Scalar Ambiguity and Freeness in Matrix Semigroups over Bounded Languages

Paul C. Bell[1], Shang Chen[1], and Lisa Jackson[2]

[1] Dept. of Computer Science, Loughborough Univ., Loughborough, LE11-3TU, UK
[2] Dept. of Aero. and Auto. Engineering, Loughborough Univ., LE11-3TU, UK
{P.Bell, S.Chen3, L.M.Jackson}@lboro.ac.uk

Abstract. There has been much research into freeness properties of finitely generated matrix semigroups under various constraints, mainly related to the dimensions of the generator matrices and the semiring over which the matrices are defined. A recent paper has also investigated freeness properties of matrices within a bounded language of matrices, which are of the form $M_1M_2\cdots M_k \subseteq \mathbb{F}^{n\times n}$ for some semiring $\mathbb{F}$ [9]. Most freeness problems have been shown to be undecidable starting from dimension three, even for upper-triangular matrices over the natural numbers. There are many open problems still remaining in dimension two.
We introduce a notion of freeness and ambiguity for scalar reachability problems in matrix semigroups and bounded languages of matrices. Scalar reachability concerns the set $\{\rho^T M\tau | M \in \mathcal{S}\}$, where $\rho, \tau \in \mathbb{F}^n$ are vectors and $\mathcal{S}$ is a finitely generated matrix semigroup. Ambiguity and freeness problems are defined in terms of uniqueness of factorizations leading to each scalar. We show various undecidability results.

Keywords: matrix semigroup freeness, scalar ambiguity, bounded languages, undecidability

1 Introduction

We start with some general notations and motivation.

Let $A = \{x_1, x_2, \ldots, x_k\}$ be a finite set of *letters* called an *alphabet*. A word w is a finite sequence of letters from A, the set of all words over A is denoted A^* and the set of nonempty words is denoted A^+. The *empty word* is denoted by ε. For two words $u = u_1u_2\cdots u_i$ and $v = v_1v_2\cdots v_j$, where $u, v \in A^*$, the concatenation of u and v is denoted by $u \cdot v$ (or by uv for brevity) such that $u \cdot v = u_1u_2\cdots u_iv_1v_2\cdots v_j$. Given a word $u = u_1u_2\cdots u_i$, a prefix of u is any word $u = u_1u_2\cdots u_j$, where $j \leq i$. A subset L of A^* is called a *language*. A language $L \subseteq A^*$ is called a *bounded language* if and only if there exist words $w_1, w_2 \ldots, w_m \in A^+$ such that $L \subseteq w_1^*w_2^*\cdots w_m^*$.

We denote by $\mathbb{F}^{n\times n}$ the set of all $n \times n$ matrices over a semiring $\mathbb{F}$. Given $M \in \mathbb{F}^{m\times m}$ and $N \in \mathbb{F}^{n\times n}$, we define the direct sum $M \oplus N$ of M and N by:

$$M \oplus N = \begin{pmatrix} M & \overline{\varnothing} \\ \overline{\varnothing} & N \end{pmatrix},$$

where $\overline{\varnothing}$ is the zero matrix of appropriate dimension. Given a finite set of matrices $\mathcal{G} \subseteq \mathbb{F}^{n\times n}$, $\langle \mathcal{G} \rangle$ is the semigroup generated by $\mathcal{G}$.

For a semigroup $\mathcal{S}$, and a subset $\mathcal{G}' \subseteq \mathcal{S}$, we say that $\mathcal{G}'$ is a *code* if $x_1 \cdots x_{k_1} = y_1 \cdots y_{k_2}$, where $x_i, y_i \in \mathcal{G}'$ implies that $k_1 = k_2$ and $x_i = y_i$ for $1 \leq i \leq k_1$. Alternatively stated, $\mathcal{G}'$ is not a code if and only if some element of $\mathcal{S}$ has more than one factorization over $\mathcal{G}'$. We call $\mathcal{G}'$ a *prefix code* if no $w_1 \in \mathcal{G}'$ is a prefix of another word $w_2 \in \mathcal{G}'$.

Given a set $\mathcal{G} \subseteq \mathbb{F}^{n\times n}$, the *freeness problem* is to determine if $\mathcal{G}$ is a code for $\mathcal{S} = \langle \mathcal{G} \rangle$. It was proven by Klarner et al. that the freeness problem is undecidable over $\mathbb{N}^{3\times 3}$ in [12] and this result was improved by Cassaigne et al. to hold even for upper-triangular matrices over $\mathbb{N}^{3\times 3}$ in [6].

There are many open problems related to freeness in 2×2 matrices, see [8–10] for good surveys. The freeness problem over $\mathbb{H}^{2\times 2}$ is undecidable [4], where $\mathbb{H}$ is the skew-field of quaternions (in fact the result even holds when all entries of the quaternions are rationals). The freeness problem for two upper-triangular 2×2 rational matrices remains open, despite many partial results being known [9].

The freeness problem for matrix semigroups defined by a bounded language was recently studied. Given a finite set of matrices $\{M_1, \ldots, M_k\} \subseteq \mathbb{Q}^{n\times n}$, we define a bounded language of matrices to be of the form:

$$\{M_1^{j_1} \cdots M_k^{j_k} | j_i \geq 0 \text{ where } 1 \leq i \leq k\}.$$

The freeness problem for a bounded language of matrices asks if there exists $j_1, \ldots, j_k, j_1', \ldots, j_k' \geq 0$, where at least one $j_i \neq j_i'$ such that $M_1^{j_1} \cdots M_k^{j_k} = M_1^{j_1'} \cdots M_k^{j_k'}$ in which case the bounded language of matrices is not free. This problem was shown to be decidable when $n = 2$, but undecidable in general [9].

In this paper we will introduce two notions of freeness in matrix semigroups called Scalar Ambiguity and Scalar Freeness problems. These are related to the uniqueness of factorizations of a set of scalar values of the form $\{\rho^T M \tau | M \in \mathcal{S}\}$, where $\mathcal{S}$ is a finitely generated matrix semigroup (see Section 2 for details). Such a set of scalars can be used to represent computations in many models. Related problems for *vector ambiguity* were studied in [3], where we were interested in the uniqueness of factorizations of a set of *vectors* $\{M\tau | M \in \mathcal{S}\}$.

