Why don't we have a quantum computer (yet)?

Alex E. Moylett

Quantum Engineering Technology Labs and Quantum Engineering Centre for Doctoral Training
University of Bristol

alex.moylett@bristol.ac.uk

16th November 2017

What is a quantum computer?

A computer which uses the laws of quantum mechanics to solve some problems asymptotically faster than classical computers.

Pros and cons of a quantum computer

Pros:

Cons:

[1]Montanaro, npj Quantum Information 2, 15023 (2016)
[2]Moylett et al., Phys. Rev. A 95, 032323 (2017)

Pros and cons of a quantum computer

Pros:

- They push the limits of our best security protocols, via polynomial time algorithms for hard problems including factoring and discrete log[1]

Cons:

[1] Montanaro, npj Quantum Information 2, 15023 (2016)

[2] Moylett et al., Phys. Rev. A 95, 032323 (2017)

Pros and cons of a quantum computer

Pros:

- They push the limits of our best security protocols, via polynomial time algorithms for hard problems including factoring and discrete log[1]
- They allow us to simulate scientific experiments exponentially faster

Cons:

[1] Montanaro, npj Quantum Information 2, 15023 (2016)

[2] Moylett et al., Phys. Rev. A 95, 032323 (2017)

Pros and cons of a quantum computer

Pros:

- They push the limits of our best security protocols, via polynomial time algorithms for hard problems including factoring and discrete log[1]
- They allow us to simulate scientific experiments exponentially faster
- They can help us solve large search problems – including NP-hard problems[2] – quadratically faster

Cons:

[1] Montanaro, npj Quantum Information 2, 15023 (2016)
[2] Moylett et al., Phys. Rev. A 95, 032323 (2017)

Pros and cons of a quantum computer

Pros:

- They push the limits of our best security protocols, via polynomial time algorithms for hard problems including factoring and discrete log[1]
- They allow us to simulate scientific experiments exponentially faster
- They can help us solve large search problems – including NP-hard problems[2] – quadratically faster
- They provide exponential speedups for some machine learning problems (SVM, PCA, recommendation systems)

Cons:

[1] Montanaro, npj Quantum Information 2, 15023 (2016)
[2] Moylett et al., Phys. Rev. A 95, 032323 (2017)

Pros and cons of a quantum computer

Pros:

- They push the limits of our best security protocols, via polynomial time algorithms for hard problems including factoring and discrete log[1]
- They allow us to simulate scientific experiments exponentially faster
- They can help us solve large search problems – including NP-hard problems[2] – quadratically faster
- They provide exponential speedups for some machine learning problems (SVM, PCA, recommendation systems)

Cons:

- They don't exist(-ish)

[1] Montanaro, npj Quantum Information 2, 15023 (2016)

[2] Moylett et al., Phys. Rev. A 95, 032323 (2017)

Do quantum computers exist?

We do have quantum computers, including some which you can program on right now: `https://quantumexperience.ng.bluemix.net/qx`

The problem is that they are not currently large enough to outperform classical computers at the problems I mentioned earlier.

The largest number factorised by Shor's algorithm so far is 21[3]. Other quantum computing methods have achieved 291311[4], but this is still a way off breaking RSA.

[3] Martín-López et al., Nature Photonics, 6, 773

[4] Li et al., arXiv:1706.08061

D-Wave 2000Q: The world's largest quantum computer

[5]

[5] USC Viterbi School of Engineering (Flickr) https://www.flickr.com/photos/uscviterbi/, via Digital Trends https://www.digitaltrends.com/computing/d-wave-2000-qubit-processor-quantum-computing/

D-Wave 2000Q: The world's largest quantum computer

[5]

[5]USC Viterbi School of Engineering (Flickr) https://www.flickr.com/photos/uscviterbi/, via Digital Trends https://www.digitaltrends.com/computing/d-wave-2000-qubit-processor-quantum-computing/

Pictured: People standing in front of a D-Wave quantum computer.

D-Wave 2000Q: The world's largest quantum computer

[6]

[6] https://www.scottaaronson.com/blog/?p=2448

D-Wave 2000Q: The world's largest quantum computer

[6]

[6] https://www.scottaaronson.com/blog/?p=2448

- Pictured left: Sarah Kaiser and Scott Aaronson in front of a whiteboard. Sarah is wearing a costume of a D-Wave quantum computer.
- Pictured right: Scott Aaronson and Sarah Kaiser. Scott has written on Sarah's costume "VERIFIED Does exactly what it's supposed to – Scott Aaronson".

How to access a D-Wave machine yourself!

- Buy one, for $15 million[7]

[7] https://www.wired.co.uk/article/d-wave-2000q-quantum-computer

[8] https://github.com/alex1770/QUBO-Chimera

[9] http://www.archduke.org/stuff/d-wave-comment-on-comparison-with-classical-computers/harder-qubo-instances-on-a-chimera-graph/

How to access a D-Wave machine yourself!

