A Note on the Emptiness of Semigroup Intersections

Paul Bell
Department of Computer Science,
The University of Liverpool, Ashton Building,
Ashton Street, Liverpool, L69 3BX, U.K.
pbell@csc.liv.ac.uk

Abstract

We consider decidability questions for the emptiness problem of intersections of matrix semigroups. This problem was studied by A. Markov [7] and more recently by V. Halava and T. Harju [5]. We give slightly strengthened results of their theorems by using a different matrix encoding. In particular, we show that given two finitely generated semigroups of non-singular upper triangular $3 \times 3$ matrices over the natural numbers, checking the emptiness of their intersections is undecidable. We also show that the problem is undecidable even for unimodular matrices over $3 \times 3$ rational matrices.

1 Introduction

Matrices and matrix semigroups are objects that appear in a wide variety of settings in different areas of science. However many natural questions about multiplicative matrix semigroups are not only intractable, but in fact undecidable. For example, given a semigroup generated by a finite set of $3 \times 3$ matrices over the integers, M. Paterson showed it is undecidable if the zero matrix is in the semigroup [9]. It is also undecidable if a semigroup generated by $3 \times 3$ integer matrices is free, see [6], [3]. It was recently proven that it is undecidable whether a particular scalar matrix $kI_4$ is in a finitely generated $4 \times 4$ integral matrix semigroup is undecidable [1].

We shall show an adaption of a theorem of A. Markov [7] concerning the emptiness testing of the intersection of two matrix semigroups, reducing the dimensions and number of matrices used in the construction. This problem was recently studied by V. Halava and T. Harju [5]. A. Markov used semigroups of matrices over $\mathbb{N}^{4 \times 4}$ where the matrices are unimodular. The authors of [5] improve this result to semigroups over $\mathbb{Z}^{3 \times 3}$ and require just 7 matrices in one semigroup and 2 in the other using Claus instances. Their matrices are no longer over $\mathbb{N}$ however and are not unimodular (just non-singular).
We show how to obtain a similar result over $\mathbb{N}^{3\times 3}$ using non-singular but upper triangular matrices. We also obtain a similar result over $\mathbb{Q}^{3\times 3}$ where the matrices are both upper triangular and unimodular.

Post’s correspondence problem (PCP) is a well known undecidable problem. Given a binary alphabet $\Gamma = \{a, b\}$ and a finite set of pairs of words $P = \{(u_j, v_j) | 1 \leq j \leq n\}$ where each $u_j, v_j \in \Gamma^*$. The problem is to determine if there exists a finite sequence $(i_1, i_2, \ldots, i_k)$ with $1 \leq i_j \leq n$ called a solution to PCP such that $u_{i_1}u_{i_2}\cdots u_{i_k} = v_{i_1}v_{i_2}\cdots v_{i_k}$. PCP is known to be undecidable for $n = 7$ [8]. Furthermore, it is undecidable even when the first and last pairs of words, $(u_1, v_1), (u_n, v_n)$ are fixed and $n = 7$ [4]. In other words, $i_1 = 1, i_k = 7$ and $2 \leq i_j \leq 6$ for all $2 \leq j \leq n - 1$. These are known as Claus instances of PCP whereby a semi-Thue system is encoded within a PCP instance, they were recently studied in [5].

We shall use the traditional notations $\mathbb{N}, \mathbb{Z}$ and $\mathbb{Q}$ for the sets of natural numbers (including 0), integers and rational numbers respectively. We shall use the notation $\mathbb{F}^{n\times n}$ to denote an $n$-dimensional matrix over the arbitrary ring $\mathbb{F}$. Let $X = \{M_1, M_2, \ldots, M_n\}$ be a finite set of square matrices. We denote by $\langle X \rangle$ the semigroup generated by $X$. Our primary aim shall be to determine if the intersection of two semigroups generated by a finite set of matrices is empty or not. In other words, is there some matrix in one semigroup that is also in the other semigroup? We shall examine this question in the next section.

2 Matrix Problems

The emptiness problem for matrix semigroup intersection was shown to be undecidable by A. Markov, although we have written the theorem in a different but equivalent form, [7]:

**Theorem 1.** [7] Given two sets $X = \{X_1, X_2, \ldots, X_n\}$ and $Y = \{Y_1, Y_2\}$ of $4 \times 4$ non-negative integer unimodular matrices. It is undecidable if $|\langle X \rangle \cap \langle Y \rangle| = 0$. We may assume all matrices in $X, Y$ except $X_1$ are fixed.

Note that Markov’s result was recently improved by V. Halava and T. Harju. They stated the following theorem (again in a different but equivalent form):

**Theorem 2.** [5] Given two sets $X = \{X_1, X_2, \ldots, X_n\}$ and $Y = \{Y_1, Y_2\}$ of $3 \times 3$ integer non-singular matrices. It is undecidable if $|\langle X \rangle \cap \langle Y \rangle| = 0$.

Note that the authors in [5] used semigroups over $\mathbb{Z}^{3\times 3}$ rather than $\mathbb{N}^{4\times 4}$ as was used by Markov. We use a new encoding to show that it is in fact possible to obtain a similar theorem over $\mathbb{N}^{3\times 3}$ even with upper triangular matrices. We shall also show that we may prove a similar result on unimodular matrices as Markov did, but we require matrices over $\mathbb{Q}^{3\times 3}$ instead.

