


Acceptance Ambiguity for Quantum Automata

Paul C. Bell 

Department of Computer Science, Byrom Street, Liverpool John Moores University,
Liverpool, L3-3AF, UK
p.c.bell@ljmu.ac.uk

Mika Hirvensalo

Department of Mathematics and Statistics, University of Turku, FI-20014, Turku, Finland
mikhirve@utu.fi

Abstract

We consider notions of freeness and ambiguity for the acceptance probability of Moore-Crutchfield Measure Once Quantum Finite Automata (MO-QFA). We study the distribution of acceptance probabilities of such MO-QFA, which is partly motivated by similar freeness problems for matrix semigroups and other computational models. We show that determining if the acceptance probabilities of all possible input words are unique is undecidable for 32 state MO-QFA, even when all unitary matrices and the projection matrix are rational and the initial configuration is defined over real algebraic numbers. We utilize properties of the skew field of quaternions, free rotation groups, representations of tuples of rationals as a linear sum of radicals and a reduction of the mixed modification Post's correspondence problem.

2012 ACM Subject Classification Theory of computation → Quantum computation theory

Keywords and phrases Quantum finite automata, matrix freeness, undecidability, Post's correspondence problem, quaternions

Digital Object Identifier 10.4230/LIPIcs.MFCS.2019.70

Funding *Mika Hirvensalo*: Supported by Väisälä Foundation

1 Introduction

Measure-Once Quantum Finite Automata (MO-QFA) were introduced in [24] as a natural quantum variant of probabilistic finite automata. The model is defined formally in Section 3, but briefly a MO-QFA over an alphabet Σ is defined by a three tuple $\mathcal{Q} = (P, \{X_a | a \in \Sigma\}, u)$ where P is a projection matrix, X_a is a complex unitary matrix for each alphabet letter $a \in \Sigma$ and u is a unit length vector with respect to the Euclidean (ℓ^2) norm. Given an input word $w = w_1 \cdots w_k \in \Sigma^*$, then the acceptance probability $f_{\mathcal{Q}} : \Sigma^* \rightarrow \mathbb{R}$ of w under \mathcal{Q} is given by

$$f_{\mathcal{Q}}(w) = \|PX_{w_k} \cdots X_{w_1}u\|^2.$$

The related model of Probabilistic Finite Automata (PFA) with n states over an alphabet Σ is defined as $\mathcal{P} = (\mathbf{x}, \{M_a | a \in \Sigma\}, \mathbf{y})$ where $\mathbf{y} \in \mathbb{R}^n$ is the initial probability distribution (unit length under ℓ^1 norm); $\mathbf{x} \in \{0, 1\}^n$ is the final state vector and each $M_a \in \mathbb{R}^{n \times n}$ is a stochastic matrix. For a word $w = w_1 w_2 \cdots w_k \in \Sigma^*$, we define the acceptance probability $f_{\mathcal{P}} : \Sigma^* \rightarrow \mathbb{R}$ of \mathcal{P} as:

$$f_{\mathcal{P}}(w) = \mathbf{x}^T M_{w_k} M_{w_{k-1}} \cdots M_{w_1} \mathbf{y}.$$

For any $\lambda \in [0, 1]$ and automaton \mathcal{A} (either PFA or QFA) over alphabet Σ , we define a cut-point language to be: $L_{\geq \lambda}(\mathcal{A}) = \{w \in \Sigma^* | f_{\mathcal{A}}(w) \geq \lambda\}$, and a strict cut-point language $L_{> \lambda}(\mathcal{A})$ by replacing \geq with $>$. The (strict) emptiness problem for a cut-point language is to determine if $L_{\geq \lambda}(\mathcal{A}) = \emptyset$ (resp. $L_{> \lambda}(\mathcal{A}) = \emptyset$).



© Paul C. Bell and Mika Hirvensalo;
licensed under Creative Commons License CC-BY

44th International Symposium on Mathematical Foundations of Computer Science (MFCS 2019).

Editors: Peter Rossmanith, Pinar Heggernes, and Joost-Pieter Katoen; Article No. 70; pp. 70:1–70:14

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The MO-QFA model is very restricted due to unitarity constraints and can recognize only group languages (those regular languages whose syntactic monoid is a group [10]). Whereas the emptiness question for a strict cut-point stochastic languages is undecidable, it surprisingly becomes decidable for MO-QFA [9]. The decidability is established via the compactness of the group generated by unitary matrices: a compact algebraic group has a finite polynomial basis, and the decision procedure is then based on Tarski's quantifier elimination theorem [9].

Another surprising undecidability result was already manifested in [9]: The emptiness problem for non-strict (allowing equality) cut-point languages is undecidable. The sizes of the automata exhibiting undecidability were subsequently improved in [17]. As the aforementioned examples illuminate, the border between decidability and undecidability may be crossed with a minor modification to the model or premises.

Underlying each linear automata model are matrices, which represent the dynamics of the computational model as input symbols are read. For deterministic/nondeterministic finite automata, the underlying matrices are binary matrices; for weighted automata, the matrices are integer; for probabilistic automata the matrices are stochastic (the set of columns of each matrix should be a probability distribution); and for quantum finite automata, the matrices are unitary (the set of columns of each matrix should be orthonormal).

Reachability problems for matrix semigroups have attracted a great deal of attention over the past few years. Typically in such problems we are given a finite set of generating matrices \mathcal{G} forming a semigroup $\mathcal{S} = \langle \mathcal{G} \rangle$ and we ask some question about \mathcal{S} . As an example, it was shown even back in 1970 by M. Paterson that the mortality problem for integer matrix semigroups is undecidable in dimension three [25]. In this problem, $\mathcal{G} \subseteq \mathbb{Z}^{3 \times 3}$ and we ask whether the zero matrix belongs to $\mathcal{S} = \langle \mathcal{G} \rangle$. It was later shown that the similar identity problem (does the identity matrix belong to the semigroup generated by a given set of generating matrices) is also undecidable for four-dimensional integral matrices [5].

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} (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 $\mathbb{N}^{3 \times 3}$ in [20] and this result was improved by Cassaigne et al. to hold even for *upper-triangular* matrices over $\mathbb{N}^{3 \times 3}$ in [11].

There are many open problems related to freeness in 2×2 matrices; see [12, 13, 14] 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 [13].

The freeness problem for matrix semigroups defined by a *bounded language* was recently studied. Given a finite set of matrices $\{M_1, \dots, M_k\} \subseteq \mathbb{Q}^{n \times n}$, we define a bounded language of matrices to be of the form: $\{M_1^{j_1} \cdots M_k^{j_k} \mid j_i \geq 0 \text{ where } 1 \leq i \leq k\}$.

The freeness problem for such a bounded language of matrices asks if there exists a choice of these variables such that $j_1, \dots, j_k, j'_1, \dots, j'_k \geq 0$, 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 [13].

In a similar vein, we may study the vector freeness and ambiguity problems, where we are given a finite set of matrices $\mathcal{G} \subseteq \mathbb{F}^{n \times n}$ and a vector $u \in \mathbb{F}^n$. The *ambiguity problem* is to determine whether there exists two matrices $M_1, M_2 \in \mathcal{S} = \langle \mathcal{G} \rangle$ with $M_1 \neq M_2$ such that $M_1 u = M_2 u$ and the *freeness problem* is to determine the uniqueness of factorizations of $\{M u \mid M \in \mathcal{S}\}$ i.e., does $M_{i_1} \cdots M_{i_k} u = M_{j_1} \cdots M_{j_k} u$, where each $M_i \in \mathcal{G}$, imply that

$k = k'$ and $M_{i_r} = M_{j_r}$ for $1 \leq r \leq k$? It should be noted that these (related but distinct) problems are more difficult to solve than freeness for matrix semigroups, since by multiplying matrix M_1 and M_2 with u , some information may be lost. The motivation for such a problem is that many linear dynamic systems/computational models are defined in this way. The freeness question now asks whether starting from some initial point, we have two separate computational paths which coincide at some later point, or else whether every configuration starting from u is unique. Such vector ambiguity and freeness questions were studied in [3] and the problems were shown to be undecidable when $\mathcal{S} \subseteq \mathbb{Z}^{4 \times 4}$, or when $\mathcal{S} \subseteq \mathbb{Q}^{3 \times 3}$. The NP-completeness of the vector ambiguity and freeness problems for $\text{SL}(2, \mathbb{Z})$ was recently shown in [21] (where $\text{SL}(2, \mathbb{Z})$ is the special linear group of 2×2 matrices).

