

Quantum Computation

(Introduction)

Luís Soares Barbosa



Universidade do Minho



UNITED NATIONS
UNIVERSITY

UNU-EGOV

MFES - Arquitectura e Cálculo

March 2019

Quantum is trendy ...

The second quantum revolution

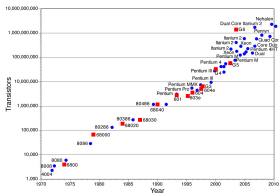
For the first time the viability of quantum computing may be **demonstrated in a number of real problems** extremely difficult to handle, if possible at all, classically, and **its utility discussed across industries**.

- **huge investment** by both the States, large companies and startups
- the **race for quantum** rising between major IT players (e.g. IBM, Intel, Google, Microsoft)
- **proof-of-concept machines** up to 50 qubits announced
- **national and regional programmes** (from the 2016 Quantum Manifesto to the EU QT Flagship)

... and full of promises ...

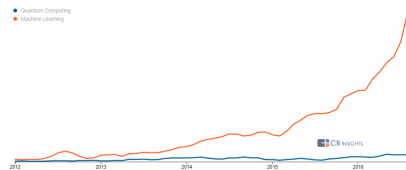
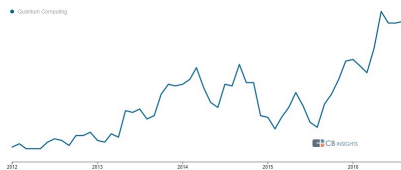
Actually,

- Real difficult, complex problems remain **out of reach** of classical supercomputers
- Classical approaches to computer technology are beginning to run up against **fundamental size limitations** (Moore's law),



- ... somehow quantum effects are beginning **to interfere** in the functioning of ever smaller electronic devices at nano scales

... but the race is just starting



- Clearly, quantum computing will have a **substantial impact on societies** even if, being a so **radically different technology**,
- ... it is difficult to **anticipate its evolution** and future applications ...
- ... and its **commercial potential** in the near term (5 to 10 yrs) is still debatable

The questions

- What is really new about Quantum Computing?

... information processing through quantum systems

- Which impact can be anticipated?
- Where exactly do we stand?

Computer Science + Quantum Physics

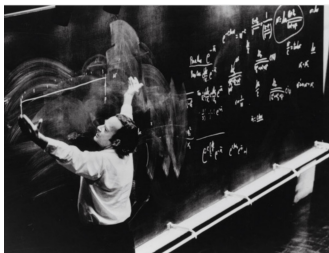
Two main intellectual achievements of the 20th century met

- Computer Science and Information theory progressed by **abstracting** from the physical reality.
- ... this was the key of its success to an extent that its origin was almost forgotten
- On the other hand **quantum mechanics** ubiquitously underlies ICT devices at the implementation level (e.g. transistor, laser, ...),
- but had no influence on the **computational model** itself
- ... until **now!**

Quantum computing?

The early 1980's

- **C. Bennet** and **G. Brassard** showed how properties of quantum measurements could provide a provably secure mechanism for defining a cryptographic key.
- **R. Feynmam** recognised that certain quantum phenomena could not be simulated efficiently by a classical Turing machine, and suggested computational simulations may build on **quantum phenomena regarded as computational resources**.



From weird quantum effects to computational resources

Effects as computational resources

1. Superposition
2. Interference
3. Entanglement
4. Uncertainty

International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have

Quantum effects as computational resources

1. Superposition

Our perception is that an object exists in a well-defined state, even when we are not looking at it.

However: At a very small scale an object **can hazily be in more than one state at one time.**

Such haziness affects familiar physical properties, like energy, momentum, position or spin.

Classic vs Quantum states

Tossing a coin, the result will either be *heads* and *tails* — a binary and **deterministic** state.



Tails = 0



Heads = 1

Classic vs Quantum states

A quantum state is a combination of both *heads* and *tails* ...

