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.

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`

Any questions?

Post-credits

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