Whilst vector reachability questions are interesting from the point of view of dynamical systems, many computational models have the notion of a projection being taken at the end, in order to determine whether a computation path is successful or not. This usually takes the form of defining a partition of configurations into accepting or nonaccepting states. This leads to the notion of *scalar reachability* (also known as half-space reachability [15]), which may be defined in terms of *two* vectors, u and v , where we now study the set of scalars $\{u^T M v \mid M \in \mathcal{S}\}$. The *scalar ambiguity* question then asks whether or not this set of scalars is unique i.e., does there exist two matrices $M_1, M_2 \in \mathcal{S}$ with $M_1 \neq M_2$ such that $u^T M_1 v = u^T M_2 v$? The difficulty with extending the undecidability result for vector reachability is that all information about each matrix M needs to be stored within a single scalar value $u^T M v$ in a unique way.

In [1], the freeness problem (defined formally in Section 3.1) for 4-state weighted and 6-state probabilistic automata was shown to be undecidable together with results concerning the related ambiguity problem. The undecidability result was shown to hold even when the input words come from a bounded language, thus the matrices appear in some fixed order, and are taken to an arbitrary power. 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 [22] and Theorem 3.4 of [18]. As mentioned above, several reachability problems for PFA (such as emptiness of cut-point languages) are known to be *undecidable* [26], even in a fixed dimension [8, 17]. 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 [2]. We may note that the scalar freeness and ambiguity problems are a similar concept to the *threshold isolation problem* which asks whether a given cutpoint may be approached arbitrarily closely and which is known to be undecidable [6, 8].

It is therefore natural to ask whether the *freeness and ambiguity problems* are undecidable for MO-QFA. This problem appears more difficult to prove than for weighted/probabilistic automata, since the acceptance probability of a MO-QFA \mathcal{Q} has the form $f_{\mathcal{Q}}(w) = \|PX^R u\|^2$ and it is thus difficult to encode sufficient information about the matrix X within $f_{\mathcal{Q}}(w)$ to guarantee uniqueness of matrices from \mathcal{G} . We show that freeness and ambiguity are undecidable for 32 (resp. 33) state MO-QFA by using an encoding of the mixed modification Post's Correspondence Problem and a result related to linear independence of rationals of a basis of squarefree radicals as well as techniques from linear algebra and properties of quaternions.

2 Notation

Let $\Sigma = \{x_1, x_2, \dots, x_k\}$ be a finite set of *letters* called an *alphabet*. A word w is a finite sequence of letters from Σ , the set of all words over Σ is denoted Σ^* and the set of nonempty words is denoted Σ^+ . The *empty word* is denoted by ε . We use $|u|$ to denote the length of a word u and thus $|\varepsilon| = 0$. For two words $u = u_1u_2 \cdots u_i$ and $v = v_1v_2 \cdots v_j$, where $u, v \in \Sigma^*$, the concatenation of u and v is denoted by $u \cdot v$ (or by uv for brevity) such that $u \cdot v = u_1u_2 \cdots u_iv_1v_2 \cdots v_j$. Word $u^R = u_i \cdots u_2u_1$ denotes the mirror image or reverse of word u . A subset L of Σ^* is called a *language*. A language $L \subseteq \Sigma^*$ is called a *bounded language* if and only if there exist words $w_1, w_2, \dots, w_m \in A^+$ such that $L \subseteq w_1^*w_2^* \cdots w_m^*$. Given an alphabet Σ as above, we denote by Σ^{-1} the set $\{x_1^{-1}, \dots, x_k^{-1}\}$, where each x_i^{-1} is a new letter with the property that $x_ix_i^{-1} = x_i^{-1}x_i = \varepsilon$ are the only identities of the group $\langle \Sigma \cup \Sigma^{-1} \rangle$. A word $w = w_1w_2 \cdots w_i \in (\Sigma \cup \Sigma^{-1})^*$ is called *reduced* if there does not exist $1 \leq j < i$ such that $w_{j+1} = w_j^{-1}$; i.e., no two consecutive letters are inverse.

Given any two rings R_1 and R_2 we use the notation $R_1 \hookrightarrow R_2$ to denote a *monomorphism* i.e., an injective homomorphism between R_1 and R_2 . Given a finite set \mathcal{G} , we use the notation $\langle \mathcal{G} \rangle$ (resp. $\langle \mathcal{G} \rangle_{\text{gp}}$) to denote the *semigroup* (resp. *group*) generated by \mathcal{G} .

Semirings and quaternions

We denote by \mathbb{N} the natural numbers, \mathbb{Z} the integers, \mathbb{Q} the rationals, \mathbb{C} the complex numbers and \mathbb{H} the quaternions. We denote by $\mathbb{C}(\mathbb{Q})$ the complex numbers with rational parts, by $\mathbb{H}(\mathbb{Q})$ the quaternions with rational parts and by $\mathbb{A}_{\mathbb{R}}$ the real algebraic numbers.

Given any semiring \mathbb{F} we denote by $\mathbb{F}^{i \times j}$ the set of $i \times j$ matrices over \mathbb{F} . We denote by e_i the i 'th basis vector of some dimension (which will be clear from the context).

In a similar style to complex numbers, a rational quaternion $\vartheta \in \mathbb{H}(\mathbb{Q})$ can be written $\vartheta = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ where $a, b, c, d \in \mathbb{Q}$. To ease notation let us define the vector: $\mu = (1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ and it is now clear that $\vartheta = (a, b, c, d) \cdot \mu$ where \cdot denotes the inner or “dot” product.

Quaternion addition is simply the componentwise addition of elements. It is well known that quaternion multiplication is not commutative (hence they form a skew field). Multiplication is completely defined by the equations $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$, $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$, $\mathbf{jk} = \mathbf{i} = -\mathbf{kj}$ and $\mathbf{ki} = \mathbf{j} = -\mathbf{ki}$. Thus for two quaternions $\vartheta_1 = (a_1, b_1, c_1, d_1)\mu$ and $\vartheta_2 = (a_2, b_2, c_2, d_2)\mu$, we can define their product as $\vartheta_1\vartheta_2 = (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)\mathbf{i} + (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)\mathbf{j} + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\mathbf{k}$.

In a similar way to complex numbers, we define the conjugate of $\vartheta = (a, b, c, d) \cdot \mu$ by $\bar{\vartheta} = (a, -b, -c, -d) \cdot \mu$. We can now define a norm on the quaternions by $\|\vartheta\| = \sqrt{\vartheta\bar{\vartheta}} = \sqrt{a^2 + b^2 + c^2 + d^2}$. Any non zero quaternion has a multiplicative (and obviously an additive) inverse [23]. The other properties of being a skew field can be easily checked.

A *unit* quaternion (norm 1) corresponds to a rotation in three dimensional space [23].

Linear Algebra

Given $A = (a_{ij}) \in \mathbb{F}^{m \times m}$ and $B \in \mathbb{F}^{n \times n}$, we define the direct sum $A \oplus B$ and Kronecker product $A \otimes B$ of A and B by:

$$A \oplus B = \left[\begin{array}{c|c} A & \mathbf{0}_{m,n} \\ \hline \mathbf{0}_{n,m} & B \end{array} \right], \quad A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{bmatrix},$$

where $\mathbf{0}_{i,j}$ denotes the zero matrix of dimension $i \times j$. Note that neither \oplus nor \otimes are commutative in general. Given a finite set of matrices $\mathcal{G} = \{G_1, G_2, \dots, G_m\} \subseteq \mathbb{F}^{n \times n}$, $\langle \mathcal{G} \rangle$ is the semigroup generated by \mathcal{G} . We will use the following notations:

$$\bigoplus_{j=1}^m G_j = G_1 \oplus G_2 \oplus \dots \oplus G_m, \quad \bigotimes_{j=1}^m G_j = G_1 \otimes G_2 \otimes \dots \otimes G_m.$$

Given a single matrix $G \in \mathbb{F}^{n \times n}$, we inductively define $G^{\otimes k} = G \otimes G^{\otimes(k-1)} \in \mathbb{F}^{n^k \times n^k}$ with $G^{\otimes 1} = G$ as the k -fold Kronecker power of G . Similarly, $G^{\oplus k} = G \oplus G^{\oplus(k-1)} \in \mathbb{F}^{n^k \times n^k}$ with $G^{\oplus 1} = G$. The following properties of \oplus and \otimes are well known; see [19] for proofs.

