can be verified by using the construction of automaton B, are used in the sequel.

1. $B_2(x_1, x_2, \ldots, x_6; y_1, y_2, \ldots, y_6)B_1$
   $= B_2(x_2, x_3, \ldots, x_1x_7; y_2, y_3, \ldots, y_1y_7)$

2. $B_2(x_1, \ldots, x_6; y_1, \ldots, y_6)B_1^6 = B_2(x_7x_1, \ldots, x_7x_6; y_7y_1, \ldots, y_7y_6)$

3. $B_2(x_1, \ldots, x_6; y_1, \ldots, y_6)B_2(x'_1, \ldots, x'_6; y'_1, \ldots, y'_6)$
   $= B_2(x_1x'_1, x_1x'_2, \ldots, x_1x'_6; y_1y'_1, y_1y'_2, \ldots, y_1y'_6)$

4. If $1 \leq i \leq 5$, then $B_1^i B_2(x_1, \ldots, x_6; y_1, \ldots, y_6)$ can be obtained from $B_2(x_1, \ldots, x_6; y_1, \ldots, y_6)$ by applying the cyclic permutation $(1, 2, \ldots, 12)$ to rows i times. That is, by removing rows $13-i, 13-i+1, \ldots, 12$, and adding them to the top of the matrix.

All the above identities can be proved correct by direct matrix multiplication, but it may be easier to formulate the matrices by using the transition function. For the first identity, we notice that the product B_2B_1 is the transition matrix for word 12 in automaton B. For $j \in \{1, \ldots, 13\}$,

$$(B_2B_1)_{1j} = \delta'(j, 12, 1) = \sum_k \delta'(j, 1, k)\delta'(k, 2, 1)$$

$$= \begin{cases} \delta'(j+1, 2, 1) = (B_2)_{1,j+1}, & \text{if } j < 6. \\ \delta'(6,1,1)\delta'(1,2,1) + \delta'(6,1,13)\delta'(13,2,1) = (B_1)_{1,6}(B_2)_{1,1}, & \text{if } j = 6. \\ 0, & \text{if } j > 6. \end{cases}$$

For $i \in \{2, \ldots, 6, 8, \ldots, 12\}$ $(B_2B_1)_{ij} = \delta'(j, 12, i) = 0$, because $\delta'(k, 2, i) \neq 0$ for only $i \in \{1, 7, 13\}$ by the definition.

Equality

$$(B_2B_1)_{7,j} = \begin{cases} 0 & \text{if } j \leq 6 \text{ or } j = 13 \\ (B_2)_{7,j+1} & \text{if } 7 \leq j \leq 11 \\ (B_1)_{7,12}(B_2)_{7,7} & \text{if } j = 12 \end{cases}$$

can be found similarly.

Finally, to figure out the last row, we have

$$(B_2B_1)_{13,j} = \sum_k \delta'(j, 1, k)\delta'(k, 2, 13),$$

which implies that for $1 \leq j \leq 5$, $(B_2B_1)_{13,j} = (B_2)_{13,j+1}$. For $j = 6$, we have

$$\begin{aligned}(B_2B_1)_{13,6} &= \sum_k \delta(6,1,k)\delta(k,2,13) \\ &= \delta(6,1,1)\delta(1,2,13) + \delta(6,1,13)\delta(13,2,13) \\ &= 3^{|x_7|}\sigma(x_1) + \sigma(x_7)\cdot 1 = \sigma(x_1x_7),\end{aligned}$$

and the rest of the row 13 in matrix B_2B_1 can be treated similarly.

Facts 2, 3, and 4 can also be proved in a similar manner, or directly by matrix multiplication (cf. matrices in the Appendix).

Identities 1 – 3 imply that for any word $w \in \{1,\ldots,7\}^*$

$$B_{\psi(w)^R} = B_2(x_w,\ldots,;y_w,\ldots), \tag{6}$$

meaning that $(B_{\psi(w)^R})_{11} = 3^{|x_w|}$, $(B_{\psi(w)^R})_{77} = 3^{|y_w|}$, $(B_{\psi(w)^R})_{13,1} = \sigma(x_w)$, and $(B_{\psi(w)^R})_{13,7} = \sigma(y_w)$ for any word $w \in \{1,\ldots,7\}^*$.

