Quantum Finite State Automata

LIKE QUANTUM COMPUTING, BUT SMALLER

Priscilla Raucci
priscilla.raucci@unimi.it

Università degli studi di Milano

Presentation

Hello, I am Priscilla Raucci.

I am a 3^{rd} year PhD student in Computer Science from the UNIVERSITY OF MILAN in a visiting period at the INSTITUT FÜR INFORMATIK of the JLU.

My PhD thesis is in the area of Theoretical Computer Science, Formal Languages and Automata Theory.

Table of contents

1. Introduction
2. Finite State Automata
3. Introducing Quantum
4. Example of QFA
5. Final remarks

Introduction

Introduction

$$\underbrace{\text{Quantum}}_{\text{physics}}\ \overbrace{\text{finite state automata}}^{\text{computer science}}$$

QUANTUM COMPUTING: The discipline that combines physics and computer science, by studying new models of computation based on quantum physics.

Firsts steps in quantum computing

- **R. Feynman**, Simulating physics with computers, Int. J. Theor. Phys. 21, 467 (1982)
- **P. Benioff**, Quantum mechanical Hamiltonian models of Turing machines, J. Stat. Phys. 29, 515 (1982)
- **D. Deutsch**, Quantum theory, the Church-Turing principle, and the universal quantum computer, Proc. R. Soc. London, Ser. A 400, 97 (1985)

"Quantum power" (1)

Shor's Algorithm shows that a quantum computer is capable of factoring very large numbers in *polynomial time*.

- **P. Shor**, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26, 1484 (1997)

NOTE 1: there is no classical polynomial time factoring algorithm

NOTE 2: current cryptographic protocols are based on the difficulty of the factoring problem

But, only theoretically

"Quantum power" (2)

Shor's Algorithm shows that a quantum computer is capable of factoring very large numbers in *polynomial time*.

- **P. Shor**, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26, 1484 (1997)

NOTE 1: there is no classical polynomial time factoring algorithm

NOTE 2: current cryptographic protocols are based on the difficulty of the factoring problem

But, only theoretically

"Quantum power" (3)

Shor's Algorithm shows that a quantum computer is capable of factoring very large numbers in *polynomial time*.

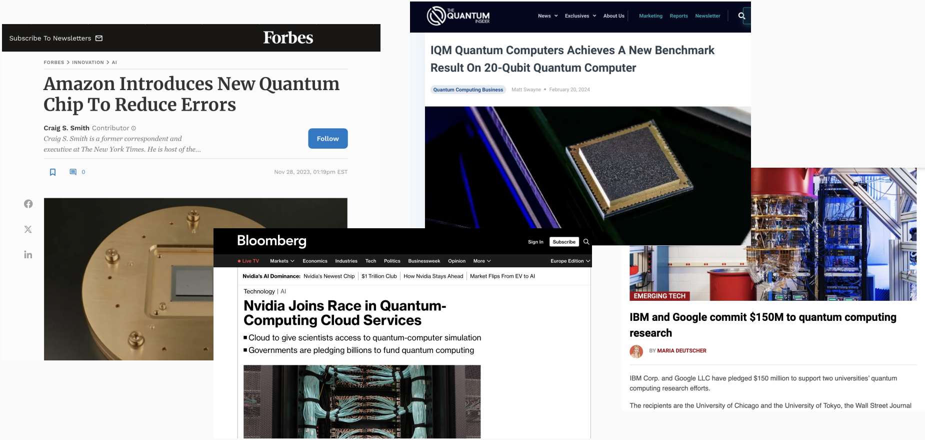
- **P. Shor**, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26, 1484 (1997)

NOTE 1: there is no classical polynomial time factoring algorithm

NOTE 2: current cryptographic protocols are based on the difficulty of the factoring problem

But, only theoretically

Building a quantum computer



- Extremely complex to realise
- Difficult to program
- Have still "small" size

Like quantum computers, but smaller

Theoretical computer science

Quantum finite state automata

Quantum mechanics

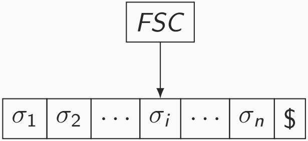
QUANTUM FINITE STATE AUTOMATA: small model of computation with a finite amount of internal memory that uses the quantum paradigm to work.

