A course in Quantum Computation
Introduction

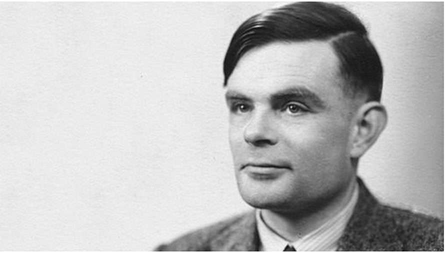
Luís Soares Barbosa

Mestrado em Engenharia Física

Universidade do Minho, 2025-26

The subject

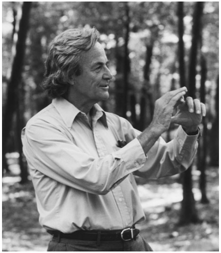
Alan Turing (1912 - 1934)



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

The subject

Richard Feynman (1918 - 1988)



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

The subject

Davis Deutsch (1953)

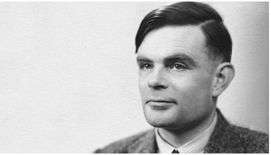
Quantum theory, the Church-Turing principle and the universal quantum computer (1985)
(quantum computability and computational model:
first example of a quantum algorithm that is exponentially faster than any possible deterministic classical one)

The subject

quantum resources

quantum algorithms

computability

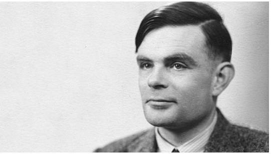


The subject

quantum resources

quantum algorithms

computability

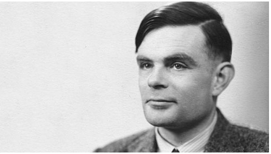


The subject

quantum resources

quantum algorithms

computability



Quantum is trendy ...

Quantum Computing is coming of age
. . . moving from a potential far-future technology to a stage where prototypes become available and major investments arise

- The race for quantum rising between major IT players (IBM, Google, Microsoft, and Intel)
- Public investment (UK, Sweden, Canada, Australia, Portugal)
- EU Flagship initiative with a 10 year timespan and an estimated budget of over one billion euros

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.

(cf, Sycamore, 2019 and Zuchongzhi, 2021)

Why this growing interest?

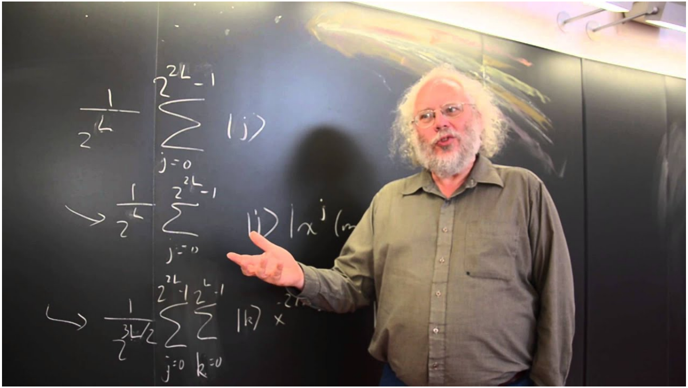
A strategic use of quantum effects potentially provides remarkable speedups to certain kinds of computational tasks

- Cryptography
- Molecular simulation and weather prediction
- Processing of large data

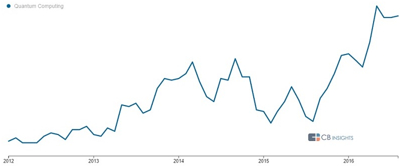
A Concrete Example

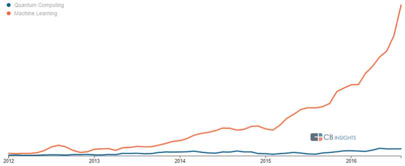
Cryptographic schemes often assume that factoring large integers is computationally intractable

In 1994 Peter Shor presented a quantum algorithm for factoring integers that runs in polynomial time



... but the race is just starting





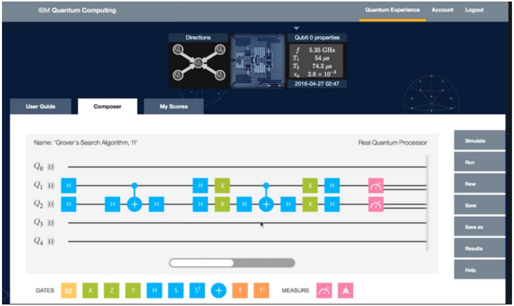
- Clearly, quantum computing will have a substantial impact on societies even if, being a so radically different technology,
- ... it is difficult to anticipate its evolution and future applications ...
- ... quantum computers are currently unreliable for performing useful computational tasks
- ... and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

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



Where exactly do we stand?

Longer term

Fault tolerant quantum computing, base 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

Learning Outcomes

On successful completion of the course students should be able

- To understand basic concepts of computability, computational complexity, and underlying mathematical structures;
- To master the quantum computational model;
- To design and analyse quantum algorithms;
- To implement and run quantum algorithms.

Course Information and Pragmatics

Refer to the course website at

`lmf.di.uminho.pt/quantum-computation-2526/`