The past, present, and future history of quantum computing

Ashley Montanaro
ashley.montanaro@bristol.ac.uk

School of Mathematics, University of Bristol
Bristol, UK

25 November 2015

Quantum computing

A quantum computer is a machine designed to use the principles of quantum mechanics to do things which are fundamentally impossible for any computer which only uses classical physics.

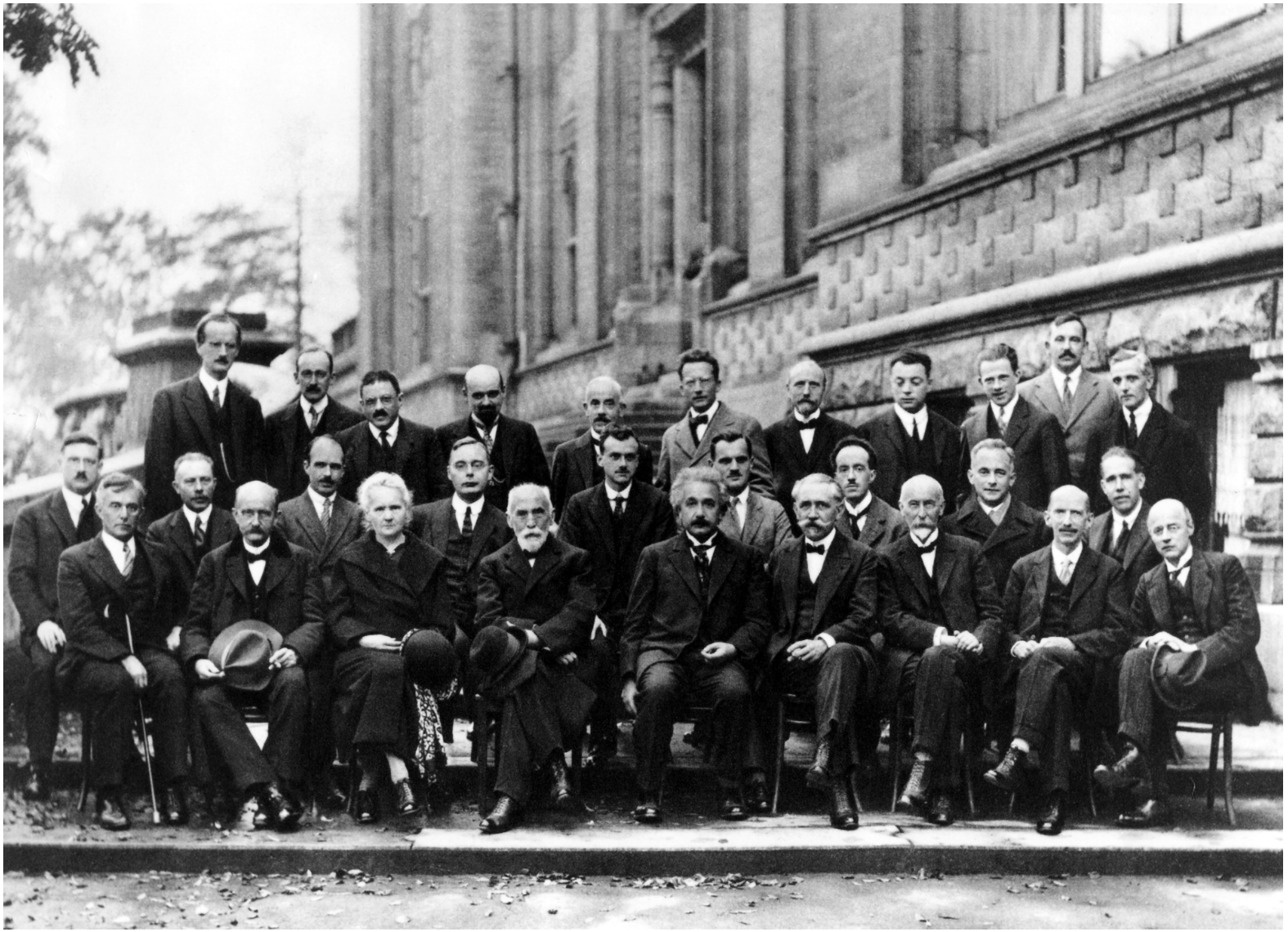
Quantum computing

A quantum computer is a machine designed to use the principles of quantum mechanics to do things which are fundamentally impossible for any computer which only uses classical physics.

This lecture will discuss the history of quantum computing, including:

1. The basic concepts behind quantum mechanics
2. How we can use these concepts for teleportation and cryptography
3. Quantum algorithms outperforming classical algorithms
4. Experimental implementations of quantum computing
5. Commercialisation of quantum technologies

The Solvay conference 1927



Pic: Wikipedia/Solvay conference

The Solvay conference 1927

Pic: Wikipedia/Solvay conference

Key ingredients of quantum mechanics

Quantum mechanics has certain bizarre features which do not occur in standard, or “classical” physics, such as:

Key ingredients of quantum mechanics

Quantum mechanics has certain bizarre features which do not occur in standard, or "classical" physics, such as:

1. Superposition. If a system can be in state A or state B, it can also be in a "mixture" of the two states. If we measure it, we see either A or B, probabilistically.

Key ingredients of quantum mechanics

Quantum mechanics has certain bizarre features which do not occur in standard, or "classical" physics, such as:

1. Superposition. If a system can be in state A or state B, it can also be in a "mixture" of the two states. If we measure it, we see either A or B, probabilistically.

