Emulation of quantum Turing machines

Paulo Mateus

SQIG - Instituto de Telecomunicações
DM -IST - U. Lisboa

Joint work with A. Sernadas and A. Souto

Context

- Quantum automata
- Open problems concerning QA (and other automata) and their importance
- Category of bilinear automata
- How Category Theory and (computational) Algebraic Theory of the ROF helped solving the OP
- Quantum Turing machines as morphisms
- Towards quantum Kolmogorov theory

Quantum automata

A *quantum automaton* is a tuple

$$\mathcal{Q} = \langle \Sigma, H, s_i, U, O, \rho \rangle$$

where

- Σ is a finite set of inputs,
- H is a finite Hilbert space of states,
- s_i is a unitary vector in H denoting the initial state,
- U is a Σ-indexed family $\{U_\sigma\}_{\sigma \in \Sigma}$ of unitary transformations in H,
- O is a Hilbert space of outputs and $P_O : H \to O$ is a projection (there is a subspace H' of H isomorphic to O).

Quantum automata

- A stochastic language over Σ is a map $\beta : \Sigma^* \to [0,1]$.
- The *quantum behaviour* of a quantum automaton $\mathcal{Q}$ is the map

$$\beta_{\mathcal{Q}} : \Sigma^* \to O$$

where $\beta_{\mathcal{Q}}(\omega) = P_O U_\omega s_i$ with $U_\omega = U_{\sigma_k} \dots U_{\sigma_1}$ and $\omega = \sigma_1 \dots \sigma_k$.

- The *stochastic behaviour* of a quantum automaton $\mathcal{Q}$ is the stochastic language

$$\beta_{\mathcal{Q}} : \Sigma^* \to [0,1]$$

where

$$\beta_{\mathcal{Q}}(\omega) = |P_O U_\omega s_i|^2.$$

Motivation

- In practice quantum automata are the implementable quantum gadgets;
- They are currently used to implement quantum protocols and quantum machines
  - A large spectrum of such gadgets is used to implement perfectly secure communications
  - There is already a large quantum computer
- Engineering bottleneck: High dimensional quantum automata are hard to implement

Open problems

- How to obtain the minimal dimensional QA that behaves the same as a given one? [Moore and Crutchfield TCS 2000]
- (How to find the minimal cover of a stochastic Mealy machines: Paz 1971)
- Is it even decidable?
- If so, what is the complexity.

Categorical context

Recall that $\mathbb{C}$-**Lin** is a weak symmetric monoidal category furnished with $\bigotimes_{\mathbb{C}}$ as the monoidal operator and $\mathbb{C}$ as unit.

A *bilinear automaton* over a finite alphabet Σ is a tuple

$$A = \langle Q, \delta, \Gamma, \gamma, I, \lambda \rangle$$

where:

- $Q \in \mathbb{C}$-**Lin** (state object);
- $\Gamma \in \mathbb{C}$-**Lin** (output object);
- $I \in \mathbb{C}$-**Lin** (initialization object);
- $\delta : (\langle \Sigma \rangle_{\mathbb{C}} \bigotimes Q) \to Q \in \mathbb{C}$-**Lin** (next-state morphism);
- $\gamma : Q \to \Gamma \in \mathbb{C}$-**Lin** (output morphism);
- $\lambda : I \to Q \in \mathbb{C}$-**Lin** (initialization morphism).

where $\langle \Sigma \rangle_{\mathbb{C}}$ denotes the $\mathbb{C}$ - linear space generated by Σ.

Categorical context

Since we have a natural bijection

$$\hom_{\mathbb{C}}(\langle\Sigma\rangle_{\mathbb{C}} \bigotimes_{\mathbb{C}} Q, Q) \cong \hom_{\mathbb{C}}(\langle\Sigma\rangle_{\mathbb{C}}, \hom_{\mathbb{C}}(Q,Q)),$$

