Freeness Properties of Weighted and Probabilistic Automata over Bounded Languages

Paul C. Bell[1,†], Shang Chen[†], Lisa Jackson[‡]

Dept of Computer Science †, Dept of Aeronautical and Automotive Engineering ‡, Loughborough University, Loughborough, LE11-3TU, UK

p.c.bell@ljmu.ac.uk, Chenshangcn@gmail.com, L.M.Jackson@lboro.ac.uk

Abstract

There has been much research into freeness properties of finitely generated matrix semigroups under various constraints, such as the dimensions of the generator matrices and the semiring over which the matrices are defined. 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. A recent paper has also investigated freeness properties of bounded languages of matrices, which are matrices from a set $M_1^* M_2^* \cdots M_k^* \subseteq \mathbb{F}^{n\times n}$ for some semiring $\mathbb{F}$ and a fixed value $k \in \mathbb{N}_{>0}$, where matrices $M_1, \ldots, M_k$ are given [1].

We consider 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 $\mathcal{S} \subseteq \mathbb{F}^{n\times n}$ is a finitely generated matrix semigroup. Ambiguity and freeness problems are defined in terms of the uniqueness of factorizations for each scalar. Such problems have also been studied in connection to formal power series. We show various undecidability results and their connections to weighted and probabilistic finite automata.

Keywords: matrix semigroup freeness, bounded languages, undecidability, weighted automata, probabilistic automata

1. Introduction

Classical (non)-deterministic finite automata (NFA/DFA) act as acceptors for the regular languages. In this Boolean setting, each word is either *accepted* or *rejected* by a given automaton; the set of languages accepted forming the regular language of the automaton. There are many possible generalisations of the model of DFA and NFA. One such model is that of *Weighted Finite*

[1]Permanent address: Dept of Computer Science, Liverpool John Moores University, Liverpool, L3-3AF, UK

Automata (WFA), whose transition function is a partial function defined on accepting words to values from $\mathbb{Q}$. A related model is that of *Probabilistic Finite Automata* (PFA), where for each letter of the input alphabet, we assign a rational weight to each outgoing transition from each state such that the weights form a probability distribution. Depending upon the properties of the chosen semiring and the acceptance conditions, we obtain interesting language theoretic decision problems for such models. Our aim in this paper is to explore the undecidability of the uniqueness of acceptance weights for WFA and the uniqueness of acceptance probabilities for PFA under various constraints. We call these scalar reachability problems. Such problems over PFA are also related to the threshold isolation of cut-points as studied in [2]. A motivation for the study of the threshold isolation problem is that the set of words accepted by a PFA with a probability strictly greater than an isolated threshold is a regular language [2, 3].

Another motivation for studying scalar reachability problems is the *freeness problem* for matrix semigroups. Decision problems on matrices have long been studied, with one of the earliest results being Paterson's result showing that the *mortlity problem* is undecidable for 3×3 integer matrices [4]. The mortality problem asks whether a finitely generated semigroup contains the zero matrix. A related problem is the freeness problem for integer matrices - given a set $\mathcal{G} \subseteq \mathbb{F}^{n\times n}$, where $\mathbb{F}$ is a semiring, determine if $\mathcal{G}$ is a code for the semigroup generated by $\mathcal{G}$, denoted $\langle\mathcal{G}\rangle$ (i.e. if every element of $\langle\mathcal{G}\rangle$ has a unique factorization over elements of $\mathcal{G}$). It was proven by Klarner et al. that the freeness problem is undecidable over $\mathbb{N}^{3\times3}$ in [5] and this result was improved by Cassaigne et al. to hold even for upper-triangular matrices over $\mathbb{N}^{3\times3}$ in [6].

There are many open problems related to freeness in 2×2 matrices, see [1, 7, 8] for good surveys. The freeness problem over $\mathbb{H}^{2\times2}$ is undecidable [9], 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 [1].

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 such 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 [1].

In this paper we consider two notions of freeness for 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 and ρ, τ are two given vectors of appropriate dimension (see Section 3 for details). Related problems for *vector*

ambiguity were studied in [10], where problems related to the uniqueness of factorizations of a set of *vectors* $\{M\tau | M \in \mathcal{S}\}$ was studied. The problem was shown to be undecidable when $\mathcal{S} \subseteq \mathbb{Z}^{4\times4}$, or when $\mathcal{S} \subseteq \mathbb{Q}^{3\times3}$.

The scalar reachability problem has implications for several computational models, depending upon the properties of the vectors, matrices and update rules that we may apply. We initially interpret our results for *Weighted Finite Automata* (WFA), defined formally in Section 2.2. The formulation of this model is dependent upon the semiring over which the model is defined. A well studied problem is the *universality problem* for WFA, whereby we are given some threshold and we ask whether all possible input words have an acceptance weight below the threshold. Decision problems for WFA over the *tropical semiring* are studied in [11, 12, 13], although in this paper we focus exclusively on the integers and rationals. Weighted automata have a variety of applications, for example in automatic speech or image recognition [14] or in the verification of quantative properties [15]. In this paper we consider instead the problem of determining whether the acceptance weight of each input word is unique over the integers. We show that this problem is undecidable over a 4 state WFA by an encoding of the *Mixed Modification Post's Correspondence Problem* and show that the undecidability holds even when the input words come from a bounded language. The problem can also be stated in terms of *formal power series*: given a formal power series r, determine if r has two equal coefficients. This problem was studied in [16] and Theorem 3.4 of [17] (more details appear in Section 4 of this paper).

In Section 4, we also study a related ambiguity problem for *Probabilistic Finite Automata* (PFA), defined in Section 2.3. Several reachability problems for PFA (such as emptiness of cut-point languages) are known to be *undecidable* [18], even in a fixed dimension [2, 19]. 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 shown to be undecidable in [20].

Associated with each input word w over an alphabet A is the probability of that word being accepted by a PFA $\mathcal{R}$, which we denote by $f_{\mathcal{R}}(w)$, defined formally in Section 2.3. In this paper, we show that determining whether every probability is unique is undecidable, even over a bounded language. In other words, given a bounded language $L \subset A^*$, then to determine if there exist two words $w_1, w_2 \in L$ with $w_1 \neq w_2$ such that $f_{\mathcal{R}}(w_1) = f_{\mathcal{R}}(w_2)$ is undecidable. This is a similar concept to the *threshold isolation problem* which is known to be undecidable, see [3, 2].

A preliminary version of this paper appeared in [21].