► **Lemma 1.** *Let $A, B, C, D \in \mathbb{F}^{n \times n}$. We note that:*

- $(A \otimes B) \otimes C = A \otimes (B \otimes C)$ and $(A \oplus B) \oplus C = A \oplus (B \oplus C)$, thus $A \otimes B \otimes C$ and $A \oplus B \oplus C$ are unambiguous.
- *Mixed product properties:* $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$ and $(A \oplus B)(C \oplus D) = (AC) \oplus (BD)$.
- *If A and B are unitary matrices, then so are $A \oplus B$ and $A \otimes B$.*

Given two vectors $u \in \mathbb{F}^{n_1}$ and $v \in \mathbb{F}^{n_2}$, we define $u \oplus v \in \mathbb{F}^{n_1+n_2}$ as $u \oplus v = (u_1, \dots, u_{n_1}, v_1, \dots, v_{n_2})$.

3 Quantum Finite Automata and Undecidability

► **Definition 2.** *A measure-once n -state quantum automaton (MO-QFA) over a k -letter alphabet Σ is a triplet $(P, \{X_a \mid a \in \Sigma\}, u)$, where $P \in \mathbb{C}^{n \times n}$ is a projection, each $X_a \in \mathbb{C}^{n \times n}$ is a unitary matrix (where rows form an orthonormal set), and $u \in \mathbb{C}^n$ is a unit-length vector.*

A morphism $\Sigma^ \rightarrow \langle X_a \rangle$ is defined as $w = a_{i_1} \dots a_{i_t} \mapsto X_w \stackrel{\text{def}}{=} X_{i_1} \dots X_{i_t}$ and the acceptance probability of a MO-QFA \mathcal{Q} is defined as $f_{\mathcal{Q}}(w) = \|PX_w u\|^2$. We use the reverse of the word w , denoted w^R , so that w_1 is applied first, then w_2 etc.*

3.1 Ambiguity and Freeness for QFA

Consider a finite set of unitary matrices $\mathcal{G} = \{X_1, X_2, \dots, X_k\} \subset \mathbb{C}^{n \times n}$, a projection matrix $P \in \mathbb{Z}^{n \times n}$ and a unit column vector $u \in \mathbb{C}^n$. Let $\mathcal{Q} = (P, \mathcal{G}, u)$ be a QFA and define $\Lambda(\mathcal{Q})$ be the set of scalars such that $\Lambda(\mathcal{Q}) = \{\|PXu\|^2; X \in \langle \mathcal{G} \rangle\}$. If for $\lambda \in \Lambda(\mathcal{Q})$ there exists a unique matrix $X \in \langle \mathcal{G} \rangle$ such that $\lambda = \|PXu\|^2$, then we say that λ is *unambiguous* with respect to \mathcal{Q} . We call $\Lambda(\mathcal{Q})$ unambiguous if every $\lambda \in \Lambda(\mathcal{Q})$ is unambiguous.

An acceptance probability $\lambda \in \Lambda(\mathcal{Q})$ is called *free* with respect to \mathcal{Q} if

$$\lambda = \|PX_{i_1} X_{i_2} \dots X_{i_m} u\|^2 = \|PX_{j_1} X_{j_2} \dots X_{j_{m'}} u\|^2,$$

where each $X_{i_k}, X_{j_{k'}} \in \mathcal{G}$ for $1 \leq k \leq m$ and $1 \leq k' \leq m'$ implies that $m = m'$ and each $i_k = j_k$ for $1 \leq k \leq m$. We call $\Lambda(\mathcal{Q})$ free if every $\lambda \in \Lambda(\mathcal{Q})$ is free.

► **Problem 3** (QFA Scalar Ambiguity). *Given a Quantum Finite Automaton \mathcal{Q} , is $\Lambda(\mathcal{Q})$ unambiguous?*

► **Problem 4** (QFA Scalar Freeness¹). *Given a Quantum Finite Automaton \mathcal{Q} , is $\Lambda(\mathcal{Q})$ free?*

¹ We may also call this the *injectivity problem* for QFA; does there exist two distinct words $w_1, w_2 \in \Sigma^*$ such that $f_{\mathcal{Q}}(w_1) = f_{\mathcal{Q}}(w_2)$?

► **Example 5.** Let $A = \begin{pmatrix} \frac{3}{5} & \frac{4}{5} \\ -\frac{4}{5} & \frac{3}{5} \end{pmatrix}$, $P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $u = (1, 0)^T$. We thus see that $\mathcal{Q} = (P, \{A\}, u)$ is a unary 2-state QFA. Note that A represents rotations of the Euclidean plane of angle $\arccos(3/5)$, and thus we see that $f_{\mathcal{Q}}(a^k) = \|PA^k u\|^2$ is dense in $[0, 1]$ for $k \in \mathbb{N}$. Since the angle of rotation of A is an irrational multiple of π , then every acceptance probability of \mathcal{Q} is unique, and thus \mathcal{Q} is both free and unambiguous.

We show that freeness and ambiguity are undecidable for MO-QFA in Section 5. The reduction is from the Mixed Modification Post's Correspondence Problem, now defined.

► **Problem 6 (Mixed Modification PCP (MMPCP)).** *Given set of letters $\Sigma = \{s_1, \dots, s_{|\Sigma|}\}$, binary alphabet Σ_2 , and pair of homomorphisms $h, g : \Sigma^* \rightarrow \Sigma_2^*$, the MMPCP asks to decide whether there exists a word $w = x_1 \cdots x_k \in \Sigma^+$, $x_i \in \Sigma$ such that*

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

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

► **Theorem 7.** [11] - *The Mixed Modification PCP is undecidable for $|\Sigma| \geq 9$.*

► **Definition 8.** *We call an instance of the (MM)PCP a Claus instance if the minimal solution words are of the form $w = s_1 x_2 x_3 \cdots x_{k-1} s_{|\Sigma|}$, where $x_2, \dots, x_{k-1} \in \Sigma - \{s_1, s_{|\Sigma|}\}$, i.e., the minimal solution words must start with letter s_1 , end with letter $s_{|\Sigma|}$, and all other letters are not equal to s_1 or $s_{|\Sigma|}$.*

In fact most proofs of the undecidability of (MM)PCP have this property [16]. Claus instances can be useful for decreasing the resources required for showing certain undecidability results, and we use this property later.

► **Theorem 9.** [16] - *Mixed Modification PCP is undecidable for Claus instances, when $|\Sigma| \geq 9$.²*

4 A mapping from arbitrary words to rational unitary matrices

Let $\Sigma_n = \{x_1, x_2, \dots, x_n\}$ be an n -letter alphabet for some $n > 0$. We begin by deriving a monomorphism $\gamma : \Sigma_n^* \hookrightarrow \mathbb{Q}^{4 \times 4}$ such that $\gamma(w)$ is a unitary matrix for any $w \in \Sigma_n^*$. The mapping γ will be a composition of several monomorphisms.

Given alphabet $\Sigma_n = \{x_1, x_2, \dots, x_n\}$, we now show that there exists a monomorphism $\gamma : \Sigma_n^* \hookrightarrow \mathbb{Q}^{4 \times 4}$ where $\gamma(w)$ is unitary for all $w \in \Sigma_n^*$.

We first describe a monomorphism γ_1 from an arbitrary sized alphabet to a binary alphabet. We then show monomorphism γ_2 from a binary alphabet to unit quaternions, and conclude by injectively mapping such quaternions to unitary matrices.