The system is not in just one of the states, **but holds the information of both possible states, at the same time.**



Classic vs Quantum states

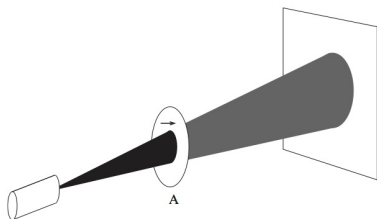
A quantum state is a combination of both *heads* and *tails* ...

The system is not in just one of the states, **but holds the information of both possible states, at the same time.**

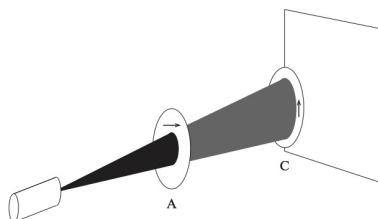


Information stored grows exponentially with the number of spinning coins

Quantum states



$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \text{horizontal polarization}$$

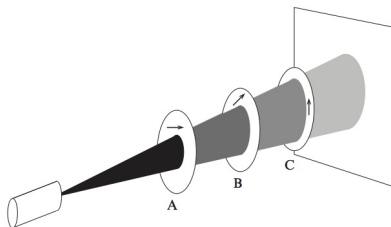


$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} - \text{vertical polarization}$$

(from [Reifell & Polak, 2011])

- The probability that a photon passes through the polaroid is the square of the magnitude of the amplitude of its polarization in the direction of the polaroid's preferred axis.
- On passing it becomes polarized in the direction of that axis.

Quantum states



The polarization of the new polaroid is a non trivial **linear combination** of vectors $|0\rangle$ and $|1\rangle$

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|0\rangle$$

i.e. a **superposition** which explains why a visible effect appears when the last polaroid is introduced.

Warning: A quantum state **is not a probabilistic mixture**: it is **not** true that the state takes either one or another of the classical values and we just do not happen to know which...

Quantum states

Photon's polarization states are represented as unit vectors in a 2-dimensional complex vector space, typically as a

non trivial linear combination \equiv **superposition** of vectors in a basis

$$|v\rangle = \alpha|0\rangle + \beta|1\rangle$$

A basis provides an **observation** (or **measurement**) tool, e.g.

$$\bigcirc\text{---}\bigcirc = \{|0\rangle, |1\rangle\} \quad \text{or} \quad \bigcirc\text{---}\bigcirc = \{|\nearrow\rangle, |\searrow\rangle\}$$

Quantum states

However, all this potential is **hidden** in the system: when **observed** a quantum state

$$|v\rangle = \alpha|u\rangle + \beta|u'\rangle$$

collapses into a classic one, i.e. one of the basis vectors in

$$\text{○} \text{---} \text{○} = \{|u\rangle, |u'\rangle\}$$

st the **probability of collapsing** into $|u\rangle$ is the square of the modulus of the amplitude of its component in the direction of $|u\rangle$, i.e.

$$|\alpha|^2$$

A subsequent measurement wrt the same $\text{○} \text{---} \text{○}$ returns $|u\rangle$ with probability 1.

which calls for a second ingredient ...

Quantum effects as computational resources

2. God plays dice indeed

Our perception is that the laws of Physics are deterministic: there is a unique outcome to every experiment.

However: one can only know the probability of the outcome, for example the probability of a system in a superposition to collapse into a specific state when measured.

Quantum effects as computational resources

The outcome of an observation is **probabilistic**; thus

$$|\alpha|^2 + |\beta|^2 = 1$$

which forces quantum states to be normalised to length 1.

... moreover whatever results interfere

amplitudes α and β are not real values that can only increase when added, but **complex** numbers so that they **can cancel each other or lower their probability**, cf.

$$|\alpha + \beta|^2 \text{ needs not to be bigger than } |\alpha|^2 \text{ or } |\beta|^2$$

Qubits

The space of possible polarization states of a photon, as any other quantum system (e.g. the spin of an electron) that can be modelled by a two-dimensional complex vector space, forms a **quantum bit (qubit)**.