2. Preliminaries

2.1. Notations and Definitions

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. We use $|u|$ to denote the length of a word u, i.e. how many letters the word u contains. Also we have $|\varepsilon| = 0$. 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 a word $u_1u_2\cdots u_m$, where $m \leq i$. If $m < i$, then the prefix is called *proper*. A suffix of u is a word of the form $u_mu_{m+1}\cdots u_i$, where $1 \leq m \leq i$. If $m > 1$ then the suffix is called *proper*. 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 $L \subseteq w_1^*w_2^*\cdots w_m^*$.

Recall that a *semiring* is a set $\mathbb{F}$, with two operations called addition and multiplication defined on it, denoted $+$ and $\cdot$, and two distinct elements $0, 1$ such that $(\mathbb{F}, +, 0)$ is a commutative monoid and $(\mathbb{F}, \cdot, 1)$ is a monoid. Also multiplication left and right distributes over addition and multiplication by 0 annihilates $\mathbb{F}$.

We denote by $\mathbb{F}^{n\times n}$ the set of all $n \times n$ matrices over a semiring $\mathbb{F}$. Throughout the paper the structure over the matrices is the multiplicative structure with the operations on matrices defined via the addition and multiplication of the semiring. 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 $w_2 \in \mathcal{G}'$.

2.2. Weighted Finite Automata

We use similar definitions of a Weight Finite Automata/Automaton (WFA) as in [12]. A WFA is defined as an 8-tuple, given by $\mathcal{W} = (\Sigma, Q, \Delta, c, Q_0, Q_F, i, f)$, where $\Sigma = \{x_1, x_2, \ldots, x_n\}$ is a finite alphabet of input letters, $Q = \{q_1, q_2, \ldots, q_m\}$ is the finite set of states, $\Delta \subseteq Q \times \Sigma \times Q$ is the transition function, $c : \Delta \to \mathbb{Q}$ is a cost function associated to each transition, $Q_0 \subseteq Q$ is the set of initial states, $Q_F \subseteq Q$ is the set of final states, $i : Q_0 \to \mathbb{Q}$ is the initial-weight function and $f : Q_F \to \mathbb{Q}$ is the final-weight function. Transitions of the system are of the form $\Delta(q, l, q')$, which we also write $\Delta(q, l) = q'$. We understand this to mean that when in state q and we read the input letter l, the WFA changes to state q'. WFA may be nondeterministic, since they have a set of initial states and the transition function may be nondeterministic.

Given a word $w = w_1w_2\cdots w_k \in \Sigma^*$, a *run* of $\mathcal{W}$ on w is a sequence $r_w = (r_0, r_1, \ldots, r_k) \in Q^{k+1}$, such that $r_0 \in Q_0$, $r_k \in Q_F$, and there exists $d_j = (r_{j-1}, w_j, r_j) \in \Delta$ for each $1 \leq j \leq k$. We denote the set of all runs of $\mathcal{W}$

on w by $R_{\mathcal{W}}(w)$ and associated with each run is a *cost*. For a WFA over the integers/rationals, the cost of a run $r_w = (r_0, r_1, \ldots, r_k) \in Q^{k+1}$ is defined as:

$$c(r_w) = i(r_0) \times \prod_{j=1}^{k} c(d_j) \times f(r_n).$$

Note here that we overload function c, although this should not cause confusion. Since the WFA may be nondeterministic, there may be more than one run defined for word w on $\mathcal{W}$, and hence more than one associated cost. Moreover, the cost of an accepting word w on $\mathcal{W}$ is defined to be the (semiring) sum of costs of all accepting runs of the WFA on w:

$$L_{\mathcal{W}}(w) = \sum_{r_w \in R_{\mathcal{W}}(w)} c(r_w)$$

WFA over the integers can equivalently be represented in terms of vectors and matrix operations. Given the WFA $\mathcal{W}$ as above, we can define a vector $\tau \in \mathbb{Z}^m$ such that $\tau_j = 0$ if $q_j \notin Q_0$ and $\tau_j = i(q_j)$ if $q_j \in Q_0$. Vector ρ is defined such that $\rho_j = 0$ if $q_j \notin Q_F$ and $\rho_j = f(q_j)$ if $q_j \in Q_F$. Then, for each $x_j \in \Sigma$, matrix $X^{(j)} \in \mathbb{Z}^{m \times m}$ is defined such that for $d^j_{b,a} = (b, x_j, a) \in Q \times \Sigma \times Q$, then $X^{(j)}_{[a,b]} = 0$ if $d^j_{b,a} \notin \Delta$, and $X^{(j)}_{[a,b]} = c(d^j_{b,a})$ if $d^j_{b,a} \in \Delta$. We then find that $L_{\mathcal{W}}(w) = \rho^T X^{(i_k)} \cdots X^{(i_2)} X^{(i_1)} \tau$ for word $w = x_{i_1} x_{i_2} \cdots x_{i_k} \in \Sigma^*$. See also Example 3 for a detailed example.

There are a variety of interesting questions for WFA. The *universality problem* asks given a WFA $\mathcal{W}$ and a threshold value $\lambda \in \mathbb{Q}$, is $L_{\mathcal{W}}(w) < \lambda$ for all words $w \in \Sigma^*$? The *equality problem* is to determine for two WFA $\mathcal{W}_1$ and $\mathcal{W}_2$ over an alphabet Σ if $L_{\mathcal{W}_1}(w) = L_{\mathcal{W}_2}(w)$ for all $w \in \Sigma^*$. We are interested in this paper in the *freeness problem* for WFA: given a WFA $\mathcal{W}$, do there exist $w_1, w_2 \in \Sigma^*$ with $w_1 \neq w_2$ such that $L_{\mathcal{W}}(w_1) = L_{\mathcal{W}}(w_2)$? We later show that this problem is undecidable when $\mathcal{W}$ has three states and an alphabet of size 16 (over rationals) and when $\mathcal{W}$ has four states (over the integers). The problem remains undecidable even when input words must come from a given bounded language, although the resulting WFA has many more states and a larger alphabet (an equivalent undecidability result was discussed in [16] in the context of formal power series). In all of our proofs, we assume the initial-weight function and the final-weight function of the WFA have values of the identity element of the weight semigroup for all states, and hence they are not given in constructions.

2.3. 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 [18, 2] 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. [2]

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 $w \in A^*$.

In this paper we study the *freeness problem* for PFA over a bounded language which is similarly defined as the problem for WFA above: given a PFA $\mathcal{R} = (u, \varphi, v)$ over a bounded language $L \in A^*$, do there exist two different words $w_1, w_2 \in L$ such that $u^T \varphi(w_1) v = u^T \varphi(w_2) v$? We show that this problem is also undecidable, depending upon the number of states of $\mathcal{R}$ and the size of the input alphabet A.