2. Collapse. Any further measurements will give the same result.

Key ingredients of quantum mechanics

Quantum mechanics has certain bizarre features which do not occur in standard, or "classical" physics, such as:

1. Superposition. If a system can be in state A or state B, it can also be in a "mixture" of the two states. If we measure it, we see either A or B, probabilistically.

2. Collapse. Any further measurements will give the same result.

3. Entanglement. There exist systems of multiple parts which cannot be described only in terms of their constituent parts.

Key ingredients of quantum mechanics

Quantum mechanics has certain bizarre features which do not occur in standard, or "classical" physics, such as:

1. Superposition. If a system can be in state A or state B, it can also be in a "mixture" of the two states. If we measure it, we see either A or B, probabilistically.

2. Collapse. Any further measurements will give the same result.

3. Entanglement. There exist systems of multiple parts which cannot be described only in terms of their constituent parts.

4. Uncertainty. There are pairs of measurements where greater certainty of the outcome of one measurement implies greater uncertainty of the outcome of the other measurement.

Key ingredients of quantum mechanics

Quantum mechanics has certain bizarre features which do not occur in standard, or "classical" physics, such as:

1. Superposition. If a system can be in state A or state B, it can also be in a "mixture" of the two states. If we measure it, we see either A or B, probabilistically.

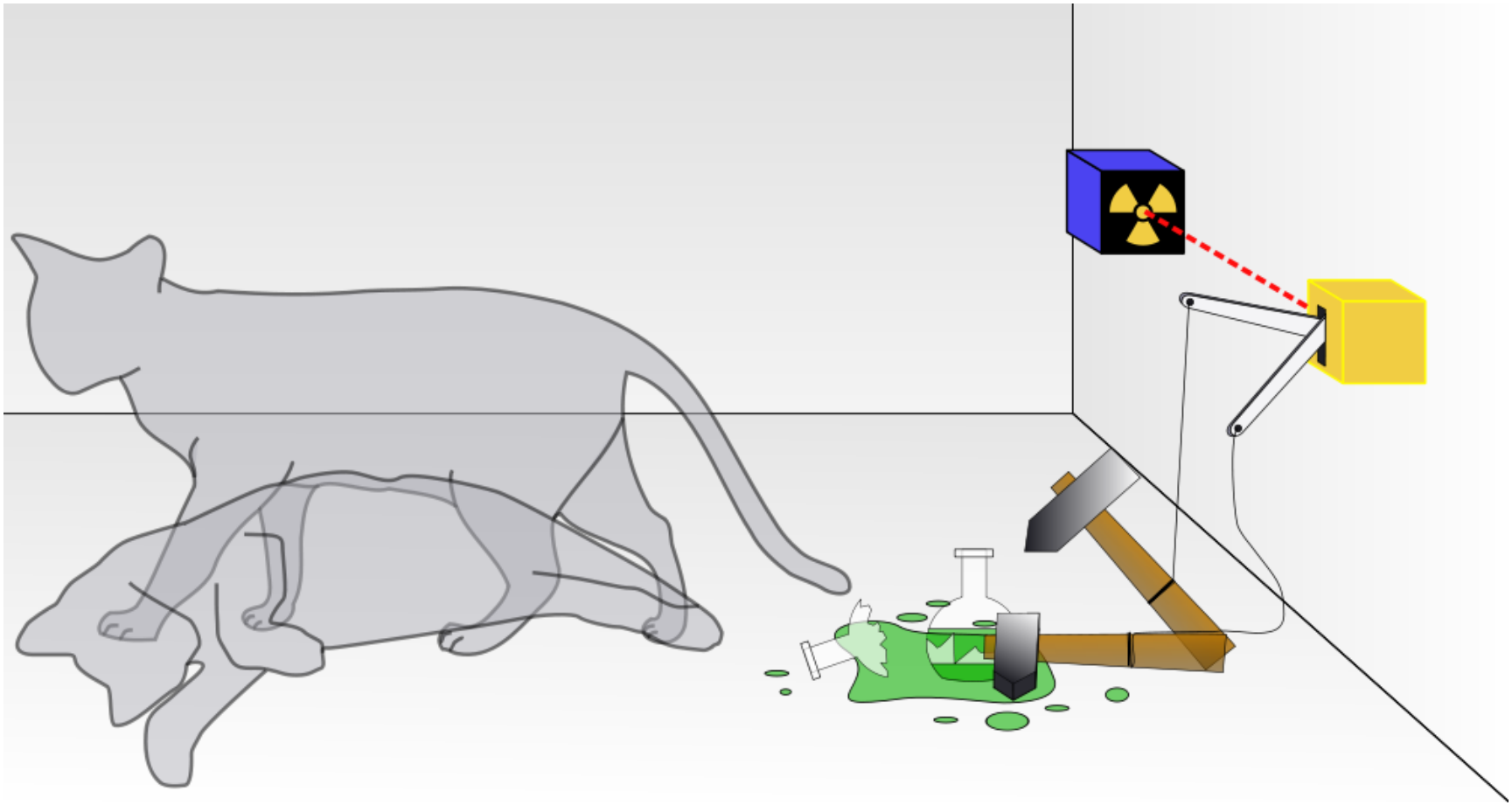
2. Collapse. Any further measurements will give the same result.

3. Entanglement. There exist systems of multiple parts which cannot be described only in terms of their constituent parts.

4. Uncertainty. There are pairs of measurements where greater certainty of the outcome of one measurement implies greater uncertainty of the outcome of the other measurement.

The basic idea behind quantum computing is to use these effects to our advantage.

