Quantum Computing

Ashley Montanaro
ashley@cs.bris.ac.uk

Department of Computer Science, University of Bristol
Bristol, UK

12 February 2014
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 built only based on 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 built only based on classical physics.

Google tries to save the world: Internet giant explains how its move into quantum computing could solve global warming

- Google's D-Wave computer is 3,600 times faster than a normal computer
- It uses qubits to perform calculations and solve optimisation problems
- In the video, Google and Nasa explain the basics of quantum computing
- They discuss multi-verse theory and give an example of optimisation
- Faster speeds mean it can tackle complex problems such as disease, climate change and genetics
- Google hopes it will help develop sophisticated artificial life, and find aliens

Daily Mail, 15 October 2013
This talk

1. A brief introduction to the quantum computing model
2. Quantum algorithms: what quantum computers can do
3. Experimental implementations
4. Further reading
The quantum model: qubits

On a normal ("classical") computer, we store information as bits.
The quantum model: qubits

On a normal ("classical") computer, we store information as bits.

- A bit can be either in the state 0, or the state 1.
The quantum model: qubits

On a normal ("classical") computer, we store information as bits.

- A bit can be either in the state 0, or the state 1.
- Physically, we can store a bit in some object that has two states:

![Two coins](coins-of-the-uk.co.uk)
The quantum model: qubits

On a normal (“classical”) computer, we store information as **bits**.

- A bit can be either in the state 0, or the state 1.
- Physically, we can store a bit in some object that has **two states**:

A **qubit** (“quantum bit”) is stored in a tiny physical system like an individual atom that behaves **quantum mechanically**.
The quantum model: qubits

As well as being in states corresponding to 0 or 1, a qubit can be anywhere in between!

\[ \alpha \ 0 \quad + \quad \beta \ 1 \]

- Here \( \alpha \) and \( \beta \) are any numbers (in fact, more generally complex numbers...) satisfying \( \alpha^2 + \beta^2 = 1 \).
The quantum model: qubits

As well as being in states corresponding to 0 or 1, a qubit can be anywhere in between!

\[ \alpha 0 + \beta 1 \]

- Here \( \alpha \) and \( \beta \) are any numbers (in fact, more generally complex numbers...) satisfying \( \alpha^2 + \beta^2 = 1 \).
- This is called superposition.
The quantum model: qubits

As well as being in states corresponding to 0 or 1, a qubit can be anywhere in between!

\[ \alpha 0 + \beta 1 \]

- Here \( \alpha \) and \( \beta \) are any numbers (in fact, more generally complex numbers...) satisfying \( \alpha^2 + \beta^2 = 1 \).
- This is called superposition.

If we have \( n \) qubits, they can be in a superposition of \( 2^n \) different states:

\[ \alpha 00 + \beta 01 + \gamma 10 + \delta 11 \]
The quantum model: qubits

As well as being in states corresponding to 0 or 1, a qubit can be anywhere in between!

\[ \alpha 0 + \beta 1 \]

- Here \( \alpha \) and \( \beta \) are any numbers (in fact, more generally complex numbers...) satisfying \( \alpha^2 + \beta^2 = 1 \).
- This is called superposition.

If we have \( n \) qubits, they can be in a superposition of \( 2^n \) different states:

\[ \alpha 0 0 + \beta 0 1 + \gamma 1 0 + \delta 1 1 \]

This allows a quantum computer to run an algorithm on many possible inputs simultaneously.
Measurement and entanglement

- If we measure some qubits, we see each outcome with probability equal to its corresponding coefficient squared.

- For example, imagine we have two qubits in the state

$$\sqrt{\frac{1}{2}}|0\rangle + \sqrt{\frac{1}{2}}|1\rangle$$

- Then if we measure the qubits, we get outcome 00 with probability $\frac{1}{2}$, and outcome 11 with probability $\frac{1}{2}$.

- But what if the first qubit is in Bristol, and the second is on the Moon? It seems that the measurement result in Bristol has instantaneously affected the qubit on the Moon. . .