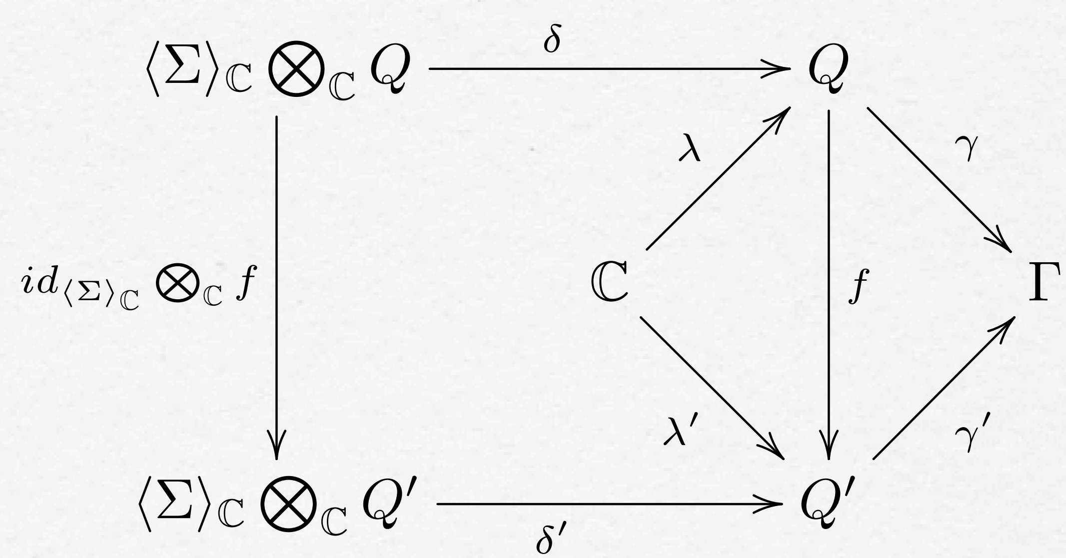
giving $\delta : (\langle\Sigma\rangle_{\mathbb{C}} \bigotimes Q) \to Q$ is the same as giving a morphism

$$\delta^\sharp : \langle\Sigma\rangle_{\mathbb{C}} \to \hom_{\mathbb{C}}(Q,Q),$$

that is uniquely defined by a finite family of morphisms $\{\delta_\sigma : Q \to Q\}_{\sigma\in\Sigma}$.

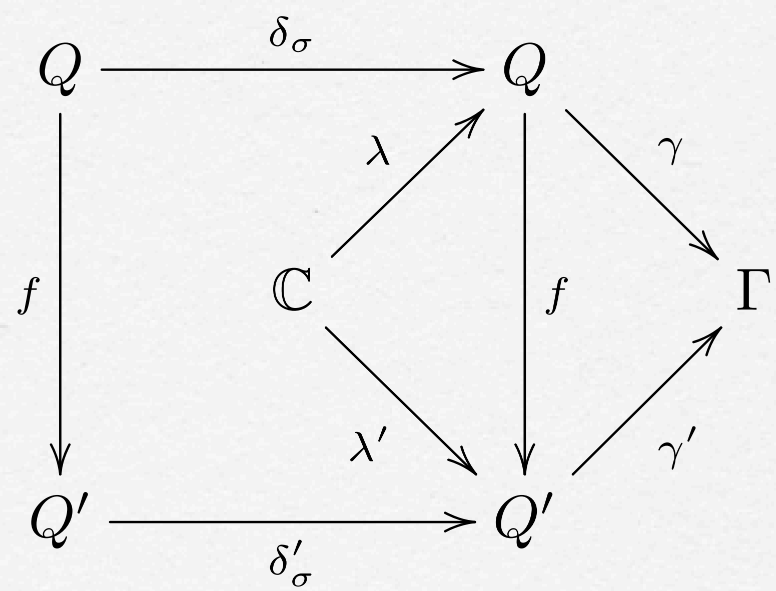
Categorical context

A morphism between two bilinear automata $A = \langle Q, \delta, \Gamma, \gamma, I, \lambda \rangle$ and $A' = \langle Q', \delta', \Gamma, \gamma', I, \lambda' \rangle$ is a $\mathbb{C}$-**Lin** morphism $f : Q \rightarrow Q'$ such that the following diagram commutes



Categorical context

Or equivalently, such that the Σ-indexed family of commutative diagrams



We shall denote the resulting category of bilinear automata by $\mathbf{BAut}^{\Gamma}_{\mathbb{C}}$.