Schrödinger's cat



Pic: Wikipedia/Schrodinger's cat

The qubit: the basic building-block of quantum computers

- Quantum mechanics deals with very small systems, like atoms or photons (“particles of light”).
- A quantum system which has two distinct states is called a qubit.
- Just as classical computers operate on bits, quantum computers operate on qubits.

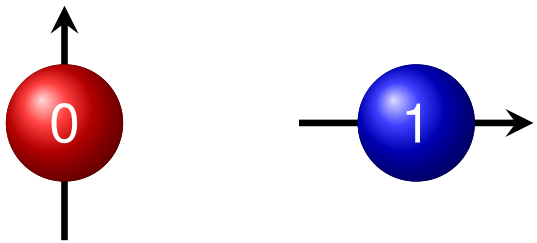
The qubit: the basic building-block of quantum computers

- Quantum mechanics deals with very small systems, like atoms or photons (“particles of light”).
- A quantum system which has two distinct states is called a qubit.
- Just as classical computers operate on bits, quantum computers operate on qubits.

For example, one property of a photon is polarisation: a photon can be either vertically or horizontally polarised ($\uparrow$ or $\rightarrow$), so this gives us a qubit.

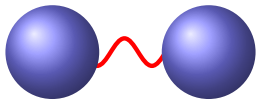
Pic: coins-of-the-uk.co.uk

vs.

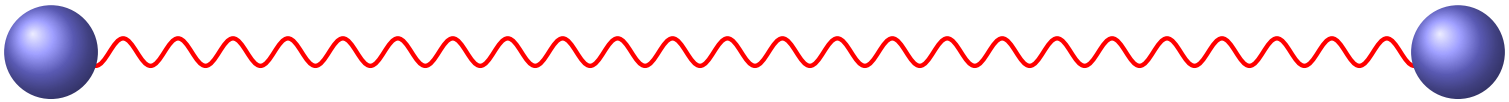


Non-locality and entanglement

Imagine we have a pair of entangled qubits:



Non-locality and entanglement



- Even if we move one of the qubits to the Moon, the global state of the two qubits cannot be described solely in terms of the individual state of each of them!

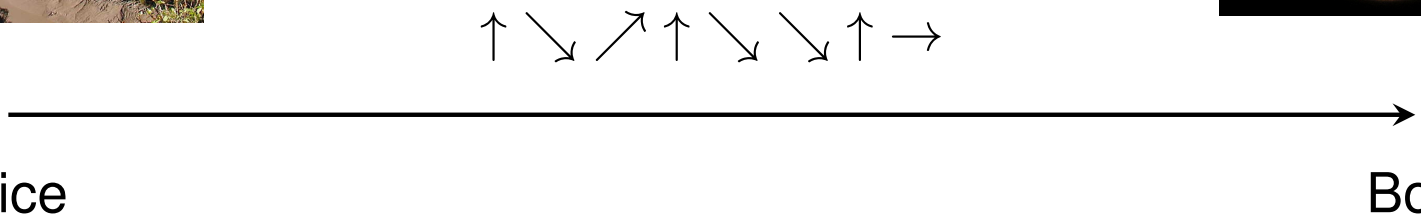
- In particular, if we measure one of the qubits, this apparently instantaneously affects the other one.

Quantum cryptography

- 1984: Bennett and Brassard propose to use quantum mechanics for secure distribution of cryptographic keys
- 1989: Quantum key distribution demonstrated experimentally

Quantum cryptography

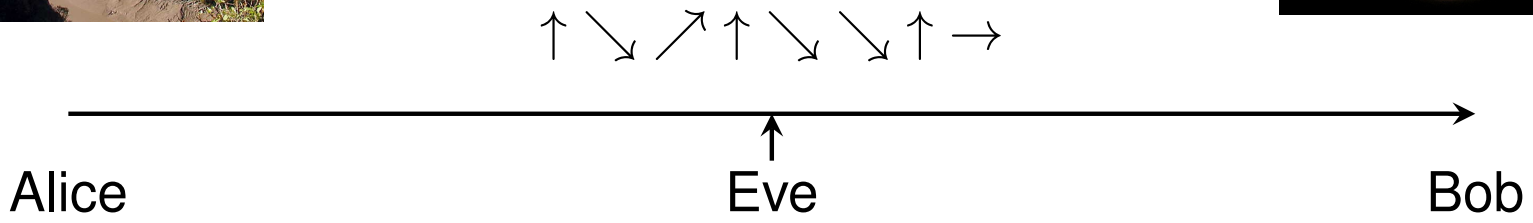
- 1984: Bennett and Brassard propose to use quantum mechanics for secure distribution of cryptographic keys
- 1989: Quantum key distribution demonstrated experimentally



- The basic idea is to use the principles of uncertainty and collapse to detect an eavesdropper.

Quantum cryptography

- 1984: Bennett and Brassard propose to use quantum mechanics for secure distribution of cryptographic keys
- 1989: Quantum key distribution demonstrated experimentally



- The basic idea is to use the principles of uncertainty and collapse to detect an eavesdropper.
- If Eve wants to read Alice's message to Bob, she has to measure it – and that can be detected.