In Section 3, we also study a related ambiguity problem for *Probabilistic Finite Automata* (PFA), defined in Section 1.1. The reachability problem for PFA (or emptiness problem) is known to be *undecidable* [14], even in a fixed dimension [5, 11]. The reachability problem for PFA defined on a bounded language (i.e. where input words are from a bounded language which is given as part of the input), was recently shown to be undecidable [2].

Associated with each input word is the probability of that word being accepted by the PFA. In this paper, we show that determining whether every probability is unique is undecidable over a bounded language. In other words, to determine if there exists two input words which have the same probability of being accepted is undecidable. This is a similar concept to the *threshold isolation problem* shown in [5] to be undecidable, where we ask if each probability can be approximated arbitrarily closely.

1.1 Probabilistic Finite Automata

A vector $y \in \mathbb{Q}^n$ is a *probability distribution* if its elements are nonnegative and sum to 1 (y has an L_1 norm of 1). Matrix M is called a *column stochastic matrix* if each column is a probability distribution, a *row stochastic matrix* if each row is a probability distribution and it is called a *doubly stochastic matrix* if it is both row and column stochastic. For any row stochastic matrix M, if y is a probability distribution, then so is $y^T M$, since M preserves the L_1 norm on vectors and is nonnegative. The product of two row/column/doubly stochastic matrices is also row/column/doubly stochastic (respectively) as is not difficult to verify.

A *Probabilistic Finite Automaton* (PFA, see [5, 14] for further details) over an alphabet A is a triplet (u, φ, v), where $u \in \mathbb{Q}^n$ is the *initial probability distribution*, $\varphi : A^* \to \mathbb{Q}^{n \times n}$ is a monoid homomorphism whose range is the set of n-dimensional row stochastic matrices and $v \in \mathbb{Q}^n$ is the *final state vector* whose ith coordinate is 1, if state i is final, and 0 otherwise. [1]

For a given PFA denoted $R = (u, \varphi, v)$ and a word $w \in A^*$, we can define a function $f_R : A^* \to [0, 1]$, where:

$$f_R(w) = u^T \varphi(w) v \in [0, 1]\,; \quad w \in A^*.$$

This is the probability of R being in a final state after reading word $w \in A^*$.

We will require the following undecidable problem for proving later results, which is a variant of the famous *Post's Correspondence Problem* (PCP).

Problem 1 (Mixed Modification PCP (MMPCP)) *Given a finite set of letters Σ, a binary alphabet Δ, and a pair of homomorphisms $h, g : \Sigma^* \to \Delta^*$, the MMPCP asks to decide whether there exists a word $w = x_1 \dots x_k \in \Sigma^+, x_i \in \Sigma$ such that*

$$h_1(x_1)h_2(x_2)\dots h_k(x_k) = g_1(x_1)g_2(x_2)\dots g_k(x_k),$$

where $h_i, g_i \in \{h, g\}$, and there exists at least one j such that $h_j \neq g_j$.

Theorem 1 *[7] - The Mixed Modification PCP is undecidable.*

2 Scalar Ambiguity and Freeness for Matrices

Consider a finite set $\mathcal{G} = \{G_1, G_2, \dots, G_k\} \subset \mathbb{F}^{n \times n}$, generating a semigroup of matrices $\mathcal{S} = \langle \mathcal{G} \rangle$ and two column vectors $\rho, \tau \in \mathbb{F}^n$. Let $\Lambda(\mathcal{G})$ be the set of scalars such that $\Lambda(\mathcal{G}) = \{\lambda : \lambda = \rho^T M \tau | M \in \mathcal{S}\}$. If for $\lambda \in \Lambda(\mathcal{G})$ there exists a unique matrix $M \in \mathcal{S}$ such that $\lambda = \rho^T M \tau$, then we say that λ is *unambiguous* with respect to $\mathcal{G}, \rho, \tau$. $\Lambda(\mathcal{G})$ is called unambiguous if every $\lambda \in \Lambda(\mathcal{G})$ is unambiguous. If for $\lambda \in \Lambda(\mathcal{G})$ there exists a unique product $G_{i_1} G_{i_2} \cdots G_{i_m} \in \mathcal{S}$, with each $G_{i_l} \in \mathcal{G}$ such that $\lambda = \rho^T G_{i_1} G_{i_2} \cdots G_{i_m} \tau$, then we say that λ is *free* with respect to $\mathcal{G}, \rho, \tau$. $\Lambda(\mathcal{G})$ is called free if every $\lambda \in \Lambda(\mathcal{G})$ is free.

[1] The definition of a PFA in the literature often interchanges the roles of u and v from our definition and requires column stochastic matrices, but the two can easily be seen to be equivalent by transposing all matrices and interchanging u and v.

Problem 2 (Scalar Ambiguity) *Is $\Lambda(\mathcal{G})$ unambiguous with respect to $\mathcal{G}, \rho, \tau$?*

Problem 3 (Scalar Freeness) *Is $\Lambda(\mathcal{G})$ free with respect to $\mathcal{G}, \rho, \tau$?*

Problem 2 and Problem 3 look similar at first glance. However, the scalar ambiguity problem concentrates more on the properties of the semigroup $\mathcal{S}$ while the scalar freeness problem cares more about the properties of the set $\mathcal{G}$. A fact one can see from the definitions is that if the identity matrix I is contained in set $\mathcal{G}$, then the corresponding scalar set $\Lambda(\mathcal{G})$ is not free, but the same property does not hold for the scalar ambiguity problem. Also, we define the scalar freeness problem in a similar way of the matrix semigroup freeness problem. The links between the scalar ambiguity problem, scalar freeness problem and matrix semigroup freeness problem are illustrated in the following theorem.

