QUANTUM COMPUTING 8.

Jozef Gruska

Faculty of Informatics
Brno
Czech Republik

October 27, 2020

8. QUANTUM FINITE AUTOMATA

as models of small memory quantum processors

WHY to STUDY QUANTUM PROCESSORS WITH SMALL MEM

There are three main reasons why it is of interest and importance to investigate models of quantum processors that use little of quantum resources. and importance.

1. Experiences with classical information processing strongly suggest that investigation of the models of processors with finite memory and working in real-time brings a huge variety of fundamental theoretical results for information processing and, at the same time, provides a variety of methods and tools to design such processors.

2. Two decades of the research in quantum information processing start to make clear that not very powerful, with hundreds of qubits, quantum processors, but processors using only little of quantum resources, are to be seen currently as the goal that could be both feasible and worth to make – because theoretical results have already demonstrated that they can, in some cases, bring significant increase of the information processing power.

3. Processors combining huge classical and small quantum resources should therefore be seen as the next goal in quantum information processing once the current concentration of the research on few qubits storage, few particles entanglement and few unitary operations circuits start to rich fully satisfactory outcomes.

MODELS OF QUANTUM AUTOMATA

Models of quantum automata
For most of the main classical models of automata there are also their quantum versions. For example for finite automata, Turing machines and quantum cellular automata (QCA).
Models of quantum automata are used:

- To get an insight into the power of different quantum computing models and modes, using language/automata theoretic methods.
- To discover the simplest models of computation at which one can demonstrate large (or huge) difference in the power of quantum versus classical models.
- To develop quantum automata (networks, algorithms) design methodologies.
- To explore mutual relations between different quantum computation models and modes.
- To discover, in a transparent and elegant form, limitations of quantum computations and communications.

WHY to STUDY QUANTUM PROCESSORS WITH SMALL MEM

Using such models one can also get deeper insides about:

- How much more power, concerning computation, can bring quantum (randomness) resources comparing with classical (randomness) resources?
- How much more power can have computation in linear time comparing with with that in real time?
- How much more power can bring computation with mixed states comparing that with pure states?
- When and how much more power can bring addition of very little of quantum resources?

MAIN MODELS of CLASSICAL PROCESSORS

Main classical models of processors are:

- Finite automata (deterministic, non-deterministic, probabilistic, ultrametric,...., one-way, two-way,...; one-tape, multi-tape,....)
- Turing machines (with one or more tapes, with one or more heads, with one or more dimensional tapes - deterministic, non-deterministic, probabilistic,...) - models of universal processors
- Uniform classes of circuits - models of universal processors
- Cellular automata (one-, two-, three- and more dimensional)– models of universal processors.

Of importance, especially for an understanding of the power and development of methods (of programming) for very powerful real processors are also the following models:

- RAM - Random access machines
- PRAM - Parallel and shared memory random access machines

MAIN MODELS of QUANTUM AUTOMATA

1. QUANTUM FINITE AUTOMATA (QFA)

   QFA are considered to be the simplest model of quantum processors, with "finite" quantum memory, that models well the most basic mode of quantum computing — a quantum action is performed on each classical input.

2. QUANTUM (one-tape and many-tape) TURING MACHINES (QTM)

   QTM are used to explore, at the most general level of sequential computation, the potential and limitations of quantum computing. Using this model the main computational complexity classes are defined. QTM are a main quantum abstraction of human computational processes.

3. QUANTUM CELLULAR AUTOMATA (QCA)

   QCA are used to model and to explore, on every general and basic level of parallel computation, the potential and limitations of quantum computing. QCA are a very basic quantum abstraction of computation by nature.

Main classical modes of computation:
deterministic, nondeterministic and randomized.

BASIC MODELS of CLASSICAL FINITE AUTOMATA

- Deterministic (one-way) finite automata.
- Deterministic two-way finite automata.
- Nondeterministic finite automata (one-way or two-way)
- Probabilistic (randomized) versions of finite automata

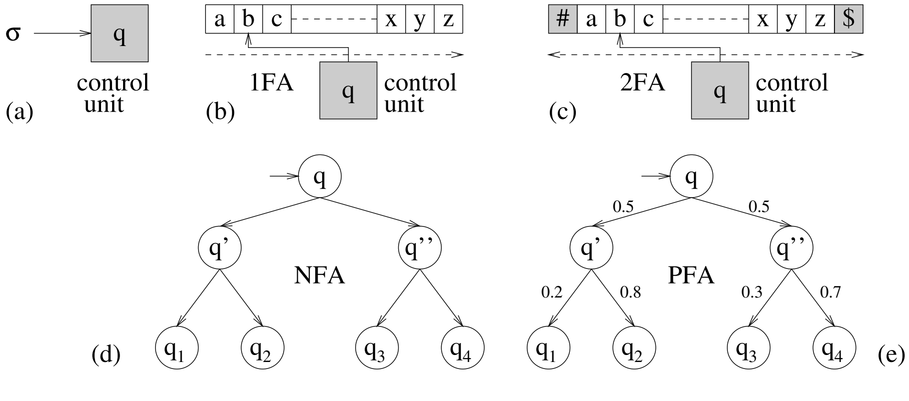


Figure 1: Models of finite automata

FROM MODELS of CLASSICAL AUTOMATA to MODELS of QUA

For the most of the main classical models of automata there are also their quantum versions.

Models of quantum automata are used:

- To get a deeper insight into the power of different quantum computing models and modes, using language/automata theoretic methods.
- To discover the simplest models of computation at which one can clearly demonstrate large (or huge) difference in the power of quantum versus classical models.
- To develop quantum automata (networks, algorithms) design methodologies.
- To explore mutual relations between different quantum computation models and modes.
- To discover, in a transparent and elegant form, limitations of quantum computations and communications.

MAIN MODES of COMPUTATION of FINITE AUTOMATA

Basic modes:

Deterministic automata (DFA): In each step next configuration is uniquely (deterministically) determined. An input is accepted if it makes the automaton to reach an accepted state.

Non-deterministic automata (NFA): In each step one of possible configurations is taken. An input is accepted if it can make the automaton to reach an accepted state.

Probabilistic automata (PFA): In each step each possible configuration has a probability assigned. An input is accepted if it makes automaton to reach an accepting state with a certain probability - several modes of that are considered.

Ultrametric automata (UFA): In each step each possible transition has a p-adic number assigned. Acceptance of an input is considered as in probabilistic case.

Quantum automata (QFA): In each step each possible configuration has a complex number, probability amplitude, assigned and automaton can be at any step in a superposition of configurations. An input is accepted if it makes automaton to reach a configuration of accepting states with a certain probability.