γ_1 : Let $\Sigma_2 = \{a, b\}$ be a binary alphabet. We define $\gamma_1 : \Sigma_n^* \hookrightarrow \Sigma_2^*$ by $\gamma_1(x_k) = a^k b$ for $1 \leq k \leq n$. It is immediate that γ_1 is injective.

γ_2 : Define mapping $\gamma_2 : \Sigma_2^* \hookrightarrow \mathbb{H}(\mathbb{Q})$ by $\gamma_2(a) = \left(\frac{3}{5}, \frac{4}{5}, 0, 0\right) \cdot \mu$ and $\gamma_2(b) = \left(\frac{3}{5}, 0, \frac{4}{5}, 0\right) \cdot \mu$.

It is known that γ_2 is an injective homomorphism [4] since such quaternions represent rotations about perpendicular axes by a rational angle (not equal to $0, \pm\frac{1}{2}, \pm 1$), thus $\gamma_2 : \Sigma_2^* \hookrightarrow \mathbb{H}(\mathbb{Q})$ and $\gamma_2(w_1) = \gamma_2(w_2)$ for $w_1, w_2 \in \Sigma_2^*$ implies that $w_1 = w_2$ [27].

² The result in [16] states undecidability for $|\Sigma| \geq 7$ since they fix the first/last letters of a potential solution.

γ_3 : Define $\gamma_3 : \mathbb{H}(\mathbb{Q}) \hookrightarrow \mathbb{Q}^{4 \times 4}$ by:

$$\gamma_3((r, x, y, z) \cdot \mu) = \begin{pmatrix} r & x & y & z \\ -x & r & z & -y \\ -y & -z & r & x \\ -z & y & -x & r \end{pmatrix}. \quad (1)$$

It is well known that γ_3 is a monomorphism in this case. Injectivity is clear, and using the rules of quaternion multiplication shows that γ_3 is a homomorphism.

We finally define $\gamma = \gamma_3 \circ \gamma_2 \circ \gamma_1$ and thus by the above reasoning $\gamma : \Sigma_n^* \hookrightarrow \mathbb{Q}^{4 \times 4}$ is an injective homomorphism. Note that the matrix $\gamma(w)$ for a word $w \in \Sigma_n^*$ contains quite a lot of redundancy, and in fact can be uniquely described by just four elements (the top row) as is shown by the matrix in Eqn. (1). Of course, these four elements simply correspond to the four elements of the quaternion used in the construction of γ . Note also that $\gamma(w)$ is a unitary matrix since γ_2 generates a *unit quaternion* (of norm 1) in each case.

Using γ , we can now find matrices $A, B \in \mathbb{Q}^{4 \times 4}$, such that $\gamma(w) \in \langle \{A, B\} \rangle_{\text{gp}}$ for all $w \in \Sigma_n^*$; i.e., the value of $\gamma(w)$ lies within the semigroup generated by $\{A, B\}$. This will prove useful later since we may reason about the structure of this freely presented semigroup.

► **Definition 10.** Given $\Sigma_2 = \{a, b\}$, then let:

$$A = \gamma_3(\gamma_2(a)) = \begin{pmatrix} \frac{3}{5} & \frac{4}{5} & 0 & 0 \\ -\frac{4}{5} & \frac{3}{5} & 0 & 0 \\ 0 & 0 & \frac{3}{5} & \frac{4}{5} \\ 0 & 0 & -\frac{4}{5} & \frac{3}{5} \end{pmatrix}, B = \gamma_3(\gamma_2(b)) = \begin{pmatrix} \frac{3}{5} & 0 & \frac{4}{5} & 0 \\ 0 & \frac{3}{5} & 0 & -\frac{4}{5} \\ -\frac{4}{5} & 0 & \frac{3}{5} & 0 \\ 0 & \frac{4}{5} & 0 & \frac{3}{5} \end{pmatrix},$$

and define $\Gamma' = \langle \{A, B\} \rangle \subset \mathbb{Q}^{4 \times 4}$, which is a free semigroup (freely generated by $\{A, B\}$). All elements in the range of γ thus belong to Γ' . We define $\Gamma \subset \Gamma'$ by $\Gamma = \{\gamma(w) | w \in \Sigma_n^*\}$.

5 Freeness and ambiguity for QFA with radicals

In order to prove that the ambiguity and freeness problems are undecidable for QFA defined over rationals (with real algebraic initial vector), we require the following (folklore) theorem. This will essentially allow us to uniquely represent a tuple of rationals as a linear sum of radicals. For completeness, we will show a simple proof of this theorem using the theory of field extensions.

► **Theorem 11 ([7]).** *The (finite) set*

$$\mathcal{S} = \{\sqrt{m_1}, \dots, \sqrt{m_n} : m_i \text{ are coprime square-free numbers}\}$$

is linearly independent over \mathbb{Q} .

Proof. Define $E_k = \mathbb{Q}(\sqrt{m_1}, \dots, \sqrt{m_k})$, so $E_0 = \mathbb{Q}$ and $E_1 = \mathbb{Q}(\sqrt{m_1})$. Clearly $[E_0 : \mathbb{Q}] = 1 = 2^0$, and $[E_1 : \mathbb{Q}] = 2^1$. As each element $\sqrt{m_i}$ satisfies a quadratic equation over \mathbb{Q} , the field extension degree $[E_n : \mathbb{Q}]$ is at most 2^n . The theorem is proven if we can show that $[E_n : \mathbb{Q}] = 2^n$.

Assume the induction hypothesis true for values less than k . We will prove it true for $k + 1$, as well, i.e., $[E_{k+1} : E_k] = 2$. For this aim, we must demonstrate that $\sqrt{m_{k+1}} \notin E_k$, so let us assume the contrary, that

$$\sqrt{m_{k+1}} \in E_k = E_{k-1}(\sqrt{m_k}),$$

hence $\sqrt{m_{k+1}} = a + b\sqrt{m_k}$, where $a, b \in E_{k-1}$. Then

$$m_{k+1} = a^2 + m_k b^2 + 2ab\sqrt{m_k}.$$

If $ab \neq 0$, then $\sqrt{m_k} \in E_{k-1}$, which implies that $[E_k : E_{k-1}] = 1$, a contradiction.

If $a = 0$, then $\sqrt{m_{k+1}} = b\sqrt{m_k}$, and hence $\sqrt{m_k}\sqrt{m_{k+1}} = bm_k \in E_{k-1}$. By the induction hypothesis we then have

$$[\mathbb{Q}(\sqrt{m_1}, \dots, \sqrt{m_{k-1}}, \sqrt{m_k m_{k+1}}) : \mathbb{Q}] = 2^k,$$

but since the last extending element belongs to E_{k-1} , the extension degree cannot be more than 2^{k-1} , a contradiction. Here we actually need the assumption that the numbers are coprime, since otherwise $m_k m_{k+1}$ would not necessarily be squarefree.

If $b = 0$, then $\sqrt{m_{k+1}} \in E_{k-1}$, and as above, the induction hypothesis gives

$$[\mathbb{Q}(\sqrt{m_1}, \dots, \sqrt{m_{k-1}}, \sqrt{m_{k+1}}) : \mathbb{Q}] = 2^k,$$

but as the last extending element belongs to E_{k-1} , the extension degree cannot be more than 2^{k-1} , a contradiction. \blacktriangleleft

For example, given $p_1, p_2, q_1, q_2 \in \mathbb{Q}$, then the equality $p_1\sqrt{2} + q_1\sqrt{3} = p_2\sqrt{2} + q_2\sqrt{3}$ is true iff $p_1 = p_2$ and $q_1 = q_2$.

