Lecture 1:
What is quantum computing ...
... and why we should care

Luís Soares Barbosa
www.di.uminho.pt/~lsb/

Universidade do Minho

Quantum Data Science
Universidade do Minho
2025-2026

Do you remember this cartoon?

Quantum is trendy ... but weird ...

Why quantum computing?

In simple terms ...

because a lot of really difficult, complex problems will forever remain out of reach of classical supercomputers ...

> *The correlations between genomes and outcomes are convoluted and there are generally not one-to-one links between genes and diseases. These problems quickly become very complex, reaching NP hardness.*
>
> (Lippert *et al*, 2002)

Why quantum computing?

Prime factorization

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268079170261221429134616704292143116022212404792747377940806653514195974598569021434 13 =

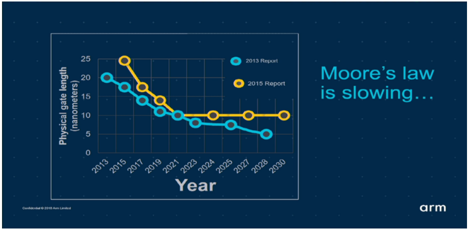
? * ?

- As factoring a 130 digit number takes around one month in a massively parallel computer network, a 400 digit number will take about the age of the universe (10^{10} years).
- However, a quantum algorithm exists such that factoring is achieved in polynomial time.

Why quantum computing?

Moreover, quantum computing comes full of promises ...

- Classical computer technology is running up against fundamental size limitations (Moore's law),



- Quantum computing brings new ideas to handle some real difficult, complex problems, which remain out of reach of classical supercomputers.

Moving fast ...

Quantum is moving (very) fast...

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

The quantum decade: the 2020s ...

- For the first time the viability of quantum computing is 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.
- A cross-industry race has begun to secure quantum talent, build quantum skills, map real-world problems to quantum algorithms, and capture quantum application intellectual property.

... but still uncertain what the future will bring

- Quantum computing will have a substantial impact on societies:
- ... indeed, questions on its impact have changed from if to when and how,
- ... even if its commercial potential in the near term (5 to 10 yrs) is still debatable.

What we know for sure

- Resorting to a so radically different technology, it is difficult to anticipate its evolution.
- Emerging as an entirely new paradigm, quantum hardware and software brings no similarity to their classical counterparts.

… but what are we talking about?

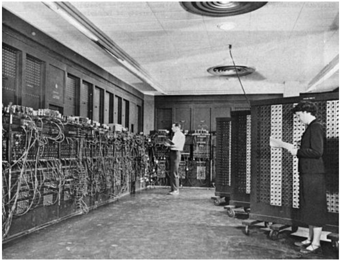
Where shall I begin, please Your Majesty?, he asked.

Begin at the beginning, the King said gravely, *and go on till you come to the end: then stop.*

Lewis Carroll, *Alice's Adventures in Wonderland*, 1865

... the beginnig?

- Information has a crucial physical dimension
- computation is always a physical process



ENIAC (1946)

IBMQ (2022)

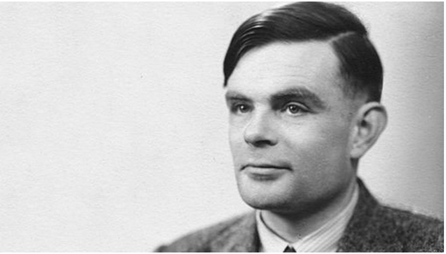
Quantum Mechanics 'meets' Computer Science

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 - 1954)



On Computable Numbers, with an Application to the Entscheidungsproblem (1936)
(computability and the birth of computer science)

Quantum Mechanics 'meets' Computer Science

Richard Feynman (1918 - 1988)

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

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.

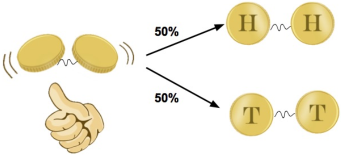
However: A quantum state holds information of both possible classical states, collapsing to one of them upon observation.

Quantum effects as computational resources

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 so strongly correlated, or entangled, that an action performed on one of them can have an immediate effect on the other even at a distance.



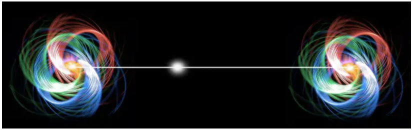
Quantum effects as computational resources

An entangled state cannot be considered as a result of the states of its individual constituents:

This phenomenon can be found in very simple mathematical structures: for example, binary relation

$$\{(0,0),(1,1)\}$$

cannot be written as a Cartesian product of subsets of $\mathcal{B} = \{0,1\}$.



