Quantum Systems

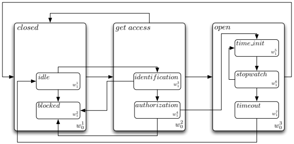
(Lecture 1: Introduction)

Luís Soares Barbosa

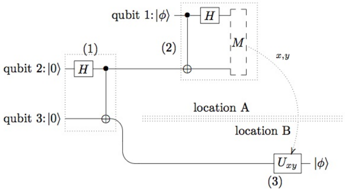
Universidade do Minho

Interaction and Concurrency

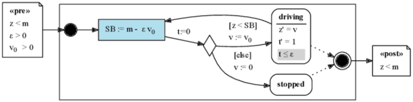
reactive systems
classical discrete interaction



quantum systems
quantum interaction



cyber-physical systems
classical continuous interaction



Why studying quantum systems?

Quantum is trendy ...

Research on quantum technologies is speeding up, and has already created first operational and commercially available applications.

For the first time the viability of quantum computing may be demonstrated in a number of problems and its utility discussed across industries.

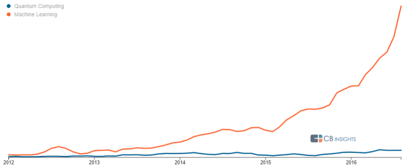
Efforts, at national or international levels, to further scale up this research and development are in place.

Why studying quantum systems?

... and full of promises ...

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

… 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.

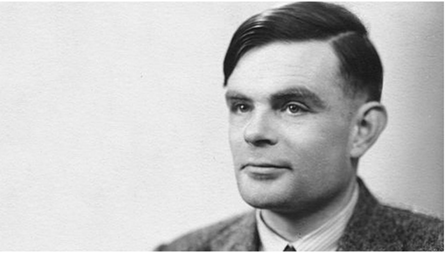
Quantum Mechanics ‘meets’ Computer Science

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, but had no influence on the computational model itself ...
- ... until now!

Quantum Mechanics 'meets' Computer Science

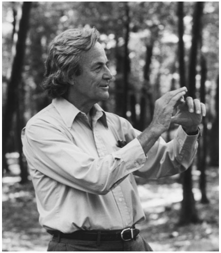
Alan Turing (1912 - 1934)



On Computable Numbers, with an Application to the Entscheidungsproblem (1936)

Quantum Mechanics 'meets' Computer Science

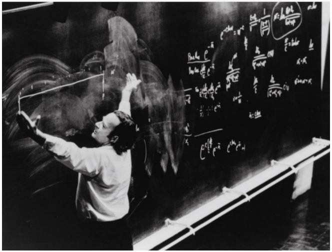
Richard Feynman (1918 - 1988)



Simulating Physics with Computers (1982)
(quantum reality as a computational resource)

Quantum Mechanics 'meets' Computer Science

- 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 effects as computational resources

Superposition

Our perception is that an object — e.g. a bit — exists in a well-defined state, even when we are not looking at it.
However: A quantum state holds information of both possible classical states.

Entanglement

Our perception is that objects are directly affected only by nearby objects, i.e. the laws of physics work in a local way.
However: two qubits can be connected, or entangled, st an action performed on one of them can have an immediate effect on the other even at distance.

Quantum effects as computational resources

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.

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

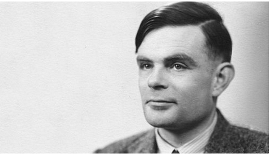
Quantum Computation

Davis Deutsch (1953)

Quantum theory, the Church-Turing principle and the universal quantum computer (1985)
(quantum computability and computational model:
first example of a quantum algorithm that is exponentially faster than any possible deterministic classical one)

Quantum Computation

quantum resources *quantum algorithms* *computability*

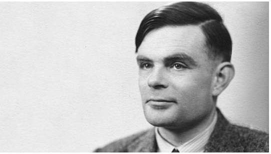


Quantum Computation

quantum resources

quantum algorithms

computability

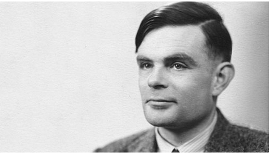


Quantum Computation

quantum resources

quantum algorithms

computability



Which problems can be addressed?

No magic ...

- A huge amount of information can be stored and manipulated 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:

To boost the probability of arriving to a solution by canceling out some computational paths and reinforcing others,

depending on the structure of the problem at hands.

Which problems a Quantum Computer can solve?

- 1994: Peter Shor's factorization algorithm (exponential speed-up),
- 1996: Grover's unstructured search (quadratic speed-up),
- 2018: Advances in hash collision search, i.e finding two items identical in a long list — serious threat to the basic building blocks of secure electronic commerce.
- 2019: Google announced to have achieved quantum supermacy

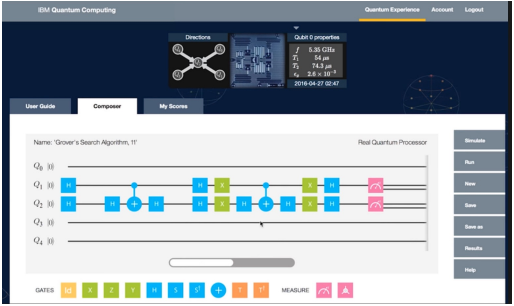
Availability of proof of concept hardware

Explosion of emerging applications in several domains: security, finance, optimization, machine learning, ...

Where exactly do we stand?