Categorical context

The free $(\langle\Sigma\rangle_{\mathbb{C}} \bigotimes_{\mathbb{C}} \_\,)$-algebra generated by $\mathbb{C}$ is

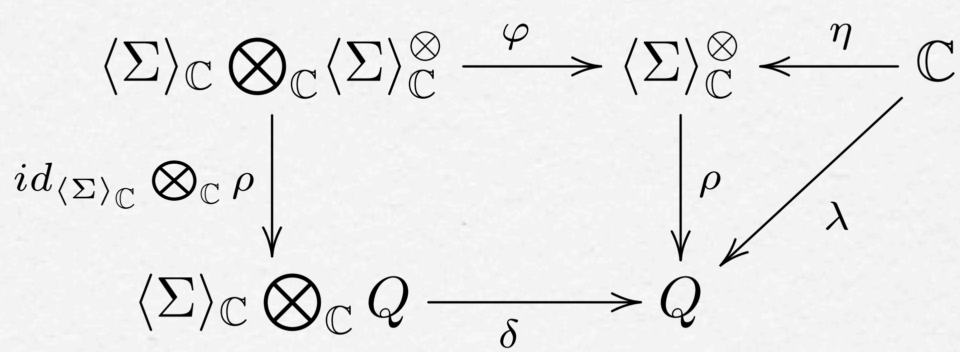
$$\langle\Sigma\rangle_{\mathbb{C}} \bigotimes_{\mathbb{C}} \langle\Sigma\rangle_{\mathbb{C}}^{\otimes} \xrightarrow{\varphi} \langle\Sigma\rangle_{\mathbb{C}}^{\otimes} \xleftarrow{\eta} \mathbb{C}$$

where $\langle\Sigma\rangle_{\mathbb{C}}^{\otimes} = \mathbb{C} \bigoplus \langle\Sigma\rangle_{\mathbb{C}} \bigoplus (\langle\Sigma\rangle_{\mathbb{C}} \bigotimes_{\mathbb{C}} \langle\Sigma\rangle_{\mathbb{C}}) \bigoplus ....$

Observe that $\langle\Sigma\rangle_{\mathbb{C}}^{\otimes} \cong \langle\Sigma^*\rangle_{\mathbb{C}}$.

Categorical context

Given a bilinear automata A, the *run map* is the unique morphism ρ such that the following diagram commutes.



If ρ is an epi, we say that A is *reachable.*

We call $\beta = \gamma \circ \rho : \langle\Sigma^*\rangle_{\mathbb{C}} \to \Gamma$ the *behaviour* of A.

We denote the category of bilinear behaviours by $\mathbf{Beh}_{\mathbb{C}}^{\Gamma}$, which has only trivial morphisms, since automata connected by a morphism must have the same behaviour.

Categorical context

A quantum automaton is a bilinear automaton with initialization object $\mathbb{C}$ such that:

- $\delta_\sigma : Q \to Q$ is unitary for all $\sigma \in \Sigma$ with complete hermitean inner product for Q;
- γ is an orthogonal projection onto a subspace $\Gamma' \subseteq Q$ followed by an isomorphism to Γ (that is, Γ is a subobject of Q);
- λ is injective (or more generally any linear map, if we wish to include automata with trivially null behaviour)

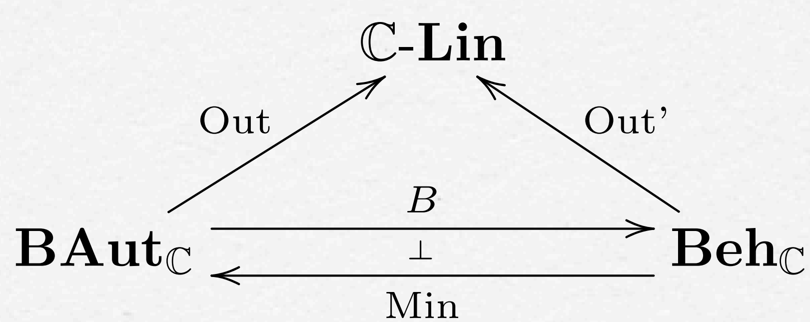
Categorical context

We denote by $\mathbf{QAut}_{\mathbb{C}}^{\Gamma}$ the full subcategory of $\mathbf{BAut}_{\mathbb{C}}^{\Gamma}$ constituted by quantum automata.

