On the Intersection Problem for Quantum Automata

Flavio D'Alessandro[1]

[1]Sapienza Università di Roma

May 14, 2025

Content of the presentation

The $(\mathcal{L}, \mathcal{Q})$ Intersection Problem

$\mathcal{L}$ is a family of languages and $\mathcal{Q}$ is a model of computation

Given the language $L(Q)$ recognized by $\mathcal{Q}$ and a language L in $\mathcal{L}$,

it is decidable whether or not

$$L(Q) \cap L = \emptyset$$

A. Bertoni, 2013

Family $\mathcal{L}$: Context-free languages,

"Matrix" context-free languages

Model $\mathcal{Q}$: Quantum finite automata

("measure-once" model

by Moore and Crutchfield, 2000)

Overview of the presentation

Introduction: Quantum finite automata

A general method for the decision problem: Algebraic groups

Results:

Bertoni, Choffrut and d. (2014)

Benso, d., and Papi (2024)

The measure once model

A finite quantum automaton is a quadruple $\mathcal{Q} = (s, \varphi, P, \lambda)$

- $s \in \mathbb{R}^n$ is a row-vector with $||s||^2 = s_1^2 + \cdots + s_n^2 = 1$
- $$\varphi : \Sigma^* \longrightarrow O_n$$

  is a morphism of the free monoid Σ^* into the group O_n of orthogonal $n \times n$-matrices in $\mathbb{R}^{n \times n}$
- P is a projection of $\mathbb{R}^n$ i.e. $P \in \{0, 1\}^{n \times n}$ with $P^2 = P$
- λ is a given value in $\mathbb{R}$ threshold

In the quantum automaton $\mathcal{Q} = (s, \varphi, P, \lambda)$

the morphism

$$\varphi : \Sigma^* \longrightarrow O_n$$

describes the computation of $\mathcal{Q}$ on a word $w \in \Sigma^*$

$$w = \sigma_1 \cdots \sigma_\ell \quad \longrightarrow \quad \varphi(\sigma_1) \cdots \varphi(\sigma_\ell) = M$$

M orthogonal real matrix

M is orthogonal if $M^{-1} = M^T$

The output function of $\mathcal{Q}$

A finite quantum automaton is a quadruple $\mathcal{Q} = (s, \varphi, P, \lambda)$

- $s \in \mathbb{R}^n$ is a row-vector of unit Euclidean norm
- $\varphi : \Sigma^* \longrightarrow O_n$ (morphism)
- P is a projection of $\mathbb{R}^n$

$$w \in \Sigma^* \longrightarrow ||\, s\varphi(w)P \,||^2$$

the output of w is the square of the norm of the vector

$$s\,\varphi(w)\,P$$

The languages accepted by $\mathcal{Q}$

$$|\mathcal{Q}_{>}| = \{w \in \Sigma^* : ||s\varphi(w)P||^2 > \lambda\}$$

with strict threshold λ

$$|\mathcal{Q}_{\geq}| = \{w \in \Sigma^* : ||s\varphi(w)P||^2 \geq \lambda\}$$

with non strict threshold λ

$$|\mathcal{Q}_{<}| = \{w \in \Sigma^* : ||s\varphi(w)P||^2 < \lambda\}$$

$$|\mathcal{Q}_{\leq}| = \{w \in \Sigma^* : ||s\varphi(w)P||^2 \leq \lambda\}$$

Measure-once Quantum Automata

- Description of good-featured quantum devices of *small size*

- Mereghetti, Palano, Cialdi, Vento, Paris, Olivares, 2020

  Method for the physical implementation of measure-once quantum automata for the recognition of periodic languages

THE DECISION PROBLEMS

The Emptiness Problem

INPUT: a finite quantum automaton $\mathcal{Q}$

QUESTION: $|\mathcal{Q}_{\#}| \cap \Sigma^* = \emptyset$ where

$$|\mathcal{Q}_{\#}| = \{w \in \Sigma^* : ||s\varphi(w)P||^2 \# \lambda\}$$ and

$\#$ can be $>$, $<$, $\geq$, $\leq$

$\mathcal{Q}$ is rational, i.e. the coefficients of the representation

$\mathcal{Q} = (s, \varphi, P, \lambda)$ are in $\mathbb{Q}$

The Emptiness Problem EP

$$|\mathcal{Q}_{\#}| \cap \Sigma^* = \emptyset$$

- Blondel, Jeandel, Koiran, Portier (2005)