- From **bits**, living in a two-value set $\{true, false\}$ or $\{1, 0\}$...
- ... to **qubits**, living in a 2-dimensional complex vector space, which
 - possesses a **continuum of possible values**, so potentially, i can store lots of classical data
 - but the amount of information that can be extracted from a qubit by measurement is severely **restricted**: a single measurement yields at most a single classical bit of information
 - as measurement changes the state, **one cannot make two measurements on the original state** of a qubit
 - an unknown quantum state **cannot be cloned**

Quantum effects as computational resources

3. Entanglement, i.e. nonlocality

Our perception is that objects are directly affected only by nearby objects or forces, i.e. the laws of physics work in a local way.

However: two particles can be connected or **entangled** st an action performed on one of them **can have an immediate effect on the other** particle light-years away.

cf. the **teleportation protocol**.

Quantum effects as computational resources

The state space of a quantum system grows exponentially:

n 2-dimensional vectors \rightsquigarrow a vector in 2^n -dimensional vector space

- Since $2^n \gg n$, the vast majority of n -qubit states cannot be described in terms of the state of n **separate** qubits. They are **entangled states**.

Entanglement can also be observed in simpler structures, e.g. **relations**, some of which cannot be **separated**, i.e. written as a Cartesian product of subsets of A , e.g.

$$\{(a, a), (b, b)\} \subseteq A \times A$$

Quantum effects as computational resources

4. Uncertainty is a feature, not a bug

Our perception is that with better tools we will be able to measure whatever seems relevant for a problem.

However: there are inherent limitations to the amount of knowledge that one can ascertain about a physical system.

cf. [Heisenberg's uncertainty principle](#).

Quantum effects as computational resources



A radically new computing paradigm

Feynman's dream: letting Nature, suitably engineered, compute for us through its own natural quantum behaviour

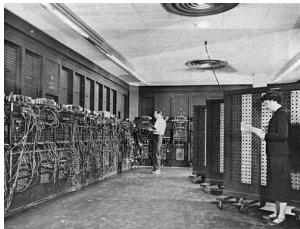
- 1970s, 1980s (Feynman, Benioff, Deutsch): how to compute with components able to harness the laws of quantum physics?
- 1985 (Deutsch): what exactly, and how efficiently, a quantum computer could compute ?
- Early results on **query complexity**:
 - Deutsch, Jozsa: some functions which took around 2^n queries to solve classically needed only a single query in a quantum setting.
 - Bernstein, Vazirani: functions whose quantum query complexity is superpolynomially better than the corresponding classical, even when one allowed some probability of error.
- 1994: Peter Shor's factorization algorithm

A radically new computing paradigm

... hopefully able to precisely control very complex, highly entangled quantum states, so complex that will never be simulated in a classical computer (because **it would require more bits than the number of atoms in the universe**), based on

- Built-in, implicit, massive parallelism (**superposition**)
- Unexpected strong correlations (**entanglement**)

... but such that we are still learning to cope with. Back to the 40's?



1943

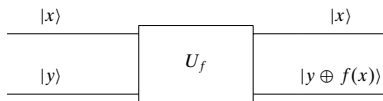


2018

My first quantum program

Is $f : \mathbf{2} \rightarrow \mathbf{2}$ constant, with a unique evaluation?

Oracle



where \oplus stands for exclusive disjunction.

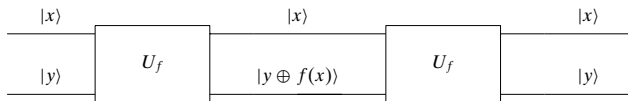
- The **oracle** takes input $|x, y\rangle$ to $|x, y \oplus f(x)\rangle$
- for $y = 0$ the output is $|x, f(x)\rangle$

My first quantum program

Is $f : \mathbf{2} \rightarrow \mathbf{2}$ constant, with a unique evaluation?