Proposition 1 *Given a semigroup of matrices $\mathcal{S}$ generated by a finite set $\mathcal{G}$, and two column vectors ρ and τ, let $\Lambda(\mathcal{G})$ be a set of scalars generated by $\mathcal{G}, \rho$ and τ. Then the following relations hold:*

(1) If $\Lambda(\mathcal{G})$ is ambiguous, then $\Lambda(\mathcal{G})$ is not free.
(2) if $\Lambda(\mathcal{G})$ is free, then $\mathcal{S}$ is free.

Proof. (1) Suppose $\Lambda(\mathcal{G})$ is ambiguous, then by definition there exist two matrices $M_1, M_2 \in \mathcal{S}, M_1 \neq M_2$ such that $\rho^T M_1 \tau = \rho^T M_2 \tau$. Thus, there exists factorizations $M_1 = G_{i_1} G_{i_2} \dots G_{i_{m_1}} \neq G_{j_1} G_{j_2} \dots G_{j_{m_2}} = M_2$, where each $G_i, G_j \in \mathcal{G}$ so $\Lambda(\mathcal{G})$ is not free.

(2) We proceed by contradiction. Suppose $\Lambda(\mathcal{G})$ is free but $\mathcal{S}$ is not. If $\mathcal{S}$ is not free, there exists $G_{i_1} G_{i_2} \dots G_{i_{m_1}} = G_{j_1} G_{j_2} \dots G_{j_{m_2}} \in \mathcal{S}$, where $G_i, G_j \in \mathcal{G}$, and for at least one k, $G_{i_k} \neq G_{j_k}$, or $m_1 \neq m_2$. Thus, clearly it also holds that $\rho^T G_{i_1} G_{i_2} \dots G_{i_{m_1}} \tau = \rho^T G_{j_1} G_{j_2} \dots G_{j_{m_2}} \tau$, which contradicts the definition of scalar freeness. □

It can be seen that by answering the scalar freeness problem, one can 'partly' answer the scalar ambiguity problem and the matrix semigroup freeness problem. However, neither problem is a sub-problem of the other, and it seems there is no direct connection between the scalar ambiguity problem and the matrix semigroup freeness problem. We are now ready to prove the main result of this section.

Theorem 2 *The Scalar Freeness Problem is undecidable over $\mathbb{Z}^{3\times 3}$ and the Scalar Ambiguity Problem is undecidable over $\mathbb{Z}^{4\times 4}$.*

Proof. We prove the result by encoding an instance of the MMPCP problem. The basic idea is inspired by [7]. We start by showing the undecidability of the scalar freeness problem. We construct a finite set of matrices $\mathcal{G}$, generating a matrix semigroup $\mathcal{S}$ and two fixed vectors ρ and τ such that the encoded MMPCP instance has a solution if and only if the scalar set $\Lambda(\mathcal{G})$ is free. In other words, there exists a scalar $\lambda \in \Lambda(\mathcal{G})$ such that $\lambda = \rho^T G_{i_1} G_{i_2} \dots G_{i_{m_1}} \tau = \rho^T G_{j_1} G_{j_2} \dots G_{j_{m_2}} \tau$, where $G_i, G_j \in \mathcal{G}$ and some $G_{i_k} \neq G_{j_k}$ or $m_1 \neq m_2$.

Let $\Sigma = \{x_1, x_2, \ldots, x_{n-2}\}$ and $\Delta = \{x_{n-1}, x_n\}$ be distinct alphabets and $h, g : \Sigma^* \to \Delta^*$ be an instance of the mixed modification PCP. The naming convention will become apparent below. We define two homomorphisms $\alpha, \beta : (\Sigma \cup \Delta)^* \to \mathbb{Q}$ by:

$$\alpha(x_{i_1}x_{i_2}\cdots x_{i_m}) = \Sigma_{j=1}^{m} i_j(n+1)^{m-j},$$
$$\beta(x_{i_1}x_{i_2}\cdots x_{i_m}) = \Sigma_{j=1}^{m} i_j(n+1)^{j-m-1},$$

and $\alpha(\varepsilon) = \beta(\varepsilon) = 0$. Thus α represents $x_{i_1}x_{i_2}\cdots x_{i_m}$ as an $(n+1)$-adic number and β represents $x_{i_1}x_{i_2}\cdots x_{i_m}$ as a fractional number $(0.x_{i_m}\cdots x_{i_2}x_{i_1})_{(n+1)}$ (e.g. the number 123 may be represented as 0.321, base 10). Note that $\forall w \in (\Sigma \cup \Delta)^*, \alpha(w) \in \mathbb{N}$ and $\beta(w) \in (0,1) \cap \mathbb{Q}$. It is not difficult to see that $\forall w_1, w_2 \in (\Sigma \cup \Delta)^*, (n+1)^{|w_2|}\alpha(w_1) + \alpha(w_2) = \alpha(w_1w_2)$ and $(n+1)^{-|w_2|}\beta(w_1) + \beta(w_2) = \beta(w_1w_2)$.

Define $\gamma' : (\Sigma \cup \Delta)^* \times (\Sigma \cup \Delta)^* \to \mathbb{Q}^{3\times 3}$ by

$$\gamma'(u,v) = \begin{pmatrix} (n+1)^{|u|} & 0 & \alpha(u) \\ 0 & (n+1)^{-|v|} & \beta(v) \\ 0 & 0 & 1 \end{pmatrix}.$$

It is easy to verify that $\gamma'(u_1,v_1)\gamma'(u_2,v_2) = \gamma'(u_1u_2, v_1v_2)$, i.e., γ' is a homomorphism. Define two more matrices T and T^{-1} :

$$T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad T^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We now define $\gamma : (\Sigma \cup \Delta)^* \times (\Sigma \cup \Delta)^* \to \mathbb{Q}^{3\times 3}$:

$$\gamma(u,v) = T\gamma'(u,v)T^{-1} = \begin{pmatrix} (n+1)^{|u|} & (n+1)^{-|v|} - (n+1)^{|u|} & \alpha(u) + \beta(v) \\ 0 & (n+1)^{-|v|} & \beta(v) \\ 0 & 0 & 1 \end{pmatrix}.$$

We can now verify that, $\gamma(u_1,v_1)\gamma(u_2,v_2) = T\gamma'(u_1,v_1)TT^{-1}\gamma'(u_2,v_2)T^{-1} = T\gamma'(u_1u_2, v_1v_2)T^{-1} = \gamma(u_1u_2, v_1v_2)$, hence γ is a homomorphism.

