Quantum Computation

Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE
SOFTWARE LABORATORY

Table of Contents

The Context

A brief history of Quantum Computation

Currently . . .

Course's Structure and Pragmatics

Context

Quantum Computing is coming of age

. . . moving from a potential far-future technology to a stage where prototypes become available and major investments arise

- Companies (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

Why the big interest?

A strategic use of quantum mechanics potentially provides remarkable speedups to hard computational problems

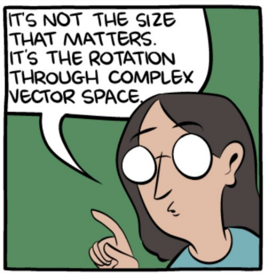
- Cryptographic mechanisms
- Molecule simulation and weather prediction
- Processing of large data

. . . and also more secure communication protocols

Why the big interest? (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


IT'S NOT THE SIZE THAT MATTERS. IT'S THE ROTATION THROUGH COMPLEX VECTOR SPACE.

smbc-comics

Why the big interest? (Concrete example II)

Transmission of information via superposition and entanglement

Eavesdropping becomes detectable

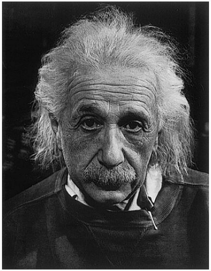


Table of Contents

The Context

A brief history of Quantum Computation

Currently . . .

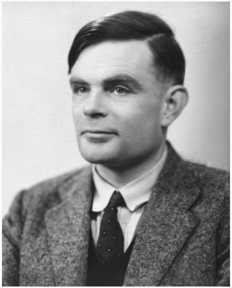
Course's Structure and Pragmatics

The Modern Reincarnation of Computing Science

On Computable Numbers, with an Application to the *Entscheidungsproblem*, 1936

↓

Homework: See/read *The Hitchhiker's Guide to the Galaxy*



A Case for Quantum Computing

Simulating Physics with Computers, 1982

"*. . . because nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.*"

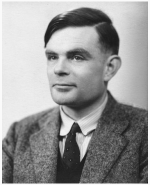
Quantum Computational Model

Quantum theory, the Church-Turing principle and the universal quantum computer, 1985

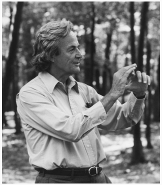
Quantum computability and computational model: first example of a quantum algorithm that is remarkably faster than any possible classical one

The Field of Quantum Computation

Computability



Quantum Computing



Quantum Computability

. . . and of course many others

Table of Contents

The Context

A brief history of Quantum Computation

Currently . . .

Course's Structure and Pragmatics

The Second Quantum Revolution

Viability of quantum computing demonstrated in problems difficult to handle classically

- Google's Sycamore, 2019
- Zuchongzhi, 2021

However . . .

The quantum race has just started

- current quantum computers are unreliable for performing actually useful computational tasks
- difficult to anticipate their evolution and future applications
- commercial/military potential in the short term (5 to 10 yrs) is still highly debatable

In the Short Term

Quantum advantage with the Noisy Intermediate-Scale Quantum (NISQ) computational model

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

Table of Contents

The Context

A brief history of Quantum Computation

Currently . . .

Course's Structure and Pragmatics

Learning Outcomes

On successful completion of the course students should be able to,

- understand basic concepts of computability and computational complexity;
- understand basic concepts and techniques in quantum algorithmics;
- design and analyse quantum algorithms;
- implement and run quantum algorithms in the QISKIT open-source software development kit.

Course Information and Pragmatics

Refer to the course's website at

`lmf.di.uminho.pt/quantum-computation-2223/`

There's a whole quantum world out there which is largely unexplored...
We think it's exciting!

PhD Comics