QUANTUM COMPUTING 8

Jozef Gruska

Faculty of Informatics
Brno
Czech Republik

November 3, 2002

8. QUANTUM FINITE AUTOMATA

For most of the main classical models of automata there are also their quantum versions. For example for finite automata, Turing machines and quantumcellular 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.

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) 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

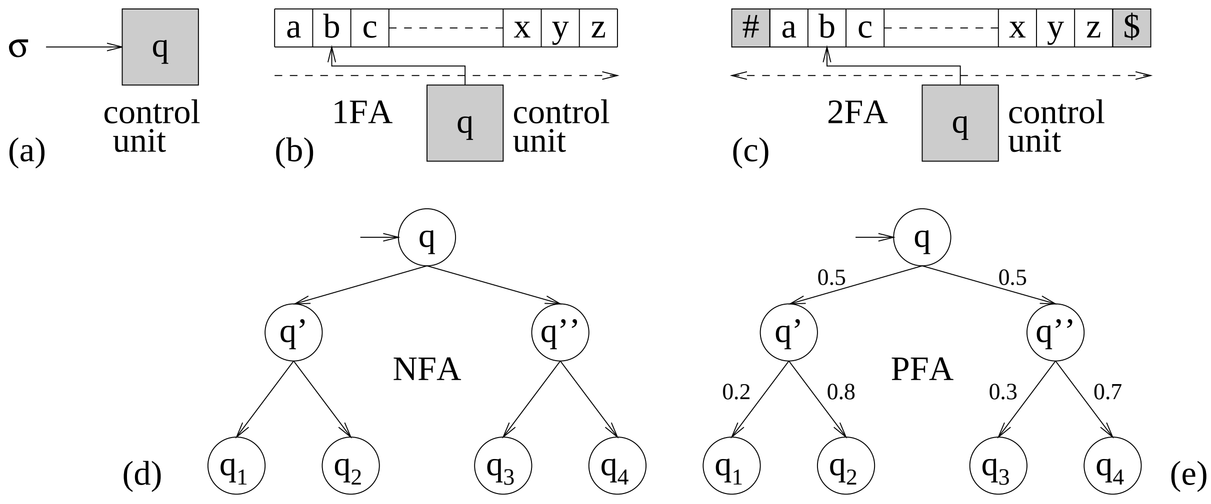


Figure 1: Models of finite automata

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: $\#w_1 \dots w_n\$$ $\qquad \#w\$$, $\qquad |w| = n$

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: $C(Q, w) = \{(q, i) \mid q \in Q, 0 \leq i \leq |w| + 1\}$

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:

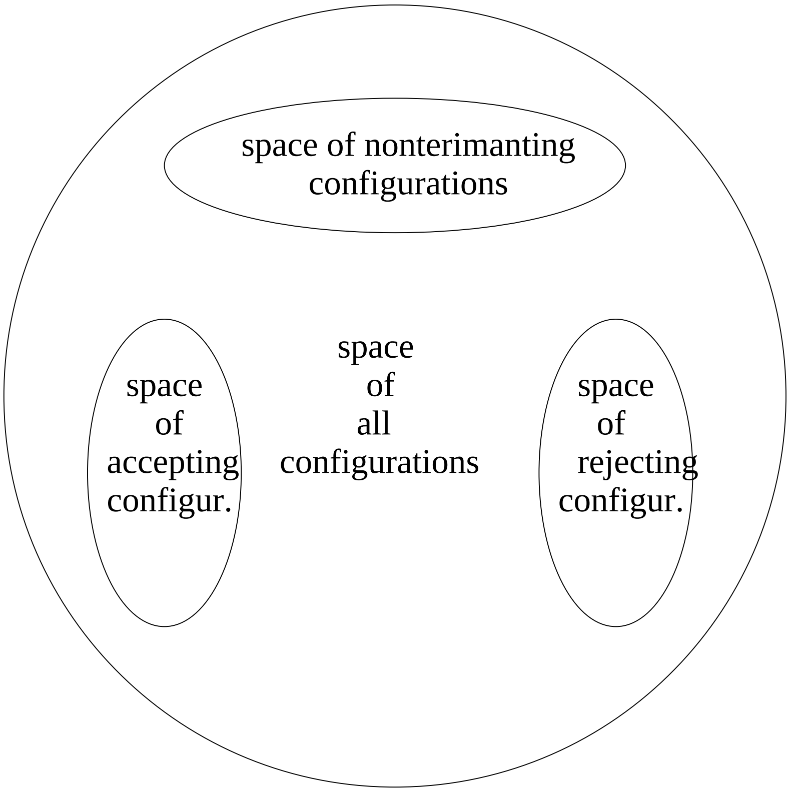
$$E_a = l(\{(q, i) \mid q \in Q_a\}), E_r = l(\{(q, i) \mid q \in Q_r\}), E_l = l(\{(q, i) \mid q \in Q_n\})$$

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.