Let $\mathcal{G} = \{\gamma(x_i, g(x_i)), \gamma(x_i, h(x_i)) | x_i \in \Sigma, 1 \le i \le n-2\}$, $\mathcal{S} = \langle \mathcal{G} \rangle$, $\rho = (1,0,0)^T$ and $\tau = (0,0,1)^T$. Assume that there exists $M_1 = G_{i_1}G_{i_2}\cdots G_{i_t} \in \langle \mathcal{G} \rangle$ and $M_2 = G_{j_1}G_{j_2}\cdots G_{j_{t'}} \in \langle \mathcal{G} \rangle$ such that $t \neq t'$ or else at least one $G_{i_p} \neq G_{j_p}$ where $1 \le p \le t$ and $\lambda = \rho^T M_1 \tau = \rho^T M_2 \tau$. We see that:

$$\lambda = \rho^T M_1 \tau = (M_1)_{[1,3]} = \alpha(x_{i_1}x_{i_2}\cdots x_{i_t}) + \beta(f_1(x_{i_1})f_2(x_{i_2})\cdots f_t(x_{i_t})),$$
$$\lambda = \rho^T M_2 \tau = (M_2)_{[1,3]} = \alpha(x_{j_1}x_{j_2}\cdots x_{j_{t'}}) + \beta(f'_1(x_{j_1})f'_2(x_{j_2})\cdots f'_{t'}(x_{j_{t'}})),$$

where each $f_i, f'_i \in \{g, h\}$. Since $\alpha(w) \in \mathbb{N}$ and $\beta(w) \in (0,1) \cap \mathbb{Q}$, $\forall w \in (\Sigma \cup \Delta)^*$, injectivity of α and β implies that if $\rho^T M_1 \tau = \rho^T M_2 \tau$, then $t = t'$ and $i_k = j_k$ for $1 \le k \le t$. Furthermore, if $\rho^T M_1 \tau = \rho^T M_2 \tau$, we have that $\beta(f_1(x_{i_1})f_2(x_{i_2})\cdots f_t(x_{i_t})) = \beta(f'_1(x_{i_1})f'_2(x_{i_2})\cdots f'_t(x_{i_t}))$ and since at least one

$f_p \neq f'_p$ for $1 \leq p \leq t$ by our above assumption, then this corresponds to a correct solution to the mixed modification PCP instance (h, g). On the other hand, if there does not exist a solution to (h, g), then $\beta(f_1(x_{i_1})f_2(x_{i_2}) \cdots f_t(x_{i_t})) \neq \beta(f'_1(x_{i_1})f'_2(x_{i_2}) \cdots f'_t(x_{i_t}))$, and injectivity of β implies that $\rho^T M_1 \tau \neq \rho^T M_2 \tau$.

Since set $\mathcal{G} \subseteq \mathbb{Q}^{3\times 3}$ is finite and has a finite description, there exists a computable constant $c \in \mathbb{N}$ such that $c \cdot \mathcal{G} \subseteq \mathbb{Z}^{3\times 3}$ (based on the least common multiple of the denominators of elements of the matrices of $\mathcal{G}$). This completes the proof of the scalar freeness problem.

For the scalar ambiguity problem, we sketch the proof technique. The above encoding has the property that if some $\lambda = \rho^T M_1 \tau = (M_1)_{[1,3]} = \rho^T M_2 \tau = (M_2)_{[1,3]}$, then it implies that $M_1 = M_2$. If there exists a solution to the PCP instance, then some matrix $M \in \mathcal{S}$ has two distinct factorizations as above, each using a different sequence of morphisms f, g. We increase the dimension of γ by 1 to store an additional word, using mapping α, which is unique for each matrix. For example $x_1^i x_2$ for matrices corresponding to $h(x_i)$ and $x_3^i x_4$ for matrices corresponding to $g(x_i)$. Any two different matrix products will now have a distinct word stored in this element since $\{x_1^i x_2, x_3^i x_4 | 1 \leq i \leq n-2\}$ is clearly a code. We modify ρ and τ to have an additional dimension which does not select this new word (i.e. they have zeros in the corresponding elements), and therefore its inclusion does not affect the set Λ. □

3 Ambiguity and Freeness over a Bounded Language

We now study the concept of scalar ambiguity and scalar freeness for a *bounded language* of matrices, showing that these problems are undecidable. We start with the definition of Hilbert's tenth problem, which was shown to be undecidable by Matiyasevich. The following problem was stated as part of 23 open problems for the 20th century by David Hilbert in his 1900 address:

Hilbert's Tenth Problem (HTP) - "Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers".

To use a more modern terminology, Hilbert's tenth problem is to determine if there exists $n_1, n_2, \ldots n_k \in \mathbb{N}$ such that $P(n_1, n_2, \ldots, n_k) = 0$ is a Diophantine equation (i.e. P is a polynomial with integer coefficients). The undecidability of Hilbert's tenth problem was shown in 1970 by Yu. Matiyasevich building upon earlier work of many mathematicians, including M. Davis, H. Putman and J. Robinson. For more details of the history of the problem as well as the full proof of its undecidability, see the excellent reference [13]. We may restrict all the variables of the problem to be natural numbers without loss of generality, see [13, p.6].

The following corollary can be found in [2], or from the proof construction shown in [1].

Corollary 1 *[2] - Given an integer polynomial $P(n_1, n_2, \ldots, n_k)$, one can construct two vectors $\rho = (1, 0, \ldots, 0)^T \in \mathbb{N}^n$ and $\tau = (0, \ldots, 0, 1)^T \in \mathbb{N}^n$, an*

alphabet $\Sigma = \{x_1, x_2, \ldots, x_k\}$ *and a homomorphism* $\mu : \Sigma^* \to \mathbb{Z}^{n\times n}$, *such that for any word of the form* $w = x_1^{y_1} x_2^{y_2} \ldots x_k^{y_k} \in \Sigma^+$:

$$\rho^T \mu(w)\tau = P(y_1, y_2, \ldots, y_k)^2,$$

and $\rho^T \mu(\varepsilon)\tau = 0$ *for the empty word* ε. *The triple* (ρ, μ, τ) *is a linear representation of a* $\mathbb{Z}$*-regular formal power series* $Z \in \mathbb{N}\langle\langle\Sigma\rangle\rangle$.