Define matrix P as

$$P = \begin{pmatrix} 1&1&1&1&1&1&0&0&0&0&0&0&1 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1 \end{pmatrix}$$

It can be easily verified that P is invertible, and that $P^{-1} \in \mathbb{Z}^{13\times 13}$. Moreover, a straightforward computation shows that for any $\Gamma \in \mathbb{Z}^{13\times 13}$,

$$(P\Gamma P^{-1})_{11} = \sum_{i\in\{1,\ldots,6,13\}} (\Gamma_{i1} - \Gamma_{i7}).$$

In particular, Equation (6) together with fact 4 above implies that

$$(PB_{(\psi(w)1^k)^R}P^{-1})_{11} = \begin{cases} 3^{|x_w|} + \sigma(x_w) - \sigma(y_w) & \text{if } k = 0, \\ 3^{|x_w|} & \text{if } 1 \leq k \leq 5. \end{cases}$$

Let $C_1 = PB_1P^{-1}$ and $C_2 = PB_2P^{-1}$. Then clearly $C_w = PB_wP^{-1}$ for any $w \in \{1,2\}^*$. Let also $\mathcal{I} = \{(u_1,v_1),\ldots,(u_7,v_7)\}$ be a Claus instance of PCP. Without loss of generality, we can assume that the words u_i and v_i are over an alphabet $\{2,3\}$. We choose $x_1 = u_1$, $y_1 = 1v_1$, and $x_i = u_i$ and $y_i = v_i$ for $2 \leq i \leq 7$.

Thus we can conclude that $(C_{w^R})_{11} \neq 0$ for each w not in the image of ψ, and

$$(C_{\psi(w)^R})_{11} = 3^{|u_w|} + \sigma(u_w) - \sigma(v) = \sigma(1u_w) - \sigma(v)$$

for some $v \in \{1,2,3\}^*$. Hence $(C_{\psi(w)^R})_{11} = 0$ if and only if $1u_w = v$. Because u_i and v_i are over an alphabet $\{2,3\}$, this can happen if and only if $w = 1w'$ for some $w' \in \{2,\ldots,7\}$ and $u_{1w'} = v_{1w'}$ is a solution to $\mathcal{I}$ (Since $\mathcal{I}$ is a Claus instance, this also implies that $w' \in \{2,\ldots,6\}^+7$). □

Even though this article is focused on matrix pair results, we mention the following corollary

Corollary 3. *Let* $\mathbf{S}$ *be a semigroup generated by* three 13×13 *integer matrices. It is undecidable whether* $\mathbf{S}$ *contains the zero matrix.*

Remark 5. By the proofs in [8] and [4] (see also [2]), it is undecidable if a semigroup generated by *two* matrices of dimension 21 contains the zero matrix.

Proof. Let C_1 and C_2 be the matrices of the above theorem, and define $A \in \mathbb{Z}^{13\times 13}$ by $A_{ij} = 0$, if $(i,j) \neq (1,1)$, and $A_{11} = 1$. Then A is idempotent, i.e., $A^2 = A$, and AC_wA is a matrix having $(C_w)_{11}$ at the left upper corner, and zeros everywhere else. Let then $\mathbf{S} = \langle C_1, C_2, A\rangle$. Hence, if $\mathbf{S}$ contains the zero matrix, we can assume that $AC_{w_1}AC_{w_2}A\ldots AC_{w_n}A = \mathbf{0}$, which implies that

$$\begin{aligned} 0 &= (AC_{w_1}AC_{w_2}A\ldots AC_{w_n}A)_{11} = (AC_{w_1}A \cdot AC_{w_2}A \cdot \ldots \cdot AC_{w_n}A)_{11} \\ &= (C_{w_1})_{11}(C_{w_2})_{11} \cdot \ldots \cdot (C_{w_n})_{11}. \end{aligned}$$