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; $Q_a \subseteq Q$, $Q_r \subseteq Q$ — sets of accepting and rejecting 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 $\{|q\rangle \mid q \in Q\}$ 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

$$E_a = \text{span}\{|q\rangle \mid q \in Q_a\}$$
$$E_r = \text{span}\{|q\rangle \mid q \in Q_r\}$$

E_n is the orthogonal complement of $E_a \oplus E_r$

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:

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

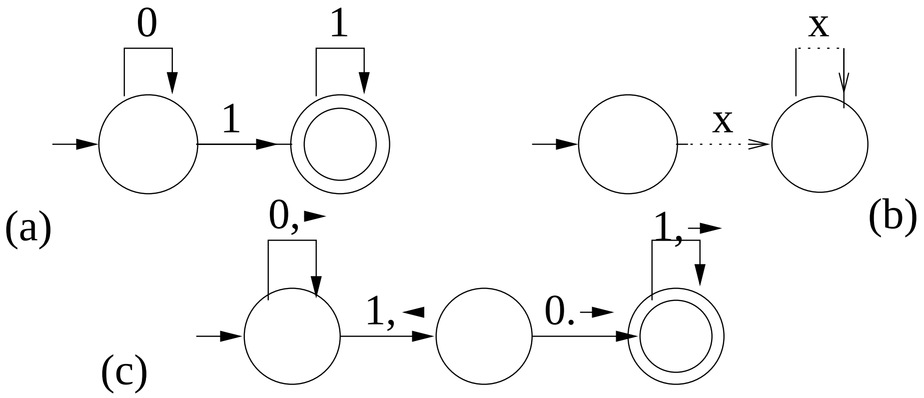
ACCEPTANCE of WORDS and LANGUAGES by 1QFA

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 $\frac{1}{2}$.



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 $L = \{0^i 1^j \mid i \geq 0.j \geq 0\}$ 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

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 $p = 0.68$ (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:**

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

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

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

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

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

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

The nonhalting part

$$\sqrt{p}|q_2\rangle$$

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

$$\sqrt{p}|q_a\rangle.$$

The acceptance probability bis therefore p.

PROOF OF ACCEPTANCE — CASE 3

Example. A 1QFA accepting $L = \{0^i 1^j \mid i \geq 0.j > 0\}$ 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:**

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

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

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

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

CASE 3 x has a prefix of the type $0^i 1^j 0^k, i \geq 0, j > 0, k > 0$. (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 $\sqrt{p}|q_2\rangle$ is changed only by first 0 into

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

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

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

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

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

The input is therefore rejected with probability

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

$\boxed{\text{A 1QFA accepting the language}}$

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

Transition matrices:

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

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

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

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

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.**
   $\Sigma_{q',d}\, \delta^*(q_1, \sigma, q', d)\delta(q_2, \sigma, q', d) = \begin{cases} 1, & \text{if } q_1 = q_2; \\ 0, & \text{otherwise.} \end{cases}$
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.**
   $\Sigma_{q'}\, \delta^*(q_1, \sigma_1, q', \rightarrow)\delta(q_2, \sigma_2, q', \leftarrow) = 0.$

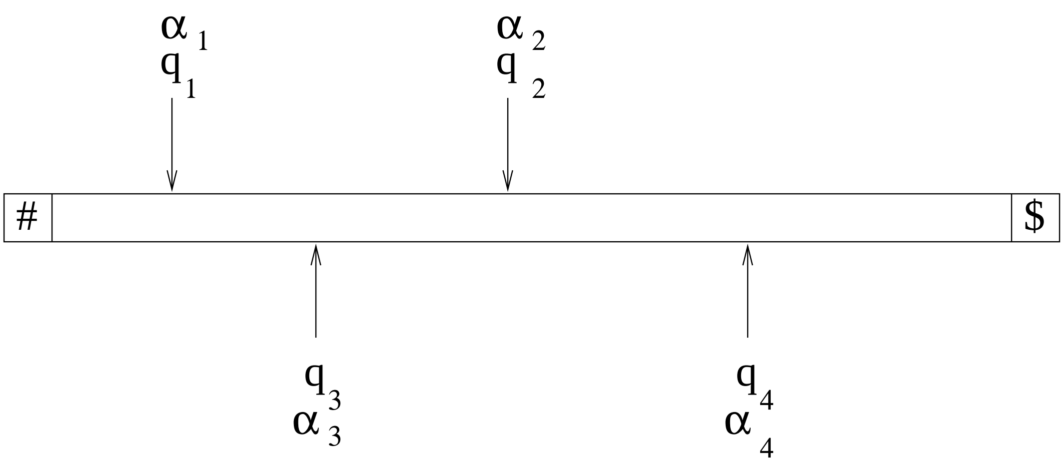
SIMPLIFIED DESCRIPTIONS of 2QFA

- 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.