The following technical lemma concerns the free group \mathcal{S} generated by $\mathcal{G} = \{\gamma_2(a), \gamma_2(b)\}$ and will crucially allow us to characterise elements of \mathcal{S} which differ only in the signs of one or more of their imaginary components. To define this lemma we require a nonstandard inversion function defined on elements of $\mathcal{S} = \langle \mathcal{G} \rangle_{gr}$. Since \mathcal{S} is free, any reduced (i.e., not containing consecutive inverses) $q_w \in \mathcal{S}$ can be uniquely written in the form

$$q_w = \gamma_2(a)^{k_0} \gamma_2(b)^{k_1} \gamma_2(a)^{k_2} \dots \gamma_2(a)^{k_{n-2}} \gamma_2(b)^{k_{n-1}} \gamma_2(a)^{k_n},$$

where $k_0, k_n \in \mathbb{Z}$ and $k_1, \dots, k_{n-1} \in \mathbb{Z} - \{0\}$, i.e., an alternating product of either positive or negative powers of $\gamma_2(a)$ and $\gamma_2(b)$ which may start and end with either element. We define the following three functions:

- i) $\lambda_a(q_w) = \gamma_2(a)^{-k_0} \gamma_2(b)^{k_1} \gamma_2(a)^{-k_2} \dots \gamma_2(a)^{-k_{n-2}} \gamma_2(b)^{k_{n-1}} \gamma_2(a)^{-k_n}$;
- ii) $\lambda_b(q_w) = \gamma_2(a)^{k_0} \gamma_2(b)^{-k_1} \gamma_2(a)^{k_2} \dots \gamma_2(a)^{k_{n-2}} \gamma_2(b)^{-k_{n-1}} \gamma_2(a)^{k_n}$;
- iii) $\lambda_{a,b}(q_w) = \gamma_2(a)^{-k_0} \gamma_2(b)^{-k_1} \gamma_2(a)^{-k_2} \dots \gamma_2(a)^{-k_{n-2}} \gamma_2(b)^{-k_{n-1}} \gamma_2(a)^{-k_n}$.

These three functions thus invert all $\gamma_2(a)$ elements in a product for λ_a , all $\gamma_2(b)$ elements in a product for λ_b and both $\gamma_2(a)$ and $\gamma_2(b)$ elements in a product for $\lambda_{a,b}$. As an example, if $q_w = \gamma_2(a)^3 \gamma_2(b)^2 \gamma_2(a)^{-4} \gamma_2(b)$, then $\lambda_a(q_w) = \gamma_2(a)^{-3} \gamma_2(b)^2 \gamma_2(a)^4 \gamma_2(b)$, $\lambda_b(q_w) = \gamma_2(a)^3 \gamma_2(b)^{-2} \gamma_2(a)^{-4} \gamma_2(b)^{-1}$ and $\lambda_{a,b}(q_w) = \gamma_2(a)^{-3} \gamma_2(b)^{-2} \gamma_2(a)^4 \gamma_2(b)^{-1}$. Bizarre as such a definition may appear, it allows us to exactly characterize those elements of \mathcal{S} which differ only in the sign of one or more of their imaginary components, as we now show.

► Lemma 12. *Given a quaternion $q_w = \gamma_2(w) = (r, x, y, z) \cdot \mu \in \langle \gamma_2(a), \gamma_2(b) \rangle_{gr}$ with $w = w_1 w_2 \dots w_{|w|}$, each $w_i \in (\Sigma_2 \cup \Sigma_2^{-1})$ and $\Sigma_2 = \{a, b\}$, then:*

- i) $q_{w^R} = \gamma_2(w^R) = (r, x, y, -z) \cdot \mu$;
- ii) $\lambda_a(q_w) = (r, -x, y, -z) \cdot \mu$;
- iii) $\lambda_b(q_w) = (r, x, -y, -z) \cdot \mu$;
- iv) $\lambda_{a,b}(q_w) = (r, -x, -y, z) \cdot \mu$.

Proof. We proceed via induction. For the base case, when $w = \varepsilon$, then $q_w = (1, 0, 0, 0) \cdot \mu$ and $q_{w^R} = \lambda_a(q_w) = \lambda_b(q_w) = \lambda_{a,b}(q_w) = (1, 0, 0, 0) \cdot \mu$ and so the properties (trivially) hold. For the induction hypothesis, assume $i) - iv)$ are true for q_w . We handle each property individually.

i) By assumption, $q_{w^R} = (r, x, y, -z) \cdot \mu$. Since $\gamma_2(a) = (\frac{3}{5}, \frac{4}{5}, 0, 0) \cdot \mu$ and $\gamma_2(b) = (\frac{3}{5}, 0, \frac{4}{5}, 0) \cdot \mu$, by the rules of quaternion multiplication, we see that:

$$\begin{aligned}\gamma_2(a) \cdot q_w &= \frac{1}{5} (3r - 4x, 3x + 4r, 3y - 4z, 3z + 4y) \cdot \mu, \\ q_{w^R} \cdot \gamma_2(a) &= \frac{1}{5} (3r - 4x, 3x + 4r, 3y - 4z, -3z - 4y) \cdot \mu\end{aligned}$$

Note that the fourth component is negated as expected. In a similar way, we also see that:

$$\begin{aligned}\gamma_2(b) \cdot q_w &= \frac{1}{5} (3r - 4y, 3x + 4z, 3y + 4r, 3z - 4x) \cdot \mu, \\ q_{w^R} \cdot \gamma_2(b) &= \frac{1}{5} (3r - 4y, 3x + 4z, 3y + 4r, -3z + 4x) \cdot \mu\end{aligned}$$

with negated fourth element. Since $\gamma_2(a^{-1}) = (\frac{3}{5}, -\frac{4}{5}, 0, 0) \cdot \mu$ and $\gamma_2(b^{-1}) = (\frac{3}{5}, 0, -\frac{4}{5}, 0) \cdot \mu$, then the property of the fourth element being negated is also clearly true for $\gamma_2(c^{-1}) \cdot q_w$ and $q_{w^R} \cdot \gamma_2(c^{-1})$ for $c \in \{a, b\}$. The other properties are similar, we give a brief proof of each.

ii) By the induction hypothesis, $\lambda_a(q_w) = (r, -x, y, -z) \cdot \mu$ and thus:

$$\begin{aligned}q_w \cdot \gamma_2(a) &= \frac{1}{5} (3r - 4x, 3x + 4r, 3y + 4z, 3z - 4y) \cdot \mu, \\ \lambda_a(q_w) \cdot \gamma_2(a)^{-1} &= \frac{1}{5} (3r - 4x, -3x - 4r, 3y + 4z, -3z + 4y) \cdot \mu,\end{aligned}$$

with the second and fourth components negated as required. Also,

$$\begin{aligned}q_w \cdot \gamma_2(a)^{-1} &= \frac{1}{5} (3r + 4x, 3x - 4r, 3y - 4z, 3z + 4y) \cdot \mu, \\ \lambda_a(q_w) \cdot \gamma_2(a) &= \frac{1}{5} (3r + 4x, -3x + 4r, 3y - 4z, -3z - 4y) \cdot \mu,\end{aligned}$$

as expected. Right multiplication of q_w and $\lambda_a(q_w)$ by either $\gamma_2(b)$ or $\gamma_2(b)^{-1}$ retains the given structure, as is not difficult to calculate.

iii) By the induction hypothesis, $\lambda_b(q_w) = (r, x, -y, -z) \cdot \mu$ and thus:

$$\begin{aligned}q_w \cdot \gamma_2(b) &= \frac{1}{5} (3r - 4y, 3x - 4z, 3y + 4r, 3z + 4x) \cdot \mu, \\ \lambda_b(q_w) \cdot \gamma_2(b)^{-1} &= \frac{1}{5} (3r - 4y, 3x - 4z, -3y - 4r, -3z - 4x) \cdot \mu,\end{aligned}$$

with the third and fourth components negated as required. Also,

$$\begin{aligned}q_w \cdot \gamma_2(b)^{-1} &= \frac{1}{5} (3r + 4y, 3x + 4z, 3y - 4r, 3z - 4x) \cdot \mu, \\ \lambda_b(q_w) \cdot \gamma_2(b) &= \frac{1}{5} (3r + 4y, 3x + 4z, -3y + 4r, -3z + 4x) \cdot \mu,\end{aligned}$$

as expected. Right multiplication of q_w and $\lambda_b(q_w)$ by either $\gamma_2(a)$ or $\gamma_2(a)^{-1}$ retains the given structure, as is not difficult to calculate.

