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

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

Universidade do Minho

Quantum Data Science
Universidade do Minho
2026-2027

Plan

Grave Why does quantum matter?

Adagio Computing with quantum mechanics

Andante Quantum programs and quantum computers

Vivace What's next?

Grave

Why does quantum matter?

Why quantum computing?

Why should we care?

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

- Classical computer technology is running up against fundamental size limitations
- Quantum computing brings new physical resources to handle some really hard problems.

Why quantum computing?

Prime factorization

1230186684530117755130494958384962720772853569595334792197322452151726400507
2636575187452021997864693899564749427740638459251925573263034537315482680791
7026122142913461670429214311602221240479274737794080665351419597459856902143413 =
? * ?

- 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, Shor's algorithm achieves this in polynomial time.

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 is still debatable.

What we know for sure

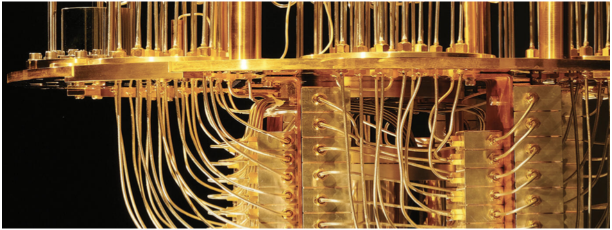
- Resorting to a so radically different technology, it is difficult to anticipate its evolution.
- Emerging as an entirely new paradigm, quantum hardware and software brings no similarity to their classical counterparts.

Adagio

Computing with quantum mechanics

… but what are we talking about?

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



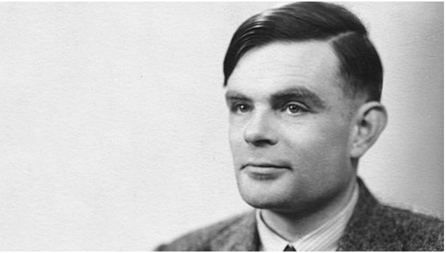
Quantum Mechanics meets' Computer Science

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

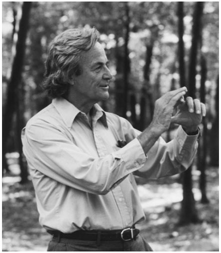
Alan Turing (1912 - 1934)



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

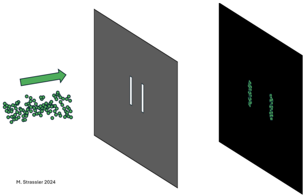
Quantum effects as computational resources

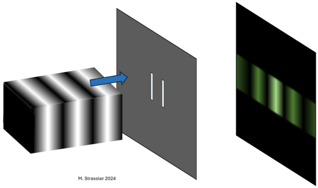
$\boxed{\text{Superposition}}$

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.

Superposition: The double slit experiment





The wave-like pattern appears even when a single photon is emitted: it somehow takes both paths and interacts with itself.

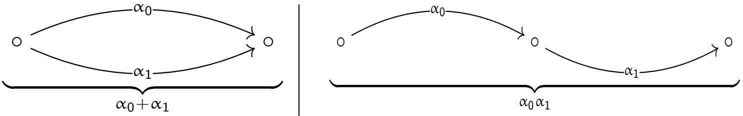
What can be said about this weird behaviour?

Just this: the rules governing the location where the photon will be found have the structure of wave interference.

What does it mean?

Let's call upon Physics, as computation is a physical process:

- Physics identify the system's structure and assign numerical probabilities to each possible path,
- and classically the language of probability theory captures its physical evolution.



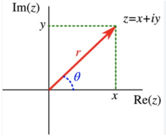
Alternative paths | Sequential paths

(Kolmogorov, 1903-1987, additivity axioms)

What does it mean?

Quantum phenomena, however, cannot be described this way:

Paths are labeled by complex numbers ($\alpha = a + bi$ or $re^{i\theta}$), called their amplitudes. Thus, they are not scalars, but have a direction.



So, when added, they interfere, canceling or reinforcing each other.

Probabilities are recovered as the norms squared of amplitudes:

$$\text{Born's rule} \quad p = |\alpha|^2 = \overline{\alpha}\alpha$$

(for Max Born, 1882-1970)

Superposition

Let's compute the total probability in $\underbrace{\circ \overset{\alpha_0}{\underset{\alpha_1}{\rightrightarrows}} \circ}_{\alpha_0+\alpha_1}$

$$
\begin{aligned}
p &= |\alpha_0 + \alpha_1|^2 \\
&= \overline{(\alpha_0 + \alpha_1)}(\alpha_0 + \alpha_1) \\
&= (\overline{\alpha_0} + \overline{\alpha_1})(\alpha_0 + \alpha_1) \\
&= |\alpha_0|^2 + |\alpha_1|^2 + \overline{\alpha_0}\alpha_1 + \alpha_0\overline{\alpha_1} \\
&= p_0 + p_1 + |\alpha_0||\alpha_1| \left(e^{i(\theta_1 - \theta_0)} + e^{-i(\theta_1 - \theta_0)} \right) \\
&= p_0 + p_1 + \underbrace{2\sqrt{p_0 p_1} \cos(\theta_1 - \theta_0)}_{\text{interference}}
\end{aligned}
$$

(expressing α_j in polar form $|\alpha_j|e^{i\theta_j}$ and resorting to $e^{i\theta} + e^{-i\theta} = 2\cos\theta$)

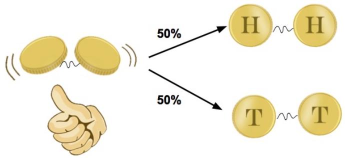
Depending on $\theta_1 - \theta_0$, interference can be either negative or positive. If the system's evolution depends only on that difference, then the system must have, somehow, experienced both paths.