- This bizarre phenomenon is known as quantum entanglement.
Measurement and entanglement

▶ If we measure some qubits, we see each outcome with probability equal to its corresponding coefficient squared.
▶ For example, imagine we have two qubits in the state

\[
\frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}
\]

▶ But what if the first qubit is in Bristol, and the second is on the Moon? It seems that the measurement result in Bristol has instantaneously affected the qubit on the Moon... This bizarre phenomenon is known as quantum entanglement.
Measurement and entanglement

- If we measure some qubits, we see each outcome with probability equal to its corresponding coefficient squared.
- For example, imagine we have two qubits in the state

\[
\frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}
\]

- Then if we measure the qubits, we get outcome 00 with probability \( \frac{1}{2} \), and outcome 11 with probability \( \frac{1}{2} \).
Measurement and entanglement

- If we measure some qubits, we see each outcome with probability equal to its corresponding coefficient squared.
- For example, imagine we have two qubits in the state

\[
\frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}
\]

- Then if we measure the qubits, we get outcome 00 with probability \(\frac{1}{2}\), and outcome 11 with probability \(\frac{1}{2}\).
- But what if the first qubit is in Bristol, and the second is on the Moon?
Measurement and entanglement

- If we measure some qubits, we see each outcome with probability equal to its corresponding coefficient squared.
- For example, imagine we have two qubits in the state

\[ \frac{1}{\sqrt{2}} 0 \uparrow 0 \downarrow + \frac{1}{\sqrt{2}} 1 \downarrow 1 \uparrow \]

- Then if we measure the qubits, we get outcome 00 with probability \( \frac{1}{2} \), and outcome 11 with probability \( \frac{1}{2} \).
- But what if the first qubit is in Bristol, and the second is on the Moon?

- It seems that the measurement result in Bristol has **instantaneously affected** the qubit on the Moon...

- This bizarre phenomenon is known as **quantum entanglement**.
Shor’s algorithm

Integer factorisation

Given an integer $N$ such that $N = p \times q$ for prime numbers $p$ and $q$, find $p$ and $q$.

For example: given 15 as input, the output should be 3 and 5.
Given an integer $N$ such that $N = p \times q$ for prime numbers $p$ and $q$, find $p$ and $q$.

For example: given 15 as input, the output should be 3 and 5.

In 1994, Peter Shor described a quantum algorithm which can factorise large integers efficiently.

No efficient classical algorithm is known for this problem.
Why should we care about integer factorisation?

The RSA cryptosystem which underlies Internet security relies on the hardness of integer factorisation. If we could factorise large numbers efficiently, we could break this cryptosystem. In 2009, a 232-digit number was factorised using hundreds of computers over a period of 2 years... by comparison, a large quantum computer could factorise a number with thousands of digits in a matter of minutes.
Factorisation and cryptography

Why should we care about integer factorisation?

- The RSA cryptosystem which underlies Internet security relies on the hardness of integer factorisation.
Factorisation and cryptography

Why should we care about integer factorisation?

- The RSA cryptosystem which underlies Internet security relies on the hardness of integer factorisation.

- If we could factorise large numbers efficiently, we could break this cryptosystem.
Factorisation and cryptography

Why should we care about integer factorisation?

▶ The RSA cryptosystem which underlies Internet security relies on the hardness of integer factorisation.

▶ If we could factorise large numbers efficiently, we could break this cryptosystem.

In 2009, a 232-digit number was factorised using hundreds of computers over a period of 2 years... by comparison, a large quantum computer could factorise a number with thousands of digits in a matter of minutes.
Grover’s algorithm

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

![Pic: Bell Labs](Image)
Grover’s algorithm

- One of the most basic problems in computer science is 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.
Grover’s algorithm

- One of the most basic problems in computer science is 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 is 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. But on a quantum computer, **Grover’s algorithm** can solve the problem with roughly $\sqrt{n}$ queries.
Experimental implementations

There are a number of different technologies which could be used to implement a quantum computer.
Experimental implementations

There are a number of different technologies which could be used to implement a quantum computer.