Oracle

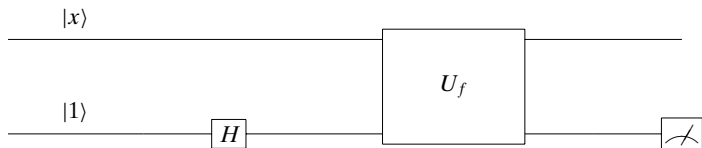
- The **oracle** is a **unitary**, i.e. **reversible** gate



$$|x, (y \oplus f(x)) \oplus f(x)\rangle = |x, y \oplus (f(x) \oplus f(x))\rangle = |x, y \oplus 0\rangle = |x, y\rangle$$

My first quantum program

Idea: Avoid double evaluation by **superposition**

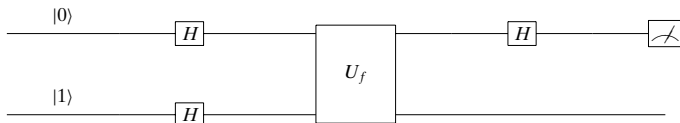


The circuit computes:

$$\begin{aligned}
 \text{output} &= |x\rangle \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \\
 &= \begin{cases} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \Leftarrow f(x) = 0 \\ |x\rangle \frac{|1\rangle - |2\rangle}{\sqrt{2}} & \Leftarrow f(x) = 1 \end{cases} \\
 &= (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}
 \end{aligned}$$

My first quantum program

Idea: Avoid double evaluation by **superposition**



$$(H \otimes I) U_f (H \otimes H)(|01\rangle)$$

Input in superposition

$$|\sigma_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

My first quantum program

$$\begin{aligned}
 |\sigma_2\rangle &= \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \\
 &= \begin{cases} (\underline{+1}) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \Leftarrow f \text{ constant} \\ (\underline{+1}) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \Leftarrow f \text{ not constant} \end{cases}
 \end{aligned}$$

$$\begin{aligned}
 |\sigma_3\rangle &= H|\sigma_2\rangle \\
 &= \begin{cases} (\underline{+1}) |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \Leftarrow f \text{ constant} \\ (\underline{+1}) |1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \Leftarrow f \text{ not constant} \end{cases}
 \end{aligned}$$

To answer the original problem is now **enough to measure the first qubit**:
if it is in state $|0\rangle$, then f is constant.

Impact

Although the set of computational problems where quantum computers enable a substantial speed-up wrt their classical counterparts is still being uncovered, quantum computing

- represents a **real change of paradigm** (and in this it is radically different from eg AI),
- whose impact, in a decade from now is **hard to anticipate**.

Impact

Accelerated evolution

- Quantum algorithms as **tools to explore complexity boundaries**: For a given problem, **as the size of the input parameter grows, can we asymptotically go faster with the use of a quantum memory than with purely classical means?**
- ... uncover several **applications** as many interesting problems have this property: from big-data to optimization, chemistry and pharma could benefit from the use of quantum algorithms.
- ... and calls for the development of a **broader research domain**:

quantum software engineering

still in its infancy ...

Towards quantum software engineering

- Current methods and tools for quantum software development are still **highly fragmentary** and **fundamentally low-level**
- Almost all **key ingredients of a mature software engineering discipline** — **compositionality, abstraction, refinement, high-order and property-enforcing type schemes**, are in their infancy.
- Standard mathematical formulation of quantum mechanics in terms of Hilbert spaces, and the associated von Neumann approach to its logical structure, is **unable to provide a sufficiently abstract framework** for specifying and analysing quantum processes.

Four application domains

System simulation

Science: Most of the computing time of supercomputers today is spent on simulating quantum systems. Some applications, such as figuring out properties of specific molecules that are beyond the reach of classical computers.

Pharmas: Drug design and personalised prescription drugs for individual patients.

Agriculture: Fertilisers; water management; ...

Four application domains

Faster search and optimization

Governments, companies, and other organizations often use their computers to solve large search or optimization problems:

- to finding efficient allocations of resources,
- to schedule work, to search through large data files,
- to design energy-efficient chips or airplanes
- ...