We will require the following lemma.

Lemma 1 *Given two integer polynomials* P_1 *and* P_2 *over variables* $(x_1, \ldots, x_k)$ *and with integer coefficients. It is undecidable to decide whether there exist integers* $(y_1, \ldots, y_k)$ *such that* $P_1^2(y_1, \ldots, y_k) = P_2^2(y_1, \ldots, y_k)$.

Proof. Let $P(x_2, \ldots, x_k)$ be an instance of Hilbert's tenth problem, i.e. a polynomial with integer coefficients and variables. Define $P_1(x_1, x_2, \ldots, x_k) = (x_1^2+1)P$ and $P_2(x_1, x_2, \ldots, x_k) = (x_1^2 + 2)P$. Since $0 < x_1^2 + 1 < x_1^2 + 2$, we see that $P_1^2(x_1, x_2, \ldots, x_k) = P_2^2(x_1, x_2, \ldots, x_k) \Leftrightarrow P_1 = P_2 = 0$, which implies that $P(x_2, \ldots, x_k) = 0$, which is undecidable to determine. This result holds for any value of x_1 since $x_1^2 + 1 \neq x_1^2 + 2$. We will use this property in the later proof. □

Now we show the main result of this section.

Theorem 3 *The Scalar Freeness Problem over a bounded language is undecidable. In other words, given* k *matrices* $M_1, M_2, \ldots, M_k \in \mathbb{Q}^{n\times n}$, *generating bounded language* $M = M_1^* M_2^* \cdots M_k^*$, *and two vectors* $\rho, \tau \in \mathbb{Z}^n$, *it is undecidable to decide if there exist* $l_1, l_2, \ldots, l_k, r_1, r_2, \ldots, r_k \in \mathbb{N}$ *such that*

$$\rho^T M_1^{l_1} M_2^{l_2} \ldots M_k^{l_k} \tau = \rho^T M_1^{r_1} M_2^{r_2} \ldots M_k^{r_k} \tau,$$

where $l_j \neq r_j$ *for at least one* j.

Proof. We prove this theorem by 4 steps. We will define a set of matrices $\{M_i, N_i | 0 \leq i \leq k+1\}$ for some $k+1 > 0$, which will define the bounded language of matrices $M = M_0^* M_1^* M_2^* \cdots M_k^* M_{k+1}^* N_0^* N_1^* N_2^* \cdots N_k^* N_{k+1}^*$. The matrices $\{M_i\}$ encode a polynomial P_1 and matrices $\{N_i\}$ will encode a separate polynomial P_2. The proof will show that if we have $\rho^T A_1 \tau = \rho^T A_2 \tau$, where $A_1, A_2 \in M$ and A_1, A_2 have different factorizations, then $A_1 = M_0^{j_0} M_1^{j_1} M_2^{j_2} \cdots M_k^{j_k} M_{k+1}^{j_{k+1}}$ and $A_2 = N_0^{j_0'} N_1^{j_1} N_2^{j_2} \cdots N_k^{j_k} N_{k+1}^{j_{k+1}'}$ (or vice versa). We will show that this implies that $P_1^2(j_1, \cdots, j_k) = P_2^2(j_1, \cdots, j_k)$, the determination of which was shown to be undecidable in Lemma 1.

Step 1. Given two integer coefficient polynomials P_1 and P_2 of same number of variables, from Corollary 1, we can construct an alphabet $\Sigma = \{x_1, x_2, \ldots, x_k\}$, two vectors $\rho' = (1, 0, \ldots, 0)^T, \tau' = (0, \ldots, 0, 1)^T \in \mathbb{N}^n$, and two homomorphisms $\mu_1, \mu_2 : \Sigma^* \to \mathbb{Z}^{n\times n}$ such that:

$$\rho'^T \mu_i(w)\tau' = \begin{cases} P_i(y_1, y_2, \ldots, y_k)^2, & \text{if} \quad w \in L\backslash\{\varepsilon\}; \\ 0, & \text{if} \quad w = \varepsilon; \end{cases}$$

where $i \in \{1,2\}$ and L is the bounded language $L = x_1^* x_2^* \dots x_k^* \subset \Sigma^*$.
Step 2. Given alphabets $K = \{0,1,\dots,k,k+1\}$ and $\Omega = K \cup \{\#,*\}$, define left and right desynchronizing morphisms l and $r : K^* \to \Omega^*$ by

$$\begin{array}{llll} l(0) = \#0, & l(1) = *1, & l(i) = \#i, & l(k+1) = \#(k+1)\#, \\ r(0) = \#0*, & r(1) = 1\#, & r(i) = i\#, & r(k+1) = (k+1)\#, \end{array}$$

where $2 \le i \le k$. In the sequel, by abuse of notation, we use l_j, r_j to represent the words derived from the morphisms $l(j), r(j), 0 \le j \le k+1$. We define a word $u \in \Omega^*$ as 'free' if there is a unique factorization of u over $\{l_j, r_j\}$.

Let $L' = l_0^* l_1^* \cdots l_{k+1}^* r_0^* r_1^* \cdots r_{k+1}^* \in \Omega^*$. We shall now prove that any word $u = l_0^{j_0} l_1^{j_1} \cdots l_{k+1}^{j_{k+1}} r_0^{j_0'} r_1^{j_1'} \cdots r_{k+1}^{j_{k+1}'} \in L'$ is *not* free if and only if all $j_i = 0$ or all $j_i' = 0$ where $1 \le i \le k$.

Note that no element of $\Gamma = \{l_t, r_t | 0 \le t \le (k+1)\}$ is a prefix of any other word from the set, except for l_0 which is a prefix of r_0. Thus, $\Gamma \setminus \{l_0\}$ is a prefix code. If u does not begin with l_0 to some nonzero power, then by the definition of L', word u thus has a unique factorization.