  EP is decidable if $\# \in \{<, >\}$ strict threshold

- Bertoni (1975, 1977)

  EP is undecidable w.r.t. probabilistic automata

- EP is un-decidable for

  – the non-strict case (measure-once model)

  Blondel et al. (2005)

  – both cases (measure-many model) Jeandel (2002)

The Intersection Problem IP

INPUT: ordered pair $(\mathcal{L}, \mathcal{Q})$ where:

$\mathcal{L}$ is a family of effectively defined formal languages

$\mathcal{Q}$ is an arbitrary finite (rational) quantum automaton

QUESTION:

$$|\mathcal{Q}_{>}| \cap L = \emptyset, \qquad L \in \mathcal{L}$$

If $\mathcal{L} = \{\Sigma^*\}$ then one gets the Emptiness Problem

A method for the decision problem: Algebraic groups

Reformulate the Intersection Problem

$$|\mathcal{Q}_{>}| = \{\, w \in \Sigma^* : ||s\varphi(w)P||^2 > \lambda \,\} \qquad |\mathcal{Q}_{>}| \;\cap\; L \;=\; \emptyset \qquad \Longleftrightarrow$$

$$\forall \;\; w \;\in\; L \qquad f(w) = \|s\varphi(w)P\|^2 \;\leq\; \lambda \qquad \Longleftrightarrow$$

$$\forall \; M \;\in\; \varphi(L) \qquad f(M) := \; ||sMP||^2 \;\leq\; \lambda \qquad\qquad (1)$$

GOAL: decidable construct to test whether (1) holds or not

$$\forall\ M \ \in \ \varphi(L) \qquad f(M) \ = \ ||sMP||^2 \ \leq \ \lambda \qquad (1) \qquad \Longleftrightarrow$$

$$\forall\ M \ \in \ \mathbf{C}l(\varphi(L)) \qquad f(M) \ = \ ||sMP||^2 \ \leq \ \lambda$$

where $\mathbf{C}l(\varphi(L))$ is the closure of $\varphi(L)$ with the Euclidean Topology on the space of matrices $\mathbb{R}^{n\times n}$

The function $f \ : \ M \longrightarrow ||sMP||^2$ is continuous with the Euclidean Topology

$$\forall\ M\ \in\ \mathbf{C}l(\varphi(L)) \qquad f(M)\ \leq\ \lambda \qquad\qquad (1)$$

- Consider the predicate over $\mathbb{Q}^{n\times n}$

$$\text{InClosure(X)}\ \equiv\ X\ \in\ \mathbf{C}l(\varphi(L))$$

- If InClosure(X) is first-order definable in $(\mathbb{R}, +, \cdot)$, then

$$\forall\ X \in \mathbb{Q}^{n\times n}\ :\ \text{InClosure(X)} \quad \Longrightarrow \quad ||sXP||^2\ \leq\ \lambda \qquad (2)$$

is also first-order definable in $(\mathbb{R}, +, \cdot)$ and corresponds to

$$\forall\ M\ \in \mathbf{C}l(\varphi(L)) \qquad ||sMP||^2\ \leq\ \lambda \qquad\qquad (1)$$

- Apply Tarski-Seidenberg Quantifier Elimination Method to (2)

Blondel, Jeandel, Koiran, Portier (2005)

GOAL: Construction of a formula for InClosure

(Emptiness Problem) $\mathcal{L} = \{\Sigma^*\}$ free monoid over Σ

$\mathbf{C}l(\varphi(\Sigma^*))$ is an effective algebraic set (over $\mathbb{R}$), i.e.,

one can construct a polynomial $p \in \mathbb{R}[x_{11}, \ldots, x_{nn}]$ such that

$$M \in \mathbb{Q}^{n \times n}, \quad M \in \mathbf{C}l(\varphi(\Sigma^*)) \iff p(M) = 0$$

$$\text{InClosure(X)} \equiv X \in \mathbb{Q}^{n \times n} \, : \, p(X) = 0$$

Group O_2 of orthogonal matrices of order 2

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \in O_2 \iff MM^T = I \iff$$

$$\begin{pmatrix} m_{11}^2 + m_{12}^2 & m_{11}m_{21} + m_{12}m_{22} \\ m_{11}m_{21} + m_{12}m_{22} & m_{21}^2 + m_{22}^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

