Quantum Processes

(Introduction to the quantum computation paradigm)

Luís Soares Barbosa

Universidade do Minho

HASLab
HIGH-ASSURANCE
SOFTWARE LABORATORY

UNITED NATIONS
UNIVERSITY
UNU-EGOV

IC

May 2019

Quantum is trendy ...

The second quantum revolution

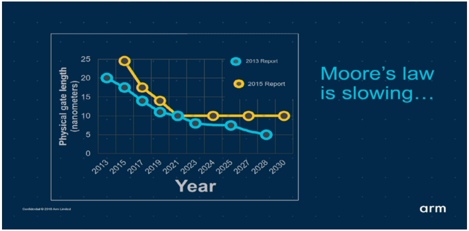
For the first time the viability of quantum computing may be demonstrated in a number of real problems extremely difficult to handle, if possible at all, classically, and its utility discussed across industries.

- 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 …

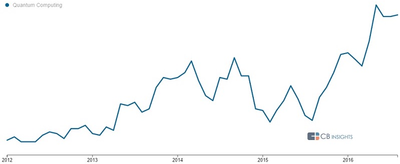
Actually,

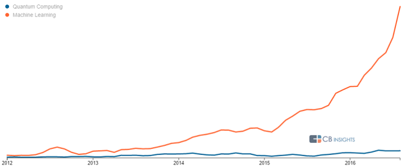
- Real difficult, complex problems remain out of reach of classical supercomputers
- Classical computer technology is running up against fundamental size limitations (Moore's law),



- … somehow quantum effects are interfering 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 should we know?
- Which impact can be anticipated?
- Where exactly do we stand?

Computer Science + Quantum Physics

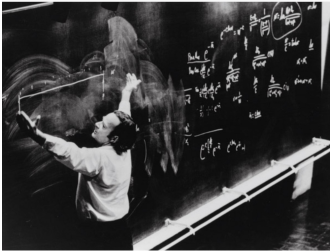
Two main intelectual achievements of the 20th century met

- 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

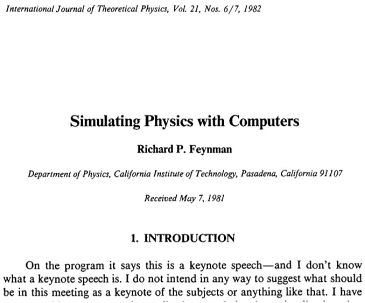
- C. Bennet and G. Brassard showed how properties of quantum measurements could provide a provably secure mechanism for defining a cryptographic key.
- R. Feynmam recognised that certain quantum phenomena could not be simulated efficiently by a classical computer, and suggested computational simulations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



Quantum computing?

Weird quantum effects as computational resources

1. Superposition
2. Interference &Uncertainity
3. Entanglement



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

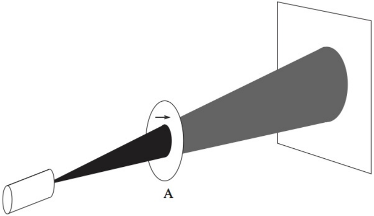
Quantum effects: 1. Superposition

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

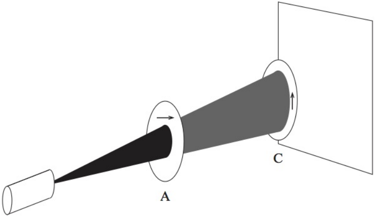
However: At a very small scale a quantum state holds the information of both possible classical states.

Information stored grows exponentially with the number of spinning coins

Quantum effects: 1. Superposition



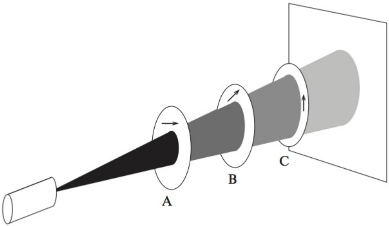
$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ - horizontal polarization



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

(from [Reifell & Polak, 2011])

Quantum effects: 1. Superposition



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

From bits to qubits

A qubit lives in a 2-dimensional complex vector space:

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

and thus possesses a continuum of possible values, so potentially, can store lots of classical data.