iv) By the induction hypothesis, $\lambda_{a,b}(q_w) = (r, -x, -y, z) \cdot \mu$ and thus:

$$\begin{aligned}\lambda_{a,b}(q_w) \cdot \gamma_2(a) &= \frac{1}{5} (3r + 4x, -3x + 4r, -3y + 4z, 3z + 4y) \cdot \mu, \\ \lambda_{a,b}(q_w) \cdot \gamma_2(b) &= \frac{1}{5} (3r + 4y, -3x - 4z, -3y + 4r, 3z - 4x) \cdot \mu, \\ \lambda_{a,b}(q_w) \cdot \gamma_2(a)^{-1} &= \frac{1}{5} (3r - 4x, -3x - 4r, -3y - 4z, 3z - 4y) \cdot \mu, \\ \lambda_{a,b}(q_w) \cdot \gamma_2(b)^{-1} &= \frac{1}{5} (3r - 4y, -3x + 4z, -3y - 4r, 3z + 4x) \cdot \mu,\end{aligned}$$

with the second and third components of each product negated with relation to $q_w \cdot \gamma_2(a)^{-1}$, $q_w \cdot \gamma_2(b)^{-1}$, $q_w \cdot \gamma_2(a)$ and $q_w \cdot \gamma_2(b)$ (resp.) as required. ◀

The following lemma allows us to represent a quaternion (and its corresponding rotation matrix) by using only absolute values and will be crucial later.

► **Lemma 13.** *Given a word $w \in \Sigma_k^*$, then $\gamma_2(\gamma_1(w)) = (r, x, y, z) \cdot \mu$ is uniquely determined by $(|r|, |x|, |y|, |z|)$. All matrices $\gamma(w) \in \Gamma$ are similarly uniquely determined by*

$$(|\gamma(w)_{1,1}|, |\gamma(w)_{1,2}|, |\gamma(w)_{1,3}|, |\gamma(w)_{1,4}|),$$

i.e., by the absolute values of each element of the top row of the matrix.

Proof. Another way to state this Lemma is that if we have $u = u_1 u_2 \cdots u_t$ and $v = v_1 v_2 \cdots v_{t'}$ with each $u_i, v_i \in \Sigma_k^*$, such that $\gamma_2(\gamma_1(u)) = (a_1, b_1, c_1, d_1) \cdot \mu$, $\gamma_2(\gamma_1(v)) = (a_2, b_2, c_2, d_2) \cdot \mu$ and $(|a_1|, |b_1|, |c_1|, |d_1|) = (|a_2|, |b_2|, |c_2|, |d_2|)$, then $t = t'$ and $u_i = v_i$ for all $1 \leq i \leq t$. A similar property holds for the top row of the unitary matrices when applying γ_3 to these elements. We shall now prove this.

By definition, $\gamma_2 : \Sigma_2^* \hookrightarrow \mathbb{H}(\mathbb{Q})$ maps to a free monoid \mathcal{S} of $\mathbb{H}(\mathbb{Q})$ generated by $\mathcal{G} = \{\gamma_2(a), \gamma_2(b)\}$ with $\gamma_2(a) = (\frac{3}{5}, \frac{4}{5}, 0, 0) \cdot \mu$ and $\gamma_2(b) = (\frac{3}{5}, 0, \frac{4}{5}, 0) \cdot \mu$. As shown in Section 4, $\gamma_2 \circ \gamma_1 : \Sigma_n^* \hookrightarrow \mathbb{H}(\mathbb{Q})$; i.e., $\gamma_2 \circ \gamma_1$ is an injective homomorphism. Let $\Gamma' = \{\gamma_2(\gamma_1(w')) | w' \in \Sigma_n^*\} \subseteq \mathbb{H}(\mathbb{Q})$. Clearly then, Γ' is freely generated by $\{\gamma_2(\gamma_1(w')) | w' \in \Sigma_n\}$ by the injectivity of $\gamma_2 \circ \gamma_1$.

Let $q_w = \gamma_2(\gamma_1(w)) = (r, x, y, z) \cdot \mu \in \Gamma' \subseteq \mathcal{S}$ and define $Q_w = \{(\pm r, \pm x, \pm y, \pm z) \cdot \mu\}$, thus $|Q_w| = 16$. We will now show that for all $q' \in Q_w - \{q_w\}$ then $q' \notin \Gamma'$ which proves the lemma.

Since (unit) quaternion inversion simply involves negating all imaginary components, then using the identities of Lemma 12, we can derive that $q_w^{-1} = (r, -x, -y, -z)$, $\lambda_a(q_w)^{-1} = (r, x, -y, z)$ and $\lambda_b(q_w)^{-1} = (r, -x, y, z)$ which we summarize in the following table.

q_w	$(r, x, y, z)\mu$	q_w^{-1}	$(r, -x, -y, -z)\mu$
$\lambda_a(q_w)$	$(r, -x, y, -z)\mu$	$\lambda_a(q_w)^{-1}$	$(r, x, -y, z)\mu$
$\lambda_b(q_w)$	$(r, x, -y, -z)\mu$	$\lambda_b(q_w)^{-1}$	$(r, -x, y, z)\mu$
$\lambda_{a,b}(q_w)$	$(r, -x, -y, z)\mu$	q_w^R	$(r, x, y, -z)\mu$

We might also notice other identities, such as $q_w^R = \lambda_{a,b}(q_w)^{-1}$ which is clear from the definition of $\lambda_{a,b}$. Note that this table covers 8 elements of Q_w .

Note q_w belongs (by definition) to $\Gamma' = (\gamma_2(a)^+ \gamma_2(b))^+ = \{\gamma_2(\gamma_1(w')) | w' \in \Sigma_n\} \subseteq \mathcal{S}$. Since $\langle \gamma_2(a), \gamma_2(b) \rangle_{gr}$ generates a free group, this means that no reduced element of \mathcal{S} is equal to a product with a nontrivial³ factor $\gamma_2(a)^{-1}$ or $\gamma_2(b)^{-1}$. Each element in the above

³ Reduced meaning the element contains no consecutive inverse elements and nontrivial meaning we ignoring any such element adjacent to its multiplicative inverse.

table contains at least one nonreducible factor $\gamma_2(a)^{-1}$ or $\gamma_2(b)^{-1}$, excluding q_w and q_{wR} . Note however that q_{wR} trivially does not belong to $\Gamma' = (\gamma_2(a)^+\gamma_2(b))^+$ since it necessarily begins with nonreducible factor $\gamma_2(b)$.

Finally, to cover the remaining 8 elements of Q_w , we consider the *free group* $\mathcal{S}_{gr} = \langle \{\gamma_2(a), \gamma_2(b)\} | \emptyset \rangle_{gr}$. For any $q'_w \in \mathcal{S}_{gr}$ then $-q'_w \notin \mathcal{S}_{gr}$ since \mathcal{S}_{gr} is free. This holds since if $-q'_w \in \mathcal{S}$, then $-1 \in \mathcal{S}$ (because $(q'_w)^{-1} \in \mathcal{S}$), which gives a nontrivial identity $-1^2 = 1$ in \mathcal{S}_{gr} (a contradiction).

This covers all sixteen possible elements of Q_w and shows that q_w is the only member of Q_w belonging to Γ' . By the definition of $\gamma_3 : \mathbb{H}(\mathbb{Q}) \hookrightarrow \mathbb{Q}^{4 \times 4}$, then also all matrices $\gamma(w) \in \Gamma$ are uniquely determined by $(|\gamma(w)_{1,1}|, |\gamma(w)_{1,2}|, |\gamma(w)_{1,3}|, |\gamma(w)_{1,4}|)$ as required. ◀

► **Theorem 14.** *The freeness problem for measure-once quantum finite automata is undecidable for 32 states over an alphabet of size 17.*

Proof. We will encode an instance (h, g) of the mixed modification Post’s Correspondence Problem into a finite set of matrices so that if there exists a solution to the instance then there exists some scalar which is nonfree, otherwise every scalar is free.