\(^1\)The statement that all matrices except $X_1$ can be fixed is not difficult to show, see [5].
**Theorem 3.** Given two sets $X = \{X_1, X_2, \ldots, X_n\}$ and $Y = \{Y_1, Y_2\}$ of $3 \times 3$ non-negative upper-triangular integral non-singular matrices. It is undecidable if $|\langle X \rangle \cap \langle Y \rangle| = 0$.

**Proof.** Let $\Gamma = \{a, b\}$ be a binary alphabet. Let $P = \{(u_j, v_j) | 1 \leq j \leq n\} \subseteq \Gamma^* \times \Gamma^*$ be an instance of Post’s correspondence problem (PCP). Define two morphisms $\sigma, \tau : \Gamma^* \rightarrow \mathbb{N}^{2 \times 2}$ where:

$$
\sigma(a) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \sigma(b) = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \tau(a) = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \tau(b) = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}.
$$

It is a well known fact that $\sigma, \tau$ are injective homomorphisms. Note that for all pairs of words $w_1, w_2 \in \Gamma^*$, $\sigma(w_1)[2,2] = \tau(w_2)[1,1] = 1$ thus the pair of $2 \times 2$ matrices, $\sigma(w_1), \tau(w_2)$, can be embedded into $\mathbb{N}^{3 \times 3}$ by using the direct sum $\sigma(w_1) \oplus \tau(w_2)$ and joining the common element 1. Let us therefore define the homomorphism $\lambda : \Gamma^* \times \Gamma^* \rightarrow \mathbb{N}^{3 \times 3}$ by:

$$
\lambda(w_1, w_2) = \sigma(w_1) \oplus \tau(w_2) = \begin{pmatrix} 2|w_1| & x & 0 \\ 0 & 1 & y \\ 0 & 0 & 2|w_2| \end{pmatrix},
$$

where $w_1, w_2 \in \Gamma^*$ and $x, y \in \mathbb{N}$. This is still a monomorphism. Define $X_i = \lambda(u_i, v_i)$ for each $1 \leq i \leq n$, $Y_1 = \lambda(a, a)$ and $Y_2 = \lambda(b, b)$. If there exists a solution to the given PCP instance $(i_1, i_2, \ldots, i_k)$ then

$$
\langle X \rangle \ni X_{i_1} X_{i_2} \cdots X_{i_k} = \lambda(u_{i_1} u_{i_2} \cdots u_{i_k}, v_{i_1} v_{i_2} \cdots v_{i_k}) = \lambda(w, w) \in \langle Y \rangle,
$$

for some $w \in \Gamma^*$. Clearly $\langle Y \rangle$ contains only matrices embedding the same two words which corresponds to a correct solution to the PCP. Thus the intersection is not empty iff there exists a solution to the PCP. Since PCP is undecidable with 7 pairs of words[8], $X$ is generated by 7 matrices and $Y$ is generated by 2 matrices.  

**Corollary 1.** Given two sets $X = \{X_1, X_2, \ldots, X_n\}$ and $Y = \{Y_1, Y_2\}$ of $3 \times 3$ non-negative upper-triangular rational unimodular matrices. It is undecidable if $|\langle X \rangle \cap \langle Y \rangle| = 0$.

**Proof.** Since each matrix in $X, Y$ is invertible we can divide through by the cubic root of the determinant $(\sqrt[3]{\det(\lambda(w_1, w_2))}) = \sqrt[3]{2^{\left|w_1\right| + \left|w_2\right|}}$ to make each unimodular (but mapping instead into $\mathbb{R}^{3 \times 3}$) and obtain the same result since the determinant is multiplicative, however the resulting matrices are real. Using a similar idea as in [5] suggested by M. Soittola, we can replace the 2 on the main diagonal in the definitions of $\sigma, \tau$ and $\lambda$ with 8. This will give 8-adic numbers on the off diagonal elements rather than 2-adic numbers and they retain their freeness. The determinant of $\lambda$ will now be a power of 8, thus the cubic root of the determinant will be a power of 2. Therefore we can map $\Gamma^* \times \Gamma^*$ into $\mathbb{Q}^{3 \times 3}$ where all matrices are unimodular non-negative and upper triangular as required.  

\[3\]
Using the idea of “Claus instances” of PCP as in [5], we can reduce the number of matrices after slight modification of the problem. Given matrices \(A, B\) and two semigroups \(X = \langle\{X_1, X_2, \ldots, X_5\}\rangle, Y = \langle\{Y_1, Y_2\}\rangle\) it is undecidable if there exists \(M \in X\) such that \(AMB \in Y\). See [5] for details.

3 Conclusion

We showed that determining if the intersection of two semigroups generated by non-negative upper triangular non-singular three dimensional integral matrices is undecidable. We also showed an analogous result for \(3 \times 3\) unimodular rational matrix semigroups. Note that an embedding of two words is not possible into \(2 \times 2\) complex matrices [3]. It was recently proven in [2] that the semigroup intersection emptiness problem is undecidable for \(2 \times 2\) rational quaternion matrix semigroups but it is open over \(2 \times 2\) complex matrices.

References