Similarly, we denote by $\mathbf{QBeh}_{\mathbb{C}}^{\Gamma}$ the full subcategory of $\mathbf{Beh}_{\mathbb{C}}^{\Gamma}$ with quantum behaviours.

Categorical context

Theorem For any behaviour $\beta : \langle\Sigma\rangle_{\mathbb{C}}^{\otimes} \to \Gamma$ there is a minimal realization for β and with initialization object $\mathbb{C}$.



Theorem Let $\beta : \langle\Sigma\rangle_{\mathbb{C}}^{\otimes} \to \Gamma$ be a behaviour in $\mathbf{QBeh}_{\mathbb{C}}^{\Gamma}$. Then there exists a minimal realization in $\mathbf{QAut}_{\mathbb{C}}^{\Gamma}$ for β.

Computational algebra

Theorem [Tarski, Renegar] Let $\mathbf{P}(x)$ be a predicate which is a Boolean function of atomic predicates either of the form $f_i(x) \geq 0$ or $f_j(x) > 0$, with f's being real polynomials. There is an algorithm to decide whether the set $\mathbb{S} = \{x \in \mathbb{R}^n : \mathbf{P}(x)\}$ is nonempty in PSPACE in n, m, d, where n is the number of variables, m is the number of atomic predicates, and d is the highest degree among all atomic predicates of $\mathbf{P}(x)$. Moreover, there is an algorithm of time complexity $(md)^{O(n)}$ for this problem. To find a sample of $\mathbb{S}$ requires $\tau d^{O(n)}$ space if all coefficients of the atomic predicates use at most τ space.

Computational algebra

Theorem: Quantum automata (and SMM, QMM, etc...) can be minimized in EXPSPACE

P. Mateus, D. Qiu, and L. Li. On the complexity of minimizing probabilistic and quantum automata. *Information and Computation*, 218:36–53, 2012.

1. Firstly, for a given automaton $\mathcal{A}$ of some type (say probabilistic, quantum, etc.) with n states, we define the set

$$\mathbb{S}_{\mathcal{A}}^{(n')} = \{\mathcal{A}' : \mathcal{A}' \text{ has } n' \text{ states, is of the same type of } \mathcal{A}\text{, and is equivalent to } \mathcal{A}\}.$$

2. Next, we show that $\mathbb{S}_{\mathcal{A}}^{(n')}$ can be described as the solution of a system of polynomial equations and/or inequations if the **automata can be bilinearized**. Then there exists an algorithm to decide whether $\mathbb{S}_{\mathcal{A}}^{(n')}$ is nonempty or not, and furthermore, if it is nonempty, we can find a sample of it.

Computational algebra

Input: an automaton $\mathcal{A}$ with n states
Output: a minimal automaton $\mathcal{A}^{'}$, of the same type of $\mathcal{A}$, and equivalent to $\mathcal{A}$
Step 1:

For $i = 1$ to $n - 1$
If ($\mathbb{S}_{\mathcal{A}}^{(i)}$ is not empty) Return $\mathcal{A}' =$ sample $\mathbb{S}_{\mathcal{A}}^{(i)}$

Step 2:

Return $\mathcal{A}' = \mathcal{A}$

Applications

N. Paunkovic, J. Bouda, and P. Mateus. Fair and optimistic quantum contract signing. *Physical Review A*, 84(6):062331, 2011.

F. Assis, A. Stojanovic, P. Mateus, and Y. Omar. Improving classical authentication over a quantum channel. *Entropy*, 14(12):2531–2549, 2012.

L. Li, D. Qiu, and P. Mateus. Quantum secret sharing with classical Bobs. *Journal of Physics A: Mathematical and Theoretical*, 46(4):045304, 2013.

Quantum Turing Machine

- By a *quantum Turing machine* we mean a binary Turing machine with two tapes, one classical and the other with quantum contents, which are infinite in both directions.
- Depending only on the state of the classical finite control automaton and the symbol being read by the classical head, the quantum head acts upon the quantum tape, a symbol can be written by the classical head, both heads can be moved independently of each other and the state of the control automaton can be changed.
- A computation ends if and when the control automaton reaches the halting state (q_h).