- Buy one, for \$15 million[7]
- Rent time on one, cheaper but still pricey

[7] https://www.wired.co.uk/article/d-wave-2000q-quantum-computer
[8] https://github.com/alex1770/QUBO-Chimera
[9] http://www.archduke.org/stuff/d-wave-comment-on-comparison-with-classical-computers/harder-qubo-instances-on-a-chimera-graph/

How to access a D-Wave machine yourself!

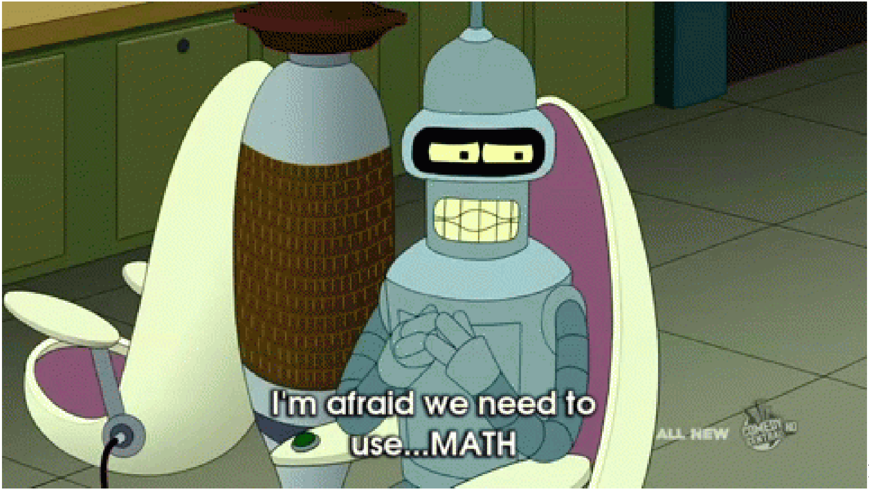
- Buy one, for $15 million[7]
- Rent time on one, cheaper but still pricey
- Use Selby's simulator, freely available on GitHub[8], demonstrated to run faster than earlier D-Wave machines and conjectured to be faster than the 2000Q[9]

[7] https://www.wired.co.uk/article/d-wave-2000q-quantum-computer

[8] https://github.com/alex1770/QUBO-Chimera

[9] http://www.archduke.org/stuff/d-wave-comment-on-comparison-with-classical-computers/harder-qubo-instances-on-a-chimera-graph/

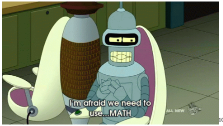
Warning: Here be ~~dragons~~ mathematics...



[10]

[10] Futurama, via Tenor https://tenor.com/view/futurama-math-mathematics-we-need-math-we-need-to-use-math-gif-3486402

Warning: Here be ~~dragons~~ mathematics...



[10] Futurama, via Tenor https://tenor.com/view/futurama-math-mathematics-we-need-math-we-need-to-use-math-gif-3486402

Pictured: Bender from TV series Futurama sat in a chair. Caption says "I'm afraid we need to use...MATH".

Quantum bits

Data is represented in a quantum computer as quantum bits (qubits):

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

$$\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

Quantum gates

Logical gates in a quantum computer are unitary matrices acting on qubits:

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$U|\psi\rangle = \alpha(a|0\rangle + b|1\rangle) + \beta(c|0\rangle + d|1\rangle)$$

Measurement and output

When we look at a quantum state $|\psi\rangle$, we find

- $|0\rangle$ with probability $|\alpha|^2$
- $|1\rangle$ with probability $|\beta|^2$

The state then collapses into the measured result.

A simple quantum simulation algorithm

Each qubit can be represented as two complex numbers.

A unitary gate operating on a qubit is a 2×2 matrix-vector product.

Measurement is just a random number generation.

Doing each of these steps shouldn't take more than $O(n)$.

So where does the complexity come from?

Interference

So far we have assumed the qubits are independent of each other.

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Is a valid quantum state.

Measuring each qubit individually gives $|0\rangle$ or $|1\rangle$ with equal probability.

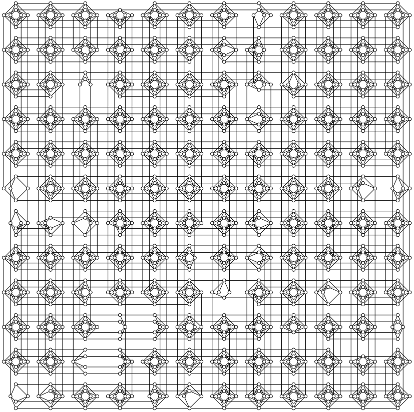
But measuring both qubits together shows that they are perfectly correlated.

Interference makes simulations harder

We now need to consider the probabilities of qubits collectively.