MAIN PROPERTIES of CLASSICAL FINITE AUTOMATA

- The concept of classical finite automata is very robust - all main variants of the basic model have the same recognition power.
- Informally, classical finite automata can do exactly that what can be done in real-time - in time needed to read input - and with finite (input length independent) memory.
- Formally, classical finite automata can recognize exactly the class of regular languages - the class of languages containing finite languages and closed under operations of union, concatenation and iteration.
- For each regular language L there is a unique minimal finite deterministic automaton accepting L - minimization problem is therefore well defined.
- There is an efficient algorithm to find the minimal deterministic finite automaton with.
- All major decision problems for finite classical automata are decidable.
- To study various classes of languages accepted by classical finite automata a variety of rich algebraic methods can be used to get deep insights.

MAIN PROBLEMS to EXPLORE for MODELS of Q

- Recognition (processing) power of various models of quantum automata - properties and characterization of the classes of languages accepted by different models of quantum automata.
- What kind of acceptance probabilities are achievable?
- Succinctness relation to the corresponding models of quantum automata - how much smaller can quantum automata be for doing the same task as classical automata of the similar type.
- Decidability of basic decision problems - for example of the equivalence problem.
- Decidability of basic decision problems - for example of the equivalence problem.
- Development and complexity study of methods to construct minimal quantum automata for the case of various models of quantum automata.

MAIN DIVISIONS of QUANTUM MODELS of FINITE AUTOMA

There are three main ways to divide models of quantum finite automata:

1. According to head moves and power:
   - all heads have always to read the same symbol and have always move in one direction
   - all heads can move only in one direction but sometimes may be stationary
   - heads can move independently in both directions
   - heads can always read only one input symbol or can read k of them for a fixed k.
2. According to the power of quantum operations and measurements - from unitary operations to completely positive trace preserving operations and from projective measurements to POVM measurements.
3. Between automata with quantum actions only to automata with some combination of classical and quantum actions.

FROM CLASSICAL TO QUANTUM AUTOMATA

The basic formal way to develop a quantum version of a classical automata model is

to replace in its probabilistic version probabilities of transitions by probability amplitudes.

The main problem is to do this replacement in such a way that a to-be-quantum automaton is really quantum, that is that its evolution is unitary.

QUANTUM FINITE AUTOMATA

Input: $\#w_1 \ldots w_n\$$ $\#w\$,$ $|w| = n$

States: $Q = Q_a \cup Q_r \cup Q_n$

Configuration (q, i) — a state and a position on the input tape
Set of configurations: $C(Q, w) = \{(q, i) \,|\, q \in Q, 0 \leq i \leq |w| + 1\}$

Hilbert space: $l(C(Q, w))$ **Transitions:**

$\delta(q, i) = \Sigma_{q' \in Q, 1 \leq j \leq n} \alpha_{q',j} |(q', j)\rangle$
(Evolution has to be unitary.)

Measurements: Projections into one of the subspaces:

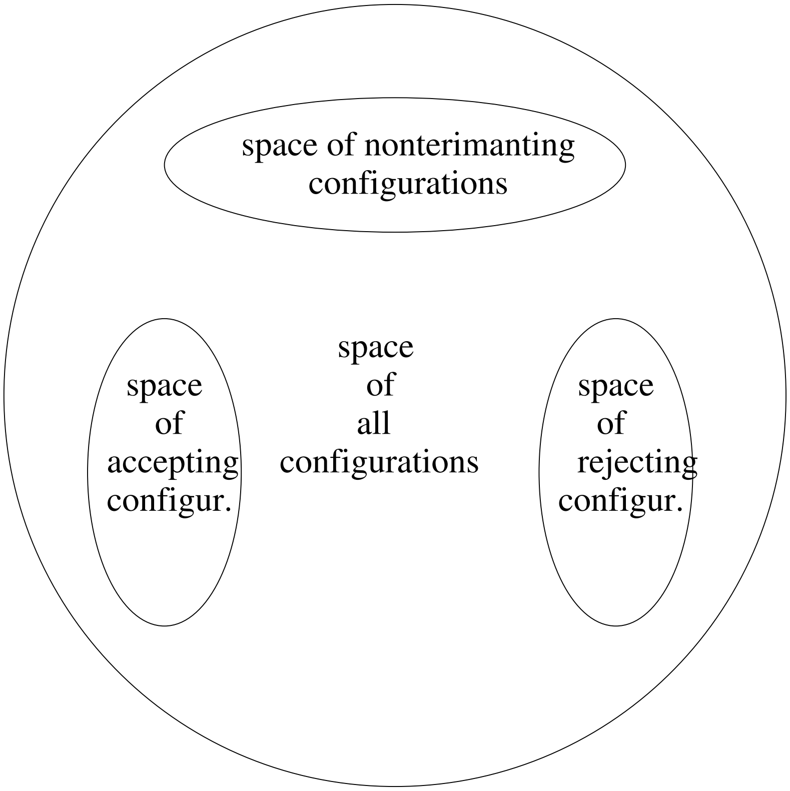
$$E_a = l(\{(q, i) \,|\, q \in Q_a\}), E_r = l(\{(q, i) \,|\, q \in Q_r\}), E_l = l(\{(q, i) \,|\, q \in Q_n\})$$

Measurement modes:

- MM-mode (*many measurements* mode)
- MO-mode (*measurement once* mode)

QUANTUM MEASUREMENT IN QUANTUM AUTOMATA

The main type of the measurement used so far in quantum finite automata theory represents a projection into three subspaces: of accepting configurations, of rejecting configurations and of nonterminating configurations.


space of nonterimanting configurations
space of accepting configur.
space of all configurations
space of rejecting configur.

ONE-WAY QUANTUM FA

Definition 0.1 *A* **one-way (real-time) quantum finite automaton** *(1QFA) $\mathcal{A}$ is given by: Σ — the input alphabet; Q — the set of states; q_0 – the initial state; $Q_a \subseteq Q$, $Q_r \subseteq Q$, $Q_n = Q - Q_a - Q_r$, $Q_a \cap Q_r = \emptyset$ are sets of accepting, rejecting and nonterminating states and the transition function*

$$\delta : Q \times \Gamma \times Q \to C_{[0,1]},$$

where $\Gamma = \Sigma \cup \{\#, \$\}$ and $\#$, $\$$ are endmarkers.

The evolution (computation) of $\mathcal{A}$ is performed on the Hilbert space $l_2(Q)$ with basis states $\{|q\rangle \,|\, q \in Q\}$ using unitary operators $V_\sigma, \sigma \in \Gamma$, defined by

$$V_\sigma|q\rangle = \sum_{q' \in Q} \delta(q, \sigma, q')|q'\rangle.$$

For **measurement** the **computational observable** is used that corresponds to the direct sum of $l_2(Q)$:

$$l_2(Q) = E_a \oplus E_r \oplus E_n,$$

where

$$E_a = \mathsf{span}\{|q\rangle \,|\, q \in Q_a\}$$
$$E_r = \mathsf{span}\{|q\rangle \,|\, q \in Q_r\}$$
$$E_n = \mathsf{span}\{|q\rangle \,|\, q \in Q_n\}$$

TWO COMPUTATION MODES for 1QFA

1. MANY-MEASUREMENT COMPUTATION MODE

   Computation of $\mathcal{A}$ on an input $\#\sigma_1 \ldots \sigma_n\$$: At first the operator $V_\#$ is applied to the initial state $|q_0\rangle$ and then the observable O is applied to the resulting state. Let $|\psi'\rangle$ be the resulting state:

   - If $|\psi'\rangle \in E_a$, the input is accepted (with probability equal to square of the norm of $|\psi'\rangle$).
   - If $|\psi'\rangle \in E_r$, the input is rejected (with probability equal to square of the norm of $|\psi'\rangle$).
   - If $|\psi'\rangle \in E_n$, then $|\psi'\rangle$ is not normalized and the pair of operators OV_{σ_1} is applied.