Hence $\mathbf{0} \in \mathbf{S}$ implies that $(C_{w_i})_{11} = 0$ for some i. On the other direction, if $(C_w)_{11} = 0$, then clearly $AC_wA = \mathbf{0}$. □

5 Appendix

The matrices of automaton C in Theorem 5:

$$C_1 = \begin{pmatrix} 0 & 0 & 0 & 2^{|u_6|} & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2^{|v_6|} & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \sigma(u_6) & 0 & 0 & 0 & \sigma(v_6) & 1 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 2^{|u_2|} & 2^{|u_3|} & 2^{|u_4|} & 2^{|u_5|} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2^{|v_2|} & 2^{|v_3|} & 2^{|v_4|} & 2^{|v_5|} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \sigma(u_2) & \sigma(u_3) & \sigma(u_4) & \sigma(u_5) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) & \sigma(v_5) & 1 \end{pmatrix}$$

The matrices of automaton B in Theorem 9:

$$B_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 3^{|x_7|} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3^{|y_7|} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \sigma(x_7) & 0 & 0 & 0 & 0 & 0 & \sigma(y_7) & 1 \end{pmatrix}$$

and

$$B_2 = \begin{pmatrix} 3^{|x_1|} & 3^{|x_2|} & \cdots & 3^{|x_6|} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 3^{|y_1|} & 3^{|y_2|} & \cdots & 3^{|y_6|} & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_6) & \sigma(y_1) & \sigma(y_2) & \cdots & \sigma(y_6) & 1 \end{pmatrix}$$

References

[1] Paul Bell and Igor Potapov: *Lowering Undecidability Bounds for Decision Questions in Matrices*. Lecture Notes in Computer Science **4036** (Proceedings of DLT'06), 375–385 (2006).

[2] Vincent D. Blondel and John N. Tsitsiklis: *When is a pair of matrices mortal?* Information Processing Letters **63**, no. 5, 283–286 (1997).

[3] Julien Cassaigne, Tero Harju, and Juhani Karhumäki: *On the undecidability of freeness of matrix semigroups*. International Journal of Algebra and Computation **9**, 295–305 (1999).

[4] Julien Cassaigne and Juhani Karhumäki: *Examples of undecidable problems for 2-generator matrix semigroups*. Theoretical Computer Science **204**, 29–34 (1998).

[5] Volker Claus: *Some remarks on $PCP(k)$ and related problems*. Bulletin of EATCS **12**, 54–61 (1980).

[6] Samuel Eilenberg: *Automata, languages, and machines Vol. A*. Academic Press (1974).

[7] Stéphane Gaubert and Ricardo D. Katz: *Reachability problems for products of matrices in semirings*. International Journal of Algebra and Computation **16**, no. 3, 603–627 (2006).

[8] Vesa Halava, Tero Harju, and Mika Hirvensalo: *Undecidability Bounds for Integer Matrices Using Claus Instances*. TUCS Technical Report 766 (2006).

[9] Tero Harju and Juhani Karhumäki: *Morphisms*. In G. Rozenberg and A. Salomaa (eds): *Handbook of Formal Languages*, Springer (1997).

[10] Yuri Matiyasevich and Géraud Sénizergues: *Decision problems for semi-Thue systems with a few rules*. Theoretical Computer Science **330** no. 1, 145–169 (2005).

[11] Michael S. Paterson: *Unsolvability in 3×3 matrices*. Studies in Applied Mathematics **49**, 105–107 (1970).

[12] Emil L. Post: *A variant of a recursively unsolvable problem*. Bulletin of the American Mathematical Society **52**, 264–268 (1946).

[13] Alan Turing: *On Computable Numbers, With an Application to the Entscheidungsproblem*. Proceedings of the London Mathematical Society Series 2 **42**, 230–265 (1936).

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 952-12-1840-1
ISSN 1239-1891