Quantum entanglement can be used to create instantaneous agreement on information across very long distances.

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: Unlike classical physics, quantum theory has processes that are irreducibly non-deterministic, i.e. that cannot be accounted for solely by a lack of knowledge about reality. One can only know the probability of the outcome.

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

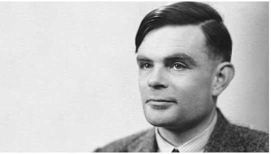
Quantum Computation

David Deutsch (1953)

The Church-Turing principle and the universal quantum computer (1985)
(first example of a quantum algorithm that is exponentially faster than any possible deterministic classical one)

Quantum Computation

quantum resources *quantum algorithms* *computability*



The *motto*

Information is a physical entity. Any computation is a physical process

Thus, any abstract computational model has always to reflect what we know about reality, and quantum theory is our current best tool in this road.

Three ways to represent information

- ... in a two-state device
- ... in a similar way but with uncertainty
- ... in a quantum device

Binary information

Computational / information states based on Boolean values 0 and 1 which can be represented by vectors:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

If rows are labelled from 0 onwards, the presence of 1 in a cell identifies the number represented by the vector.

Larger state spaces are built with the (Kronecker) tensor product:

$$\begin{bmatrix} p_0 \\ p_1 \end{bmatrix} \otimes \begin{bmatrix} q_0 \\ q_1 \end{bmatrix} = \begin{bmatrix} p_0 \begin{bmatrix} q_0 \\ q_1 \end{bmatrix} \\ p_1 \begin{bmatrix} q_0 \\ q_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} p_0 q_0 \\ p_0 q_1 \\ p_1 q_0 \\ p_1 q_1 \end{bmatrix}$$

Binary information

Examples

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$|4\rangle = |100\rangle = |1\rangle \otimes |0\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Binary information

Operations as matrices

$I(x) = x$ $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$ $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$

$X(x) = \neg x$ $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$ $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$

$\underline{1}(x) = 1$ $\begin{bmatrix}0 & 0\\1 & 1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$ $\begin{bmatrix}0 & 0\\1 & 1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$

$\underline{0}(x) = 0$ $\begin{bmatrix}1 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$ $\begin{bmatrix}1 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$

$$\begin{aligned}
I|0\rangle &= |0\rangle & I|1\rangle &= |1\rangle\\
X|0\rangle &= |1\rangle & X|1\rangle &= |0\rangle\\
\underline{1}|0\rangle &= |1\rangle & \underline{1}|1\rangle &= |1\rangle\\
\underline{0}|0\rangle &= |0\rangle & \underline{0}|1\rangle &= |0\rangle
\end{aligned}$$

Binary information

Composition

Sequential composition: matrix multiplication

Parallel composition: Kronecker product $\otimes$

$$M \otimes N = \begin{bmatrix} M_{1,1}N & \cdots & M_{1,n}N \\ \vdots & & \vdots \\ M_{m,1}N & \cdots & M_{m,n}N \end{bmatrix}$$

for example

$$X \otimes \underline{1} \otimes I\, |101\rangle = X \otimes \underline{1} \otimes I\, (|1\rangle \otimes |0\rangle \otimes |1\rangle) = = X|1\rangle \otimes \underline{1}|0\rangle \otimes I|1\rangle = |011\rangle$$

Probabilistic information

... the system is always in some well defined state, even if we do not know which:
State: is a vector of probabilities in $\mathcal{R}^n$

$$\left[p_0 \cdots p_n\right]^T \text{ such that } \sum_i p_i = 1$$

which express indeterminacy about the system's exact physical configuration

Operator: is a double stochastic matrix where $M_{i,j}$ specifies the probability of evolution from state j to i

Quantum information is a different story

A quantum state holds the information of both possible classical states:

A unit of information 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.

Quantum information is a different story

However, all this potential is hidden:

when observed $|v\rangle$ collapses into a classic state: $|0\rangle$, with probability $|\alpha|^2$, or $|1\rangle$, with probability $|\beta|^2$.

(Recall: $|\alpha| = \sqrt{\alpha\overline{\alpha}}$ for a complex α)

The outcome of an observation is probabilistic, which calls for a restriction to unit vectors, i.e. st

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

to represent quantum states.