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

Total state is then:

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

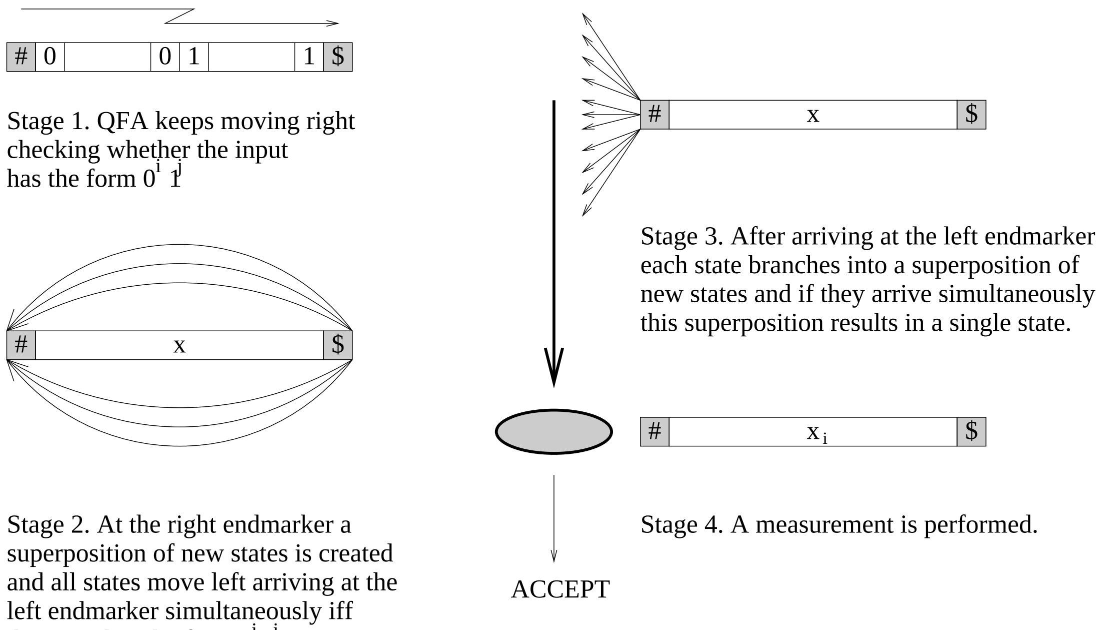
where

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

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

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

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



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.

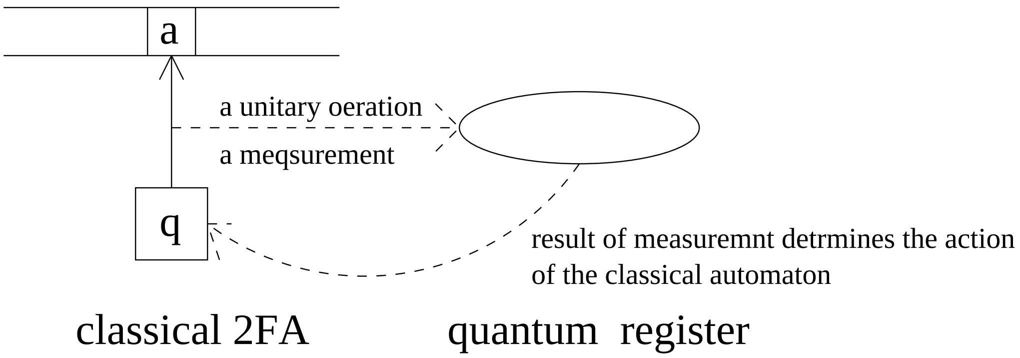
FINITE AUTOMATA WITH CLASSICAL and QUANTUM STATES

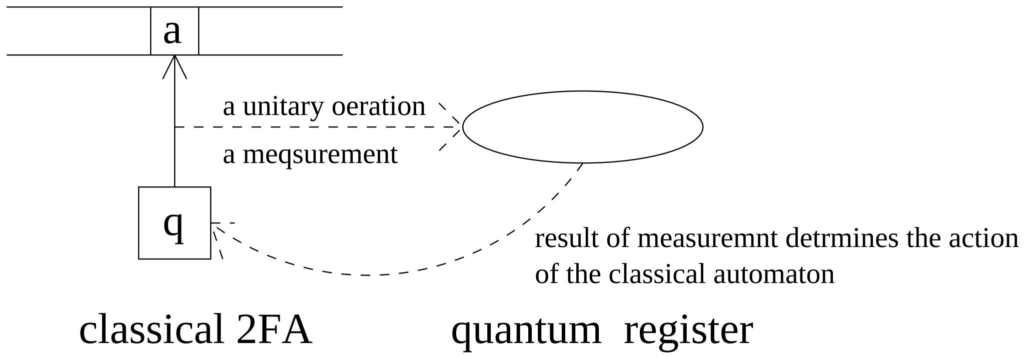
The models of QFA considered so far have all been natural quantum versions of the classical models of automata.

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 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 $\{0^i 1^i \,|\, i \geq 0\}$, 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

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

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.

$\boxed{\text{EXTRAS}}$

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 $\{|c\rangle \,|\, c \in C_{\mathcal{M}}\}$.

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).