   The above process, an application of operators

   $$OV_{\sigma_i}, i = 1, \ldots, n$$

   continues and ends by operators $OV_\$$.

2. ONE-MEASUREMENT COMPUTATION MODE

   A computation of $\mathcal{A}$ consists in an application, on $|q_0\rangle$, of the following sequence of operators:

   $$OV_\$ V_{\sigma_n} V_{\sigma_{n-1}} \ldots V_{\sigma_2} V_{\sigma_1} V_\#.$$

ACCEPTANCE and REJECTION PROBABILITIES FORMALLY

In case of 1QFA, the projection measurement can be defined through three projections

$$P_a = \sum_{q\in Q_a} |q\rangle\langle q|, \quad P_r = \sum_{q\in Q_r} |q\rangle\langle q|, P_n = \sum_{q\in Q_n} |q\rangle\langle q|$$

and then the acceptance and rejection probabilities in the case of an input string

$$\sigma_1\sigma_2\ldots\sigma_m\$$$

and the initial state $|\phi_0\rangle$ can be formally expressed as follows.

$$\mathrm{Pr}_a = \sum_{k=1}^{m+1} ||P_aV_{\sigma_k}\prod_{i=1}^{k-1}(P_nV_{\sigma_i})|\phi_0\rangle||^2$$

$$\mathrm{Pr}_r = \sum_{k=1}^{m+1} ||P_rV_{\sigma_k}\prod_{i=1}^{k-1}(P_nV_{\sigma_i})|\phi_0\rangle||^2$$

where we define $\Pi_{i=1}^{n} A_i = A_nA_{n-1}\ldots A_1$ instead of $A+1A_2\ldots A_n$.

ACCEPTANCE of WORDS and LANGUAGES by 1QFA

A 1QFA $\mathcal{A}$ accepts (rejects) a word w of length n with probability p if p is the sum of probabilities p_i that w is accepted (rejected) after i symbols of w are scanned for $i = 1, \ldots, n$.

A 1QFA $\mathcal{A}$ accepts a language L with probability $\frac{1}{2} + \varepsilon, \varepsilon > 0$, if $\mathcal{A}$ accepts (rejects) any $x \in L$ $(x \notin L)$ with probability at least $\frac{1}{2} + \varepsilon$.

If there is an ε such that $\mathcal{A}$ accepts L with probability $\frac{1}{2} + \varepsilon$, then $\mathcal{A}$ is said to accept L with **BOUNDED ERROR PROBABILITY**.

A language L is accepted by $\mathcal{A}$ with **UNBOUNDED ERROR PROBABILITY** if $x \in L$ $(x \notin L)$ is accepted (rejected) with probability at least $\frac{1}{2}$.

LANGUAGE ACCEPTANCE by QFA

For a given QFA (or a PFA) $\mathcal{A}$ and its input w over an input alphabet Σ, we denote by $Pr_{\mathcal{A}}(w)$ the probability that input w makes the automaton $\mathcal{A}$ to get to an accepting state.

On this basis one can define in several ways language, that is a set of words over the input alphabet Σ accepted by the automaton $\mathcal{A}$.

The concept of language is here a formalization of a decision problem - a problem that has for each input instance the answer "yes" or "no". Two basic modes for acceptance,

often with very different power, are that of **unbounded error acceptance** and **bounded error acceptance**

UNBOUNDED ERROR ACCEPTANCE

A language $L \subseteq \Sigma^*$ recognized by an automaton $\mathcal{A}$ with cutpoint λ is defined as

$$L = \{w \in \Sigma^* \,|\, Pr_{\mathcal{A}}(w) > \lambda\}$$

Specifically, L is recognized by $\mathcal{A}$ with

two-sided unbounded error if
$L = \{w \in \Sigma^* \,|\, Pr_{\mathcal{A}}(w) > \frac{1}{2}\}$;

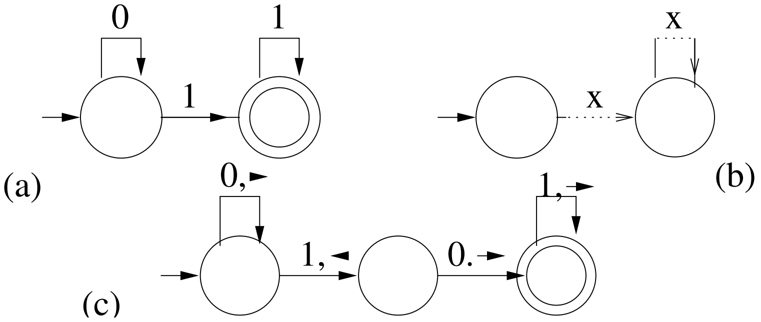
one-sided unbounded error if
$L = \{w \in \Sigma^* \,|\, Pr_{\mathcal{A}}(w) > 0\}$;

BOUNDED ERROR ACCEPTANCE

A language $L \subseteq \Sigma^*$ is recognized by an automaton $\mathcal{A}$ with an isolated cutpoint $\lambda \in [0, 1)$ if there exists an $\delta > 0$ such that $Pr_{\mathcal{A}}(w) \notin (\lambda - \delta, \lambda + \delta)$ for all $w \in \Sigma^*$.

Specifically, L is recognized by $\mathcal{A}$ with bounded error $p \in (\frac{1}{2}, 1]$ if

- $Pr_{\mathcal{A}}(w) \geq p$ when $w \in L$
- $Pr_{\mathcal{A}}(w) \leq 1 - p$ when $w \notin L$



Example. A 1QFA accepting $L = \{0^i 1^j \mid i \geq 0, j \geq 0\}$ with probability $p = 0.68$ (such that $p = 1 - p^3$).

States: $Q = \{q_0, q_1, q_2, q_a, q_r\}, Q_a = \{q_a\}$, $Q_r = \{q_r\}$. **Transitions:**

$$V_{\#}|q_0\rangle = \sqrt{1-p}|q_1\rangle + \sqrt{p}|q_2\rangle,$$

$$V_0|q_1\rangle = (1-p)|q_1\rangle + \sqrt{p(1-p)}|q_2\rangle + \sqrt{p}|q_r\rangle,$$

$$V_0|q_2\rangle = \sqrt{p(1-p)}|q_1\rangle + p|q_2\rangle - \sqrt{1-p}|q_r\rangle,$$

$$V_1|q_1\rangle = |q_r\rangle, V_1|q_2\rangle = |q_2\rangle, \quad V_{\$}|q_1\rangle = |q_r\rangle, V_{\$}|q_2\rangle = |q_a\rangle.$$

The remaining transitions are defined arbitrarily to satisfy unitarity.