Photonic quantum circuits on silicon (University of Bristol)

Pic: University of Bristol
Experimental implementations

“Bulk” optics (University of Bristol)

Pic: Carmel King
Experimental implementations

Ion trap (David Wineland group, NIST)

Pic: nobelprize.org
Quantum computing FAQs

1. When can I have one?
Quantum computing FAQs

1. When can I have one?
2. Will I have one on my desk?

To summarise:
▷ Quantum computing is a new and exciting model of computation which can do things that classical computing simply cannot.
▷ A massive international effort is ongoing to build a large-scale quantum computer, including here at Bristol.
▷ There are still many fascinating open problems to address.
Quantum computing FAQs

1. When can I have one?
2. Will I have one on my desk?
3. Can they help discover aliens?

To summarise:
▶ Quantum computing is a new and exciting model of computation which can do things that classical computing simply cannot.
▶ A massive international effort is ongoing to build a large-scale quantum computer, including here at Bristol.
▶ There are still many fascinating open problems to address.

Ashley Montanaro
ashley@cs.bris.ac.uk
Quantum computing FAQs

1. When can I have one?
2. Will I have one on my desk?
3. Can they help discover aliens?

To summarise:

- Quantum computing is a new and exciting model of computation which can do things that classical computing simply cannot.

- A massive international effort is ongoing to build a large-scale quantum computer, including here at Bristol.

- There are still many fascinating open problems to address.
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
### Partial timeline: Theory of quantum computing

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1984</td>
<td>Quantum cryptographic key distribution invented</td>
<td>[Bennett+Brassard]</td>
</tr>
<tr>
<td>1985</td>
<td>General quantum computational model proposed</td>
<td>[Deutsch]</td>
</tr>
<tr>
<td>1992</td>
<td>First exponential quantum speed-up discovered</td>
<td>[Deutsch and Jozsa]</td>
</tr>
<tr>
<td>1993</td>
<td>Quantum teleportation invented</td>
<td>[Bennett et al.]</td>
</tr>
<tr>
<td>1994</td>
<td>Shor’s algorithm rewrites the rulebook of classical cryptography</td>
<td></td>
</tr>
<tr>
<td>1995</td>
<td>Quantum error-correcting codes invented</td>
<td>[Shor]</td>
</tr>
<tr>
<td>1996</td>
<td>Quantum simulation algorithm proposed</td>
<td>[Lloyd]</td>
</tr>
<tr>
<td>1996</td>
<td>Quantum speed-up for unstructured search problems</td>
<td>[Grover]</td>
</tr>
<tr>
<td>1998</td>
<td>Efficient quantum communication protocols</td>
<td>[Buhrman et al.]</td>
</tr>
<tr>
<td>2003</td>
<td>Exponential speed-ups by quantum walks invented</td>
<td>[Childs et al.]</td>
</tr>
<tr>
<td>Year</td>
<td>Event</td>
<td>Location</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>1997-8</td>
<td>Quantum teleportation demonstrated</td>
<td>[Innsbruck, Rome, Caltech, ...]</td>
</tr>
<tr>
<td>1998</td>
<td>Quantum error-correction demonstrated</td>
<td>[MIT]</td>
</tr>
<tr>
<td>2001</td>
<td>Shor's algorithm factorises $15 = 3 \times 5$ using NMR</td>
<td>[IBM]</td>
</tr>
<tr>
<td>2005</td>
<td>8 qubits controlled in ion trap</td>
<td>[Innsbruck]</td>
</tr>
<tr>
<td>2008</td>
<td>Photonic waveguide quantum circuits demonstrated</td>
<td>[Bristol]</td>
</tr>
<tr>
<td>2010</td>
<td>Entangled states of 14 qubits created in ion trap</td>
<td>[Innsbruck]</td>
</tr>
<tr>
<td>2012</td>
<td>$21 = 3 \times 7$ factorised using quantum optics</td>
<td>[Bristol]</td>
</tr>
<tr>
<td>2012</td>
<td>100 $\mu$s coherence for superconducting electronic qubits</td>
<td>[IBM]</td>
</tr>
<tr>
<td>2013</td>
<td>First publicly-accessible “quantum cloud”</td>
<td>[Bristol]</td>
</tr>
</tbody>
</table>