2.4. Mixed Modification Post's Correspondence Problem

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* $\Sigma = \{s_1, s_2, \ldots, s_{|\Sigma|}\}$*, a binary alphabet* Σ_2*, and a pair of homomorphisms* $h, g : \Sigma^* \to \Sigma_2^*$*, the MMPCP asks to decide whether there exists a word* $w = x_1 \ldots x_k \in \Sigma^+, x_i \in \Sigma$ *such that*

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

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

Theorem 1. *[22] - The Mixed Modification PCP is undecidable for* $|\Sigma| \geq 9$*.*

It will later be useful to slightly modify the definition of this problem. As with other variants of Post's correspondence problem, the proofs of undecidability of the MMPCP often have the property that potential solution words are of the form $w = s_1 x_2 x_3 \cdots x_{k-1} s_{|\Sigma|}$, where $x_2, \ldots, x_{k-1} \in \Sigma - \{s_1, s_{|\Sigma|}\}$, i.e. potential solution words must start with letter s_1, end with letter $s_{|\Sigma|}$, and all other letters are not equal to s_1 or $s_{|\Sigma|}$. An instance of the (MM)PCP which

[2] 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.

has this property is called a *Claus instance* of the problem. In fact all known proofs of the undecidability of (MM)PCP seem to have this property [23]. Claus instances can be useful for decreasing the resources required for showing certain undecidability results, and we use this property later.

Theorem 2. *[23] - The Mixed Modification PCP is undecidable for Claus instances, when* $|\Sigma| \geq 9$.[3]

3. Scalar Ambiguity and Freeness for Matrices

Consider a finite set $\mathcal{G} = \{G_1, G_2, \ldots, G_k\} \subset \mathbb{F}^{n\times n}$, 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 $\mathcal{G}, \rho, \tau$. We call $\Lambda(\mathcal{G})$ 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 $\mathcal{G}, \rho, \tau$. We call $\Lambda(\mathcal{G})$ free if every $\lambda \in \Lambda(\mathcal{G})$ is free.

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 $\mathcal{S}$, whilst the scalar freeness problem deals more with 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 $\langle \mathcal{G} \rangle$, then the corresponding scalar set $\Lambda(\mathcal{G})$ is not free, but the same property does not hold for the scalar ambiguity problem. See the following two examples for further discussion.

Example 1. *Given a semigroup of matrices* $\mathcal{S} = \langle \mathcal{G} \rangle$ *generated by a finite set* $\mathcal{G} = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$ *and two vectors* $\rho = \tau = (1, 0)^T$*, it is well-known that* $\mathcal{S}$ *is a free semigroup (e.g.[22]). However, since*

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

then scalar 1 *is ambiguous with respect to* $\mathcal{G}, \rho, \tau$ *and thus* $\Lambda(\mathcal{G})$ *is ambiguous and not free even though* $\mathcal{G}$ *is free.*

[3] The result in [23] states the undecidability for $|\Sigma| \geq 7$ since they fix the first/last letters of a potential solution.

Example 2. *Given a semigroup of matrices* $\mathcal{S} = \langle \mathcal{G} \rangle$ *generated by a finite set* $\mathcal{G} = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \right\}$, *and two vectors* $\rho = \tau = (1,0)^T$, *it is not difficult to verify that for* $k \in \mathbb{N}$:

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 2^k & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 3^k & 0 \\ 0 & 1 \end{pmatrix}.$$

As the vectors ρ *and* τ *will only calculate the element* $M_{[1,1]}$ *for the matrix* $M \in \langle \mathcal{G} \rangle$, *every scalar in the set* $\Lambda(\mathcal{G})$ *is of the form* $2^m 3^n$, *where* $m, n \in \mathbb{N}$ *and* $m + n \neq 0$. *The only way to generate such a scalar by a single matrix is*

$$2^m 3^n = \begin{pmatrix} 1 \\ 0 \end{pmatrix}^T \begin{pmatrix} 2^m 3^n & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

thus $\Lambda(\mathcal{G})$ *is unambiguous. However, since the two matrices in the set* $\mathcal{G}$ *are commutative, the semigroup* $\mathcal{S}$ *is clearly not free, and*

$$2^m 3^n = \begin{pmatrix} 1 \\ 0 \end{pmatrix}^T \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^m \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}^T \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^m \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

which indicates that $\Lambda(\mathcal{G})$ *is also not free. Notice that if we select a different pair of vectors, for example* $\rho = (1,1)^T, \tau = (0,1)^T$, *the scalar set* $\Lambda(\mathcal{G})$ *can become neither free nor unambiguous.*

Example 1 shows that a scalar set $\Lambda(\mathcal{G})$ can be ambiguous and not free even if $\mathcal{S} = \langle \mathcal{G} \rangle$ is a free semigroup. Example 2 shows that even if a scalar set $\Lambda(\mathcal{G})$ and the corresponding matrix semigroup $\mathcal{G}$ are not free, the scalar set can be ambiguous or unambiguous, depending on the vectors given. The links between the scalar ambiguity problem, scalar freeness problem and matrix semigroup freeness problem are illustrated in the following proposition.

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 $\rho^T M_1 \tau = \rho^T M_2 \tau$. If M_1, M_2 are different, then their factorisations must be different. 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 $G_i, G_j \in \mathcal{G}$ and 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 there seems to be 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. We later show that this theorem also holds over integer matrices and vectors in Corollary 1.

Theorem 3. *The Scalar Freeness Problem is undecidable over $\mathcal{G} \subseteq \mathbb{Q}^{3\times 3}$ and the Scalar Ambiguity Problem is undecidable over $\mathcal{G}' \subseteq \mathbb{Q}^{4\times 4}$, when $|\mathcal{G}|, |\mathcal{G}'| \geq 16$.*

Proof. We prove the result by encoding an instance of the MMPCP problem. The basic idea is inspired by [22]. 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 not 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 $\Sigma = \{x_1, x_2, \dots, x_{n-2}\}$ 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 injective mappings $\alpha, \beta : (\Sigma \cup \Delta)^* \to \mathbb{Q}$ by:

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

and $\alpha(\varepsilon) = \beta(\varepsilon) = 0$. Thus α represents $x_{i_1} x_{i_2} \cdots x_{i_m}$ as a reverse $(n+1)$-adic number and β represents $x_{i_1} x_{i_2} \cdots x_{i_m}$ as a fractional number $(0.x_{i_1} x_{i_2} \cdots x_{i_m})_{(n+1)}$ (e.g. if $n = 9$, then $x_1 x_2 x_3$ is represented as $\alpha(x_1 x_2 x_3) = 321_{10}$ and $\beta(x_1 x_2 x_3) = 0.123_{10}$, where subscript 10 denotes 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 $\forall w_1, w_2 \in (\Sigma \cup \Delta)^*, (n+1)^{|w_1|}\alpha(w_2) + \alpha(w_1) = \alpha(w_1 w_2)$ and $(n+1)^{-|w_1|}\beta(w_2) + \beta(w_1) = \beta(w_1 w_2)$.