The above example is the basis of the following result:

Theorem There is a regular language that can be recognized by a MM-1QFA with probability $0.68\ldots$ but neither by MM-1QFA with probability at least $\frac{7}{9} + \varepsilon$ nor by RFA.

PROOF OF ACCEPTANCE — CASE 1

Example. A 1QFA accepting $L = \{0^i 1^j \,|\, i \geq 0.j \geq 0\}$ with probability $p = 0.68$ (t $p = 1 - p^3$).

States: $Q = \{q_0, q_1, q_2, q_a, q_r\}, Q_a = \{q_a\}$, $Q_r = \{q_r\}$. **Transitions:**

$$V_{\#}|q_0\rangle = \sqrt{1-p}|q_1\rangle + \sqrt{p}|q_2\rangle,$$

$$V_0|q_1\rangle = (1-p)|q_1\rangle + \sqrt{p(1-p)}|q_2\rangle + \sqrt{p}|q_r\rangle, \;\; V_0|q_2\rangle = \sqrt{p(1-p)}|q_1\rangle + p|q_2\rangle - \sqrt{1 -$$

$$V_1|q_1\rangle = |q_r\rangle, V_1|q_2\rangle = |q_2\rangle, \quad V_{\$}|q_1\rangle = |q_r\rangle, V_{\$}|q_2\rangle = |q_a\rangle.$$

The remaining transitions are defined arbitrarily to satisfy

CASE 1 $w = 0^i$

Since

$$V_0(\sqrt{1-p}|q_1\rangle + \sqrt{p}|q_2\rangle) = \sqrt{1-p}|q_1\rangle + \sqrt{p}|q_2\rangle$$

the automaton $\mathcal{A}$ remains in the state

$$\sqrt{1-p}|q_1\rangle + \sqrt{p}|q_2\rangle$$

while reading 0^i.

At the right endmarker the operator $V_{\$}$ provides the state

$$\sqrt{1-p}|q_r\rangle + \sqrt{p}|q_a\rangle$$

and therefore $\mathcal{A}$ accepts the input 0^i with probability p

PROOF OF ACCEPTANCE — CASE 2

Example. A 1QFA accepting $L = \{0^i 1^j \mid i \geq 0.j \geq 0\}$ with probability $p = 0.68$ ($p = 1 - p^3$).

States: $Q = \{q_0, q_1, q_2, q_a, q_r\}, Q_a = \{q_a\}$, $Q_r = \{q_r\}$. **Transitions:**

$$V_{\#}|q_0\rangle = \sqrt{1-p}|q_1\rangle + \sqrt{p}|q_2\rangle,$$

$$V_0|q_1\rangle = (1-p)|q_1\rangle + \sqrt{p(1-p)}|q_2\rangle + \sqrt{p}|q_r\rangle, \quad V_0|q_2\rangle = \sqrt{p(1-p)}|q_1\rangle + p|q_2\rangle - \sqrt{1 -$$

$$V_1|q_1\rangle = |q_r\rangle, V_1|q_2\rangle = |q_2\rangle, \quad V_{\$}|q_1\rangle = |q_r\rangle, V_{\$}|q_2\rangle = |q_a\rangle.$$

CASE 2 $x = 0^i 1^j, i \geq 0, j > 0$.

$\mathcal{A}$ will be in the state

$$\sqrt{1-p}|q_1\rangle + \sqrt{p}|q_2\rangle$$

after reading 0^i. The first 1 changes the state into

$$\sqrt{1-p}|q_r\rangle + \sqrt{p}|q_2\rangle$$

afterwards, the nonhalting part, obtained with probabilty p, is

$$|q_2\rangle$$

keep being unchanged till the right endmarker $\$$, and then it is changed into

$$|q_a\rangle.$$

The acceptance probability is therefore p.

PROOF OF ACCEPTANCE — CASE 3

States: $Q = \{q_0, q_1, q_2, q_a, q_r\}, Q_a = \{q_a\}$, $Q_r = \{q_r\}$. **Transitions:**

$$V_\#|q_0\rangle = \sqrt{1-p}|q_1\rangle + \sqrt{p}|q_2\rangle,$$

$$V_0|q_1\rangle = (1-p)|q_1\rangle + \sqrt{p(1-p)}|q_2\rangle + \sqrt{p}|q_r\rangle, \quad V_0|q_2\rangle = \sqrt{p(1-p)}|q_1\rangle + p|q_2\rangle - \sqrt{1-}$$

$$V_1|q_1\rangle = |q_r\rangle, V_1|q_2\rangle = |q_2\rangle, \quad V_\$|q_1\rangle = |q_r\rangle, V_\$|q_2\rangle = |q_a\rangle.$$

CASE 3 x has a prefix of the type $0^i1^j0^k, i \geq 0, j > 0, k > 0$. (That is $x \notin L$.) After reading the first symbol 1 $\mathcal{A}$ is in the state

$$\sqrt{1-p}|q_r\rangle + \sqrt{p}|q_2\rangle$$

and rejects with probability $1-p$.

The nonhalting part $|q_2\rangle$, obtained with probability p, is changed only by first 0 into

$$\sqrt{p(1-p)}|q_1\rangle + p|q_2\rangle - \sqrt{(1-p)}|q_r\rangle$$

and, at this moment, $\mathcal{A}$ rejects with the overall probability $p(1-p)$. The nonhalting part of the state

$$\sqrt{p(1-p)}|q_1\rangle + p|q_2\rangle$$

is not changed by 0s and only at the right endmarker it is changed into

$$\sqrt{p(1-p)}|q_r\rangle + p|q_a\rangle$$

The input is therefore rejected with probability

$$(1-p) + p(1-p) + p^2(1-p) = 1 - p^3 = p.$$

A 1QFA accepting the language

$$L = \{0^i 1^j \,|\, i \geq 0, j \geq 0\}$$

Transition matrices:

$$\begin{pmatrix} 0 & \sqrt{1-p} & \sqrt{p} & 0 & 0 \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \end{pmatrix} \quad \begin{pmatrix} - & - & - & - & - \\ 0 & 1-p & \sqrt{p(1-p)} & 0 & 0\sqrt{p} \\ 0 & \sqrt{p(1-p)} & p & 0 & -\sqrt{1-p} \\ - & - & - & - & - \\ - & - & - & - & - \end{pmatrix}$$

$$\begin{pmatrix} - & - & - & - & - \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ - & - & - & - & - \\ - & - & - & - & - \end{pmatrix} \quad \begin{pmatrix} - & - & - & - & - \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ - & - & - & - & - \\ - & - & - & - & - \end{pmatrix}$$

BASIC RESULTS - POWER and DECIDABILITY[1]

Theorem MM-1QFA can accept only regular languages but not all of them. For example not the language $L = \{0,1\}^*0$.