M is orthogonal if and only if is zero of the polynomials:

$$p_1(m_{11}, m_{12}, m_{21}, m_{22}) = m_{11}^2 + m_{12}^2 - 1$$
$$p_2(m_{11}, m_{12}, m_{21}, m_{22}) = m_{11}m_{21} + m_{12}m_{22}$$
$$p_3(m_{11}, m_{12}, m_{21}, m_{22}) = m_{21}^2 + m_{22}^2 - 1$$

Derksen, Jeandel, Koiran (2005)

Algorithm which, given a finite set S of invertible matrices,

computes the Zariski closure $\overline{\langle S \rangle}$ of the group generated by these

matrices

Nosan, Pouly, Schmitz, Shirmohammadi, Worrell (2022)

Alternative approach for the computation of the Zariski closure $\overline{\langle S \rangle}$

of the group generated by a finite set S of invertible matrices

- it provides a bound on the degree of the polynomials that define the $\overline{\langle S \rangle}$
- $\overline{\langle S \rangle}$ can be computed in elementary time

Hrushovski, Ouaknine, Pouly, Worrell (2023)

Computation of the Zariski closure $\overline{S^*}$ of the monoid S^* generated by a finite set S of (not necessarily invertible) matrices

- Computation of polynomial invariants for affine programs
- Application to the Burnside Problem for Semigroups: decidability of the finiteness of a finitely generated semigroup of rational matrices (Mandel and Simon 1977, Jacob 1978)

Membership Problem MP($\mathbb{K}$, n)

Semigroup $\mathbb{K}^{n \times n}$ of matrices, over a ring $\mathbb{K}$, of size n

MP($\mathbb{K}$, n): given a finite subset S of $\mathbb{K}^{n \times n}$, and an element $M \in \mathbb{K}^{n \times n}$, decide whether $M \in S^*$

- Paterson (1970): MP($\mathbb{Z}$, 3) is undecidable

- Potapov and Semukhin (2017): MP($\mathbb{Z}$, 2) is decidable (the matrices of S are non-singular)

The Intersection Problem for Context-free Languages

Results

Context-free Grammars

$G = \langle V, \Sigma, P, S \rangle$

V is the set of variables $\qquad S \in V$ is the start symbol

Σ is the set of terminal symbols

P is the set of productions

$$A \longrightarrow \alpha, \qquad A \in V, \qquad \alpha \in (V \cup \Sigma)^*$$

Derivation Relation: $\stackrel{*}{\Longrightarrow}$

Language generated by G:

$$L(G) = \{ w \in \Sigma^* : S \stackrel{*}{\Longrightarrow} w \}$$

The Set of cycles of A

With each variable $A \in V$ associate the subset of $\Sigma^* \times \Sigma^*$

$$C_A = \{ (u, v) \in \Sigma^* \times \Sigma^* : A \overset{*}{\Longrightarrow} uAv \}$$

Ginsburg and Spanier techniques (1966)

sets of cycles are used for the combinatorial structuring of the derivations of a context-free grammar (decision methods)

The Monoid of Cycles

$$C_A \;=\; \{\; (u,\; v) \;\in\; \Sigma^* \times \Sigma^* \;:\; A \stackrel{*}{\Longrightarrow} uAv \;\}$$

We associate with C_A the set of orthogonal matrices

$$M_A \;=\; \left\{ \begin{pmatrix} \varphi(u) & \mathsf{O} \\ \mathsf{O} & \varphi(v)^T \end{pmatrix} \;:\; A \stackrel{*}{\Longrightarrow} uAv \right\}$$

where $\varphi : \Sigma^* \longrightarrow O_n$ is the morphism of the automaton $\mathcal{Q}$

CRUCIAL FACT: M_A is a monoid (the monoid of cycles of A)