NISQ - Noisy Intermediate-Scale Quantum Hybrid machines:

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

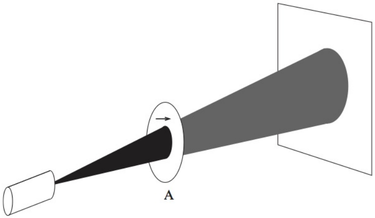


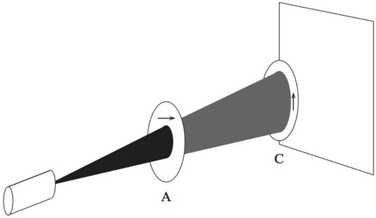
Still a long way to go ...

- Quantum computations are fragile: noise and decoherence.
- Current methods and tools for quantum software development are still highly fragmentary and fundamentally low-level.
- A lack of reliable approaches to quantum programming will put at risk the expected quantum advantage of the new hardware.

Time to go deeper ...

A photon's behaviour





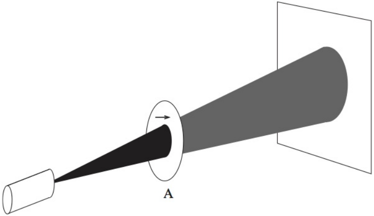
$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ - horizontal polarization

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

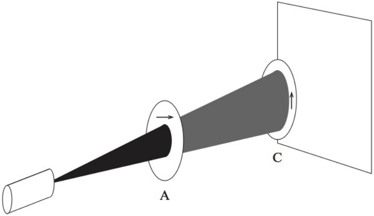
(from [Reifell & Polak, 2011])

- 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.

A photon's behaviour



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



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

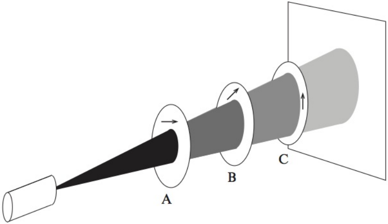
(from [Reifell & Polak, 2011])

If the photon is polarized as

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

it will go through A with probability $\| \alpha \|^2$ and be absorbed with $\| \beta \|^2$.

A photon's behaviour



The polarization of the new polaroid is

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

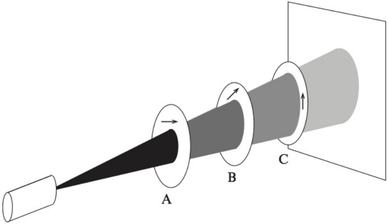
i.e. represented as a superposition of vectors $|0\rangle$ and $|1\rangle$

Hadamard basis

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

$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

A photon's behaviour



Expressing

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

explains why a visible effect appears when the last polaroid is introduced: the photon goes through C with 50% of probability (i.e. $\| \frac{1}{\sqrt{2}} \|^2 = \frac{1}{2}$).

Superposition and interference

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.

$$\bigcirc\!\frown\!\bigcirc = \{|0\rangle, |1\rangle\} \quad \text{or} \quad \bigcirc\!\frown\!\bigcirc = \{|\nearrow\rangle, |\nwarrow\rangle\}$$

Superposition and interference

Observation of a state

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

transforms the state into one of the basis vectors in

$$\bigcirc\!\frown\!\bigcirc = \{|u\rangle, |u'\rangle\}$$

In other (the quantum mechanics) words:
measurement collapses $|v\rangle$ into a classic, non superimposed state

Superposition and interference

The probability that observed $|v\rangle$ collapses into $|u\rangle$ is the square of the modulus of the amplitude of its component in the direction of $|u\rangle$, i.e.

$$\| \alpha \|^2$$

where, for a complex γ, $\| \gamma \| = \sqrt{\overline{\gamma}\gamma}$

A subsequent measurement wrt the same basis returns $|u\rangle$ with probability 1

This observation calls for a restriction to unit vectors, i.e. st

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

to represent quantum states

Superposition and interference

The notion of superposition is basis-dependent: all states are superpositions with respect to some bases and not with respect to others.

But it is not a probabilistic mixture: it is not true that the state is really either $|u\rangle$ or $|u'\rangle$ and we just do not happen to know which.

State $|u\rangle$ is a definite state, which, when measured in certain bases, gives deterministic results, while in others it gives random results:

The photon with polarization

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

behaves deterministically when measured with respect to the Hadamard basis but non deterministically with respect to the standard basis

Superposition and interference

In a sense $|u\rangle$ can be thought as being simultaneously in both states, but be careful: states that are combinations of basis vectors in similar proportions but with different amplitudes, e.g.

$$\frac{1}{\sqrt{2}}(|u\rangle + |u'\rangle) \quad \text{and} \quad \frac{1}{\sqrt{2}}(|u\rangle - |u'\rangle)$$

are distinct and behave differently in many situations.

Amplitudes are not real (e.g. probabilities) that can only increase when added, but complex so that they can cancel each other or lower their probability, thus capturing another fundamental quantum resource:

interference

Qubits

The space of possible polarization states of a photon, as any other quantum system (e.g. photon polarization, electron spin, and the ground state together with an excited state of an atom) that can be modelled by a two-dimensional complex vector space, forms a

$$\boxed{\text{quantum bit (qubit)}}$$

which has a continuum of possible values.

In practice it is not yet clear which two-state systems will be most suitable for physical realizations of qubits: it is likely that a variety of physical representation will be used.

Qubits

A qubit has ... a continuum of possible values

- potentially, it 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.
- as an unknown quantum state cannot be cloned, it is not possible to measure a qubit's state in two ways, even indirectly by copying its state and measuring the copy.