The power of quantum computers

Andrew Childs
University of Maryland

JOINT CENTER FOR
QUANTUM INFORMATION
AND COMPUTER SCIENCE

What are quantum computers?

Store and process information according to the principles of quantum mechanics

Information is encoded in quantum bits (qubits), which store a superposition of classical data with positive and negative amplitudes

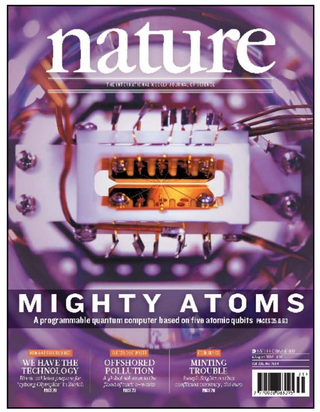
Such a device would let us solve certain problems much faster than is possible with ordinary, classical computers

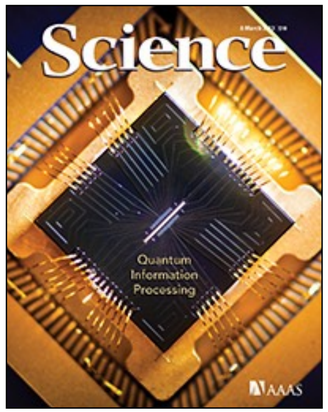
Sounds great! Can I have one?

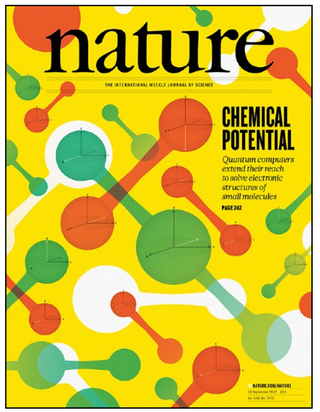
Building a quantum computer that can run interesting algorithms is really hard!

Need exquisite control + isolation from the environment

There is a massive effort underway to build and scale up quantum computers, and even evidence that they can outperform classical devices







But we are still far from running useful quantum algorithms

The origin of quantum speedup

Quantum computers allow for *interference between computational paths*

To perform a computation, we should arrange that

- paths to the solution interfere constructively
- paths to non-solutions interfere destructively

Quantum mechanics gives an *efficient representation of high-dimensional interference*

Quantum computing ≠ exponential parallelism

Can we just explore all potential solutions in parallel and pick out the correct one?

No! The linearity of quantum mechanics prohibits this.

To get significant speedup, quantum computers need to exploit structure

For exponential speedup, need to have a promise on the input, the problem cannot have too much symmetry, etc.

Key question: What kinds of problems have the right structure for quantum computers to exploit?

Quantum attacks on public-key cryptography

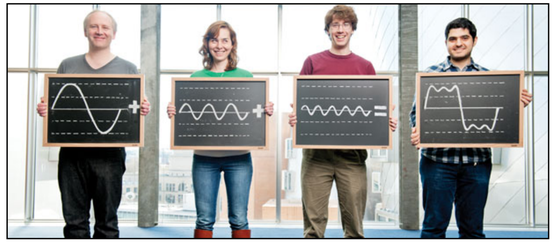
Basic problem: Write an integer as a product of prime factors

$$\begin{array}{c} 3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609 \end{array} = \begin{array}{c} 1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579 \end{array} \times \begin{array}{c} 1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571 \end{array}$$

This is widely believed to be hard for classical computers RSA

Shor 1994: Efficient quantum algorithm for factoring integers

Main idea: find period of $f(x) = a^x \bmod N$ for random a using the quantum Fourier transform, revealing factors of N



Related quantum attacks break Diffie-Helman, elliptic curve discrete log, Buchman-Williams, and other cryptosystems

Quantum-secure cryptography

Can we still keep secrets in a world with quantum computers?

Probably! There are many proposals for public-key cryptosystems based on problems we think are hard even for quantum computers:

- lattice problems/learning with errors
- decoding linear error-correcting codes
- solving multivariate polynomial equations
- supersingular elliptic curve isogenies

Quantum information also enables new kinds of crypto

NIST

Search NIST

Menu

NEWS

NIST's Post-Quantum Cryptography Program Enters 'Selection Round'

Chosen algorithms will become part of first standard devised to counter quantum decryption threat.

July 22, 2020

Credit: B. Hayes/NIST

A select few algorithms, some of which fall into one of three mathematical "families," are undergoing a final leg of review. Some will form the core of the first post-quantum cryptography standard.

The race to protect sensitive electronic information against the threat of quantum computers has entered the home stretch.