Monoids of cycles and the IP

The study of the IP reduces to two ingredients:

– $\mathbf{C}l(M_A)$ is an algebraic set (machinery to compute the algebraic closure of matrices)

– *Ginsburg and Spanier - like* techniques:

suitably defined effective structuring of the derivations of G

Bertoni, Choffrut, and d. (2014)

- If $L \in$ CFL then $\mathbf{C}l(\varphi(L))$ is semialgebraic, that is,

$\mathbf{C}l(\varphi(L))$ is the set of matrices satisfying a finite Boolean combination of predicates of polynomial form

$$p(x_{11}, \ldots, x_{nn}) > 0 \quad \text{or} \quad p(x_{11}, \ldots, x_{nn}) = 0$$

for some polynomials p in $\mathbb{R}[x_{11}, \ldots, x_{nn}]$

- If all $\mathbf{C}l(M_A)$ are effectively algebraic then $\mathbf{C}l(\varphi(L))$ is computable

Bertoni, Choffrut, and d. (2014)

The Intersection Problem is decidable for:

- Linear context-free languages

- Bounded semi-linear languages, i.e., languages of the form

$$L \subseteq u_1^* \cdots u_k^*, \qquad u_1, \ldots, u_k \in \Sigma^*$$

accepted by Reversal bounded non deterministic counter machines

REASON: $\mathbf{C}l(\varphi(L))$ is computable since all the monoids M_A are finitely generated and thus $\mathbf{C}l(M_A)$ computable

Example

$$L \;=\; \{uu^{\sim} \;:\; u \in \Sigma^*\}, \qquad \Sigma \;=\; \{a,\; b\}$$

L is generated by the grammar G whose productions are:

$$p_0 = (S \longrightarrow \varepsilon)$$

$$\sigma \in \Sigma, \qquad p_\sigma = (S \;\longrightarrow\; \sigma S \sigma)$$

Example

$$L = \{uu^{\sim} : u \in \Sigma^*\}, \qquad \Sigma = \{a, b\}$$

Given a matrix $M \in \mathbb{R}^{n \times n}$

$$M \in \varphi(L) \iff M = \varphi(u)\varphi(u^{\sim}) = \varphi(\sigma_1)\cdots\varphi(\sigma_k)\,\varphi(\sigma_k)\cdots\varphi(\sigma_1)$$

$\mathcal{N} = \{\varphi(a) \oplus \varphi(a)^T, \ \varphi(b) \oplus \varphi(b)^T\}^*$ is the monoid generated by

$$\sigma \in \Sigma, \quad \varphi(\sigma) \oplus \varphi(\sigma)^T := \begin{pmatrix} \varphi(\sigma) & \mathsf{O} \\ \mathsf{O} & \varphi(\sigma)^T \end{pmatrix}$$

$$M \in \mathcal{N} \iff M = \begin{pmatrix} \varphi(u) & \mathsf{O} \\ \mathsf{O} & \varphi(u)^T \end{pmatrix}$$

Example

$$M \in \mathcal{N} \iff M = \begin{pmatrix} \varphi(u) & \mathsf{O} \\ \mathsf{O} & \varphi(u)^T \end{pmatrix}$$

$$M \in \mathbf{C}l(\varphi(L)) \iff M \in \mathbf{C}l(\ \{\varphi(u)\varphi(u)^T \ : \ u \in \ \Sigma^*\}\ ) \iff$$

$$\exists\ X\ \exists\ Y\ :\ M = XY\ \wedge\ X \oplus Y = \begin{pmatrix} X & \mathsf{O} \\ \mathsf{O} & Y \end{pmatrix} \in\ \mathbf{C}l(\mathcal{N})$$

$\mathbf{C}l(\mathcal{N})$ is algebraic, i.e., for some computable polynomial P

$$\mathbf{C}l(\mathcal{N}) = \{M \in \mathbb{R}^{2n \times 2n} \ : \ P(M) = 0\}$$

$$M \in \mathbf{C}l(\varphi(L)) \iff \exists\ X\ \exists\ Y\ :\ M = XY\ \wedge\ P(X \oplus Y) = 0$$

Thank you for your attention