Quantum Turing Machine

Initially:

- the QTM is in the starting state ($\mathsf{q_s}$);
- the classical tape is filled with blanks (that is, with $\Box$'s) outside the finite input sequence x of bits,
- the classical head is positioned over the rightmost blank before the input bits,
- the quantum tape contains three independent sequences of qubits – an infinite sequence of $|0\rangle$'s followed by the finite input sequence $|\psi\rangle$ of possibly entangled qubits followed by an infinite sequence of $|0\rangle$'s,
- the quantum head is positioned over the rightmost $|0\rangle$ before the input qubits.

Quantum Turing Machine

The QTM is a partial map

$$\delta : Q \times \mathbb{A} \rightharpoonup \mathbb{U} \times \mathbb{D} \times \mathbb{A} \times \mathbb{D} \times Q$$

where:

- Q is the finite set of control states containing at least the two states $\mathsf{q_s}$ and $\mathsf{q_h}$ mentioned above;
- $\mathbb{A}$ is the alphabet composed of 0, 1 and $\Box$;
- $\mathbb{U}$ is the set $\{\mathsf{Id}, \mathsf{H}, \mathsf{S}, \pi/8, \mathsf{Sw}, \mathsf{c\text{-}Not}\}$ of primitive unitary operators that can be applied to the quantum tape; and
- $\mathbb{D}$ is the set $\{\mathsf{L}, \mathsf{N}, \mathsf{R}\}$ of possible head displacements – one position to the left, none, and one position to the right.

Quantum Turing Machine

- The machine is said *to start from* $(x, |\psi\rangle)$ or to receive *input* $(x, |\psi\rangle)$ if:
  - the initial content of the classical tape is x surrounded by blanks and the classical head is positioned in the rightmost blank before the classical input x;
  - the initial content of the quantum tape is $|\psi\rangle$ surrounded by $|0\rangle$'s and the quantum head is positioned in the rightmost $|0\rangle$ before the quantum input $|\psi\rangle$.

Quantum Turing Machine

- The machine is said *to halt at* $(y, |\varphi\rangle)$ if the computation terminates and:
  - the final content of the classical tape is y surrounded by blanks and the classical head is positioned in the rightmost blank before the classical output y;
  - the final content of the quantum tape is $|\varphi\rangle$ surrounded by $|0\rangle$'s and the quantum head is positioned in the rightmost $|0\rangle$ before the quantum output $|\varphi\rangle$.

In this situation we may write

$$M(x, |\psi\rangle) = (y, |\varphi\rangle).$$

Categorical context

Consider the category **QTur** where:

- Objects are pairs $(x, |\psi\rangle)$ where $x \in 2^*$ and $|\psi\rangle$ is a (computable) unit vector;
- Morphisms are quantum Turing machines $M = (Q, \delta)$ such that

  $$M : (x, |\psi\rangle) \to (y, |\varphi\rangle)$$

  if $M(x, |\psi\rangle) = (y, |\varphi\rangle)$.

Turing machines can be composed, and moreover the trivial Turing machine (with just the halting state) is the identity.

We assume that **QTur** is endowed with a tensor product

$$(x_1, |\psi_1\rangle) \otimes (x_2, |\psi_2\rangle) = (\gamma(x_1, x_2), |\psi_1\rangle \otimes |\psi_2\rangle)$$

where γ is an encoding of a pair of strings to a string. Such tensor product makes **QTur** a symmetric monoidal category.

Categorical context

Let

- $Id_Q : \mathbf{QTur} \to \mathbf{QTur}$ be the identity functor.
- $D : Id_Q \downarrow Id_Q \to 2^* \times 2^* \times 2^*$ be the description functor that maps each quantum Turing machine to the triple containing a string that describes the Turing machine, as well as the domain and codomain of the morphism.

Theorem[Existence of universal machine] The universal functor

$$U(w, \underline{x}, \underline{y}) : (w, |\varepsilon\rangle) \otimes (x, |\psi\rangle) \to (y, |\varphi\rangle)$$

is left adjoint to D.

Kolmogorov complexity

- $K(|\varphi\rangle || \psi\rangle)$ is the minimum number of states of QTM M such that $M(\varepsilon, |\psi\rangle) = (\varepsilon, |\varphi\rangle)$.
- It is undecidable
- Relevant for classifying quantum states in terms of preparation hardness
- Again a minimization issue!
- P. Mateus, A. Sernadas and A. Souto. Universality of quantum Turing machines with deterministic control, submitted for publication 2014.

Thank you...