Theorem The family of languages accepted by MM-1QFA is closed under complement, inverse homomorphism and word quotients, but not under homomorphism.

Results concerning succinctness of quantum finite automata:

- In some cases (sequential) quantum one-way finite automata can be, due to the parallelism in their evolution, exponentially more succinct than classical DFA.
- In some cases quantum one-way finite automata can be, due to their requirement on unitarity of their evolution, exponentially larger, with respect to the number of states, as the corresponding DFA.

[1] Results are due to Ambainis, Brodsky, Freivalds, Kondacs, Pippenger, Watrous

TYPES OF QUANTUM FINITE AUTOMATA

2QFA — Two way quantum finite automata
Heads can move in both directions

g1QFA — Generalized one-way quantum automata
Heads can (but do not have to) move only in one direction.

1QFA —- Real-time one-way quantum automata
In each step all heads move in the same direction.

RFA — reversible deterministic finite automata (DFA)

2QFA — WELL-FORMEDNESS CONDITIONS

A two-way quantum finite automaton $\mathcal{A}$ is specified by the finite (input) alphabet Σ, the finite set of states Q, the initial state q_0, the sets $Q_a \subset Q$ and $Q_r \subset Q$ of accepting and rejecting states, respectively, with $Q_a \cap Q_r = \emptyset$, and the transition function

$$\delta : Q \times \Gamma \times Q \times \{\leftarrow, \downarrow, \rightarrow\} \longrightarrow \mathbf{C}_{[0,1]},$$

where $\Gamma = \Sigma \cup \{\#, \$\}$ is the tape alphabet of $\mathcal{A}$ and $\#$ and $\$$ are endmarkers not in Σ, which satisfies the following conditions (of well-formedness) for any $q_1, q_2 \in Q$, $\sigma, \sigma_1, \sigma_2 \in \Gamma$, $d \in \{\leftarrow, \downarrow, \rightarrow\}$:

1. **Local probability and orthogonality condition.**
   $\Sigma_{q',d}\, \delta^*(q_1, \sigma, q', d)\delta(q_2, \sigma, q', d) = \begin{cases} 1, & \textbf{if } q_1 = q_2; \\ 0, & \textbf{otherwise.} \end{cases}$
2. **Separability condition I.**
   $\Sigma_{q'}\, \delta^*(q_1, \sigma_1, q', \rightarrow)\delta(q_2, \sigma_2, q', \downarrow) + \Sigma_{q'}\, \delta^*(q_1, \sigma_1, q', \downarrow)\delta(q_2, \sigma_2, q', \leftarrow) = 0.$
3. **Separability condition II.**
   $\Sigma_{q'}\, \delta^*(q_1, \sigma_1, q', \rightarrow)\delta(q_2, \sigma_2, q', \leftarrow) = 0.$

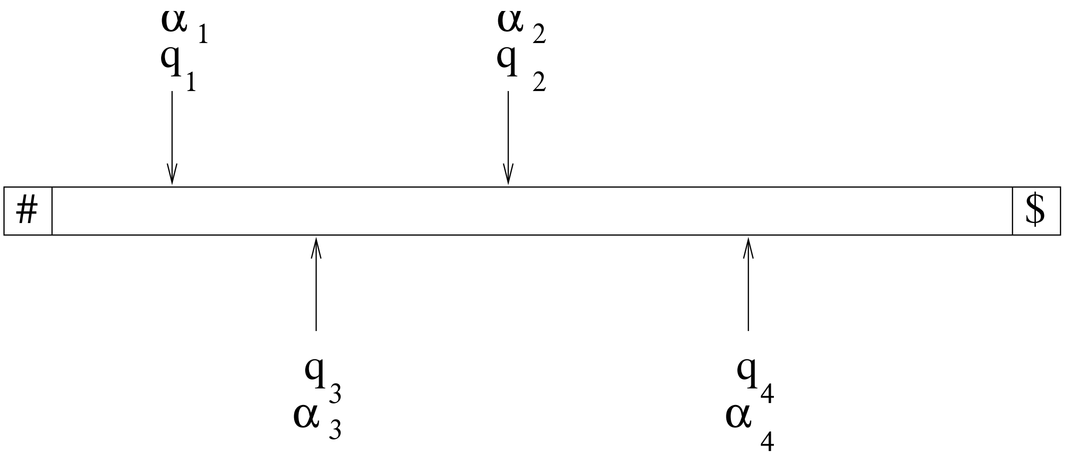
SIMPLIFIED DESCRIPTIONS of 2QFA

- **To each two-way quantum finite automaton there is an equivalent one (the so-called *unidirectional* or *simple*) 2QFA in which**
  1. **For each pair of states q and q' a probability amplitude is assigned that the automaton moves from the state q to the state q'.**
  2. **To each state q a head movement $D(q)$ — to right, to left or no movement — is defined with the interpretation that if automaton comes to a state q, then the head always moves in the direction $D(q)$.**

RECOGNITION POWER OF 2QFA

2QFA can accept any regular language and also some non-regular (even non-context

Power of 2QFA comes from the fact that during their computations the heads of the automaton can be simultaneously on different input symbols and in different states.



$$Q_a = \{s_n\}, Q_r = \{s_1, \ldots, s_{n-1}\}$$

Total state is then:

$$\alpha_1|q_1\rangle + \alpha_2|q_2\rangle + \alpha_3|q_3\rangle + \alpha_4|q_4\rangle,$$