Finite State Automata

(Classical) Finite state automata

FINITE STATE AUTOMATA: small model of computation with a finite amount of internal memory.

Its "hardware" is composed by an internal *Finite State Control* that scans an *input tape*, consisting in a sequence of cells.



For each step the automaton:

1. reads the current cell;
2. changes the internal state;
3. moves to the next cell.

Encoding a problem

We encode the input of the problem as a string: $w = \sigma_1, \sigma_2, \ldots \sigma_n$ where $\sigma_i \in \Sigma, \forall i$.

σ_1	σ_2	$\cdots$	σ_i	$\cdots$	σ_n	\$

We then ask: Does w respect *some* characteristics?

THE OUTPUT: either YES or NO according how the machine is built.

Given a problem P...

Problem

Input: $k \in \mathbb{N}$

Question: Is k a multiple of $m \in \mathbb{N}$?

Input tape: $\underbrace{\boxed{a}\,\boxed{a}\,\boxed{a}\,\boxed{\cdots}\,\boxed{a}\,\boxed{a}\,\boxed{a}}_{k \text{ times}}\,\boxed{\$}$

I accept (I say YES) whenever the input length is such that

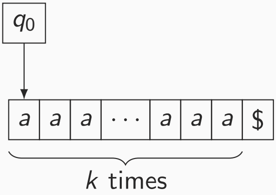
$$k \bmod m = 0$$

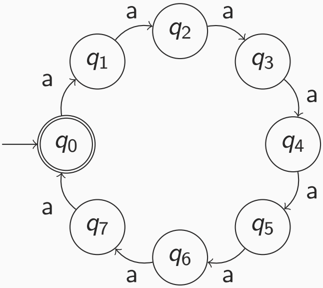
Example for a FSA

Problem

Input: $k \in \mathbb{N}$

Question: Is k a multiple of 8?





When the computation end in the state q_0, k is actually a multiple of 8.

Formal Definition

A FINITE STATE AUTOMATON A is defined by:

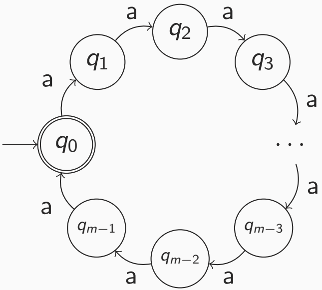
- a finite set of internal states Q;
- a set of character for the input string Σ;
- a function $\delta : Qx\Sigma \rightarrow Q$ defining the behaviour

$$\delta(q_i, \sigma_i) = q_j;$$

- the starting internal state $q_0 \in Q$;
- the set of final states $F \subseteq Q$.

Formally: $A = (Q, \Sigma, \delta, q_0, F)$

Formal definition for the example

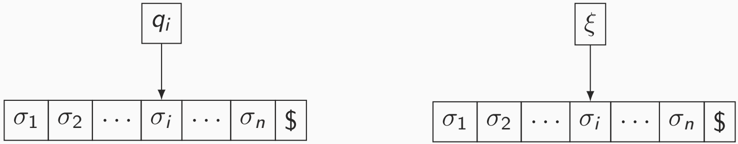


$$A = (Q = \{q_0, q_1 \ldots q_{m-1}\}, \Sigma = \{a\}, q_0, \delta, q_0),$$

where $\delta(q_i, a) = q_{(i+1) \bmod (m)}$.