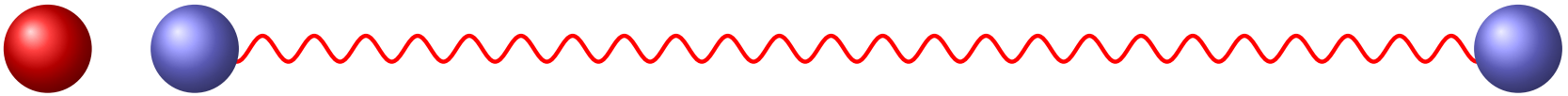
Teleportation: using entanglement to our advantage

- 1993: Quantum teleportation is proposed
- 1997-8: Quantum teleportation demonstrated experimentally

Richard Jozsa, Bill Wootters, Charlie Bennett,
Gilles Brassard, Claude Crépeau, Asher Peres,

cat.

Pic: www.cs.mcgill.ca/∼crepeau/tele.html



The teleportation protocol proceeds as follows:

1. Alice and Bob start by sharing a pair of entangled qubits.

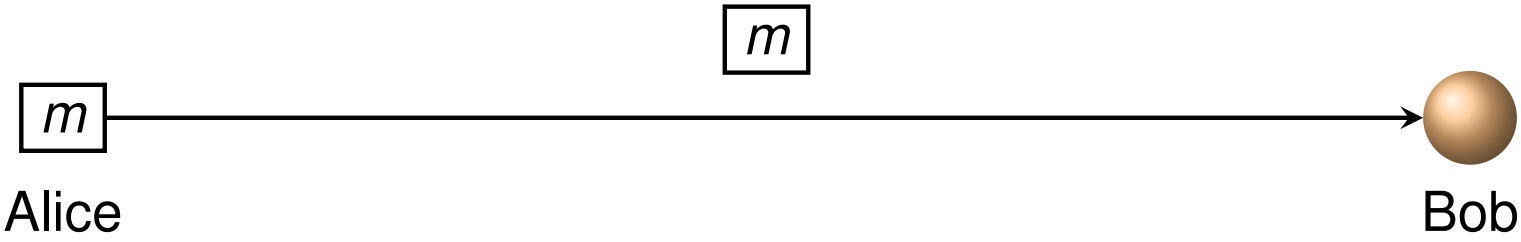
m

Alice

Bob

The teleportation protocol proceeds as follows:

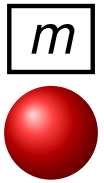
1. Alice and Bob start by sharing a pair of entangled qubits.
2. Alice performs a measurement involving both her half of the pair, and the qubit she wants to send.



The teleportation protocol proceeds as follows:

1. Alice and Bob start by sharing a pair of entangled qubits.
2. Alice performs a measurement involving both her half of the pair, and the qubit she wants to send.
3. She sends the measurement result m to Bob.

Alice

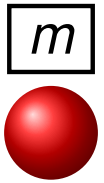


Bob

The teleportation protocol proceeds as follows:

1. Alice and Bob start by sharing a pair of entangled qubits.
2. Alice performs a measurement involving both her half of the pair, and the qubit she wants to send.
3. She sends the measurement result m to Bob.
4. Bob performs a correction based on the measurement result.

Alice



Bob

The teleportation protocol proceeds as follows:

1. Alice and Bob start by sharing a pair of entangled qubits.
2. Alice performs a measurement involving both her half of the pair, and the qubit she wants to send.
3. She sends the measurement result m to Bob.
4. Bob performs a correction based on the measurement result.

At the end of the protocol, the state of Alice's qubit has been transferred to Bob's qubit.

The dawn of quantum computing

There is no efficient general-purpose method known to simulate quantum physics on a standard computer.

The dawn of quantum computing

There is no efficient general-purpose method known to simulate quantum physics on a standard computer.

- 1982: Nobel Laureate Richard Feynman asked whether quantum physics could be simulated efficiently using a quantum computer.

"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."

Pic: Wikipedia/Richard Feynman

The dawn of quantum computing

But nobody knew what such a quantum computer would look like. . .

The dawn of quantum computing

But nobody knew what such a quantum computer would look like...

- 1985: David Deutsch proposes the mathematical concept of the quantum Turing machine to model quantum computation.

"Computing devices resembling the universal quantum computer can, in principle, be built and would have many remarkable properties not reproducible by any Turing machine."

Pic: www.physics.ox.ac.uk/al/people/Deutsch.htm

This put the concept of quantum computing on a sound theoretical footing for the first time.

The dawn of quantum computing

But could a quantum computer actually outperform a classical computer?

The dawn of quantum computing

But could a quantum computer actually outperform a classical computer?

- 1992: David Deutsch and Richard Jozsa give the first such example.

"The quantum computation solves the problem with certainty in exponentially less time than any classical deterministic computation."

Pic: www.damtp.cam.ac.uk/people/r.jozsa

The dawn of quantum computing

But could a quantum computer actually outperform a classical computer?

- 1992: David Deutsch and Richard Jozsa give the first such example.

"The quantum computation solves the problem with certainty in exponentially less time than any classical deterministic computation."

Pic: www.damtp.cam.ac.uk/people/r.jozsa

- 1993: Ethan Bernstein and Umesh Vazirani show that quantum computers can be significantly faster than classical computers, even if the classical computer is allowed a small probability of error.
- 1994: Dan Simon shows that quantum computers can be exponentially faster.

The dawn of quantum computing

But could a quantum computer actually outperform a classical computer?

- 1992: David Deutsch and Richard Jozsa give the first such example.

"The quantum computation solves the problem with certainty in exponentially less time than any classical deterministic computation."

Pic: www.damtp.cam.ac.uk/people/r.jozsa

- 1993: Ethan Bernstein and Umesh Vazirani show that quantum computers can be significantly faster than classical computers, even if the classical computer is allowed a small probability of error.
- 1994: Dan Simon shows that quantum computers can be exponentially faster.