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 $\gamma'(u_1, v_1)\gamma'(u_2, v_2) = \gamma'(u_1 u_2, v_1 v_2)$, 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 $\mathcal{G} = \{\gamma(x_i,g(x_i)),\gamma(x_i,h(x_i))|x_i \in \Sigma, 1 \leq i \leq n-2\}$, $\mathcal{S} = \langle\mathcal{G}\rangle$, $\rho = (1,0,0)^T$ and $\tau = (0,0,1)^T$. Assume that there exist $M_1 = G_{i_1}G_{i_2}\cdots G_{i_t} \in \langle\mathcal{G}\rangle$ 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 $1 \leq p \leq t$ 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 $1 \leq k \leq t$. 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 MMPCP 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 $\rho^T M_1\tau \neq \rho^T M_2\tau$.

By Theorem 1, this implies that the result holds for $|\mathcal{G}| \geq 18$ since the MMPCP is undecidable over an alphabet of size 9. We now prove that the result holds for $|\mathcal{G}| \geq 16$. By Theorem 2 above, we may assume that $h,g : \Sigma^* \to \Delta^*$ is a Claus instance of the MMPCP problem, and that $|\Sigma| \geq 9$. Let then $\Sigma = \{x_1,x_2\ldots,x_9\}$. Since h,g is a Claus instance, then any potential solution word w is of the form $w = x_1w'x_9$, with $w' \in (\Sigma - \{x_1,x_9\})^*$. By symmetry, we may assume that $h_1 = h$ and by the proof in [23], $g_i = g$ and $h_i = h$ for all $1 \leq i \leq t$. Clearly then, one of $h(x_1)$ and $g(x_1)$ is a proper prefix of the other (assume $h(x_1)$ is a prefix of $g(x_1)$), otherwise a shorter solution must exist. Similarly one of $h(x_9)$ and $g(x_9)$ is a proper suffix of the other (assume that $g(x_9)$ is a suffix of $h(x_9)$; the opposite case is similar). Now, we redefine $\rho'^T = \rho^T\gamma(x_1,h(x_1))$ and $\tau' = \gamma(x_9,g(x_9))\tau$. Finally we remove the matrices corresponding to $h(x_1)$ and $g(x_9)$ from $\mathcal{G}$ and redefine the matrices corresponding to $g(x_1)$ and $h(x_9)$ by $g'(x_1) = \gamma(x_1,h(x_1)^{-1}g(x_1))$ and $h'(x_9) = \gamma(x_9,h(x_9)g(x_9)^{-1})$ respectively. Since $h(x_1)$ is a proper prefix of $g(x_1)$, then $h(x_1)^{-1}g(x_1)$ is the suffix of $g(x_1)$ after removing the common prefix with $h(x_1)$ (similarly for $h(x_9)g(x_9)^{-1}$). Then, we see that

$$\begin{aligned} h_1(x_{i_1})h_2(x_{i_2})\cdots h_{t-1}(x_{i_{t-1}})h_t(x_{i_t}) &= g_1(x_{i_1})g_2(x_{i_2})\cdots g_{t-1}(x_{i_{t-1}})g_t(x_{i_t}) \\ \Leftrightarrow h(x_1)h(x_{i_2})\cdots h(x_{i_{t-1}})h(x_9) &= g(x_1)g(x_{i_2})\cdots g(x_{i_{t-1}})g(x_9) \\ \Leftrightarrow h(x_{i_2})\cdots h(x_{i_{t-1}})h'(x_9) &= g'(x_1)g(x_{i_2})\cdots g(x_{i_{t-1}}) \end{aligned}$$

This completes the proof of the scalar freeness problem for 16 rational matrices of dimension 3.

We now show the undecidability of the scalar ambiguity problem by a reduction of the scalar freeness problem shown above. 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 MMPCP instance, then some matrix $M \in \mathcal{S}$ has two distinct factorizations as above, one using morphisms from h, the other using morphisms from g (see the proof of the undecidability for Claus instances of MMPCP, Theorem 13 of [23]). We increase the dimension of γ by 1 to store an additional element. Each matrix of the form $\gamma(x_i, g(x_i)) \in \mathcal{G}$ is modified to $\gamma(x_i, g(x_i)) \oplus 3 \in \mathbb{Q}^{4\times 4}$ and each matrix of the form $\gamma(x_i, h(x_i)) \in \mathcal{G}$ is modified to $\gamma(x_i, h(x_i)) \oplus 5 \in \mathbb{Q}^{4\times 4}$. We modify ρ to $\rho \oplus 0$ and τ to $\tau \oplus 0$, which have an additional dimension which does not select this new element (of the form 3^t or 5^t). A solution to the MMPCP instance will now have two different factorizations, and the corresponding matrices will differ in one component. Therefore the ambiguity problem is undecidable for 16 matrices over $\mathbb{Q}^{4\times 4}$. □

Let $\mathcal{G} \subseteq \mathbb{Q}^{n\times n}$ be a set of matrices and $\rho, \tau \in \mathbb{Q}^n$ be two vectors such that $\Lambda(\mathcal{G})$ is free (resp. ambiguous) with respect to $\mathcal{G}$, ρ and τ. Unfortunately, it is not the case that for all $z \in \mathbb{Z} - \{0\}$ then $\Lambda(z\mathcal{G})$ is free (resp. ambiguous) with respect to $z\mathcal{G}$, $z\rho$ and $z\tau$ (where $z\mathcal{G}$ denotes multiplying each matrix of $\mathcal{G}$ by z). The reason this is unfortunate is that otherwise we may multiply all matrices and vectors by some large enough constant z so that they become integer. In order to show a reduction from the rational to integer version of Theorem 3, we require a new technique which is shown in the following Lemma.

Lemma 1. *If the scalar freeness or scalar ambiguity problem is undecidable for two vectors $\rho', \tau' \in \mathbb{Z}^{n-1}$ and a set of matrices $\mathcal{G}' = \{G'_1, G'_2, \ldots, G'_k\} \subseteq \mathbb{Q}^{(n-1)\times(n-1)}$, where non-free scalars must have the same number of factors, then the problem is also undecidable for computable vectors $\rho, \tau \in \mathbb{Z}^n$ and set of matrices $\mathcal{G} = \{G_1, G_2, \ldots, G_k\} \subseteq \mathbb{Z}^{n\times n}$.*

Proof. Notice in the proof of Theorem 3 that if a scalar is non-free or ambiguous, then the scalar can be generated by two matrices X_1 and X_2, each of which is the product of the same number of matrices from the generator. We use this property in the proof below.

