Quantum Turing Machines

José Espírito Santo

CMAT, Universidade do Minho

Q DAYS

11 April 2019

Overview

1. Classical computation
2. Quantum computation
3. Final remarks

Goals

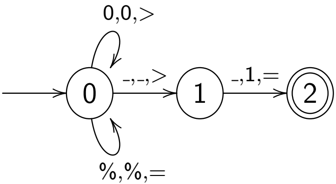
- Models of computation
- Introduction to (quantum) Turing machines in 40 minutes
- Smooth transition from classical to quantum
- Background material for other tutorial talks of Q Days

CLASSICAL COMPUTATION

Models of computation

- The models in 1936
  - Turing machines (Turing)
  - λ-calculus (Church)
  - Recursive functions (Kleene)
- Church-Turing thesis
- The fate of the models after the II World War
  - Turing machines: basis for complexity theory
  - λ-calculus: rediscovered as a programming language
  - Recursive functions: recursion theory
- How about boolean circuits?

A Turing machine



```
0.   read;       if   0  then write 0  ; move > ; goto 0
            else if   %  then write %  ; move = ; goto 0
            else if   _  then write _  ; move > ; goto 1
1.   read;       if   _  then write 1  ; move = ; goto 2
```

0	0	0	>	0
0	%	%	=	0
0	_	_	>	1
1	_	1	=	2

Turing machines

A Turing machine consists of

- a set of states Q
- an input alphabet
- a tape alphabet (containing the input alphabet)
- a designated initial state
- designated acceptance states

and a transition (partial) function

$$\delta : Q \times \Gamma \hookrightarrow \Gamma \times \{<, =, >\} \times Q$$

Back to the example

set of states $Q = \{0,1,2\}$

input alphabet $A = \{0,1\}$

tape alphabet $\Gamma = \{0,1,\_,\%\}$

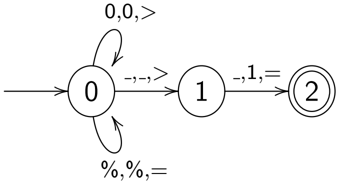
initial state 0

acceptance state 2

transition function

$$\delta : Q \times \Gamma \hookrightarrow \Gamma \times \{<,=,>\} \times Q$$

given by



or

0	0	0	>	0
0	%	%	=	0
0	_	_	>	1
1	_	1	=	2

Turing machines

A configuration of a TM M is a snapshot of M consisting of:

- the contents of the tape
- the current state (contents of the "program counter")
- the location of the head

By convention, input x determines an initial configuration $\mathcal{C}_x$
M determines a time evolution function

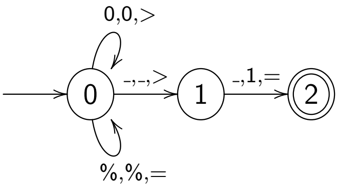
$$U_M : \mathbb{C}onfigs \hookrightarrow \mathbb{C}onfigs$$

where $\mathbb{C}onfigs$ is the set of configurations of M
Input x determines a computation path

$$\mathcal{C}_x = \mathcal{C}_0 \to \mathcal{C}_1 \to \mathcal{C}_2 \to \cdots \qquad\qquad (\mathcal{C}_{i+1} = U_M(\mathcal{C}_i))$$

If the path is finite, we can read output YES or NO

Back to the example - 1



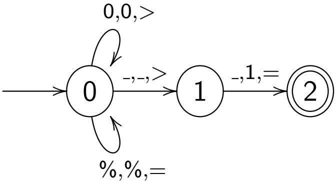
0	0	0	>	0
0	%	%	=	0
0	_	_	>	1
1	_	1	=	2

Input $x = 00$

config.	current state	tape and head
$\mathcal{C}_x$	0	$\boxed{0}0$
$\mathcal{C}_1$	0	$0\boxed{0}$
$\mathcal{C}_2$	0	$00\boxed{\_}$
$\mathcal{C}_3$	1	$00\_\boxed{\_}$
$\mathcal{C}_4$	2	$00\_\boxed{1}$