Introducing Quantum

From classic to quantum



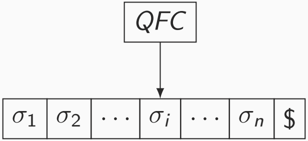
We have so far described a **classic** Automata, with a classic set of internal states Q and transitions defined by a classic deterministic function δ.

$$A = (Q,\ \Sigma,\ \delta,\ q_0,\ F)$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$M = (Q,\ \Sigma,\ \{U\}_{\sigma \in \Gamma},\ \pi_0,\ F)$$

Formal definition



A QUANTUM FINITE STATE AUTOMATON M, with n basis states, is defined by the triple

$$M = (\pi_0, \{U\}_{\sigma \in \Gamma}, P),$$

where:

- π_0 is the initial superposition of states, with $\|\pi_0\| = 1$;
- $\{U\}_{\sigma \in \Gamma} \in \mathbb{C}^{nxn}$ is a set of unitary transition where $\Gamma = \{\Sigma \cup \$\}$;
- $P \in \mathbb{C}^{nxn}$ is the projector into the subspace of $\mathbb{C}^n$ spanned by accepting basis states.

States in QFAs

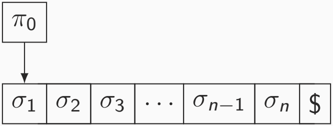
- The set of *basis states* is $Q = q_0, \ldots, q_{n-1}$, where each q_i is represented by the characteristic vector $e_i \in \{0, 1\}^n$ having 1 at the ith position and 0 elsewhere.
- A *quantum state* on Q is a superposition $\xi \in \mathbb{C}^n$ of basis states of the form

$$\xi = \sum_{i=1}^{n} \alpha_i e_i,$$

with α_i being complex amplitudes and satisfying $\|\xi\| = 1$.

Computation steps in a QFA (1)

The computation begins from the starting superposition π_0.



After the first step of the computation the internal state is:

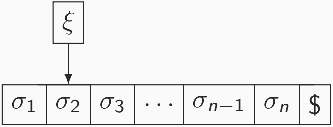
$$\xi = \pi_0 \cdot U_{\sigma_1}.$$

We have then the (reversible) computation:

$$\xi = \pi_0 \cdot U_{\sigma_1} \cdot U_{\sigma_2} \cdots U_{\sigma_n} \cdot U_{\$}.$$

Computation steps in a QFA (2)

The computation begins from the starting superposition π_0.



After the first step of the computation the internal state is:

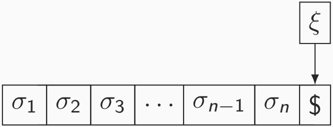
$$\xi = \pi_0 \cdot U_{\sigma_1}.$$

We have then the (reversible) computation:

$$\xi = \pi_0 \cdot U_{\sigma_1} \cdot U_{\sigma_2} \cdots U_{\sigma_n} \cdot U_{\$}.$$

Computation steps in a QFA (3)

The computation begins from the starting superposition π_0.



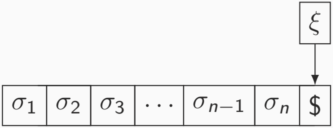
After the first step of the computation the internal state is:

$$\xi = \pi_0 \cdot U_{\sigma_1}.$$

We have then the (reversible) computation:

$$\xi = \pi_0 \cdot U_{\sigma_1} \cdot U_{\sigma_2} \cdots U_{\sigma_n} \cdot U_{\$}.$$

Measurement of the outcome



$$\xi = \pi_0 \cdot U_{\sigma_1} \cdots U_{\sigma_n} \cdot U_{\$}$$

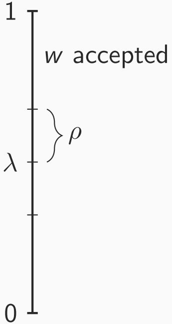
At the end of the computation M is observed using the projector P, it will be in an accepting basis state with probability:

$$p_M(w) = \|\pi_0 \cdot U_{\sigma_1} \cdots U_{\sigma_n} \cdot U_{\$} \cdot P\|^2.$$

- After observing this measurement the system collapses to the superposition $\xi P / \|\xi P\|^2$.

Acceptance policy

We consider only the set of problems that are acceptable with *isolated cut-point*.