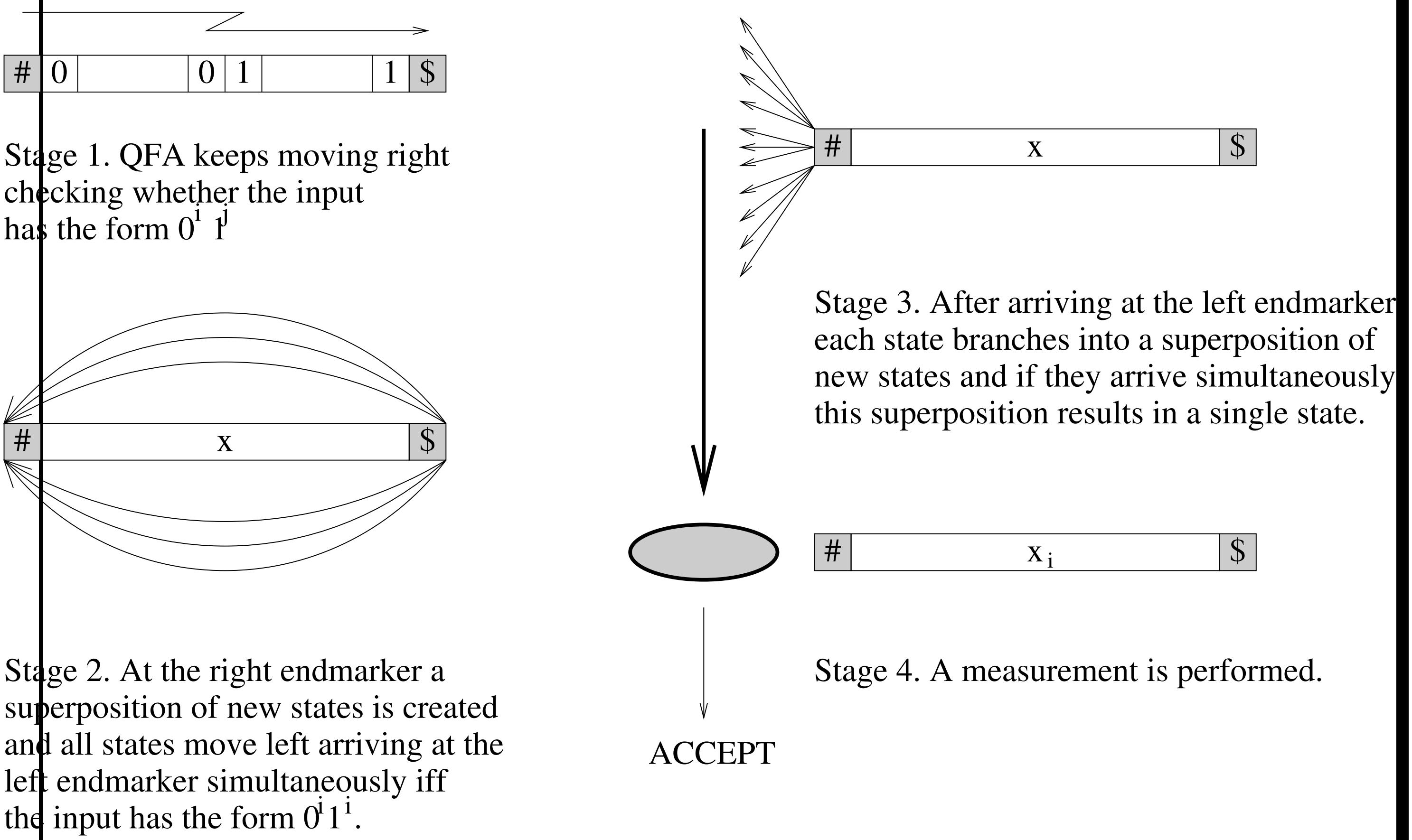
where

$$|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 + |\alpha_4|^2 = 1$$

2QFA accepting the language $\{0^i 1^i \,|\, i \geq 0\}$

$Q = \{q_0, q_1, q_2, q_3\} \cup \{s_j \,|\, 1 \leq j \leq n\} \cup \{r_{j,k} \,|\, 1 \leq j \leq n, 1 \leq k \leq n-j+1\}, Q_a = \{$

$$\begin{array}{|ll|}
\hline
V_{\#}|q_0\rangle = |q_0\rangle, & V_{\$}|q_0\rangle = |q_3\rangle, \\
V_{\#}|q_1\rangle = |q_3\rangle, & V_{\$}|q_2\rangle = \frac{1}{\sqrt{n}} \Sigma_{j=1}^{n} |r_{j,0}\rangle, \\
V_{\#}|r_{j,0}\rangle = \frac{1}{\sqrt{n}} \Sigma_{l=1}^{n} e^{\frac{2\pi i}{n} jl}|s_l\rangle, 1 \leq j \leq n, & \\
V_0|q_0\rangle = |q_0\rangle, & D(q_0) = \rightarrow, \\
V_0|q_1\rangle = |q_2\rangle, & D(q_1) = \leftarrow, \\
V_0|q_2\rangle = |q_3\rangle, & D(q_2) = \rightarrow, \\
V_0|r_{j,0}\rangle = |r_{j,j}\rangle, 1 \leq j \leq n, & D(q_3) = \downarrow, \\
V_0|r_{j,k}\rangle = |r_{j,k-1}\rangle, 1 \leq k \leq j, 1 \leq j \leq n, & \\
V_1|q_0\rangle = |q_1\rangle, & D(r_{j,0}) = \leftarrow, 1 \leq j \leq n, \\
V_1|q_2\rangle = |q_2\rangle, & D(r_{j,k}) = \downarrow, 1 \leq j \leq n, k \neq 0, \\
V_1|r_{j,0}\rangle = |r_{j,n-j+1}\rangle, 1 \leq j \leq n, & D(s_j) = \downarrow, 1 \leq j \leq n, \\
V_1|r_{j,k}\rangle = |r_{j,k-1}\rangle, 1 \leq k \leq j \leq n. & \\
\hline
\end{array}$$



Stage 1. QFA keeps moving right checking whether the input has the form $0^i 1^j$

Stage 2. At the right endmarker a superposition of new states is created and all states move left arriving at the left endmarker simultaneously iff the input has the form $0^i 1^i$.

Stage 3. After arriving at the left endmarker each state branches into a superposition of new states and if they arrive simultaneously this superposition results in a single state.

Stage 4. A measurement is performed.

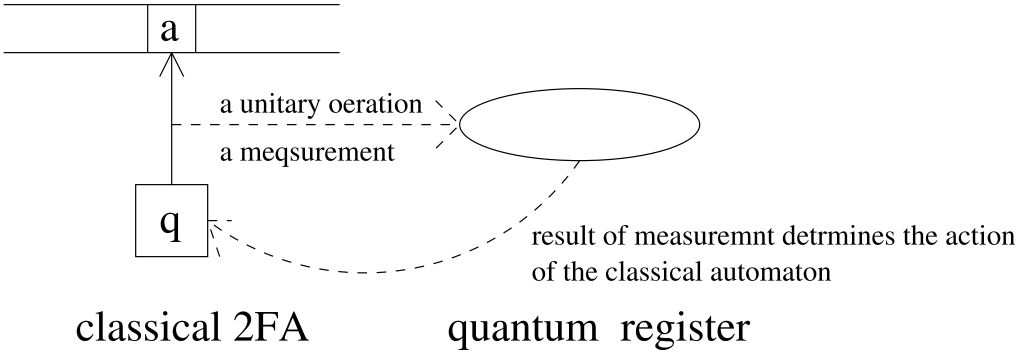
FINITE AUTOMATA WITH CLASSICAL and QUANTUM STATES

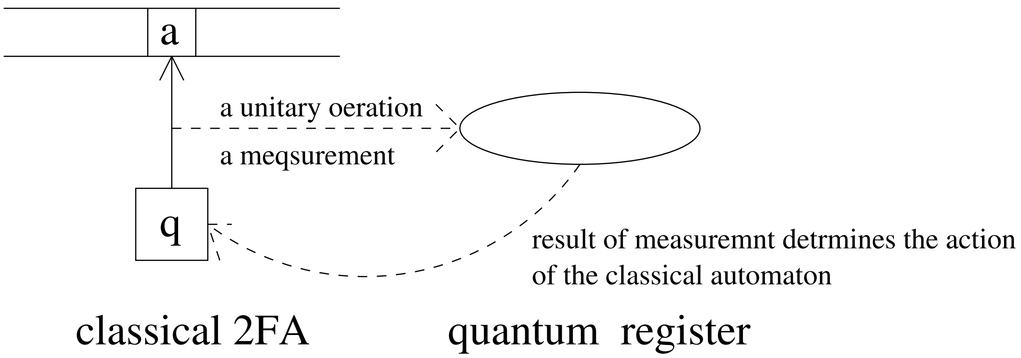
The models of QFA considered so far have all been natural quantum versions of the classical models of automata.