Output = YES

Back to the example - 2



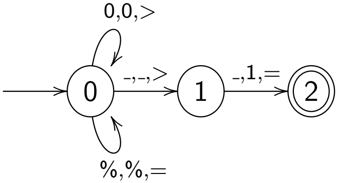
0	0	0	>	0
0	%	%	=	0
0	_	_	>	1
1	_	1	=	2

Input $x = 000100$

config.	current state	tape and head
$\mathcal{C}_x$	0	$\boxed{0}00100$
$\mathcal{C}_1$	0	$0\boxed{0}0100$
$\mathcal{C}_2$	0	$00\boxed{0}100$
$\mathcal{C}_3$	0	$000\boxed{1}00$

Output = NO

Back to the example - 3

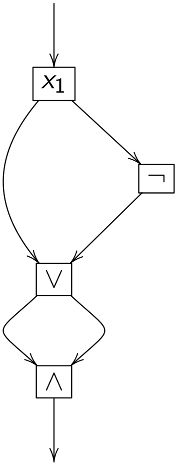


0	0	0	>	0
0	%	%	=	0
0	_	_	>	1
1	_	1	=	2

config.	current state	tape and head
$\mathcal{C}_1$	0	$\boxed{0}\,\%$
$\mathcal{C}_2$	0	$0\,\boxed{\%}$
$\mathcal{C}_3$	0	$0\,\boxed{\%}$
$\mathcal{C}_4$	0	$0\,\boxed{\%}$
...	...	...

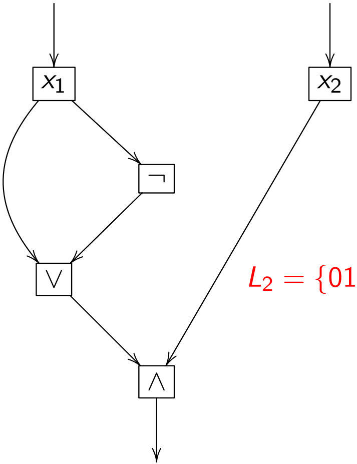
Non-termination

Boolean circuits



$L_1 = \{0, 1\}$

$(x_1 \vee \neg x_1) \wedge (x_1 \vee \neg x_1)$



$L_2 = \{01, 11\}$

$(x_1 \vee \neg x_1) \wedge x_2$

Families of circuits

Languages $L \subseteq (0+1)^*$ are decided by families of circuits $(C_n)_{n\in\mathbb{N}}$ with each C_n taking care of the "slice" L_n of L

Every language is decided by some family of circuits...

... including every undecidable language

In fact, there are undecidable language which are decided by linear size families of circuits

The question is not about size, it's about uniformity

A family of circuits $(C_n)_{n\in\mathbb{N}}$ is uniform if the function

$$n \mapsto C_n$$

may be calculated efficiently by some Turing machine

QUANTUM COMPUTATION

Smooth transition from classical to quantum

From Bernstein-Vazirani 1997, Fortnow 2003

$$
\begin{aligned}
\text{deterministic} \quad & \delta : Q \times \Gamma \hookrightarrow \Gamma \times \{<, =, >\} \times Q \\
\text{non-deterministic} \quad & \delta : Q \times \Gamma \rightarrow \wp(\Gamma \times \{<, =, >\} \times Q) \\
& \delta : Q \times \Gamma \rightarrow (\Gamma \times \{<, =, >\} \times Q \rightarrow \{0, 1\}) \\
& \delta : Q \times \Gamma \times \Gamma \times \{<, =, >\} \times Q \rightarrow \{0, 1\} \\
\text{probabilistic} \quad & \delta : Q \times \Gamma \times \Gamma \times \{<, =, >\} \times Q \rightarrow [0, 1] \\
\text{quantum} \quad & \delta : Q \times \Gamma \times \Gamma \times \{<, =, >\} \times Q \rightarrow \mathbb{C}
\end{aligned}
$$

More precisely...

$$\delta : Q \times \Gamma \times \Gamma \times \{<, =, >\} \times Q \to \tilde{\mathbb{C}}$$

where $\tilde{\mathbb{C}}$ is the set of complex numbers whose real and imaginary parts can be computed by a deterministic algorithm to within 2^{-n} in time polynomial in n.