Let $\Sigma = \{x_1, x_2, \dots, x_{n-2}\}$ and $\Delta = \{x_{n-1}, x_n\}$ be distinct alphabets and $h, g : \Sigma^* \rightarrow \Delta^*$ be an instance of the mixed modification PCP and let $\Sigma_n = \Sigma \cup \Delta$. The naming convention will become apparent below, but intuitively we will be applying γ , from Section 4 to both the input and output alphabets.

Recall that we showed the injectivity of γ in Section 4, and thus have a monomorphism $\gamma : \Sigma_n^* \hookrightarrow \mathbb{Q}^{4 \times 4}$. We define a function $\varphi : \Sigma_n^* \times \Sigma_n^* \hookrightarrow \mathbb{Q}^{32 \times 32}$ by

$$\varphi(w_1, w_2) = \bigoplus_{j=1}^4 \gamma(w_1) \oplus \bigoplus_{j=1}^4 \gamma(w_2).$$

We may note that $\varphi(w_1, w_2)$ remains a unitary matrix since $\gamma(w_i)$ is unitary and the direct sum of unitary matrices is unitary. Define $\mathcal{G} = \{\varphi(x_i, h(x_i)), \varphi(x_i, g(x_i)) | x_i \in \Sigma\} \subset \mathbb{Q}^{32 \times 32}$.

Let p_i denote the i 'th prime number and define $u_i = \sqrt[4]{p_i} \cdot e_i \in \mathbb{A}_{\mathbb{R}}^4$, $v_i = \sqrt[4]{p_{4+i}} \cdot e_i \in \mathbb{A}_{\mathbb{R}}^4$ for $1 \leq i \leq 4$ ($\mathbb{A}_{\mathbb{R}}^4$ denotes a 4-tuple of elements from $\mathbb{A}_{\mathbb{R}}$) and $u' = \bigoplus_{j=1}^4 u_j \oplus \bigoplus_{j=1}^4 v_j \in \mathbb{A}_{\mathbb{R}}^{32}$. Now, we normalise this vector so that $u = \frac{u'}{\sqrt{\sum_{i=1}^8 \sqrt{p_i}}} \in \mathbb{A}_{\mathbb{R}}^{32}$, with u a unit vector. Note

that each element of u is a real algebraic number. Let $P_1 = 1 \oplus \mathbf{0}_3$ where $\mathbf{0}_3$ is the 3×3 zero matrix, thus P_1 has a 1 in the upper left element and zero elsewhere. Then define $P = P_1^{\oplus 8} \in \mathbb{Q}^{32 \times 32}$. Note that $P^2 = P$ and P is a projection matrix.

We are now ready to define our QFA \mathcal{Q} by the triple $\mathcal{Q} = (P, \mathcal{G}, u)$ and prove the claim of the theorem.

Let $X = X_{i_1} \cdots X_{i_p} = \varphi(x_{i_1}, f_{i_1}(x_{i_1})) \cdots \varphi(x_{i_p}, f_{i_p}(x_{i_p}))$, with $f_{i_k} \in \{g, h\}$ for $1 \leq k \leq p$ be one factorization of a matrix $X \in \mathcal{G}$. Define $x = x_{i_1} \cdots x_{i_p}$ and $f(x) = f_{i_1}(x_{i_1}) \cdots f_{i_p}(x_{i_p})$. Then we see that:

$$\|PXu\|^2 = \left\| \frac{\bigoplus_{j=1}^4 (P_1\gamma(x)u_j) \oplus \bigoplus_{j=1}^4 (P_1\gamma(f(x))v_j)}{\sqrt{\sum_{i=1}^8 \sqrt{p_i}}} \right\|^2 \quad (2)$$

$$= \left\| \frac{\bigoplus_{j=1}^4 (P_1\gamma(x)\sqrt[4]{p_j} \cdot e_j) \oplus \bigoplus_{j=1}^4 (P_1\gamma(f(x))\sqrt[4]{p_{4+j}} \cdot e_j)}{\sqrt{\sum_{i=1}^8 \sqrt{p_i}}} \right\|^2 \quad (3)$$

$$= \left(\frac{\sqrt{\sum_{j=1}^4 (\gamma(x)_{1,j}\sqrt[4]{p_j})^2 + \sum_{j=1}^4 (\gamma(f(x))_{1,j}\sqrt[4]{p_{4+j}})^2}}{\sqrt{\sum_{i=1}^8 \sqrt{p_i}}} \right)^2 \quad (4)$$

$$= \frac{\sum_{j=1}^4 \gamma(x)_{1,j}^2 \sqrt{p_j} + \sum_{j=1}^4 \gamma(f(x))_{1,j}^2 \sqrt{p_{4+j}}}{\sqrt{\sum_{i=1}^8 \sqrt{p_i}}}. \quad (5)$$

Assume that matrix X has two distinct factorizations $X = X_{i_1} \cdots X_{i_p} = X_{j_1} \cdots X_{j_q} \in \mathcal{G}^+$ and $p \neq q$ or $X_{i_k} \neq X_{j_k}$ for some $1 \leq k \leq p$, such that

$$\|PXu\|^2 = \|PX_{i_1} \cdots X_{i_p} u\|^2 = \|PX_{j_1} \cdots X_{j_q} u\|^2,$$

and thus $\Lambda(\mathcal{Q})$ is not free. Let $X = X_{j_1} \cdots X_{j_q} = \varphi(x_{j_1}, f'_{j_1}(x_{j_1})) \cdots \varphi(x_{j_q}, f'_{j_q}(x_{j_q}))$, with $f'_{j_k} \in \{g, h\}$ for $1 \leq k \leq q$ and define $x' = x_{j_1} \cdots x_{j_q}$ and $f'(x') = f'_{j_1}(x_{j_1}) \cdots f'_{j_q}(x_{j_q})$ with each $f'_{j_k} \in \{g, h\}$. Note that in Eqn. (5) the denominator is constant and thus when determining equality $\|PX_{i_1} \cdots X_{i_p} u\|^2 = \|PX_{j_1} \cdots X_{j_q} u\|^2$ we may ignore it. By Lemma 13, each $\gamma(w)$ is uniquely determined by the absolute value of the top four elements of the matrix (e.g. $|\gamma(w)_{1,j}|$ for $1 \leq j \leq 4$). Since each p_j is squarefree, for $1 \leq j \leq 8$, then by Theorem 11, the following equation is satisfied if and only if $|\gamma(x)| = |\gamma(x')|$ and $|\gamma(f(x))| = |\gamma(f'(x'))|$:

$$\begin{aligned} & \sum_{j=1}^4 \gamma(x)_{1,j}^2 \sqrt{p_j} + \sum_{j=1}^4 \gamma(f(x))_{1,j}^2 \sqrt{p_{4+j}} \\ &= \sum_{j=1}^4 \gamma(x')_{1,j}^2 \sqrt{p_j} + \sum_{j=1}^4 \gamma(f'(x'))_{1,j}^2 \sqrt{p_{4+j}}. \end{aligned}$$

Finally, note that $\gamma(x) = \gamma(x')$ if and only if $x = x'$. As before, let $x = x_{i_1} \cdots x_{i_p}$, then $\gamma(f(x)) = f_{i_1}(x_{i_1}) \cdots f_{i_p}(x_{i_p}) = f_{j_1}(x_{i_1}) \cdots f_{j_p}(x_{i_p}) = \gamma(f'(x'))$ with some $f_{i_k} \neq f_{j_k}$ for $1 \leq k \leq p$ if and only if the instance of the MMPCP has a solution.