Of a different type is the model introduced by Ambainis and Watrous (1999), and called *two-way finite automata with quantum and classical states* (2QCFA).

This model is also more powerful than classical (probabilistic) 2FA and at the same time it seems to be more realistic, and really more "finite" than 2QFA because 2QFA need quantum memory of size $\mathcal{O}(\lg n)$ to process an input of the size n. 2QCFA can be seen as an intermediate model between 1QFA and 2QFA.

A 2QCFA is defined similarly as a classical 2FA, but, in addition, it has a fixed size quantum register (which can be in a mixed state) upon which the automaton can perform either a unitary operation or a measurement.


a
a unitary oeration
a meqsurement
q
result of measuremnt detrmines the action
of the classical automaton
classical 2FA
quantum register


a
a unitary oeration
a meqsurement
q
result of measuremnt detrmines the action
of the classical automaton
classical 2FA
quantum register

A 2QCFA has a classical initial state q_0 and an initial quantum state $|\phi_0\rangle$.

The evolution of a quantum state of the register is specified by a mapping Θ that assigns to each classical state q and a tape symbol σ an action $\Theta(q,\sigma)$.

One possibility is that $\Theta(q,\sigma) = (q', d, U)$, where q' is a new state, d is next movement of the head (to left, no movement or to right), and U is a unitary operator to be performed on the current quantum register state.

The second possibility is that

$$\Theta(q,\sigma) = (M, m_1, q_1, d_1, m_2, q_2, d_2, \ldots, m_k, q_k, d_k)$$

where M is a measurement, $m_1, \ldots, m_k$ are its possible classical outcomes and for each measurement outcome new state and new movement of the head is determined. In such a case the state transmission and the head movement are probabilistic.

Ambainis and Watrous (1999) have shown that 2QCFA with 1 qubit of quantum memory are already very powerful. Such 2QCFA can accept with bounded error the language of palindromes over the alphabet $\{0,1\}$, which cannot be accepted by probabilistic 2FA at all, and also the language $\{0^i1^i \,|\, i \geq 0\}$, in polynomial time — this language can be accepted by probabilistic 2FA, but only in exponential time.

RECOGNITION of $L = \{w \mid w = w^R, w \in \{a, b\}^*\}$

Quantum states: $|q_0\rangle, |q_1\rangle, |q_2\rangle$; initial state $|q_0\rangle$.

UNITARY OPERATORS

$$U_a|q_0\rangle = \frac{4}{5}|q_0\rangle - \frac{3}{5}|q_1\rangle \qquad U_b|q_1\rangle = \frac{4}{5}|q_0\rangle - \frac{3}{5}|q_2\rangle$$
$$U_a|q_1\rangle = \frac{3}{5}|q_0\rangle + \frac{4}{5}|q_1\rangle \qquad U_b|q_1\rangle = |q_1\rangle$$
$$U_a|q_2\rangle = |q_2\rangle \qquad U_b|q_2\rangle = \frac{3}{5}|q_0\rangle + \frac{4}{5}|q_2\rangle$$

AUTOMATON

1. Automaton moves to the leftmost symbol of the input in $\#w\$$, and sets the quantum state to $|q_0\rangle$.
2. Automaton goes through input, from left to right, and each time it reads a symbol σ, it applies U_σ to its quantum state.
3. Automaton returns to the left endmarker making no change on its quantum state.
4. Automaton moves from left to right and each time it reads a symbol σ it applies U_σ^{-1} on its quantum state.
5. Quantum state is measured. If outcome is not $|q_0\rangle$ the input is rejected.
6. $b \leftarrow 0$
7. Automaton moves from right to left and at each symbol simulates tossing k coins. If all outcomes are heads b is set to 1.
8. If $b = 1$ the input is accepted.
9. The cycle specified by points 1 to 7 are repeated infinitely many times.

OTHER MODELS of QUANTUM FINITE AUTOMATA

The idea to consider finite automata with a combination of quantum and classical states that could be really seen as finite memory automata led to investigation of various interesting models of quantum finite automa:

- One-way version of 2QCFA - 2QCFA with one-way movement of classical head - 1QCFA
- One-way quantum automata with classical states – MM-1QFA extended by a classical head -1QFAC

1QCFA

This is a very natural model, a one-way version of 2QCFA, and has several interesting properties:

- DFA, 1PFA, MM-1QFA, MO-1QFA and also 1QFACC automata discussee later can be in a atraightforward way simulated by 1QCFA.
- The class of languages accepted by 1QCFA is closed under Boolean operations.
- 1QCFA can be for some regular langauges exponentially smaller than1PFA and also MM-QFA. Namely for each m there is a regular language L_m that cannot be recognzed for any fixed ε by a MM-1QFA with bounded error $\frac{7}{9}+\varepsilon$ and any 1PFA recognizing this langauge has to have m states, but there is a 1QCFA recognizing L_m with $\mathcal{O}(\lg m)$ quantum states, 12 classical states and bounded error ε.

MM-1QFA with classical states - 1QFAC

This model is an extention of MO-1QFA model. In addition to a quantum register being initailly in a starting quantum state, there is also a finite set of classical states and one of them is initial. In each computation step current classical state and a current classical input determine new classical state and unitary operation to be performed on quantum register. After last input symbol is processed the current classical states specifies a projective measuremnt to be performed on quantum register and its outcome specifies either acceptance or rejection. The model has a variety of very nice properties:

- In both cases, working with pure states, unitary operations and projective measuremnts and with mixed states, all quantum operations and POVM, accept exactly all regular languages.
- Equivalence probelm is decidable and minimization problem is solvable.

QFA with a REGULAR CONTROL LANGUAGE - 1QFACC

Bertoni, Mereghetti and Palano (2003) introduced a new model of quantum automata.

1QFACC are actually the usual 1QFA that work in the MM-mode, but the measurement that is used after each move is defined by an arbitrary though fixed Hermitian observable and its classical outcomes (eigenvalues) are seen as elements of a special alphabet Λ. With each 1QFACC $\mathcal{A}$

a regular language $L \subseteq \Lambda^*$ is associated and an input word is accepted iff the corresponding word of eigenvalues obtained by measurements is in L.

Mereghetti and Palano (2006) have shown that 1QFACC accept, with respect to the isolated cut point, exactly regular languages and that for some regular languages 1QFACC are more succinct than the corresponding classical finite automata.