Let $z \in \mathbb{N}_{>1}$ be large enough such that $zG'_i \in \mathbb{Z}^{(n-1)\times(n-1)}$ for each $G'_i \in \mathcal{G}'$. Such a z clearly exists and can be taken as the least common multiple of the denominators of elements from each matrix and vector. Let $\rho = \rho' \oplus 1$ and $\tau = \tau' \oplus 1$ (i.e. ρ is ρ' with a '1' appended at the end). Finally, we define $\mathcal{G} = \{G_1, G_2, \ldots, G_k\} \subseteq \mathbb{Z}^{n\times n}$ by $G_i = z^2 G'_i \oplus z$.

Assume that $\Lambda(\mathcal{G}')$ is free with respect to $\mathcal{G}', \rho', \tau'$. We now show that $\Lambda(\mathcal{G})$ is free with respect to $\mathcal{G}, \rho, \tau$.

Assume by contradiction that there exists $M_1 = G_{i_1} G_{i_2} \cdots G_{i_{k_1}} \in \langle \mathcal{G} \rangle$ and $M_2 = G_{j_1} G_{j_2} \cdots G_{j_{k_2}} \in \langle \mathcal{G} \rangle$ such that either $k_1 \neq k_2$ or at least one $G_{i_t} \neq G_{j_t}$ for $1 \leq t \leq k_1$, where $\rho M_1 \tau = \rho M_2 \tau$. We see that

$$\rho M_1 \tau = z^{2k_1} \rho' M'_1 \tau' + z^{k_1} = z^{2k_2} \rho' M'_2 \tau' + z^{k_2} = \rho M_2 \tau,$$

where $M'_1 = G'_{i_1} G'_{i_2} \cdots G'_{i_{k_1}} \in \langle \mathcal{G}' \rangle$ and $M'_2 = G'_{j_1} G'_{j_2} \cdots G'_{j_{k_2}} \in \langle \mathcal{G}' \rangle$. Now, if $k_1 = k_2$, then this implies that $\rho' M'_1 \tau' = \rho' M'_1 \tau'$, which is a contradiction since

$\Lambda(\mathcal{G}')$ is free with respect to $\mathcal{G}', \rho', \tau'$. Thus, assume that $k_2 > k_1$ (the other case is similar). In this case we can divide both sides of equation $z^{2k_1}\rho' M_1' \tau' + z^{k_1} = z^{2k_2}\rho' M_2' \tau' + z^{k_2}$ by z^{k_1} to see that

$$z^{k_1}\rho' M_1' \tau' + 1 = z^{2k_2-k_1}\rho' M_2' \tau' + z^{k_2-k_1}$$

Now, $z^{k_1}\rho' M_1' \tau' + 1 \mod z \equiv 1$ and $z^{2k_2-k_1}\rho' M_2' \tau' + z^{k_2-k_1} \mod z \equiv 0$, therefore they cannot be equal. Thus, if $\Lambda(\mathcal{G})$ is free with respect to $\mathcal{G}, \rho, \tau$, then it implies that $\Lambda(\mathcal{G}')$ is free with respect to $\mathcal{G}', \rho', \tau'$ as required.

Finally, assume that $\Lambda(\mathcal{G}')$ is *not* free with respect to $\mathcal{G}', \rho', \tau'$. By the assumption of the Lemma, then there exists two matrices $X_1 = G'_{i_1} G'_{i_2} \cdots G'_{i_{k_1}}$ and $X_2 = G'_{j_1} G'_{j_2} \cdots G'_{i_{k_1}}$ such that $\rho' X_1 \tau' = \rho' X_1 \tau'$. Notice that X_1 and X_2 are the product of the same number of matrices k_1. We now see that:

$$\rho G_{i_1} G_{i_2} \cdots G_{i_{k_1}} \tau = z^{2k_1}\rho' X_1 \tau' + z^{k_1} = z^{2k_1}\rho' X_2 \tau' + z^{k_1} = \rho G_{j_1} G_{j_2} \cdots G_{j_{k_1}} \tau$$

and therefore $\Lambda(\mathcal{G})$ is *not* free with respect to $\mathcal{G}, \rho, \tau$. □

We can now state Theorem 3 is undecidable over integer matrices, with an increase in the dimension (note that this increased dimension was erroneously omitted in [21]).

Corollary 1. *The Scalar Freeness Problem is undecidable over $\mathcal{G} \subseteq \mathbb{Z}^{4\times4}$ and the Scalar Ambiguity Problem is undecidable over $\mathcal{G}' \subseteq \mathbb{Z}^{5\times5}$, when $|\mathcal{G}|, |\mathcal{G}'| \geq 16$.*

Proof. Immediate from Theorem 3 and Lemma 1. □

Corollary 2. *Given a four-state Weighted Finite Automaton $\mathcal{W}$, determining if the cost of $\mathcal{W}$ is distinct for every possible accepting word is undecidable over the integers, even when the initial and final weight functions of $\mathcal{W}$ equal the identity.*

Proof. We use the set of matrices $\mathcal{G} = \{\gamma(x_i, g(x_i)), \gamma(x_i, h(x_i)) | x_i \in \Sigma, 1 \leq i \leq n-2\}$, $\rho = (1,0,0)^T$ and $\tau = (0,0,1)^T$ defined in the proof of Theorem 3. We label the matrices in $\mathcal{G}$ by h_i, g_i for $1 \leq i \leq n-2$ (with the obvious correspondence). Since Corollary 1 proves it is undecidable to determine if there exists two matrices $X_1, X_2 \in \langle\mathcal{G}\rangle$ such that X_1 and X_2 have different factorizations and $\rho^T X_1 \tau = \rho^T X_2 \tau$, therefore it is undecidable to determine if there exists two words $w_1, w_2 \in \Sigma'^*$ where $\Sigma' = \{h_i, g_i | 1 \leq i \leq n-2\}$ and $w_1 \neq w_2$, such that $L_{\mathcal{W}}(w_1) = L_{\mathcal{W}}(w_2)$. □

Example 3. *We consider in Fig. 1. the weighted automaton $\mathcal{W}$ corresponding to some $\gamma(u,v) \in \mathcal{G}$ in the proof of Theorem 3, where $u, v \in \Sigma^*$ is from the encoding of the PCP. In this example we consider a WFA over a unary input alphabet Σ_1. Recall that $\rho^T = (1,0,0)$ and $\tau^T = (0,0,1)$ are the vectors used in the proof to compute a value $\rho^T \gamma(u,v) \tau$, which corresponds to state '3' being the initial state and state '1' being the final state (with initial and final weights being identity).*