For **BQP** it suffices

$$\delta : Q \times \Gamma \times \Gamma \times \{<, =, >\} \times Q \to \{-1, -\tfrac{4}{5}, -\tfrac{3}{5}, 0, \tfrac{3}{5}, \tfrac{4}{5}, 1\}$$

(Adleman, DeMarrais and Huang, 1997)

Additionally...

For each state q and scanned symbol σ

probabilistic $\sum_{\sigma',d,q'} \delta(q,\sigma,\sigma',d,q') = 1$

quantum $\sum_{\sigma',d,q'} |\delta(q,\sigma,\sigma',d,q')|^2 = 1$

In fact, for each QTM M one requires more: the time evolution operator U_M must be *unitary*.

Time evolution operator

Like any TM, a QTM M determines a time evolution operator

Given a configuration $\mathcal{C}$ of M with current state q and scanned symbol σ

- each trio σ', d and q' such that $\delta(q, \sigma, \sigma', d, q')$ is a nonzero probability amplitude $\alpha_i \in \mathbb{C}$ determines a configuration $\mathcal{C}_i$
- therefore $\mathcal{C}$ and δ determine a linear combination

$$\alpha_1 \mathcal{C}'_1 + \cdots + \alpha_k \mathcal{C}'_k$$

understood as a superpositions of configurations

Recall $\sum_i |\alpha_i|^2 = 1$

Time evolution operator

Let $\mathbb{C}$*onfigs* be the complex vector space of the *finite complex linear combinations of configurations* of M

(understood as superpositions of configurations of M)

M's time evolution is the linear application

$$U_M : \mathbb{C}\mathit{onfigs} \to \mathbb{C}\mathit{onfigs}$$

that extends the map

$$\mathcal{C} \mapsto \alpha_1 \mathcal{C}'_1 + \cdots + \alpha_k \mathcal{C}'_k$$

of the previous slide

Computation paths

Measuring a superposition $\alpha_1 \mathcal{C}'_1 + \cdots + \alpha_k \mathcal{C}'_k$ collapses the superposition to a configuration $\mathcal{C}'_i$ with probability $|\alpha_i|^2$

$$\begin{tikzcd}
 & & \mathcal{C}'_1 \\
\mathcal{C} \arrow[r, mapsto, "U_M"] & \alpha_1 \mathcal{C}'_1 + \cdots + \alpha_k \mathcal{C}'_k \arrow[ur, "|\alpha_1|^2"] \arrow[dr, "|\alpha_k|^2"'] & \vdots \\
 & & \mathcal{C}'_k
\end{tikzcd}$$

By measuring after every computation step, we generate a tree of computation paths and, at each path, M runs like a probabilistic machine

Quantum computation

Quantum execution of QTM M:

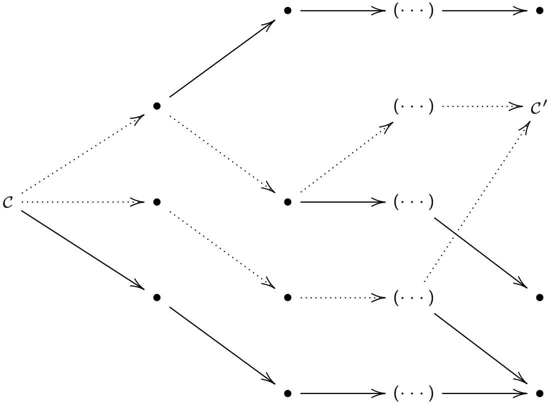
- The time evolution operator U_M acts on superpositions
- No measurement/observation until the end of computation

$$\mathcal{C} \quad \xmapsto{U_M} \quad U_M(\mathcal{C}) \quad \xmapsto{U_M} \quad U_M^2(\mathcal{C}) \quad \xmapsto{U_M} \quad \cdots$$