These problems were all somewhat contrived. . .

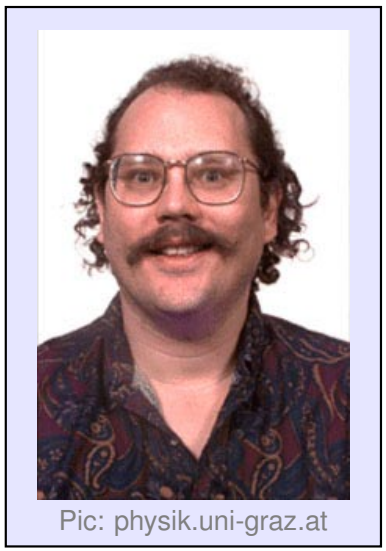
Shor's algorithm

But could a quantum computer solve a problem which people actually care about?

Shor's algorithm

But could a quantum computer solve a problem which people actually care about?

- 1994: Peter Shor shows that quantum computers can factorise large integers efficiently.



Pic: physik.uni-graz.at

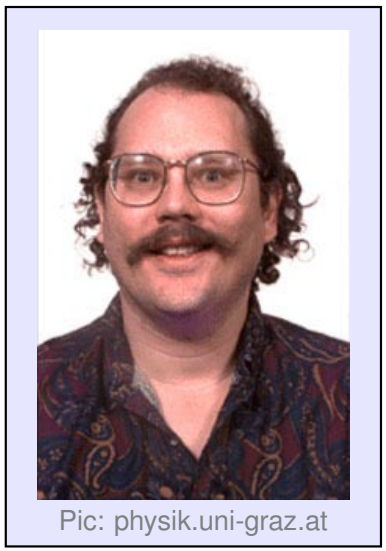
Given an integer $N = p \times q$ for prime numbers p and q, Shor's algorithm outputs p and q.

No efficient classical algorithm for this task is known.

Shor's algorithm

But could a quantum computer solve a problem which people actually care about?

- 1994: Peter Shor shows that quantum computers can factorise large integers efficiently.



Pic: physik.uni-graz.at

Given an integer $N = p \times q$ for prime numbers p and q, Shor's algorithm outputs p and q.

No efficient classical algorithm for this task is known.

Shor's algorithm breaks the RSA public-key cryptosystem on which Internet security is based.

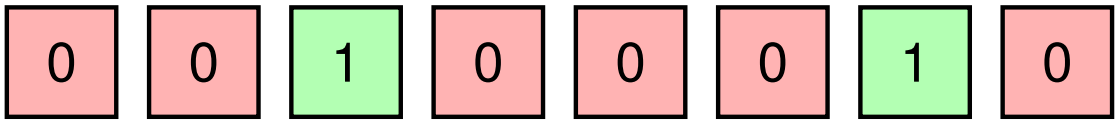
Grover's algorithm

One of the most basic problems in computer science: unstructured search.

Grover's algorithm

One of the most basic problems in computer science: unstructured search.

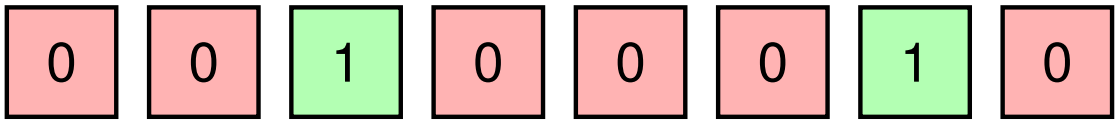
- Imagine we have n boxes, each containing a 0 or a 1. We can look inside a box at a cost of one query.



Grover's algorithm

One of the most basic problems in computer science: unstructured search.

- Imagine we have n boxes, each containing a 0 or a 1. We can look inside a box at a cost of one query.

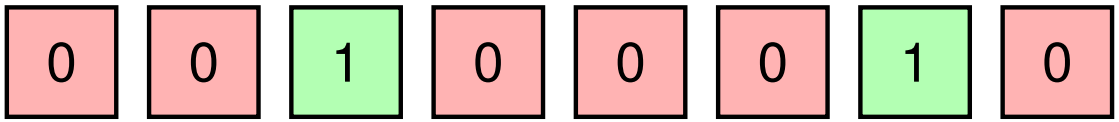


- We want to find a box containing a 1. On a classical computer, this task could require n queries in the worst case.

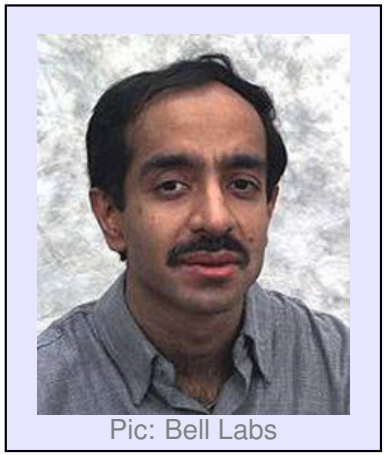
Grover's algorithm

One of the most basic problems in computer science: unstructured search.

- Imagine we have n boxes, each containing a 0 or a 1. We can look inside a box at a cost of one query.



- We want to find a box containing a 1. On a classical computer, this task could require n queries in the worst case.
- 1996: Lov Grover gives a quantum algorithm which solves this problem using about $\sqrt{n}$ queries.


Pic: Bell Labs

The square-root speedup of Grover's algorithm finds many applications to search and optimisation problems.

Quantum simulation

The third important algorithmic development in the late 90's was the resolution of Feynman's conjecture.