The cost value $L_{\mathcal{W}}(w)$ for a word $w \in \Sigma_1^+$ is thus $\alpha(u^{|w|}) + \beta(v^{|w|})$ as required.

$$\begin{pmatrix}1 & 0 & 0\end{pmatrix}\begin{pmatrix}x & y-x & \alpha(u)+\beta(v)\\ 0 & y & \beta(v)\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}0\\0\\1\end{pmatrix}$$

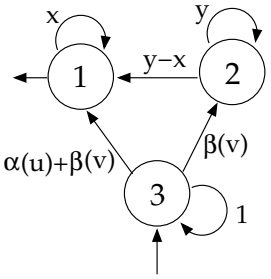

Figure 1: The matrix representation and WFA for a pair $\gamma(u,v)$, where $x=(n+1)^{|u|}$ and $y=(n+1)^{-|v|}$. The cost for a single letter is $\alpha(u)+\beta(v)$.

4. Ambiguity and Freeness over a Bounded Language

We now study the concept of scalar ambiguity, scalar freeness and vector ambiguity 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.

Hilbert's tenth problem is to determine if a given Diophantine equation $P(n_1,n_2,\ldots,n_k)=0$ has a solution for variables $n_1,n_2,\ldots n_k\in\mathbb{N}$ (P is thus 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. Putnam 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 [24]. We may restrict all the variables of the problem to be natural numbers without loss of generality, see [24, p.6].

The following corollary follows from the proof construction in Theorem 2 of [25].

Corollary 3. *[25] - 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, which follows from the undecidability of Hilbert's tenth problem.

Lemma 2. *Given two integer polynomials P_1 and P_2 over variables $(n_1,\ldots,n_k)$ 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 $P(n_2,\ldots,n_k)$ be an instance of Hilbert's tenth problem, i.e. a polynomial with integer coefficients and variables. Define $P_1(n_1,n_2,\ldots,n_k)=$

$(n_1^2+1)P(n_2,\ldots,n_k)$ and $P_2(n_1,n_2,\ldots,n_k) = (n_1^2+2)P(n_2,\ldots,n_k)$. Since $0 < n_1^2+1 < n_1^2+2$, we see that $P_1^2(n_1,n_2,\ldots,n_k) = P_2^2(n_1,n_2,\ldots,n_k)$ implies that $P_1^2(n_1,n_2,\ldots,n_k) = 0$ and $P_2^2(n_1,n_2,\ldots,n_k) = 0$, which then implies that $P(n_2,\ldots,n_k) = 0$, which is undecidable to determine [24]. This result holds for any value of n_1 since $n_1^2+1 \neq n_1^2+2$. We will use this property in the later proof. □

Now we show that the scalar freeness problem remains undecidable even over bounded languages. The problem can also be stated in terms of formal power series: given a formal power series r, determine if r has two equal coefficients. This problem was shown to be undecidable for formal power series over the integers in Theorem 8.15 of [16] and even over the natural numbers in Theorem 3.4 of [17].[4] We include the proof below, which uses a different encoding technique from [16, 17], for completeness and since the proof allows us to directly show the related *vector ambiguity problem* to be undecidable in Corollary 4.

Theorem 4. *The Scalar Freeness Problem over a bounded language of integer matrices is undecidable. In other words, given k matrices $M_1, M_2, \ldots, M_k \in \mathbb{Z}^{n\times n}$, generating a bounded language of matrices $M = M_1^* M_2^* \cdots M_k^*$, and two vectors $\rho, \tau \in \mathbb{Z}^n$, it is undecidable to decide if there exist $l_1, \ldots, l_k, r_1, \ldots, r_k \in \mathbb{N}$ 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 in 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 set of matrices $\{M_i \mid i = 0, ..., k+1\}$ encodes a polynomial P_1 and the set of matrices $\{N_i \mid i = 0, ..., k+1\}$ encodes 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 2.

Step 1. Given two integer coefficient polynomials P_1 and P_2 of same number of variables, from Corollary 3, 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 $L = x_1^* x_2^* \ldots x_k^* \subset \Sigma^*$.

[4] Note that the relevant theorems in [16, 17] do not specifically state that they hold for bounded languages, but the result can be easily derived by the technique used to encode rational formal power series into matrices [16].

Step 2. Given alphabets $K = \{0, 1, \ldots, k, k+1\}$ 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 $2 \leq i \leq k$. In the sequel, by abuse of notation, we use l_j, r_j to represent the words derived from the morphisms $l(j), r(j), 0 \leq j \leq k+1$. 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 for any word of the form $u = l_0^{j_0} l_1^{j_1} \cdots l_{k+1}^{j_{k+1}} r_0^{j_0'} r_1^{j_1'} \cdots r_{k+1}^{j_{k+1}'} \in L'$ which is *not* free, it has two factorizations, in one of which all $j_i = 0$ and in the other all $j_i' = 0$.

Note that no element of $\Gamma = \{l_t, r_t | 0 \leq t \leq (k+1)\}$ 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 $2 \leq p \leq k$. 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:

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

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

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

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 3:

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

and $\beta(\varepsilon) = 0$, where $n = |X| = k+4$. Moreover, we use a similar definition as in the proof of Theorem 3 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 injective mappings 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 $\rho = (\rho'^T, \rho''^T)^T, \tau = (\tau'^T, \tau''^T)^T, w_1, w_2 \in L, v_1, v_2 \in 0^*1^* \dots (k+1)^* \subseteq K^*$. 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 mutatis mutandis. 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 2, 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 2, which is undecidable.