Given $\lambda \in [0,1]$ and $\rho \in (0,1/2]$, it is the set of problem s.t.

$$|p_M(w) - \lambda| > \rho,$$

for any given problem and

$$p_M(w) > \lambda,$$

when the outcome of the problem is actually positive.

Example of QFA

Setting the problem

Problem

Input: $k \in \mathbb{N}$

Question: Is k a multiple of $m \in \mathbb{N}$?

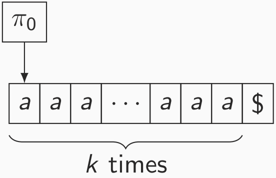
$$\underbrace{\boxed{a}\boxed{a}\boxed{a}\boxed{\cdots}\boxed{a}\boxed{a}\boxed{a}}_{k \text{ times}}\boxed{\$}$$

We define the QFA

$$M = \left(\pi_0 = (1, 0), U_a = \begin{pmatrix} \cos(\pi/m) & \sin(\pi/m) \\ -\sin(\pi/m) & \cos(\pi/m) \end{pmatrix}, P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right),$$

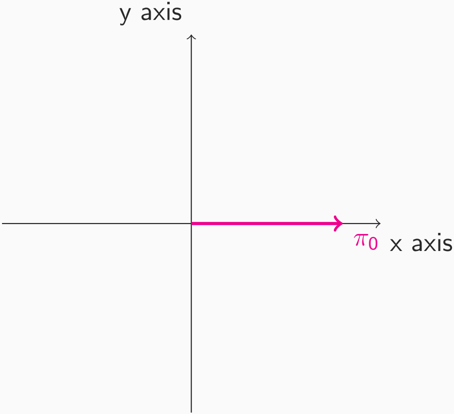
the unitary matrix $U_\$$ is the identity I of dimension 2×2

The starting point



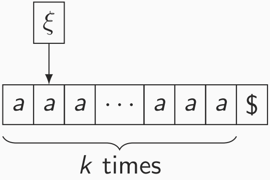
We set $\theta = \pi/m$, so we have:

$$U_a = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$$



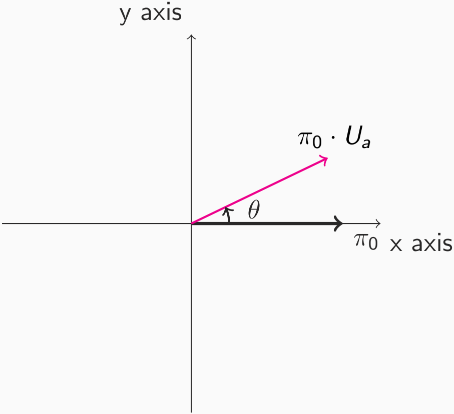
$$\xi = \pi_0$$

First steps (1)



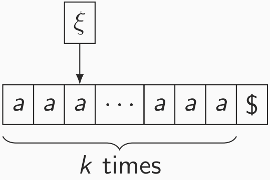
We set $\theta = \pi/m$, so we have:

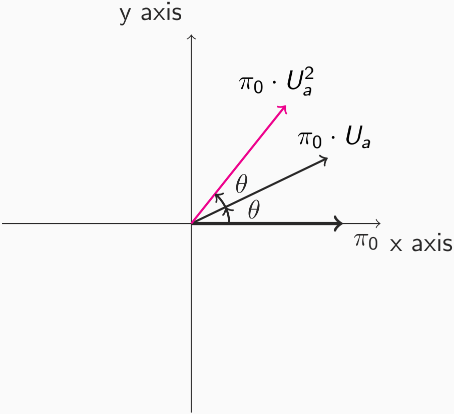
$$U_a = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$$



$$\xi = \pi_0 \cdot U_a$$

First steps (2)