- 1996: Seth Lloyd proposes a quantum algorithm which can simulate quantum-mechanical systems.

Pic: MIT

"A quantum computer with a few tens of quantum bits could perform in a few tens of steps simulations that would require Avogadro's number [6×10^{23}] of memory sites and operations on a classical computer."

Quantum simulation

The third important algorithmic development in the late 90's was the resolution of Feynman's conjecture.

- 1996: Seth Lloyd proposes a quantum algorithm which can simulate quantum-mechanical systems.

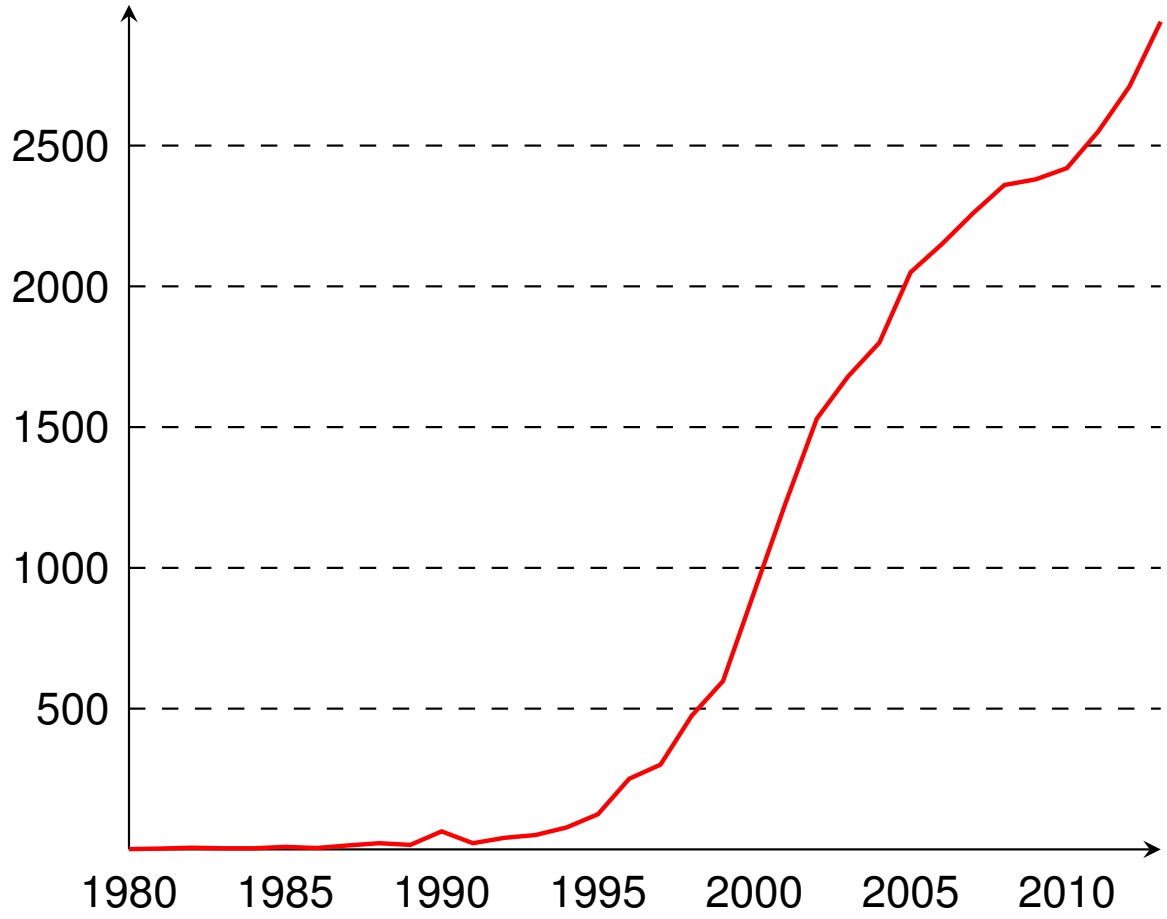
Pic: MIT

"A quantum computer with a few tens of quantum bits could perform in a few tens of steps simulations that would require Avogadro's number [6×10^{23}] of memory sites and operations on a classical computer."

Simulating quantum mechanics has applications to drug design, materials science, high-energy physics, ...

The rise of quantum computing

Following the publication of these algorithms, there was an explosion of interest in quantum computing:



No. of published papers using phrase “quantum computer” per year (Google Scholar)

But can we actually build one?

Building a large-scale quantum computer is extremely challenging because of decoherence.

If a quantum computer interacts with the outside world and is subject to noise, it can lose its “quantumness” and behave like a classical computer.

But can we actually build one?

Building a large-scale quantum computer is extremely challenging because of decoherence.

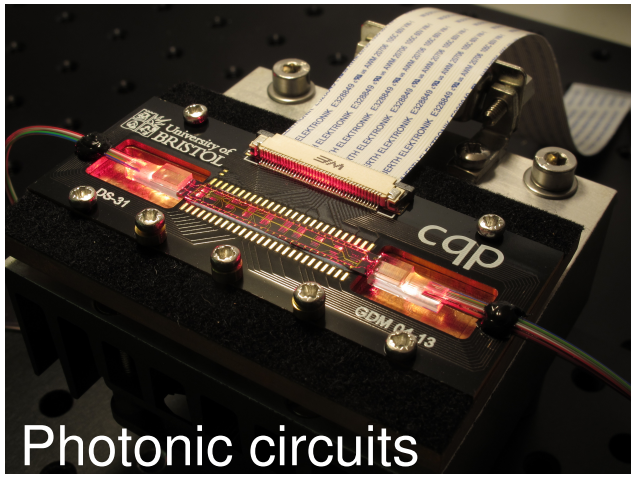
If a quantum computer interacts with the outside world and is subject to noise, it can lose its "quantumness" and behave like a classical computer.