Finally, from the above proof we know that if some scalar λ is not free, it must be that $\lambda = \rho^T X\tau = \rho^T Y\tau$, where $X = X_{i_1} X_{i_2} \cdots X_{i_t} \in \{M_i\}^*$ and $Y = Y_{i_1} Y_{i_2} \cdots Y_{i_t} \in \{N_i\}^*$. Since X and Y have the same number of factors, by Lemma 1, we may increase the size of the dimension by 1 and obtain the undecidability result instead for *integer matrices.* □

Theorem 5. *The Scalar Ambiguity Problem over a bounded language of integer matrices is undecidable.*

Proof. We can use the same idea as in the proof of Theorem 3, increasing the dimension of matrices M_i, N_i constructed in the proof of Theorem 4 to store an additional prime 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 4. *Vector ambiguity over a bounded language of integer matrices is undecidable.*

Proof. Follows from Theorem 5 in the case when only one vector τ is considered. Note that by Step 4 of Theorem 4, ambiguous scalars can be written in the form:

$$\lambda = \rho^T M_0 M_1^{p_1} \dots M_k^{p_k} M_{k+1} \tau = \rho^T N_0 N_1^{q_1'} \cdots N_k^{q_k'} N_{k+1} \tau. \quad (1)$$

Define $M_0' = \rho\rho^T M_0$ and $N_0' = \rho\rho^T N_0$. We thus see that:

$$\rho\lambda = M_0' M_1^{p_1} \dots M_k^{p_k} M_{k+1} \tau = N_0' N_1^{q_1'} \cdots N_k^{q_k'} N_{k+1} \tau = \rho\lambda,$$

thus if element λ is ambiguous then vector $\rho\lambda$ is ambiguous. Clearly if every λ is unique, then every $\rho\lambda$ is also unique and therefore the problem is undecidable over bounded language $M_0' M_1^{p_1} \cdots M_k^{p_k} M_{k+1} N_0' N_1^{q_1} \cdots N_k^{q_k} N_{k+1}$.

Note that if one defines $M_{k+1}' = M_{k+1}\tau\tau^T$ and $N_{k+1}' = N_{k+1}\tau\tau^T$, then Equation (1) implies that:

$$\rho\lambda\tau^T = M_0' M_1^{p_1} \dots M_k^{p_k} M_{k+1}' \tau = N_0' N_1^{q_1'} \cdots N_k^{q_k'} N_{k+1}' \tau = \rho\lambda\tau^T,$$

and thus matrix $\rho\lambda\tau^T$ has more than one factorization over bounded language $M_0' M_1^{p_1} \cdots M_k^{p_k} M_{k+1}' N_0' N_1^{q_1} \cdots N_k^{q_k} N_{k+1}'$. This is equivalent to showing that the freeness problem for matrices over a bounded language is undecidable. This result was proven with different methods in [1]. □

Corollary 5. *Given a Weighted Finite Automaton $\mathcal{W}$, and a bounded language L, determining if the output of $\mathcal{W}$ is distinct for every possible input word from language L is undecidable over the integers.*

Proof. Immediate from the proof of Corollary 2 when using the encoding of an instance of Hilbert's tenth problem from Theorem 5. □

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

Corollary 6. *The PFA freeness problem over a bounded language is undecidable.*

Proof. In this proof, we will construct a PFA (u, φ, v) over a bounded language L on an alphabet A. We will show that the problem to decide if 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 freeness problem and hence is undecidable. The proof uses a modification of the construction in Lemma 1 of [26]; see also [19, 20].

Define $\{M_i', N_i' | 0 \le i \le k+1\} \subseteq \mathbb{Z}^{(t-3)\times(t-3)}$ and $\rho', \tau' \in \mathbb{Z}^{t-3}$ to be the modified integer version of the matrices $\{M_i, N_i | 0 \le i \le k+1\}$ and vectors ρ, τ defined in the proof of Theorem 4, where $t > 3$ is the appropriate dimension. We increase the dimension of each M_i', N_i' and ρ', τ' by one by defining $M_i'' = tM_i' \oplus 1, N_i'' = tN_i' \oplus 1$, for each $0 \le i \le k+1$ and $\rho'' = \rho' \oplus 1, \tau'' = \tau' \oplus 1$.

Define the morphism $\zeta : A = \{a_0, a_1, \dots, a_{2k+3}\} \to \{M_i'', N_i''\}$ by

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

Then for a word $w \in A^*$, we have

$$\rho''^T \zeta(w) \tau'' = t^{|w|} \rho'^T X'_w \tau' + 1 = t^{|w|}\lambda + 1,$$

where X'_w is the matrix generated by M'_i, N'_i according to the word w and $\lambda = \rho'^T X'_w \tau' \in \mathbb{Z}$.

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

$$\zeta'(a_j) = \begin{pmatrix} 0 & 0 & 0 \\ p_j & \zeta(a_j) & 0 \\ r_j & q_j^T & 0 \end{pmatrix},$$

where $p_j, q_j \in \mathbb{Z}^{(t-2)}$ and $r_j \in \mathbb{Z}$ are chosen such that, for each $\zeta'(a_j)$, the row and column sums of $\zeta'(a_j)$ are all 0 (note that these values are well defined and unique).

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. Let $c \in \mathbb{Z}^+$ be chosen so that $\zeta'(a_j) + c\Delta$ is a strictly positive matrix for all $1 \le j \le 2k+3$, and define $\hat{\zeta} : A^* \to \mathbb{Z}_+^{t\times t}$ as

$$\hat{\zeta}(a_j) = \zeta'(a_j) + c\Delta \in \mathbb{N}_{>0}^{t\times t}.$$

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 $u = (0, \frac{1}{3}\rho''^T, 0)^T$ and $v = (0, \frac{1}{3}\tau''^T, 0)^T$, we have constructed a PFA (u, φ, v) over a bounded language $L = a_0^* a_1^* \dots a_{2k+3}^* \subseteq A^*$. Note that u, v have an L_1 norm of 1.

To see that the scalar freeness problem for PFA (u, φ, v) is undecidable, we note 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,

$$\begin{aligned} u^T\varphi(w)v &= u^T \left(\left(\frac{1}{ct}\right)^{|w|} \zeta'(w) + \left(\frac{1}{t}\right)^{|w|} \Delta^{|w|} \right) v \\ &= \left(\frac{1}{ct}\right)^{|w|} (\frac{1}{9}\rho''^T \zeta(w)\tau'') + u^T \left(\frac{\Delta}{t}\right) v \quad ;(\text{since } \Delta^{|W|} = t^{|W|-1}\Delta) \\ &= \frac{1}{9}\left(\frac{1}{ct}\right)^{|w|} (t^{|w|}\lambda + 1) + \frac{1}{t} \end{aligned}$$

Now assume there exist two different words $w_1, w_2 \in L$ with $u^T\varphi(w_1)v = u^T\varphi(w_2)v$. Then we have

$$\frac{1}{9}\left(\frac{1}{ct}\right)^{|w_1|} (t^{|w_1|}\lambda_1 + 1) + \frac{1}{t} = \frac{1}{9}\left(\frac{1}{ct}\right)^{|w_2|} (t^{|w_2|}\lambda_2 + 1) + \frac{1}{t} \qquad (2)$$

If $|w_1| = |w_2|$, since c and t are all fixed, we immediately get $\lambda_1 = \lambda_2$, which implies the corresponding scalar freeness problem has a solution.