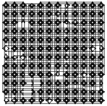
For n qubits, this means keeping track of 2^n complex numbers!

Quantum interference on a D-Wave machine

[11]

[11] King et al., arXiv:1508.05087

Quantum interference on a D-Wave machine

 [11]

[11] King et al., arXiv:1508.05087

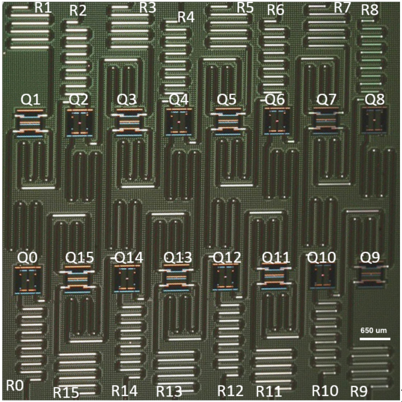
Pictured: Structure of qubits in a D-Wave 2X quantum computer. Circles represent qubits, and two circles connected by a line indicates that those qubits can interact with each other.

Interference on IBM's chips

IBM have also developed quantum computation chips, which are based on a model which cannot be simulated by Selby's algorithm.

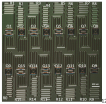
So how many qubits have they got?

16



[12]

[12] https://github.com/QISKit/ibmqx-backend-information/blob/master/backends/ibmqx5/README.md



[12]

[12] https://github.com/QISKit/ibmqx-backend-information/blob/master/backends/ibmqx5/README.md

Pictured: IBM QX5 quantum chip. Text overlay indicates each of the qubits, labelled Q0-Q15, and corresponding readout components, labelled R0-R15.

Where do we go from here?

Getting interaction between every qubit is near impossible.

But significant research is currently going into creating quantum architectures which are hard to simulate and scalable.

The largest device so far is 50 qubits, developed by IBM but not yet public[13].

There is also significant work on error correction schemes, so that quantum operations can take longer.

[13] https://www-03.ibm.com/press/us/en/pressrelease/53374.wss

Quantum computational advantage

What is the smallest quantum experiment that is easier to build and run than it is to simulate?

Possible options include[14]

- Linear optics
- Random circuits
- Low depth circuits
- Nuclear Magnetic Resonance[15]

[14] Harrow & Montanaro, Nature 549, 203209 (2017)
[15] Jones, PhysChemComm 11 (2001)

Conclusion

Quantum computers have a lot of potential to outperform our best classical computers.

But there are lots of hurdles currently in the way.

The need for interaction between qubits is one such hurdle.

Other issues include noise and errors, which build up in quantum states over time.

Quantum Engineering Centre for Doctoral Training

- 1 year MRes including experimental, theoretical and taught work, plus 3 year PhD on a research project of your choice
- Fully funded
- Opportunities to travel and collaborate with other researchers in academia and industry

Open day 5th December: `https://www.eventbrite.co.uk/e/quantum-engineering-bristol-tickets-39609797972`

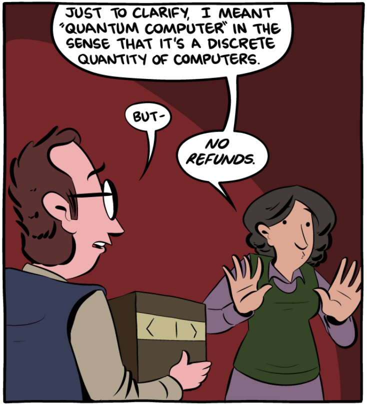
Quantum Engineering Centre for Doctoral Training

- 1 year MRes including experimental, theoretical and taught work, plus 3 year PhD on a research project of your choice
- Fully funded
- Opportunities to travel and collaborate with other researchers in academia and industry

Open day 5th December: `https://www.eventbrite.co.uk/e/quantum-engineering-bristol-tickets-39609797972`

Pictured: Two PhD students on the Quantum Engineering Centre for Doctoral Training. The students are wearing laser safety goggles and adjusting some optics equipment.

The end



It was surprisingly easy to get $100 million from NASA. [16]

Any questions?

[16] http://www.smbc-comics.com/comic/quantum-computer

2017-11-16

Why don't we have a quantum computer?
└─The End

└─The end

The end

It was surprisingly easy to get $100 million from NASA. [16]

Any questions?

[16] http://www.smbc-comics.com/comic/quantum-computer

Pictured: Comic where a feminine-presenting person on the right has handed a box to a masculine-presenting person on the left. The box has bra-ket notation $\langle | \rangle$ on the side. Dialogue reads:

"Just to clarify, I meant "quantum computer" in the sense that it's a discrete quantity of computers."

"But-"

"No refunds."

Caption reads: "It was surprisingly easy to get $100 million from NASA."

Post-credits

The slide is as useful as a current-day quantum computer.