However, all this potential is hidden in the system: when observed $|v\rangle$ collapses into a classic state: $|0\rangle$ or $|1\rangle$.

The outcome of an observation is probabilistic:

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

Thus,

Quantum effects: 2. Interference & Uncertainity

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

However: God plays dice indeed — one can only know the probability of the outcome

$\boxed{\text{Observation changes the state}}$

- A subsequent measurement returns $|u\rangle$ with probability 1.
- Thus, an unknown quantum state cannot be cloned.
- ... but note that 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

Quantum effects: 3. Entanglement

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

HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.

Dilbert.com DilbertCartoonist@gmail.com

4-17-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick

Which problems a Quantum Computer can solve?

Quantum computers are expected to precisely control very complex, highly entangled quantum states, so complex that will never be simulated in a classical computer (because this would require more bits than the number of atoms in the universe), based on

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

Which problems a Quantum Computer can solve?

No magic ...

- One can store and manipulate a huge amount of information in the states of a relatively small number of qubits,
- ... but measurement will pick up just one of the computed solutions and colapse the whole (quantum) state

... but engineering:

As amplitudes interfere, a suitably engineered algorithm will ensure that computational paths leading to a wrong answer would cancel out, and the ones leading to a correct answer would reinforce, thus boosting the probability of finding them when the state is measured at the end.

Which problems a Quantum Computer can solve?

- 1994: Peter Shor's factorization algorithm (exponential speed-up),
- 1996: Grover's unstructured search (modest, quadratic speed-up, most relevant in practice),
- 2017: Quantum hash collision search,
- ...
- ... but no quantum algorithm is known to solve a NP-complete problem.

Some 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; ...

Some application domains

Faster search and optimization

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

Machine learning

Even if building very large quantum-addressable classical memories is technologically demanding, and will not be available soon, most probably only quantum computing will allow us to start making use of all of this data created at an exponential rate.

Some application domains

Cryptography and cryptoanalysis

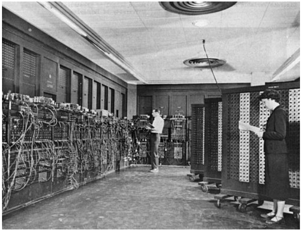
Even if it will take decades to actually build a quantum computer big enough to factor large numbers, for things that have to remain secret for the next 20 to 30 years, the future quantum threat is already an acute problem now: spies can already hoover up encrypted communication today, store it, and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

Approaches

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

Where exactly do we stand?

Back to the 1940's?



1943

2018

Where exactly do we stand?

Decoherence & Noise

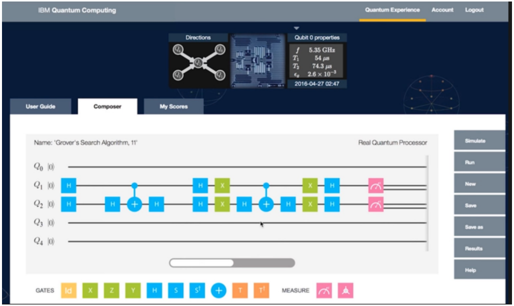
- Current quantum computations are fragile: A qubit does not hold its state indefinitely, but undergoes random bit-flips over time.
- Quantum devices have associated decoherence times, which limit the number of quantum operations that can be performed before the results are 'drowned' by noise.
- Each 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.

Where exactly do we stand?

Short term: NISQ

Noisy Intermediate-Scale Quantum Hybrid computational models:

- the quantum device as a coprocessor
- typically accessed as a service over the cloud



f 5.35 GHz
T_1 54 μs
T_2 74.3 μs
ϵ_g 2.6×10^{-3}
2016-04-27 02:47

Name: 'Grover's Search Algorithm, 11'

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
- development of a true engineering
- anticipating social impacts and challenges

The QuantaLab initiative

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

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?

Summer School 2018

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
- Multidisciplinar, international teams
- A problem-driven research

QUANTA ⟨L|A|B⟩

Universidade do Minho

INL
INTERNATIONAL IBERIAN
NANOTECHNOLOGY
LABORATORY

INESCTEC

CEiiA