ONE-WAY "MULTI-LETTER" QUANTUM FINITE AUTOMATA –

- Multi-letter quantum automata (Qiu et al. 2011) are a natural quantum generalization of one-way multi-head classical finite automata introduced by Hromkovič (1983).
- Roughly speaking, a k-letter ML-1QFA works as MO-1QFA, but at each step can see up-to k of the last input symbols and on them next quantum state transition depends.
- For $k = 1$ ML-1QFA are exactly MO-1QFA. For $k > 1$ k-letter ML-1QFA accept larger family of languages than $(k-1)$-ML 1QFA, but smaller than the family of all regular languages.
- ML-1QFA can accept exactly also some languages not accepted by MM-1QFA with bounded error.
- An important property of ML-1QFA is that equivalence problem for them is decidable in polynomial time and that minimization problem is also solvable in EXPSPACE.

EQUIVALENCE DECIDABILITY - BASIC IDEA

The basic idea behind showing that the equivalence problem is decidable for ML-1QFA is to show that there is a polynomial emxb$p$ of two variables such that a k_1-letter ML 1QFA *A1* and a k_2-letter ML 1QFA *A2* are equivalent iff they are $p(k_1, k_2)$-equivalent.

In other word, they are equivalent if they exhibit the same probability of acceptance for all input strings of the length at most $p(k_1, k_2)$. In a

similar way, decidability of the equivalence problem has been shown for several other models of 1QFA.

For example, for two MM-1QFA with n_1 and n_2 states it holds that they are equivalent if and only if they are $(n_1^2 + n_2^2 - 1)$ equivalent.

CLASSICAL versus QUANTUM AUTOMATA

Comparing with classical finite automata quantum finite automata have

- **special strength, due to the power of quantum superposition (parallelism)**

  As a consequences for doing some tasks quantum automata can be exponentially smaller than classical ones.

- **special weakness, for example in the case that they have to be reversible**

  As consequences for doing some tasks quantum automata can be exponentially larger than classical ones.

Open problem

- The result that one-way quantum finite automata with most general physical operations and measurements has the same power as classical ones is not fully satisfactory because very powerful tools are needed to reach full power of the classical finite automata.
- Can we have a simpler model of quantum finite automata with the same power as classical ones?

EXTRAS

QUANTUM TURING MACHINES

Definition 0.2 *A (one-tape)* **quantum Turing machine** *(QTM) $\mathcal{M} = \langle \Sigma, Q, q_0, q_f, \delta\rangle$, QTM in short, is defined by sets of states and tape symbols, the initial state q_0 and the final state q_f, and the transition amplitude mapping*

$$\delta : Q \times \Sigma \times \Sigma \times Q \times \{\leftarrow, \downarrow, \rightarrow\} \longrightarrow \mathbf{C}_{[0,1]}$$

which is required to be such that quantum evolution of $\mathcal{M}$ is unitary.

A **configuration** of $\mathcal{M}$ is determined by the content τ of the tape, $\tau \in \Sigma^{\mathbf{Z}}$, by an $i \in \mathbf{Z}$ which specifies the position of the head, and by a $q \in Q$, the current state of the tape.

Let $C_{\mathcal{M}}$ denote the set of all configurations of $\mathcal{M}$. Computation (evolution) of $\mathcal{M}$ is performed in the inner-product space $H_{\mathcal{M}} = l_2(C_{\mathcal{M}})$ with the basis $\{|c\rangle \mid c \in C_{\mathcal{M}}\}$.

The transition function δ uniquely determines a mapping $a : C_{\mathcal{M}} \times C_{\mathcal{M}} \rightarrow \mathbf{C}$ such that for $c_1, c_2 \in C_{\mathcal{M}}$, $a(c_1, c_2)$ is the amplitude of the transition of $\mathcal{M}$ from the basis state $|c_1\rangle$ to $|c_2\rangle$.
The time evolution mapping $U_{\mathcal{M}} : H_{\mathcal{M}} \rightarrow H_{\mathcal{M}}$ is defined for a basis state by

$$U_{\mathcal{M}}|c\rangle = \sum_{c' \in C_{\mathcal{M}}} a(c, c')|c'\rangle.$$

WELL-FORMEDNESS CONDITIONS

Definition 0.3 *A QTM* $\mathcal{M} = \langle \Sigma, Q, q_0, q_f, \delta \rangle$ *with the transition mapping*

$$\delta : Q \times \Sigma \times \Sigma \times Q \times \{\leftarrow, \downarrow, \rightarrow\} \longrightarrow \mathbf{C}$$

is said to be strongly well-formed if the following conditions are satisfied.

1. **Local probability condition.** *For any* $(q_1, \sigma_1) \in Q \times \Sigma$*;*

$$\sum_{(\sigma,q,d)\in\Sigma\times Q\times\{\leftarrow,\downarrow,\rightarrow\}} |\delta(q_1, \sigma_1, \sigma, q, d)|^2 = 1.$$

2. **Separability condition I.** *For any two different pairs* $(q_1, \sigma_1), (q_2, \sigma_2)$ *from the set* $Q \times \Sigma$*:*

$$\sum_{(q,\sigma,d)\in Q\times\Sigma\times\{\leftarrow,\downarrow,\rightarrow\}} \delta^*(q_1, \sigma_1, \sigma, q, d)\delta(q_2, \sigma_2, \sigma, q, d) = 0.$$

3. **Separability condition II.** *For any* $(q, \sigma, d), (q', \sigma', d')$ *from the set* $Q \times \Sigma \times \{\leftarrow, \downarrow, \rightarrow\}$ *such that* $(q, \sigma, d) \neq (q', \sigma', d')$*:*

$$\sum_{(q_1,\sigma_1)\in Q\times\Sigma} \delta^*(q_1, \sigma_1, \sigma, q, d)\delta(q_1, \sigma_1, \sigma', q', d') = 0.$$

4. **Separability condition III.** *For any* $(q_1, \sigma_1, \sigma_1'), (q_2, \sigma_2, \sigma_2') \in Q \times \Sigma \times \Sigma$ *and* $d_1 \neq d_2 \in \{\leftarrow, \downarrow, \rightarrow\}$*:*

$$\sum_{q\in Q} \delta^*(q_1, \sigma_1, \sigma_1', q, d_1)\delta(q_2, \sigma_2, \sigma_2', q, d_2) = .$$

BASIC RESULTS

- There exists universal quantum Turing machines that can efficiently simulate any other quantum Turing machine.
- Quantum Turing machines and (uniform families of) quantum circuits are polynomially equivalent models of quantum computers.
- Well-formedness conditions have been formulated also for multitape quantum Turing machines.
- A variety of normal forms for one-tape QTM have been established. For example, the so-called unidirectional QTM at which the movement of the head is uniquely determined by the state the QTM comes into.
- Power of QTM with various types of amplitudes has been explored (complex, real, rational, algebraic, computable).