If u has a prefix $\#0$, but not $\#0*$, then the prefix only matches with l_0, not r_0 and this prefix can be extracted from u since it has only a single possible factorization. We can continue this argument iteratively, until we reach u which begins with $\#0*$. Thus assume that u begins with $\#0*$. Let $u = l_0 u_1 = r_0 v_1$ be the two possible factorizations. Since u_1 must start with $*$, then $u_1 = l_1 u_2$. This implies that v_1 starts with symbol '1', which implies $v_1 = r_1 v_2$ since r_1 is the only word with prefix 1. Now, u_2 must be of the form $l_p u_3$ for some $2 \le p \le k$. Then v_2 must be of the form $r_p v_3$. This matching continues iteratively, until eventually we reach $(k+1)$, at which point we must use l_{k+1} for the u-word and r_{k+1} for the v-word.

At this point we have the two factorizations $u = l_0^* l_0 l_1 l_2^{j_2} \cdots l_k^{j_k} l_{k+1} r_{k+1}^*$ and $u = l_0^* r_0 r_1 r_2^{j_2} \cdots r_k^{j_k} r_{k+1} r_{k+1}^*$ as the only possibilities. An example of this follows:

$$\begin{aligned} u = \#0*1\#3\#5\#(k+1)\# = l_0 l_1 l_3 l_5 l_{k+1} \quad &= \#0 \cdot *1 \cdot \#3 \cdot \#5 \cdot \#(k+1)\# \\ = r_0 r_1 r_3 r_5 r_{k+1} &= \#0 * \cdot 1\# \cdot 3\# \cdot 5\# \cdot (k+1)\# \end{aligned}$$

Step 3. We now encode the words l_i and r_j $(0 \le i, j \le k+1)$ into rational numbers in the interval $(0,1)$. For simplicity we first define a mapping $\sigma : \Omega \to X$, where $X = \{x_0, x_1, \dots, x_{k+3}\}$ such that

$$\sigma(z) = \begin{cases} x_z & \text{if} \quad z \in \{0,1,\dots,k+1\}; \\ x_{k+2} & \text{if} \quad z = \#; \\ x_{k+3} & \text{if} \quad z = *. \end{cases}$$

We can extend σ to be a homomorphism $\sigma : \Omega^* \to X^*$. We then define a homomorphism $\beta : X^* \to (0,1) \cap \mathbb{Q}$ in a similar way as in the proof of Theorem 2:

$$\beta(x_{i_1} x_{i_2} \cdots x_{i_m}) = \Sigma_{j=1}^{m} i_j (n+1)^{j-m-1},$$

and $\beta(\varepsilon) = 0$, where $n = |X| = k+4$. Moreover, we use a similar definition as in the proof of Theorem 2 for γ, but only on a single word $v \in X^*$, such that

$\gamma : X^* \to \mathbb{Q}^{2\times 2}$:

$$\gamma(v) = \begin{pmatrix} (n+1)^{-|v|} & \beta(v) \\ 0 & 1 \end{pmatrix}.$$

It can be verified that $\gamma(v_1v_2) = \gamma(v_1)\gamma(v_2)$, and thus γ is a homomorphism.

Finally, we define $\gamma_l, \gamma_r : K^* \to \mathbb{Q}^{2\times 2}$ by $\gamma_l(i) = \gamma(\sigma(l_i))$ and $\gamma_r(i) = \gamma(\sigma(r_i))$, where $0 \le i \le k+1$. It can be seen that $\rho''^T\gamma_l\tau''$ and $\rho''^T\gamma_r\tau''$ are two homomorphisms from K^* to $(0,1)$, where $\rho'' = (1,0)^T$ and $\tau'' = (0,1)^T$, mapping the words derived from left and right desynchronizing morphisms l and r to $(0,1) \cap \mathbb{Q}$.

Step 4. In step 1 we showed how to encode an integer polynomial into a matrix. In step 2 and 3 we defined left and right desynchronizing morphisms and wrote them into matrix form. We now combine these steps together by defining a set of matrices $\{M_i, N_i\} \subset \mathbb{Q}^{(n+2)\times(n+2)}$:

$$\begin{array}{lll} M_0 = I \oplus \gamma_l(0), & M_i = \mu_1(x_i) \oplus \gamma_l(i), & M_{k+1} = I \oplus \gamma_l(k+1), \\ N_0 = I \oplus \gamma_r(0), & N_i = \mu_2(x_i) \oplus \gamma_r(i), & N_{k+1} = I \oplus \gamma_r(k+1), \end{array}$$

where $1 \le i \le k$, and I is the $n \times n$ identity matrix. Then we let a scalar λ be written as:

$$\begin{aligned} \lambda &= \rho^T M_0^{p_0} M_1^{p_1} \dots M_{k+1}^{p_{k+1}} N_0^{q_0} N_1^{q_1} \dots N_{k+1}^{q_{k+1}} \tau \\ &= \rho'^T \mu_1(w_1)\mu_2(w_2)\tau' + \rho''^T \gamma_l(v_1)\gamma_r(v_2)\tau'', \end{aligned}$$

where $\rho = (\rho'^T, \rho''^T)^T, \tau = (\tau'^T, \tau''^T)^T, w_1, w_2 \in L, v_1, v_2 = 0^*1^* \dots (k+1)^* \in K^*$. It can be seen that scalar λ contains two parts, one part consists of the homomorphisms μ_1, μ_2 we constructed in step 1 related to the polynomials, which is the integer part; the other part consists of the homomorphisms γ_l, γ_r we constructed in step 3 related to the desynchronizing morphisms, which is the fractional part. We now show that scalar λ is *not* free if and only if there exists some nonzero integer variables $(y_1, \dots, y_k)$ such that $P_1^2(y_1, \dots, y_k) = P_2^2(y_1, \dots, y_k)$.