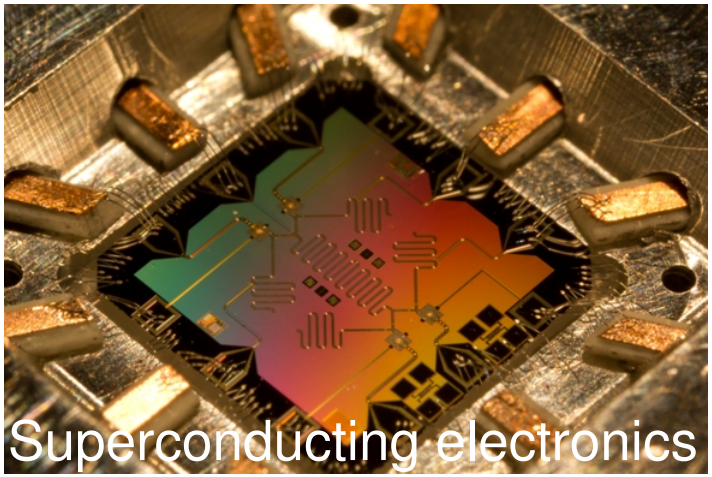
- 1995-6: Peter Shor and Andrew Steane devise quantum error-correcting codes which can be used to fight decoherence.

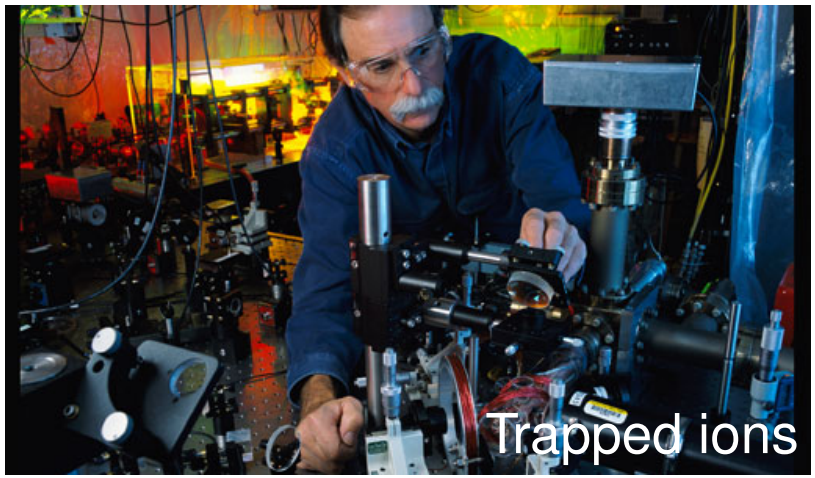
The most optimistic current estimates are that a fault-tolerant quantum computer could be built from components which have an error rate of up to about 1%.

Quantum computing technologies

It isn't clear yet which technology will be used to build a large-scale quantum computer. Some examples:







Pics: University of Bristol, UCSB, NIST

Some experimental progress

1997-8	Quantum teleportation demonstrated [Innsbruck, Rome, Caltech, . . .]
1998	Quantum error-correction demonstrated [MIT]
2001	Shor's algorithm factorises $15 = 3 \times 5$ using NMR [IBM]
2005	8 qubits controlled in ion trap [Innsbruck]
2008	Photonic waveguide quantum circuits demonstrated [Bristol]
2010	Entangled states of 14 qubits created in ion trap [Innsbruck]
2012	$21 = 3 \times 7$ factorised using quantum optics [Bristol]
2012	100μs coherence for superconducting electronic qubits [IBM]
2013	First publicly-accessible "quantum cloud" [Bristol]
2014	Superconducting qubits at fault-tolerant threshold [UCSB]

Quantum technologies you can buy today

Quantum random number generators:

Quantis-PCIe-16M Card

- 16Mbps of true quantum randomness
- PCI Express interface
- Certified by Swiss National Laboratory
- OS Support: Windows, Linux, Solaris, FreeBSD
- Demo application

2565 €

Quantity : 0 (Promotional offer : free shipping for online purchases)

Quantum technologies you can buy today

Quantum random number generators:

Quantis-PCIe-16M Card

- 16Mbps of true quantum randomness
- PCI Express interface
- Certified by Swiss National Laboratory
- OS Support: Windows, Linux, Solaris, FreeBSD
- Demo application

2565 €

Quantity : 0 (Promotional offer : free shipping for online purchases)

Quantum key distribution solutions:

Both of these products marketed by ID Quantique.

Quantum technologies you can buy today

The D-Wave Two “quantum computer”:

Pic: NASA

The D-Wave Two device

D-Wave Systems, Inc. claims that their system is the world's first large-scale quantum computer, with up to 512 qubits.

The D-Wave Two device

D-Wave Systems, Inc. claims that their system is the world's first large-scale quantum computer, with up to 512 qubits.

However, their claims are controversial:

The D-Wave Two device

D-Wave Systems, Inc. claims that their system is the world's first large-scale quantum computer, with up to 512 qubits.

However, their claims are controversial:

- Their machine isn't a general-purpose quantum computer, but can only be used to run one optimisation algorithm.

The D-Wave Two device

D-Wave Systems, Inc. claims that their system is the world's first large-scale quantum computer, with up to 512 qubits.

