$\langle i|$ntrodução à Computação Quânt$|i\rangle$ca

Gustavo Bezerra (Koruja)

Programa de Educação Tutorial - Ciência da Computação
Universidade Federal do Rio Grande do Norte

06 de abril de 2018

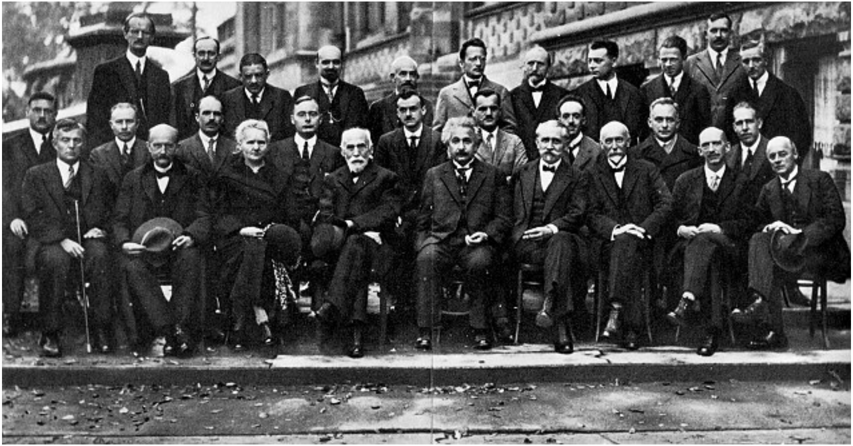
⟨References|

1. Nielsen, Michael A., and Isaac L. Chuang. Quantum computation and quantum information. Cambridge university press, 2010.
2. Kaye, Phillip, Raymond Laflamme, and Michele Mosca. An introduction to quantum computing. Oxford University Press, 2007.

A "bit" of History - Physics Background

A "bit" of History - Physics Background

Plankh (light frequency), Atomic models, Einstein & Others



A "bit" of History - Physics Background

Global perspectives - Computation

- **Moore's law**

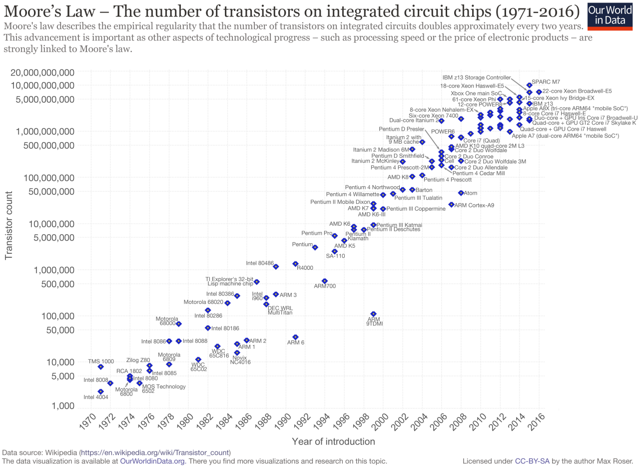


Figura 1: source: en.wikipedia.org/wiki/Moore%27s_law (just trust it, ok?)

Global perspectives - Computation

- **Issue: component size**
- **Turing Machine**
- **Universal Turing Machine**
- **Church-Turing Thesis**

Global perspectives - Stronger Computation

- **Strengthened version of the Church–Turing thesis**
  Any algorithmic process can be simulated efficiently using a Turing machine

- **Randomized algorithm for prime numbers**

- **Modification of the strong Church–Turing thesis**
  Any algorithmic process can be simulated efficiently using a probabilistic Turing machine

Global perspectives - Even Stronger Computation

- **Simulation of physical systems**
- **Universal Quantum Computer**
  Deutsch's notion of a Universal Quantum Computer is sufficient to efficiently simulate an arbitrary physical system
- **Peter Shor: prime factors & discrete logarithm**
- **Other Problems**
  What other problems can quantum computers solve more quickly than classical computers? The short answer is that we don't know

Global perspectives - Information Theory

- **Shannon's noiseless channel coding theorem**
  quantifies the physical resources required to store the output from an information source
- **Charles Bennett and Stephen Wiesner: superdense coding**
- **Shannon's noisy channel coding theorem**
  quantifies how much information it is possible to reliably transmit through a noisy communication channel
- **Error correction**
  compact disc players, computer modems, and satellite communications systems

Global perspectives - Information Theory

- **Distributed quantum computation**
  may require exponentially less communication
- **Single communications channel VS many channels**
- **Send information through noisy channel?**

Global perspectives - Cryptography

- **Private and Public keys**

- **How can quantum computers help?**
- **Entanglement**

Quantum Bits

- **Math model VS Physical model**
- **Bit representation**
  - 0 and 1 or $|0\rangle$ and $|1\rangle$?
  - Not a coin!
  - Linear Combination
  - Superposition
  - "Yes" a coin!