If λ is not free, by definition there must be integers $p_0, \dots, p_{k+1}, q_0, \dots, q_{k+1}$ and $p'_0, \dots, p'_{k+1}, q'_0, \dots, q'_{k+1}$ such that

$$\lambda = \rho^T M_0^{p_0} \dots M_{k+1}^{p_{k+1}} N_0^{q_0} \dots N_{k+1}^{q_{k+1}} \tau = \rho^T M_0^{p'_0} \dots M_{k+1}^{p'_{k+1}} N_0^{q'_0} \dots N_{k+1}^{q'_{k+1}} \tau,$$

where $p_t \ne p'_t$ or $q_t \ne q'_t$ for at least one $0 \le t \le k+1$. Since the value of the fractional part of λ only depends on the desynchronizing morphisms, l, r, and the fractional parts are identical in both factorizations, from step 2 we have

$$\begin{array}{l} p_i = q'_i \text{ and } q_i = p'_j = 0, \text{ for } 1 \le i, j \le k, \text{ or} \\ p_i = q'_i = 0 \text{ and } q_j = p'_j, \text{ for } 1 \le i, j \le k. \end{array}$$

We only consider the first case, the second case can be analysed in a similar way. As the integer parts of λ in both factorizations are also identical, and

$M_0, M_{k+1}, N_0, N_{k+1}$ are defined in a way that the value of $p_0, p_{k+1}, q_0, q_{k+1}$ and $p'_0, p'_{k+1}, q'_0, q'_{k+1}$ do not affect the value of the integer part, we have

$$\rho'^T \mu_1^{p_1}(x_1) \dots \mu_1^{p_k}(x_k) \tau' = \rho'^T \mu_2^{p_1}(x_1) \dots \mu_2^{p_k}(x_k) \tau',$$

which implies that $P_1^2(p_1, \dots, p_k) = P_2^2(p_1, \dots, p_k)$. So $(p_1, \dots, p_k)$ is a solution.

If λ is free, we show there is no solution such that $P_1^2 = P_2^2$ by contradiction. Assume there is a nonzero solution $(y_1, \dots, y_k)$, such that $P_1^2(y_1, \dots, y_k) = P_2^2(y_1, \dots, y_k)$. From the way we construct P_1 and P_2 in Lemma 1, we know the value of y_1 can be any integer value without changing the equality. Thus it must be true that $P_1^2(1, y_2, \dots, y_k) = P_2^2(1, y_2, \dots, y_k)$, and there exists a word $w = x_1 x_2^{y_2} \dots x_k^{y_k} \in L^*$ such that

$$\rho'^T \mu_1(w) \tau' = \rho'^T \mu_2(w) \tau',$$

which implies that

$$\rho'^T \mu_1(x_1) \mu_2^{y_2}(x_2) \dots \mu_k^{y_k}(x_k) \tau' = \rho'^T \mu_1(x_1) \mu_2^{y_2}(x_2) \dots \mu_k^{y_k}(x_k) \tau'.$$

Since

$$M_i = \mu_1(x_i) \oplus \gamma_l(i),$$
$$N_i = \mu_2(x_i) \oplus \gamma_r(i),$$

for $1 \le i \le k$, we can set $v = 0 \cdot 1 \cdot 2^{y_2} \cdots k^{y_k} \cdot (k+1)$, and scalar λ can be written as

$$\begin{aligned} \lambda &= \rho'^T \mu_1(w) \tau' + \rho''^T \gamma_l(v) \tau'' = \rho^T M_0 M_1 M_2^{y_2} \cdots M_k^{y_k} M_{k+1} \tau \\ &= \rho'^T \mu_2(w) \tau' + \rho''^T \gamma_r(v) \tau'' = \rho^T N_0 N_1 N_2^{y_2} \cdots N_k^{y_k} N_{k+1} \tau. \end{aligned}$$

This shows that λ has two different factorizations, which is a contradiction. Thus we showed that scalar freeness problem can be reduced to the problem stated in Lemma 1, which is undecidable. □

Theorem 4 *The Scalar Ambiguity Problem over a bounded language is undecidable.*

Proof. We can use the same idea as in the proof of Theorem 2, increasing the dimension of matrices M_i, N_i constructed in the proof of Theorem 3 to store an additional word which is unique for each matrix. Vectors ρ, τ are modified with an additional zero-value dimension such that the value of scalar λ is not affected. Hence in the case $\lambda = \rho^T M_1 \tau = \rho^T M_2 \tau$, we must have $M_1 \neq M_2$. □

Corollary 2 *Vector ambiguity over a bounded language is undecidable.*

Proof. Immediately from Theorem 4 in the case when only one vector τ is considered. □

Finally, we show a result related to Probabilistic Finite Automata (PFA).

Problem 4 (PFA Ambiguity Problem) *Given a PFA $R = (u, \varphi, v)$ over a bounded language $L \in A^*$, do there exist two different words $w_1, w_2 \in L$ such that $u^T \varphi(w_1) v = u^T \varphi(w_2) v$?*

Corollary 3 *Ambiguity for PFA over a bounded language is undecidable.*

Proof. This proof follows the construction of [15]; see also [2, 11].

Let $M_i, N_i \in \mathbb{Q}^{(t-2)\times(t-2)}$ be matrices of dimension $(t-2)$ defined in the proof of Theorem 3, where $0 \le i \le k+1$. First, define a morphism $\zeta : A^* = \{a_0, a_1, \ldots, a_{2k+3}\}^* \to \{M_i, N_i\}$:

$$\zeta(a_j) = \begin{cases} M_j & \text{if} \quad 0 \le j \le k+1; \\ N_{j-(k+2)} & \text{if} \quad k+2 \le j \le 2k+3. \end{cases}$$

We then extend the dimension of the matrix $\zeta(a_j)$ to t by defining $\zeta' \to \mathbb{Q}^{t\times t}$:

$$\zeta'(a_j) = \begin{pmatrix} 0 & 0 & 0 \\ p_j & \zeta(a_j) & 0 \\ r_j & q_j & 0 \end{pmatrix},$$

where $p_j, q_j \in \mathbb{Q}^{(t-2)\times(t-2)}$ and $r_j \in \mathbb{Q}$ are properly chosen such that, for each $\zeta'(a_j)$, the row and column sums of $\zeta'(a_j)$ are all 0.