However, their claims are controversial:

- Their machine isn't a general-purpose quantum computer, but can only be used to run one optimisation algorithm.
- Their qubits are "noisy", and do not operate below the fault-tolerant threshold.

The D-Wave Two device

D-Wave Systems, Inc. claims that their system is the world's first large-scale quantum computer, with up to 512 qubits.

However, their claims are controversial:

- Their machine isn't a general-purpose quantum computer, but can only be used to run one optimisation algorithm.
- Their qubits are "noisy", and do not operate below the fault-tolerant threshold.
- They have not demonstrated large-scale quantum entanglement.

The D-Wave Two device

D-Wave Systems, Inc. claims that their system is the world's first large-scale quantum computer, with up to 512 qubits.

However, their claims are controversial:

- Their machine isn't a general-purpose quantum computer, but can only be used to run one optimisation algorithm.
- Their qubits are "noisy", and do not operate below the fault-tolerant threshold.
- They have not demonstrated large-scale quantum entanglement.
- Recent research suggests that fine-tuned classical optimisation algorithms can sometimes outperform their machine.

The D-Wave Two device

D-Wave Systems, Inc. claims that their system is the world's first large-scale quantum computer, with up to 512 qubits.

However, their claims are controversial:

- Their machine isn't a general-purpose quantum computer, but can only be used to run one optimisation algorithm.
- Their qubits are "noisy", and do not operate below the fault-tolerant threshold.
- They have not demonstrated large-scale quantum entanglement.
- Recent research suggests that fine-tuned classical optimisation algorithms can sometimes outperform their machine.

Characterising the power and potential of the D-Wave approach is currently an active area of research.

The commercial future of quantum computing

Can quantum computing make money?

The commercial future of quantum computing

Can quantum computing make money?

- Several major technology companies now have their own quantum computing research efforts, e.g. IBM, Microsoft (two groups!), Google.

The commercial future of quantum computing

Can quantum computing make money?

- Several major technology companies now have their own quantum computing research efforts, e.g. IBM, Microsoft (two groups!), Google.
- 2002: ID Quantique is first commercial company to demonstrate quantum key distribution.
- 2013: Mike Lazaridis (founder of BlackBerry) announces $100M venture capital fund to invest in quantum computing.
- 2014: The UK government announces £270M funding for research into, and commercialisation of, quantum technologies.

The commercial future of quantum computing

Can quantum computing make money?

- Several major technology companies now have their own quantum computing research efforts, e.g. IBM, Microsoft (two groups!), Google.
- 2002: ID Quantique is first commercial company to demonstrate quantum key distribution.
- 2013: Mike Lazaridis (founder of BlackBerry) announces $100M venture capital fund to invest in quantum computing.
- 2014: The UK government announces £270M funding for research into, and commercialisation of, quantum technologies.

Estimates (perhaps not reliable) for the value of the quantum computing market are into the 10's of billions by 2020.

Challenges for quantum computing

Although there has been significant progress in quantum computing, the field faces a number of challenges:

- The difficulty of building a large-scale quantum computer;
- The difficulty of designing new quantum algorithms;
- The difficulty of applying existing quantum algorithms to practical problems;
- The difficulty of proving limitations on quantum computers.

So there is still much to be done...

Summary

- Quantum computers can solve certain problems more efficiently than classical computers.

Summary

- Quantum computers can solve certain problems more efficiently than classical computers.
- We don't have large-scale, general-purpose quantum computers yet...

Summary

- Quantum computers can solve certain problems more efficiently than classical computers.
- We don't have large-scale, general-purpose quantum computers yet...
- ...but physicists and engineers are working on it!

Summary

- Quantum computers can solve certain problems more efficiently than classical computers.
- We don't have large-scale, general-purpose quantum computers yet...
- ...but physicists and engineers are working on it!
- The most important application of a large-scale quantum computer is likely to be simulating quantum-mechanical systems.

Summary

- Quantum computers can solve certain problems more efficiently than classical computers.
- We don't have large-scale, general-purpose quantum computers yet...
- ...but physicists and engineers are working on it!
- The most important application of a large-scale quantum computer is likely to be simulating quantum-mechanical systems.
- There are still many interesting open questions about the power and potential of quantum computing to be explored.

Further reading

- Winning a Game Show with a Quantum Computer
  Ashley Montanaro
  `http://www.cs.bris.ac.uk/~montanar/gameshow.pdf`

- Quantum Computing Since Democritus
  Scott Aaronson
  `http://www.scottaaronson.com/democritus/`

- Introduction to Quantum Computing, University of Waterloo
  John Watrous
  `https://cs.uwaterloo.ca/~watrous/LectureNotes.html`

- Quantum Computation and Quantum Information
  Michael Nielsen and Isaac Chuang
  Cambridge University Press

Partial timeline: Theory of quantum computing

	⋮
1984	Quantum cryptographic key distribution invented [Bennett+Brassard]
1985	General quantum computational model proposed [Deutsch]
1992	First exponential quantum speed-up discovered [Deutsch and Jozsa]
1993	Quantum teleportation invented [Bennett et al.]
1994	Shor's algorithm rewrites the rulebook of classical cryptography
1995	Quantum error-correcting codes invented [Shor]
1996	Quantum simulation algorithm proposed [Lloyd]
1996	Quantum speed-up for unstructured search problems [Grover]
1998	Efficient quantum communication protocols [Buhrman et al.]
2003	Exponential speed-ups by quantum walks invented [Childs et al.]
	⋮