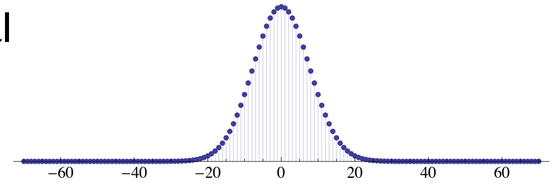
After spending more than three years examining new approaches to encryption and data protection that could defeat an assault from a quantum computer, the National Institute of Standards and Technology (NIST) has winnowed the 69 submissions it initially received down to a final group of 15. NIST has now begun the third round of public review. This "selection round" will help the agency decide on the small subset of these algorithms that will form the core of the first post-quantum cryptography standard.

Quantum search and quantum walk

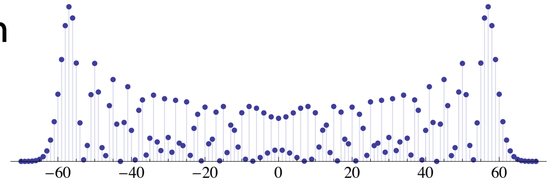
Grover 1996: Unstructured combinatorial search over N possibilities using $O(\sqrt{N})$ queries (optimal!)

More generally: Quantum analogs of random walks can explore graphs faster; quantum walk search can achieve polynomial speedup over classical computation

classical



quantum

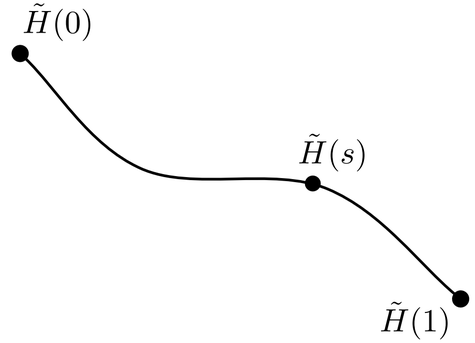


Many applications:

- polynomial speedup for brute-force search
- collision finding
- graph problems (connectivity, shortest paths, minimum spanning trees, bipartiteness, network flows, finding subgraphs, minor-closed properties, etc.)
- algebra (associativity, commutativity, etc.)
- cryptanalysis (decoding linear codes, shortest vector problem, subset sum, AES, bitcoin proof-of-work)
- pattern matching
- computational geometry

Optimization

Quantum adiabatic optimization/quantum annealing is a class of procedures for solving optimization problems by slowly changing a quantum system to remain in its ground state



Successes:

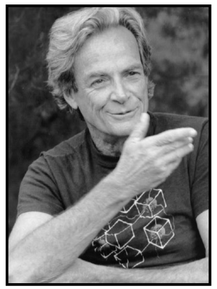
- Quadratic speedup for unstructured search (with careful schedule)
- Can efficiently minimize some simple cost functions
- By tunneling through energy barriers, can succeed in some cases where simulating annealing fails

However:

- Can fail to efficiently minimize some cost functions by getting trapped in local minima
- Can sometimes be simulated classically (e.g., by quantum Monte Carlo)
- No example with proven exponential speedup

Related approach: *quantum approximate optimization algorithm*. Discrete alternation between initial and final Hamiltonians can sometimes produce good approximate solutions quickly. May be promising, but the power of this approach is also unclear.

Quantum simulation



"... nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."

Richard Feynman
Simulating physics with computers (1981)

Quantum simulation problem: Given a description of a quantum system, an evolution time t, and an initial quantum state, produce the state after time t.

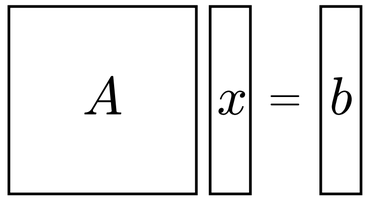
Can use this to study chemistry, materials, nuclear/particle physics…

We have very efficient quantum algorithms and good evidence that there are no efficient general-purpose classical algorithms.

In practice we need to compete with specialized classical heuristics that sometimes perform very well.

Quantum linear algebra

Basic computational problem: Solve for x in



Harrow, Hassidim, Lloyd 2009: Quantum algorithm running in time logarithmic in the size of A, provided

- A is sparse, row/column-computable, and well-conditioned
- b can be prepared as a quantum state
- it suffices to give the output x as a quantum state

Core of this algorithm: Quantum simulation

Applications to differential equations, convex optimization, machine learning (?), …

A zoo of quantum algorithms

We have discussed algorithms for cryptanalysis, simulating quantum mechanics, high-dimensional linear algebra, optimization, and search (leading to many other applications with polynomial speedup)

Other potential applications of quantum computers with exponential speedup: computing Gauss sums, approximating topological invariants/partition functions, counting points on algebraic curves, graph connectivity with cut queries, …

There are also many other problems with polynomial speedup: evaluating Boolean formulas, convex optimization, estimating volumes of convex bodies, multivariate polynomial interpolation, travelling salesman, …

For a more complete list, see quantumalgorithmzoo.org

Outlook

We have developed many quantum algorithms with potentially compelling applications…

… but we are far from a complete understanding of the power of quantum computers. What else can we do?

Building a scalable quantum computer could significantly impact the development of quantum algorithms.