If $|w_1| \neq |w_2|$, without lose of generality, we assume $|w_1| = y_1 < y_2 = |w_2|$. Then we get

$$c^{y_2-y_1}t^{y_2}\lambda_1 + (ct)^{y_2-y_1} = t^{y_2}\lambda_2 + 1,$$

But, $c^{y_2-y_1}t^{y_2}\lambda_1 + (ct)^{y_2-y_1} \mod t \equiv 0$ and $t^{y_2}\lambda_2 + 1 \mod t \equiv 1$, which gives a contradiction.

If there exist words $w_1, w_2 \in L$ such that $\rho''^T\zeta(w_1)\tau'' = \rho''^T\zeta(w_2)\tau''$ (thus the scalar freeness problem has a positive solution), then by the proof of Theorem 3, we know that $|w_1| = |w_2|$ and $\lambda_1 = \lambda_2$, therefore Equation (2) holds and therefore the PFA (u, φ, v) is not free. Hence the freeness problem for PFA over a bounded language is undecidable. □

Corollary 7. *The PFA freeness problem is undecidable for PFA with* 5 *states and an alphabet* A *of size* 16*.*

Proof. We use a combination of the techniques from Theorem 3 and Corollary 6. Theorem 3 shows how we can prove the scalar freeness problem is undecidable for vectors $\rho, \tau \in \mathbb{Q}^3$ and matrices $M_1, M_2, \ldots, M_{16} \in \mathbb{Q}^{3\times3}$. Using the Turakainen technique detailed in Corollary 6, we derive vectors $\rho', \tau' \in \mathbb{Q}^5$ and doubly stochastic matrices $M'_1, M'_2, \ldots, M'_{16} \in \mathbb{Q}^{5\times5}$, such that the initial vector is a probability distribution, which therefore defines a PFA.

Now, if there exist two words $w_1, w_2 \in A^*$ such that $w_1 \neq w_2$ and the acceptance probability of w_1 and w_2 is the same, then

$$\rho' M'_{w_1}\tau' = \rho' M'_{w_2}\tau' \Leftrightarrow \rho M_{w_1}\tau = \rho M_{w_2}\tau,$$

which is undecidable by Theorem 3. □

5. 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 (dimensions four and five respectively when considered over the integers). These two problems remain undecidable even over bounded languages, but require higher dimensions. Using these results, we showed the freeness problem for weighted and probabilistic finite automata is also undecidable, which appears to be of independent interest.

Acknowledgements

We thank the referees for their very careful reading of this manuscript, particularly the referee who pointed us to relevant references regarding Theorem 4.

References

[1] E. Charlier, J. Honkala, The freeness problem over matrix semigroups and bounded languages, Information and Computation 237 (2014) 243–256.

[2] V. Blondel, V. Canterini, Undecidable problems for probabilistic automata of fixed dimension, Theory of Computing Systems 36 (2003) 231–245.

[3] A. Bertoni, G. Mauri, M. Torelli, Some recursively unsolvable problems relating to isolated cutpoints in probabilistic automata, in: Automata, Languages and Programming, Vol. 52 of LNCS, 1977, pp. 87–94.

[4] M. S. Paterson, Unsolvability in 3×3 matrices, Studies in Applied Mathematics 49 (1) (1970) 105–107.

[5] D. Klarner, J.-C. Birget, W. Satterfield, On the undecidability of the freeness of integer matrix semigroups, International Journal of Algebra and Computation 1 (2) (1991) 223–226.

[6] J. Cassaigne, T. Harju, J. Karhumäki, On the undecidability of freeness of matrix semigroups, International Journal of Algebra and Computation 9 (3-4) (1999) 295–305.

[7] J. Cassaigne, F. Nicolas, On the decidability of semigroup freeness, RAIRO - Theoretical Informatics and Applications 46 (3) (2012) 355–399.

[8] C. Choffrut, J. Karhumäki, Some decision problems on integer matrices, Informatics and Applications 39 (2005) 125–131.

[9] P. C. Bell, I. Potapov, Reachability problems in quaternion matrix and rotation semigroups, Information and Computation 206 (11) (2008) 1353–1361.

[10] P. C. Bell, I. Potapov, Periodic and infinite traces in matrix semigroups, Current Trends in Theory and Practice of Computer Science (SOFSEM) LNCS 4910 (2008) 148–161.

[11] D. Krob, Some consequences of a fatou property of the tropical semiring, Journal of Pure and Applied Algebra 93 (3) (1994) 231–249.

[12] S. Almagor, U. Boker, O. Kupferman, What's decidable about weighted automata?, in: Automated Technology for Verification and Analysis, Vol. LNCS 6996, 2011, pp. 482–491.

[13] D. Krob, The equality problem for rational series with multiplicities in the tropical semiring is undecidable, International Journal of Algebra and Computation 4 (3) (1994) 405–425.

[14] K. Culik, J. Kari, Digital images and formal languages, Handbook of Formal Languages 3 (1997) 599–616.

[15] M. Droste, P. Gastin, Weighted automata and weighted logics, in: Automata, Languages and Programming, 2005, pp. 513–525.

[16] W. Kuich, A. Salomaa, Semirings, Automata, Languages, Vol. 5, Springer, 1986.

[17] J. Honkala, Decision problems concerning thinness and slenderness of formal languages, in: Acta Informatica, Vol. 35, 1998, pp. 625–636.

[18] A. Paz, Introduction to Probabilistic Automata, Academic Press, 1971.

[19] M. Hirvensalo, 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 (2007) 309–319.

[20] P. C. Bell, V. Halava, M. Hirvensalo, Decision problems for probabilistic finite automata on bounded languages, Fundamenta Informaticae 123 (1) (2012) 1–14.

[21] P. C. Bell, S. Chen, L. M. Jackson, Scalar ambiguity and freeness in matrix semigroups over bounded languages, in: Language and Automata Theory and Applications, Vol. LNCS 9618, 2016, pp. 493–505.

[22] J. Cassaigne, J. Karhumäki, T. Harju, On the decidability of the freeness of matrix semigroups, International Journal of Algebra and Computation 9 (3-4) (1999) 295–305.

[23] V. Halava, T. Harju, M. Hirvensalo, Undecidability bounds for integer matrices using Claus instances, International Journal of Foundations of Computer Science (IJFCS) 18,5 (2007) 931–948.

[24] Yu. Matiyasevich, Hilbert's Tenth Problem, MIT Press, 1993.

[25] P. C. Bell, V. Halava, T. Harju, J. Karhumäki, I. Potapov, Matrix equations and Hilbert's tenth problem, International Journal of Algebra and Computation 18 (2008) 1231–1241.

[26] P. Turakainen, Generalized automata and stochastic languages, Proceedings of the American Mathematical Society 21 (1969) 303–309.