If the MMPCP is undecidable for Claus instances with an alphabet of size n' (see Theorem 9), then the undecidability of the current theorem holds for $|\mathcal{G}| \geq 2n'$. We now prove that the result holds for $|\mathcal{G}| \geq 2n' - 1$. Let $\Sigma = \{x_1, \dots, x_{n'}\}$. Since h, g is a Claus instance, any solution word w is of the form $w = x_1 w' x_{n'}$, with $w' \in (\Sigma - \{x_1, x_{n'}\})^*$. By symmetry, we may assume that $h_1 = h$ and by the proof in [16], $g_i = g$ and $h_i = h$ for all $1 \leq i \leq t$. Clearly then, one of $h(x_{n'})$ and $g(x_{n'})$ is a proper suffix of the other (assume that $g(x_{n'})$ is a suffix of $h(x_{n'})$; the opposite case is similar). Now, redefine $u' = \gamma(x_{n'}, g(x_{n'}))u$, remove the matrix corresponding to $g(x_{n'})$ from \mathcal{G} and redefine the matrix corresponding to $h(x_{n'})$ by $h'(x_{n'}) = \gamma(x_{n'}, h(x_{n'}))g(x_{n'})^{-1}$. Since $g(x_{n'})$ is a proper suffix of $h(x_{n'})$, then $h(x_{n'})g(x_{n'})^{-1}$ is the prefix of $h(x_{n'})$ after removing the common suffix with $g(x_{n'})$. This means that an ambiguous scalar only exists if there exists a solution to the instance of MMPCP and we had reduced the alphabet size by 1. MMPCP is undecidable for instances of size 9 (Theorem 9), thus the undecidability holds for MO-QFA with 32 states and an alphabet size of 17. \blacktriangleleft

► **Corollary 15.** *The ambiguity problem for measure-once quantum finite automata is undecidable for 33 states over an alphabet of size 17.*

Proof. The corollary follows from the proof of Theorem 14. We notice that if there exists a solution to the encoded instance of the MMPCP, then some matrix X has two distinct factorizations over \mathcal{G} and therefore there exists two distinct matrix products giving the same scalar. Our technique in this corollary is to make these two factorizations produce distinct matrices X_1 and X_2 , such that they still lead to the same scalar. This is simple to accomplish by redefining the projection matrix P as $P' = P \oplus 0$, redefining the initial vector u as $u' = u \oplus 0$ and for each matrix $M \in \mathcal{G} - \{\varphi(x_1, h(x_1))\}$, we redefine M as $M' = M \oplus 1$ and let $\varphi(x_1, h(x_1))$ be redefined as $\varphi(x_1, h(x_1)) \oplus -1$. In this case, any matrix product containing $\varphi(x_1, h(x_1)) \oplus -1$ will have -1 in the bottom right element, otherwise the bottom right element is 1. Since we encode a Claus instance of MMPCP, one factorization has -1 in this case, and the other has 1, and thus we always have distinct matrices. If no solution exists, then each matrix leads to a unique scalar anyway.

Note that we increased the number of states of the MO-QFA by 1 and also note that the acceptance probability is unaffected by the above modifications since the projection matrix was increased by a zero row/column. ◀

6 Conclusion

An interesting question is whether Theorem 14 can be shown to hold when the initial vector is rational, rather than real algebraic. We can prove this result if a certain open problem related to rational packing functions holds (does there exist a polynomial which maps n -tuples of rationals to a single rational injectively). Such a function is well known for integer values (the Cantor polynomial), but not for rational n -tuples. This seems a difficult problem to approach however, and thus we leave the following open problem.

► **Open Problem 16.** *Can undecidability of the ambiguity and freeness problems for MO-QFA be shown when the initial vector, projection matrix and all unitary matrices are over rationals?*

We also note that in [1] the ambiguity and freeness problems for weighted finite automata and probabilistic finite automata were shown to be undecidable even when the input words were restricted to come from a given *letter monotonic language*, which is a restriction of bounded languages of the form $x_1^* x_2^* \cdots x_k^*$ where each x_i is a single letter of the input alphabet. The undecidability result of [1] used an encoding of Hilbert's tenth problem, which seems difficult to encode into unitary matrices and thus we pose the following open problem.

► **Open Problem 17.** *Can the undecidability of the ambiguity and freeness problems for MO-QFA be shown when the input word is necessarily from a given letter monotonic language?*

References

- 1 P. C. Bell, S. Chen, and L. M. Jackson. Scalar ambiguity and freeness in matrix semigroups over bounded languages. In *Language and Automata Theory and Applications*, volume LNCS 9618, pages 493–505, 2016.
- 2 P. C. Bell, V. Halava, and M. Hirvensalo. Decision Problems for Probabilistic Finite Automata on Bounded Languages. *Fundamenta Informaticae*, 123(1):1–14, 2012.
- 3 P. C. Bell and I. Potapov. Periodic and infinite traces in matrix semigroups. *Current Trends in Theory and Practice of Computer Science (SOFSEM)*, LNCS 4910:148–161, 2008.

- 4 P. C. Bell and I. Potapov. Reachability problems in quaternion matrix and rotation semigroups. *Information and Computation*, 206(11):1353–1361, 2008.
- 5 P. C. Bell and I. Potapov. On the undecidability of the identity correspondence problem and its applications for word and matrix semigroups. *International Journal of Foundations of Computer Science*, 21(6):963–978, 2010.
- 6 A. Bertoni, G. Mauri, and M. Torelli. Some recursively unsolvable problems relating to isolated cutpoints in probabilistic automata. In *Automata, Languages and Programming*, volume 52 of *LNCS*, pages 87–94, 1977.
- 7 A. S. Besicovitch. On the linear independence of fractional powers of integers. *J. London Math. Soc.*, 15:3–6, 1940.
- 8 V. Blondel and V. Canterini. Undecidable problems for probabilistic automata of fixed dimension. *Theory of Computing Systems*, 36:231–245, 2003.
- 9 V. Blondel, E. Jeandel, P. Koiran, and N. Portier. Decidable and undecidable problems about quantum automata. *SIAM Journal on Computing*, 34:6:1464–1473, 2005.
- 10 A. Brodsky and N. Pippenger. Characterizations of 1-way quantum finite automata. *SIAM Journal on Computing*, 31:1456–1478, 2002.
- 11 J. Cassaigne, T. Harju, and J. Karhumäki. On the undecidability of freeness of matrix semigroups. *International Journal of Algebra and Computation*, 9(3-4):295–305, 1999.
- 12 J. Cassaigne and F. Nicolas. On the decidability of semigroup freeness. *RAIRO - Theoretical Informatics and Applications*, 46(3):355–399, 2012.
- 13 É. Charlier and J. Honkala. The freeness problem over matrix semigroups and bounded languages. *Information and Computation*, 237:243–256, 2014.
- 14 C. Choffrut and J. Karhumäki. Some decision problems on integer matrices. *Informatics and Applications*, 39:125–131, 2005.
- 15 T. Colcombet, J. Ouaknine, P. Semukhin, and J. Worrell. On reachability problems for low dimensional matrix semigroups. In *ArXiv Manuscript (to appear ICALP’19)*, volume arXiv:1902.09597, pages 1–15, 2019.
- 16 V. Halava, T. Harju, and M. Hirvensalo. Undecidability bounds for integer matrices using Claus instances. *International Journal of Foundations of Computer Science (IJFCS)*, 18,5:931–948, 2007.
- 17 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*, 4362:309–319, 2007.
- 18 J. Honkala. Decision problems concerning thinness and slenderness of formal languages. In *Acta Informatica*, volume 35, pages 625–636, 1998.
- 19 R. A. Horn and C. R. Johnson. *Topics in matrix analysis*. Cambridge University Press, 1991.
- 20 D. A. Klarner, J.-C. Birget, and W. Satterfield. On the undecidability of the freeness of integer matrix semigroups. *International Journal of Algebra and Computation*, 1 (2):223–226, 1991.
- 21 S.-K. Ko and I. Potapov. Vector ambiguity and freeness problems in $SL(2, \mathbb{Z})$. *Fundamenta Informaticae*, 162(2-3):161–182, 2018.
- 22 W. Kuich and A. Salomaa. *Semirings, Automata, Languages*, volume 5. Springer, 1986.
- 23 E. Lengyel. *Mathematics for 3D Game Programming & Computer Graphics*. Charles River Media, 2004.
- 24 C. Moore and J. P. Crutchfield. Quantum automata and quantum grammars. *Theoretical Computer Science*, 237(1-2):275–306, 2000.
- 25 M. S. Paterson. Unsolvability in 3×3 matrices. *Studies in Applied Mathematics*, 49(1):105–107, 1970.
- 26 A. Paz. *Introduction to Probabilistic Automata*. Academic Press, 1971.
- 27 S. Swierczkowski. A class of free rotation groups. *Indag. Math.*, 5(2):221–226, 1994.