We now modify $\zeta'(a_j)$ so that every entry is positive. To do this we let Δ be the matrix of dimension t with all elements being 1. Assume b_i is in the set of entries of all $\zeta'(a_j)$, let $c > \max\{|b_i|\} \in \mathbb{Q}$. Define $\hat{\zeta} : A^* \to \mathbb{Q}_+^{t\times t}$ as

$$\hat{\zeta}(a_j) = \zeta'(a_j) + c\Delta.$$

It can be seen that all entries of the matrices $\hat{\zeta}(a_j)$ are positive. Finally, let $\varphi : A^* \to [0,1]^{t\times t}$ be

$$\varphi(a_j) = \frac{1}{ct}\hat{\zeta}(a_j) = \frac{1}{ct}\zeta'(a_j) + \frac{1}{t}\Delta.$$

Since row and column sums of $\zeta'(a_j)$ are all 0, and Δ is a matrix of dimension t with all elements being 1, it can be verified that all $\varphi(a_j)$ are stochastic matrices.

Then let $u = (0, \frac{1}{2}\rho^T, 0)^T$ and $v = (0, \frac{1}{2}\tau^T, 0)^T$, where $\rho, \tau \in \mathbb{Z}^{(t-2)\times(t-2)}$ are defined the same as in the proof of Theorem 3, we have constructed a PFA (u, φ, v) over a bounded language $w = a_0^* a_1^* \ldots a_{2k+3}^* \in L \subset A^*$.

To see that ambiguity for PFA (u, φ, v) is undecidable, we notice that $\Delta^n = t^{n-1}\Delta$ (as $\Delta^2 = t\Delta$), and by the definition of $\zeta'(a_j)$, it holds that $\zeta'(a_j) \cdot \Delta = \Delta \cdot \zeta'(a_j) = \overline{\varnothing}$ (the zero matrix). Thus,

$$\begin{aligned} u^T\varphi(w)v &= u^T\left(\left(\frac{1}{ct}\right)^{|w|}\zeta'(w) + \left(\frac{1}{t}\right)^{|w|}\Delta^{|w|}\right)v \\ &= \left(\frac{1}{ct}\right)^{|w|}(\rho^T\zeta(w)\tau) + u^T\left(\frac{\Delta}{t}\right)v \\ &= \left(\frac{1}{ct}\right)^{|w|}(\rho^T M_0^{p_0}\cdots M_{k+1}^{p_{k+1}} N_0^{q_0}\cdots N_{k+1}^{q_{k+1}}\tau) + \frac{1}{t} \\ &= \rho^T\left(\frac{M_0}{ct}\right)^{p_0}\cdots\left(\frac{M_{k+1}}{ct}\right)^{p_{k+1}}\left(\frac{N_0}{ct}\right)^{q_0}\cdots\left(\frac{N_{k+1}}{ct}\right)^{q_{k+1}}\tau + \frac{1}{t} \end{aligned}$$

Since c and t are all fixed, the question of whether there exist two different words $w_1, w_2 \in L$ such that $u^T\varphi(w_1)v = u^T\varphi(w_2)v$, can be reduced to the scalar ambiguity problem over bounded languages, hence is undecidable. □

4 Conclusion

We defined two related problems for matrix semigroups: the scalar ambiguity problem and the scalar freeness problem. We discussed the relations between these two problems and the matrix semigroup freeness problem. We showed that both problems are undecidable in low dimensions, three for ambiguity and four for freeness. These two problems remain undecidable even over bounded languages, but require higher dimensions. Using these results, we showed the ambiguity problem for probabilistic finite automata is also undecidable.

References

1. Bell, P.C., Halava, V., Harju, T., Karhumäki, J., Potapov, I.: Matrix equations and Hilbert's tenth problem. International Journal of Algebra and Computation 18, 1231–1241 (2008)
2. Bell, P.C., Halava, V., Hirvensalo, M.: Decision problems for probabilistic finite automata on bounded languages. Fundamenta Informaticae 123(1), 1–14 (2012)
3. Bell, P.C., Potapov, I.: Periodic and infinite traces in matrix semigroups. Current Trends in Theory and Practice of Computer Science (SOFSEM) LNCS 4910, 148–161 (2008)
4. Bell, P.C., Potapov, I.: Reachability problems in quaternion matrix and rotation semigroups. Information and Computation 206(11), 1353–1361 (2008)
5. Blondel, V., Canterini, V.: Undecidable problems for probabilistic automata of fixed dimension. Theory of Computing Systems 36, 231–245 (2003)
6. Cassaigne, J., Harju, T., Karhumäki, J.: On the undecidability of freeness of matrix semigroups. International Journal of Algebra and Computation 9(3-4), 295–305 (1999)
7. Cassaigne, J., Karhumäki, J., Harju, T.: On the decidability of the freeness of matrix semigroups. Tech. rep., Turku Centre for Computer Science (1996)
8. Cassaigne, J., Nicolas, F.: On the decidability of semigroup freeness. RAIRO - Theoretical Informatics and Applications 46(3), 355–399 (2012)
9. Charlier, E., Honkala, J.: The freeness problem over matrix semigroups and bounded languages. Information and Computation 237, 243–256 (2014)
10. Choffrut, C., Karhumäki, J.: Some decision problems on integer matrices. Informatics and Applications 39, 125–131 (2005)
11. Hirvensalo, M.: Improved undecidability results on the emptiness problem of probabilistic and quantum cut-point languages. SOFSEM 2007: Theory and Practice of Computer Science, Lecture Notes in Computer Science 4362, 309–319 (2007)
12. Klarner, D., Birget, J.C., Satterfield, W.: On the undecidability of the freeness of integer matrix semigroups. International Journal of Algebra and Computation 1 (2), 223–226 (1991)
13. Matiyasevich, Yu.: Hilbert's Tenth Problem. MIT Press (1993)
14. Paz, A.: Introduction to Probabilistic Automata. Academic Press (1971)
15. Turakainen, P.: Generalized automata and stochastic languages. Proceedings of the American Mathematical Society 21, 303–309 (1969)