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:

Pros and cons of a quantum computer

Pros:

- They push the limits of our best security protocols, via polynomial time algorithms for factoring and discrete log

Cons:

Pros and cons of a quantum computer

Pros:

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

Cons:

Pros and cons of a quantum computer

Pros:

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

Cons:

Pros and cons of a quantum computer

Pros:

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

Cons:

Pros and cons of a quantum computer

Pros:

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

Cons:

- They don't exist

Pros and cons of a quantum computer

Pros:

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

Cons:

- They don't exist(-ish)

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[1]. Other quantum computing methods have achieved 291311[2], but this is still a way off breaking RSA.

[1] Martn-Lpez et al., Nature Photonics, 6, 773

[2] Li et al., `arXiv:1706.08061`

D-Wave 2000: The world's biggest quantum computer

How to access a D-Wave machine yourself!

- Buy one yourself, for \$15 million[3]

[3] https://www.wired.co.uk/article/d-wave-2000q-quantum-computer
[4] https://github.com/alex1770/QUBO-Chimera
[5] 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 yourself, for \$15 million[3]
- Rent time on one, cheaper but still pricey

[3] https://www.wired.co.uk/article/d-wave-2000q-quantum-computer
[4] https://github.com/alex1770/QUBO-Chimera
[5] 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!

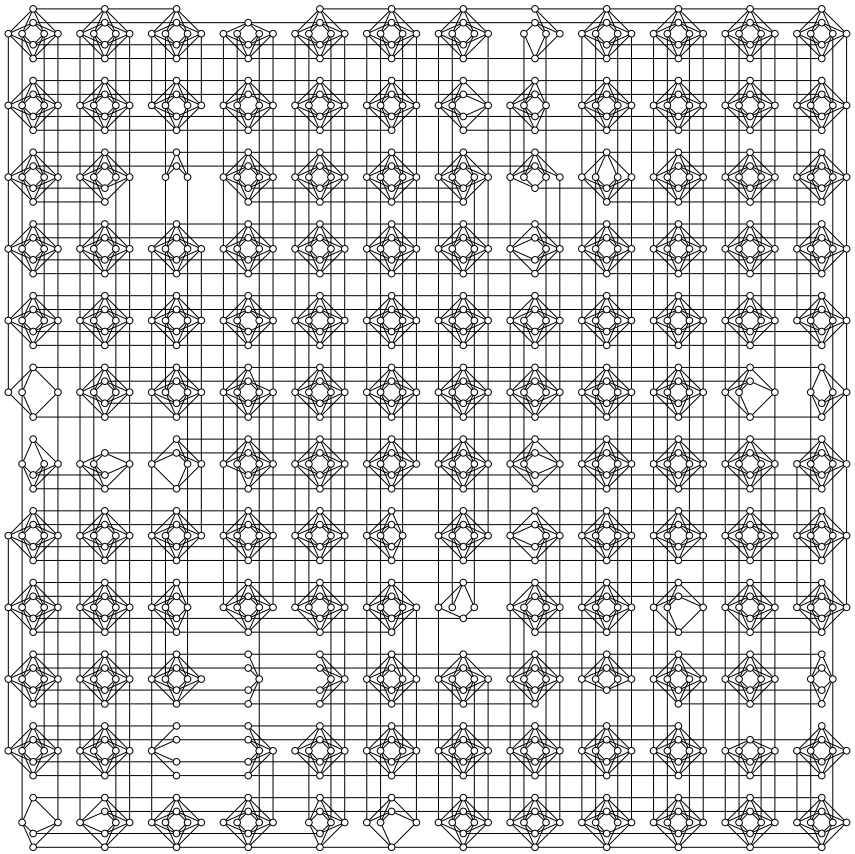
- Buy one yourself, for \$15 million[3]
- Rent time on one, cheaper but still pricey
- Use Selby's simulator, freely available on GitHub[4], demonstrated to run faster than earlier D-Wave machines and conjectured to be faster than the 2000Q[5]

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

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

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

Quantum interference on a D-Wave machine



6

[6] King et al., arXiv:1508.05087

Conclusion

World Aids Day Red Run

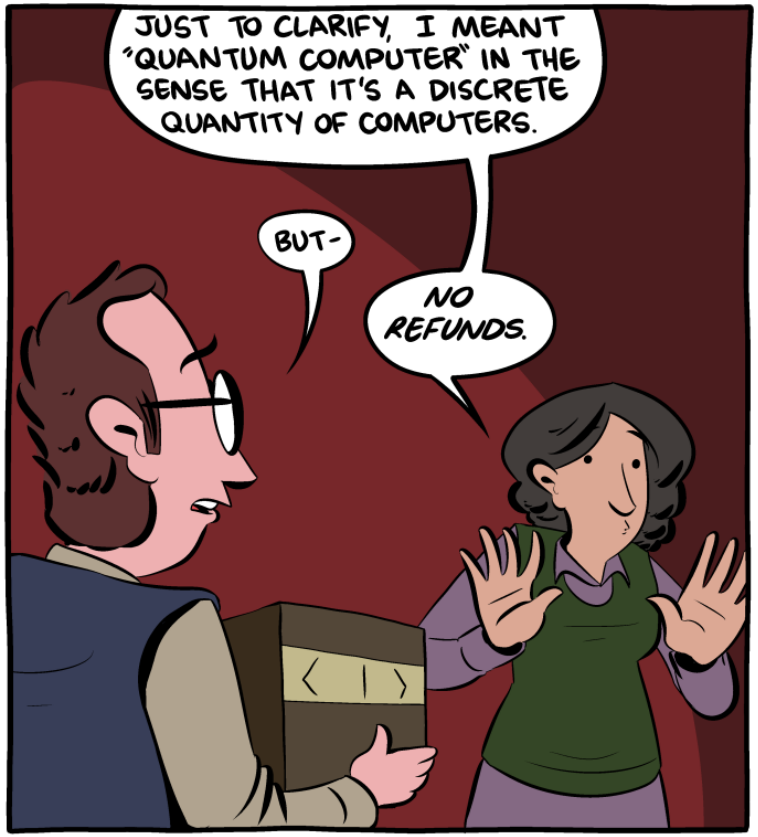
- I'm running ten kilometres
- Raising money for Brigstowe, `www.brigstowe.org`
- Please donate here `https://www.justgiving.com/fundraising/alex-moylett`
- Fancy dress suggestions appreciated!

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`

The end



It was surprisingly easy to get $100 million from NASA. [7]

Any questions?

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

Post-credits

This is the third time I've done one of these post-credit slides. A hat trick of useless slides!