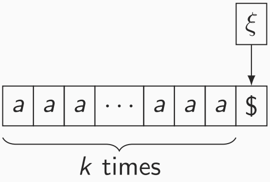


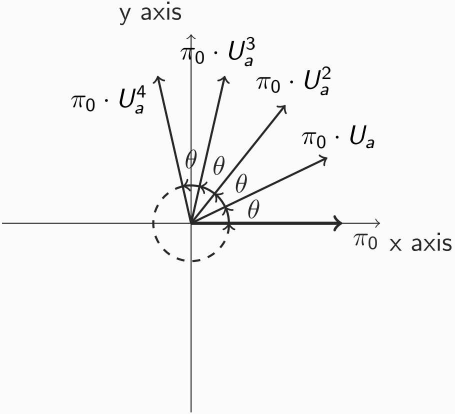
We set $\theta = \pi/m$, so we have:

$$U_a = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$$

$$\xi = \pi_0 \cdot U_a \cdot U_a$$

Final superposition





$$\xi = \pi_0 \cdot (U_a)^k \cdot U_\$$$

Measuring

- The state at the end of the computation is: $\xi = \pi_0 \cdot (U_a)^k \cdot U_\$$
- The transition matrix: $(U_a)^k = \begin{pmatrix} cos(k\pi/m) & sin(k\pi/m) \\ -sin(k\pi/m) & cos(k\pi/m) \end{pmatrix}$

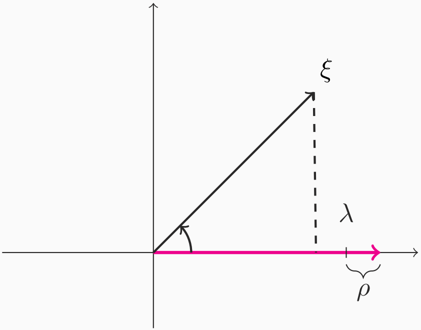
The probability of observing the automata in an *accepting state* is:

$$p_M(w) = \|\pi_0 \cdot U_a^k \cdot P\|^2 = \|(1,0) \cdot U_a^k \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\|^2$$

$$= \cos^2\left(\frac{k\pi}{m}\right) = \begin{cases} 1 & \text{if } k \text{ mod } m = 0 \\ \cos^2(\pi/m) & \text{otherwise.} \end{cases}$$

Setting the cut point

$$p_M(w) = \begin{cases} 1 & \text{if } k \bmod m = 0 \\ \cos^2(\pi/m) & \text{otherwise.} \end{cases}$$



We can set the cut-point and the isolation:

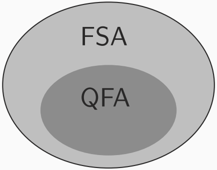
$$\rho = \frac{1 - \cos^2(\pi/m)}{2}$$

$$\lambda = \frac{1 + \cos^2(\pi/m)}{2}$$

Final remarks

Power of QFA

- For **computational power**, QFA are weaker than classical FSA
  - due to reversibility of quantum dynamics



- For **dimension** QFA are more convenient than classical FSA
  -because of quantum superposition

Problem: Minimum number fo states

FSA: m QFA: 2 (for any m)

Future studies

- Immediate application for few q-bits quantum devices.
- Tackle theoretical studies of quantum computation:
    - Exploitation of superposition to implement *quantum parallelism*
    - Exploitation of *entanglement* in quantum computation

Thank you for your attention

References i

J. E. Hopcroft, R. Motwani and J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, 3rd edn. (Addison-Wesley, 2006).

A. Ambainis, A. Yakaryılmaz, Automata and quantum computing (2015), *arXiv preprint arXiv:1507.01988*.

C. Mereghetti, B. Palano, S. Cialdi, V. Vento, M. G. A. Paris and S. Olivares, Pho- tonic realization of a quantum finite automaton, *Physical Review Research 2* (2020) p. 013089, https://doi.org/10.1103/PhysRevResearch.2.013089.

A. Candeloro, C. Mereghetti, B. Palano, S. Cialdi, M. G. A. Paris and S. Olivares, An enhanced photonic quantum finite automaton, *Applied Sciences 11* (2021) p. 8768, https://doi.org/10.3390/app11188768.