Quantum Computing

#SWFuturists
The power of quantum computing

Ashley Montanaro
@quantumashley

School of Mathematics,
University of Bristol

9 February 2016
About me

My research tries to understand what quantum computers can do... and what they can’t.

My background:

- **1998-2001**: Undergraduate degree in Computer Science & Mathematics, Manchester
- **2001-2004**: Software engineer working on mobile telephony
- **2004-2007**: PhD in quantum computing, Bristol
- **2007-2013**: Postdoctoral work in Bristol and Cambridge
- **Now**: Lecturer in Applied Mathematics and Research Fellow, University of Bristol
Quantum computers

University of Bristol

UCSB / Google

IBM

University of Oxford
Quantum mechanics

A simple example: the behaviour of a photon.
Quantum mechanics

When fired at a mirror, the photon bounces off.
Quantum mechanics

When fired at a mirror, the photon bounces off.
Quantum mechanics

Now imagine we use a partly reflective mirror.
Quantum mechanics

Now imagine we use a partly reflective mirror.
Now imagine we use a partly reflective mirror.
Quantum mechanics

Then the photon is simultaneously reflected and transmitted!
Quantum mechanics

This phenomenon is known as superposition.
Quantum computing

Imagine the photon’s path encodes a bit of information.
Quantum computing

Imagine the photon’s path encodes a bit of information.
Imagine the photon’s path encodes a bit of information.
Then the photon’s state encodes a superposition of 0 and 1.
Quantum computing

This allows us to compute on input 0 and 1 simultaneously!
If we have \( n \) photons, we have a superposition of \( 2^n \) states!
Key ingredients of quantum mechanics

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, with some probability of each.
Key ingredients of quantum mechanics

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, with some probability of each.

2. **Collapse.** Any further measurements will give the same result.
Key ingredients of quantum mechanics

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, with some probability of each.

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.

In quantum computing we use these effects to our advantage.
Key ingredients of quantum mechanics

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, with some probability of each.

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

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, with some probability of each.

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.

In quantum computing we use these effects to our advantage.
**Integer factorisation**

**Problem:** Given an integer \( N = p \times q \) for prime numbers \( p \) and \( q \), determine \( p \) and \( q \).

\[
\text{e.g. } 435808446576619170111728274257 = 940563886675753 \times 463348054024169
\]
**Problem:** Given an integer $N = p \times q$ for prime numbers $p$ and $q$, determine $p$ and $q$.

\[435808446576619170111728274257 = 940563886675753 \times 463348054024169\]

A quantum algorithm due to Peter Shor solves this problem efficiently. No efficient classical algorithm is known.

Shor’s algorithm breaks the **RSA public-key cryptosystem** on which Internet security is based.
Quantum cryptography

Conversely, quantum mechanics can be used to provide security guaranteed by the laws of physics.
Quantum cryptography

Conversely, quantum mechanics can be used to provide security guaranteed by the laws of physics.

If an eavesdropper (Eve) attempts to read Alice’s communication to Bob, the disturbance she causes can be detected.
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.
Quantum search and optimisation

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

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

2. We want to find a box containing a 1.
Quantum search and optimisation

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.

```
  0  0  1  0  0  0  1  0
```

- We want to find a box containing a 1.

A quantum algorithm due to Lov Grover can solve the search problem with roughly $\sqrt{n}$ quantum queries.

Many applications to practically important search and optimisation problems.
Summary

- Quantum computers allow fundamentally new modes of information processing and have many exciting applications.

- A large-scale, general-purpose quantum computer could have a huge impact on all of our lives.

- We don’t have one yet... but people are working on it! (see next talk)

Further reading:
Quantum algorithms: an overview, AM, npj Quantum Information 2, 2016
www.nature.com/articles/npjqi201523