Since U_M is unitary

- the successive superpositions are unit vectors of $\mathbb{C}\mathit{onfigs}$
- the computation is reversible

Tree of computation paths vs quantum computation



$$\mathcal{C} = U_M^0(\mathcal{C}) \longmapsto U_M^1(\mathcal{C}) \longmapsto U_M^2(\mathcal{C}) \longmapsto (\cdots) \longmapsto U_M^k(\mathcal{C})$$

Interference

The following are *not* necessarily equal

(1) The sum of the probabilities of the computations paths of length k from $\mathcal{C}$ to $\mathcal{C}'$

(2) $|\alpha|^2$, where α is the amplitude of $\mathcal{C}'$ in the superposition $U_M^k(\mathcal{C})$

(1) The probability of M reaching configuration $\mathcal{C}'$ when M is run like a probabilistic machine
(2) The probability of observing configuration $\mathcal{C}'$ at the end of the quantum computation of M

Explanations

- Observing/measuring the machine during its execution changes its behavior
- In the quantum computation, there is interference between computation paths

A simple example of interference

For simplicity, consider $\mathbb{C}^2$ instead of $\mathbb{C}$*onfigs*

Regard $\mathbb{C}^2$ as the space of superpositions

$$\alpha_0|0> +\alpha_1|1>$$

where

- $|0>= \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is classical bit 0 seen as an element of $\mathbb{C}^2$
- $|1>= \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ is classical bit 1 seen as an element of $\mathbb{C}^2$

The unit vectors of $\mathbb{C}^2$ are called qubits

When measured, qubit $\begin{bmatrix} \alpha_0 & \alpha_1 \end{bmatrix}^T$ collapses to the classical bit $|i>$ with probability $|\alpha_i|^2$ (for $i = 0, 1$)

A simple example of interference

For simplicity, rather than some U_M, consider the linear map $U : \mathbb{C}^2 \to \mathbb{C}^2$ given by the unitary matrix

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

Let us calculate

$$U|0{>}= \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \qquad U|1{>}= \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

For each $i \in \{0, 1\}$, $U|i{>}$ collapses to any $|j{>}$ with probability $\frac{1}{2}$

A simple example of interference

Now let us compute $k = 2$ steps

Starting from $\mathcal{C} = |0>$, each of the four computation paths has probability $1/4$, and so the probability of a computation path ending with $|j>$ is $1/2$ (for $j = 0, 1$)

The same is true if we start from $\mathcal{C} = |1>$

However

$$U^2|0> = \begin{bmatrix} 0 \\ -1 \end{bmatrix} \qquad U^2|1> = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

If we observe $U^2|0>$ we obtain $|1>$ with probability 1

If we observe $U^2|1>$ we obtain $|0>$ with probability 1

FINAL REMARKS

Timeline

1985 D. Deutsch, *Quantum theory, the Church-Turing thesis and the universal quantum computer*

1989 D. Deutsch, *Quantum computational networks*

1995 Universal quantum gates

1997 E. Bernstein and U. Vazirani, *Quantum complexity theory*

Bibliography

- D. Deutsch, *Quantum theory, the Church-Turing thesis and the universal quantum computer*, Proc. Roy. Soc. London Ser. A, 400, pp. 97 - 117, 1985
- D. Deutsch, *Quantum computational networks*, Proc. Roy. Soc. London Ser. A, 425, pp. 73 - 90, 1989
- E. Bernstein and U. Vazirani, *Quantum complexity theory*, SIAM J. Comput., vol. 26, no. 5, pp. 1411 - 1473, 1997
- L. Adleman, J. DeMarrais and M. Huang, *Quantum computability*, SIAM J. Comput., vol. 26, no. 5, pp. 1524 - 1540, 1997
- L. Fortnow, *One complexity theorist's view on quantum computing*, Theoretical Computer Science, 292, pp. 597 - 610, 2003
- N. Yanofsky and M. Mannucci, *Quantum Computing for Computer Scientists*, Cambridge University Press, 2008

OBRIGADO