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 entanglement can be used to create instantaneous agreement on information over distance (*teleportation*).

Warning: Entanglement destroys interference

Add detectors to each slit

The two systems (photon and detector) become entangled:

$$(\text{photon} \mid \text{left obs}) \qquad (\text{photon} \mid \text{right obs})$$

and the classicaly expected path re-appears:


$\longmapsto$


Through the detectors, the universe records which path was followed and the availability of this information determines the physical outcome.

Mathematically, ...

- No path information recorded: sum amplitudes (entailing interference) and then compute the probability (quantum behaviour)
- Path information recorded: compute the probability of each path and sum them (classical behaviour)

Warning: Entanglement destroys interference

This is why

- Classical behaviour seems the norm in our daily experience.

The classical world is just quantum reality seen through the blurring effect of trilions of interactions with the environment.

- Quantum states are critically unstable ... and have to be kept in isolation
- ... and quantum computers are so hard (and so costly) to build.

Andante

Quantum programs and quantum computers

Quantum computational resources

Superposition

which allows a quantum memory to hold information of many classical states "simultaneously", each of them carrying a specific weight, or amplitude, which dictates the probability of becoming manifest upon observation. This entails a form of natural parallelism.

Interference

$\cdots$ through which different superposed states combine in a wave-like fashion with positive and negative amplitudes canceling or reinforcing each other.

Entanglement

$\cdots$ witnessing strong correlations between different parts of a system such that an action performed on one of them can have an immediate effect on the other, even at an arbitrary long distance.

Can we play the quantum game with a classical computer?

Do to superposition, a single quantum state (qubit) has a continuum of possible values, potentially storing lots of classical data.

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, the way ahead is

$$\boxed{\text{to resort to quantum reality as a computational resource}}$$

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

... but quantum computing requires engineering!

If superposition entails some form of natural parallelism, making possible the simultaneous computation of all solutions to a problem (all paths), such a magic is refrained by a basic fact: when reading the outcome of such a process,

only one solution is picked up at random, all the other discarded.

No magic, but engineering

$$\boxed{\text{Quantum computation} \;=\; \text{quantum resources} \;+\; \text{engineering}}$$

quantum programming amounts to engineering this potential parallelism with suitable forms of interference to come up to the relevant outcomes with high probability.

Quantum Computation

David Deutsch (1953)

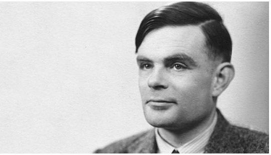
The Church-Turing principle and the universal quantum computer (1985)
(first example of a quantum algorithm that is exponentially faster than any possible deterministic classical one)

Quantum Computation

quantum resources

quantum algorithms

computability



What can be expected from quantum computation?

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

The landmark

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

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

... major steps ...

- 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 e-commerce.
- 2019: Google announced to have achieved quantum supermacy. The problem considered two random number generators, each producing a sequence of digits, trying to determine whether both sequences are completely independent from each other, or are related in a hidden way.
- ... followed by similar announcements in China.
- Explosion of emerging applications in several domains: security, finance, optimization, machine learning, etc., and huge, global research investments in quantum hardware, communications, sensors, and algorithmics.

Huge potential, but moderate expectations

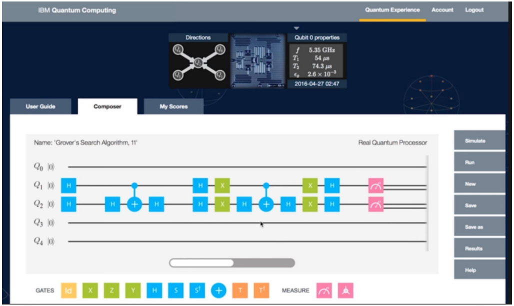
- Quantum systems are highly susceptible to environmental disruptions ... entailing physical challenges in the design of quantum computers that are both expensive and difficult to address.
- Coexistence of several alternative architectural models and physical implementation of qubits; no clear winner.
- Quantum software, as a true engineering discipline, is still in its infancy: new methods, new mathematics, new algorithmic techniques are in order.
- As of today, most of the applications remain theoretical and/or not scaled for market rollout.
- Quantum hardware and software production is extremely costly and restricted to a relatively small number of companies (although within a vibrant ecosystem)

Availability of proof of concept hardware

Where exactly do we stand?

Typical configurations & business models

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



Where exactly do we stand?

NISQ - Noisy Intermediate-Scale Quantum Hybrid (J. Preskill, 2028)

- Machines large enough to be interesting (roughly 50 to 1 000 qubits) but too error-prone.
- Each operation introduces accuracy errors in the system, which limits the size of quantum circuits that can be executed reliably.
- NISQ machines run real applications, but their practical advantage over classical computers remains limited or unproven.

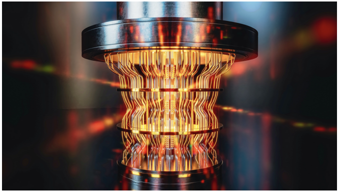
Can run:

- Variational algorithms with short circuits in classical-quantum loops.
- Quantum chemistry approximations for small molecules.
- Optimization heuristics and machine learning experiments with quantum kernel methods.

Where exactly do we stand?

Fault-tolerant machines (currently emerging!)

- Key technology: quantum error correction, which encodes quantum information across multiple physical qubits to create logical qubits that can detect and correct errors in real time
  (1 logical qubit may require 1000 physical ones)
- Can run arbitrarily long computations to completion regardless of how many gates are required, because errors are continuously corrected faster than they accumulate
- Exciting applications, but requiring from hundreds to millions of logical qubits, depending on the problem and the expected precision



Vivace

What's next? ...

This Curricular Unit

http://lmf.di.uminho.pt/qu4DataSci-2627