Four application domains

Machine learning

Even if building very large quantum-addressable classical memories is technologically demanding, and will not be available soon,

- the current rate of data creation is almost exponential (e.g. from 3.5 million text messages per minute in 2016, to over 15 million in 2017);
- most probably only quantum computing will allow us to start making use of all of this data.

Four application domains

Cryptography and cryptoanalysis

Even if it will take decades to actually build a quantum computer big enough to factor large numbers, for things that have to remain secret for the next 20 to 30 years, the **future quantum threat is already an acute problem now**: spies can already Hoover up encrypted communication today, store it, and decrypt it later when a quantum computer becomes available.

Approaches

- **Quantum crypto** (based on quantum effects)
- **Post-quantum crypto** (new hard problems)

Quantum Computing is coming of age

Research on **quantum technologies** (computing, communication, sensing and cryptography) is speeding up, and has already created first operational and commercially available applications.

Efforts, at national or international levels, to further **scale up** this research and development are in place.

This entails the need for:

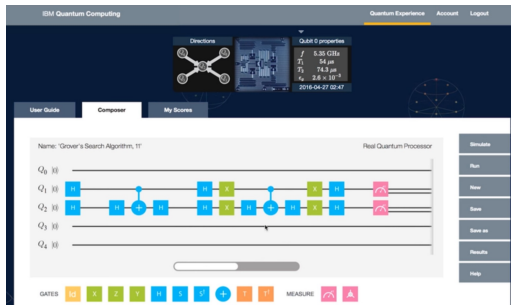
1. A **clear understanding of its potential impacts at medium term.**
2. A **broad societal debate** to explore and assess such impacts on science, industry, citizenship and society.
3. A systematic effort to **re-orient research, both fundamental and applied, and training**
4. The effective, **strategic involvement of leading companies.**

Where exactly do we stand?

Short term

Quantum advantage with **Noisy Intermediate-Scale Quantum (NISQ)**
Hybrid computational models:

- the quantum device as a coprocessor
- typically accessed as a service over the cloud, maybe for a fee, ideally enforced for commercial reasons



IBM Quantum Computing

Quantum Experience Account Logout

Directions Qubit 0 properties

f	5.35 GHz
T_1	54 μ s
T_2	74.3 μ s
ν_q	2.6×10^{-8}

2016-04-27 02:47

User Guide Composer My Scores

Name: 'Grover's Search Algorithm, IT' Real Quantum Processor

Q₀ |
Q₁ |
Q₂ |
Q₃ |
Q₄ |

GATES C₁ X Z Y H S T T MEASURE

Simulate Run New Save Save as Results Help

Where exactly do we stand?

Decoherence & Noise

- Current quantum computations are **fragile**: A physical qubit does not hold its state indefinitely, but undergoes random bit-flips over time
- Quantum devices have associated **decoherence times**, which limit the number of quantum operations that can be performed before the results are 'drowned' by noise.
- Additionally, each operation performed with quantum gates introduces **accuracy errors** in the system, which **limits the size of quantum circuits** that can be executed reliably. A typical limit is 1000 gates because the **noise will overwhelm the signal** in a larger circuit, thus imposing a ceiling on the computational power of NISQ technology.

Where exactly do we stand?

Longer term

Fault tolerant quantum computing, based on error correction codes (using millions of physical qubits to implement a logic one)

From now to then there is a need for

- basic research (in several fronts), but also
- use cases
- capacity building
- process re-engineering
- anticipating social impacts and challenges

The QuantaLab initiative

From a **collaborative research initiative** (July 2016) ...

- broad scope (quantum technologies)
- steady progress, cf



Summer School 2018



Publications

The QuantaLab initiative

... to an **Academic IBM Q HUB** (Sep 2018)

- Part of the worldwide IBM Q Network of companies and academies to exploit potential applications of Quantum Computing in Industry
- Real time, full access to IBM Q
- Multidisciplinary, international teams
- A problem-driven research