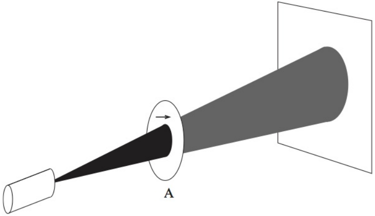
Quantum information is a different story

This quantum state is not a probabilistic mixture: it is not true that the state is really either $|0\rangle$ or $|1\rangle$ and we just do not happen to know which.

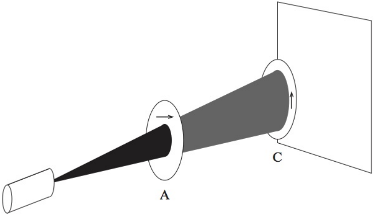
Amplitudes are not real numbers (e.g. probabilities) that can only increase when added, but complex so that they can cancel each other or lower their probability, thus capturing a fundamental quantum resource:

interference

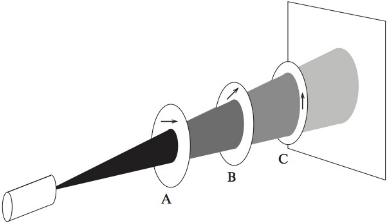
Quantum information: An experiment with a photon



$|0\rangle$ - horizontal polarization



$|1\rangle$ - vertical polarization



(from [Reifell & Polak, 2011])

Quantum information: An experiment with a photon

An explanation for a *single* photon experiment

- The photon's polarization state is modelled by a unit vector, for example the following linear combination of $|0\rangle$ and $|1\rangle$:

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

  which corresponds to a polarization of 45 degrees.

- On passing a polaroid the photon will be absorbed or leave the polaroid with its polarization aligned with the polaroid's axis.
- The probability to go through the polaroid is the square of the magnitude of the amplitude of its polarization in the direction of the polaroid's axis.

Quantum information: An experiment with a photon

- Polarization of polaroid B is $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- This vector, together with $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ forms a basis for the 2-dimensional vector space
- of which $\{|0\rangle, |1\rangle\}$ is another one
  (the so-called computational basis).
- Expressing $|0\rangle$ in terms of $|+\rangle$ and $|-\rangle$ yields

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

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

A unit of quantum information

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.

$$\bigcirc\frown\bigcirc = \{|0\rangle, |1\rangle\} \quad \text{or} \quad \bigcirc\frown\bigcirc = \{|-\rangle, |+\rangle\}$$

A unit of quantum information

Observation of a state

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

transforms the state into one of the basis vectors in

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

with a probability given by the norm square of its amplitude.

In other (the quantum mechanics) words:
measurement collapses $|v\rangle$ into a classic state
A subsequent measurement wrt the same basis returns $|u\rangle$ with probability 1.

Qubits

The space of possible polarization states of a photon is an example of a

quantum bit (qubit)

as does any quantum system (e.g. a electron spin or an atom) that can be modelled by a two-dimensional complex vector space.

- 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.
- and they are fragile and unstable which entails the need for qubits' strong isolation, typically very hard to achieve.

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.

Can we play the quantum game with a classical computer?

Simulating a computation with qubits in a classical computer would be extremely hard, i.e. extremely inefficient as the number of qubits increases:

- For 100 qubits the state space would require to store $2^{100} \approx 10^{30}$ complex numbers!
- And what about rotating a vector in a vector space of dimension 10^{30}?

Thus,

Quantum computing as using quantum reality as a computational resource

Richard Feynman, *Simulating Physics with Computers* (1982)

What can be expected from quantum computation?

- The meaning of computable remains the same ...
- ... but the order of complexity may change

The landmark

Factoring in polynomial time - $\mathcal{O}((ln\, n)^3)$

Peter Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer* (1994)

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, ...

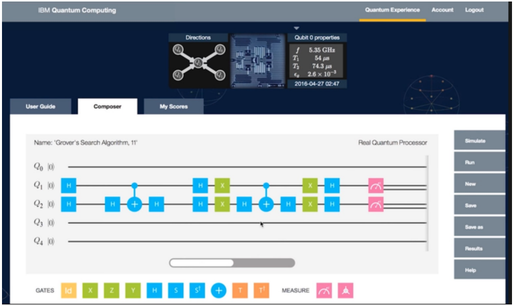
Where exactly do we stand?

- 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.

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 ...

Historically, much of fundamental physics has been concerned with discovering the fundamental particles of nature and the equations which describe their motions and interactions.

It now appears that a different programme may be equally important: to discover the ways that nature allows and prevents, information to be expressed and manipulated, rather than particles to move.

Steane, A.M., 1998.

This Curricular Unit

http://lmf.di.uminho.pt/qu4DataSci-2526