Quantum Bits - Bloch Sphere

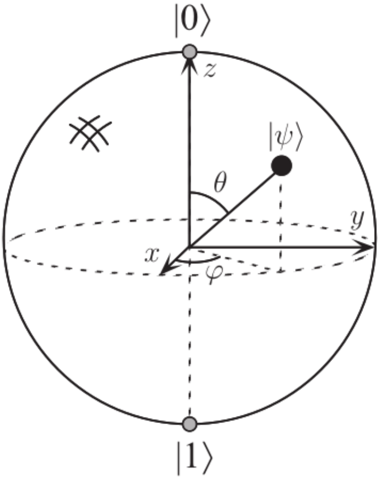


Figura 2: Source: Isaac Chuang and Michael Nielsen - Quantum Computation and Quantum Information - page 15

Quantum Bits - Mach-Zehnder Interferometer

...Now Loading...

Quantum Computing - NOT Gate

- $\alpha |0\rangle + \beta |1\rangle \rightarrow \beta |0\rangle + \alpha |1\rangle$
  This is linear. Non-linearity is dangerous!
- **Quantum gates must be Unitary**
- **More than one trivial gate! Pauli and Hadamard**

Quantum Computing - CNOT

- **Action is defined by:**
  - $|00\rangle \rightarrow |00\rangle$; $|01\rangle \rightarrow |01\rangle$; $|10\rangle \rightarrow |11\rangle$
  - $|A, B\rangle \rightarrow |A, A \oplus B\rangle$
- **Reversibility**

Quantum Computing - Quantum Circuits

- **Meaning of wire**
  physical wire, passage of time, physical particle, such as photon moving
- **Acyclic**
- **No FANIN**
- **No FANOUT**

Quantum Computing - Copying a qubit

- **Hey, I think there is FANOUT! Just use CNOT**
- **Apply to classical states:** $|00\rangle$ **and** $|10\rangle$
- **Apply to superposition state:** $|\psi\rangle\,|0\rangle$

Quantum Computing - Quantum Teleportation

- **Information cannot travel faster than light**
- **EPR State**
- **Does quantum teleportation create a copy?**

Quantum Algorithms

- **Toffoli Gate**
- **Simulate NAND and FANOUT**

Quantum Algorithms - Quantum Parallelism

- $f(x) : \{0, 1\} \rightarrow \{0, 1\}$
- **Simply compute with superposition and then... Houston?**
- **superposition states like** $\sum_x |x, f(x)\rangle$

Quantum Algorithms - Deutch's Algorithm

- **Quantum parallelism and interference**
- **Deutch's-Jozsa algorithm**

Quantum Algorithms - Fourier Transform

- **Shor's fast algorithms for factoring and discrete logarithm are based on**
- **For 2^n numbers. Classically: $n2^n$ VS Quantum: n^2**
- **Problem: hidden results**

Quantum Algorithms - Search Algorithms

- $O(n) \rightarrow O(\sqrt{n})$

Quantum Algorithms - Quantum Simulation

- **self-explanatory**

Quantum Algorithms - Power of Quantum Computation

- **Quantum Computers = Classical Computers?**
- **P, NP and PSPACE**

Quantum Information - Classical information through quantum channels

- **Improvement on noiseless channels? NOPE**
- **At least we have entangled states for Noisy channels. Don't we?**

|*References*⟩

1. Nielsen, Michael A., and Isaac L. Chuang. Quantum computation and quantum information. Cambridge university press, 2010.
2. Kaye, Phillip, Raymond Laflamme, and Michele Mosca. An introduction to quantum computing. Oxford University Press, 2007.

Questions?