Quantum algorithms and complexity

Andrew Childs
cs.umd.edu/~amchilds

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

UMIACS
University of Maryland
Institute for Advanced
Computer Studies

JOINT CENTER FOR
QUANTUM INFORMATION
AND COMPUTER SCIENCE

(Supervising students in CS, Physics, and Applied Math)

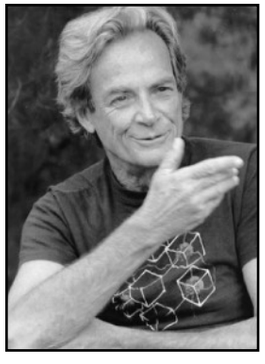
Research overview

My research studies the power of quantum systems to process information, especially through algorithms for quantum computers.

Major areas of interest include:

- Quantum simulation algorithms
- Quantum query complexity
- Quantum algorithms for optimization
- Quantum walks on graphs
- Quantum algorithms for algebraic problems/quantum cryptanalysis
- Theoretical techniques for implementing quantum algorithms on realistic hardware
- Interactive protocols for verifying quantum computation

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 (1981), *Simulating physics with computers*

Efficient algorithms for simulating the dynamics of quantum systems can be used to model physics (chemistry, materials, etc.) and as a tool for designing other quantum algorithms.

Past results:

- Quantum simulation algorithms with optimal performance (linear in evolution time, logarithmic in inverse error)
- Analysis of resource requirements for simulations on realistic devices
- Application to fast algorithms for linear algebra, differential equations

Recent and ongoing work:

- Improved algorithms for simulating systems with particular structure (geometric locality, time dependence, quantum chemistry, etc.)

Quantum query complexity

We can make precise comparisons between the power of classical and quantum computers using the model of *query complexity*, where the problem is encoded by a black box that must be queried to access parts of the input.

Recent results:

- Quantum query algorithms for polynomial interpolation
- Quantum query algorithms for convex optimization and estimating volumes of convex bodies
- Proof that graph properties cannot have exponential speedup in the adjacency matrix model, but can in the adjacency list model

Ongoing work:

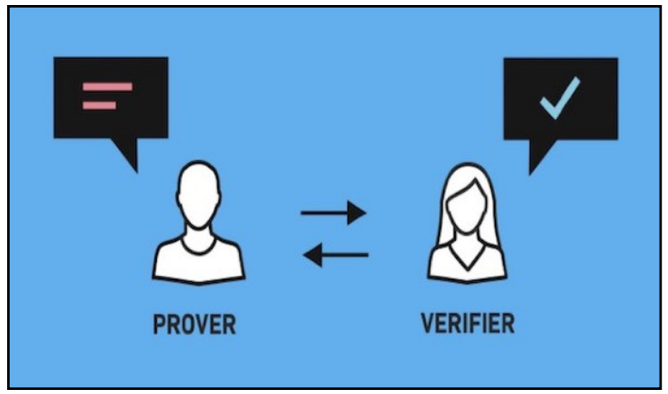
- Quantum query complexity of minimizing quadratic forms
- Possibility of speedup for graph property *testing* in the adjacency list model

Classical verification of quantum computation

How can we be sure that a quantum computation is done correctly?

Challenging because (probably) not all efficient quantum computations have efficiently checkable proofs.

But we can efficiently verify using interaction between a prover (quantum computer) and verifier (which can be a classical computer, using a recent breakthrough of Mahadev).

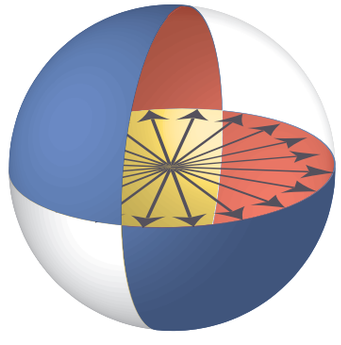


Recent results:

- Protocol for verification with minimal interaction: offline setup + one message from prover to verifier
- Non-interactive zero-knowledge argument systems

Ongoing work:

- Interactive protocols for sampling problems
- Protocols suitable for use on near-term devices



JOINT CENTER FOR
QUANTUM INFORMATION
AND COMPUTER SCIENCE

Large center for research on quantum information and computation, in collaboration between NIST (federal research lab) and UMD.

Synergistic with other quantum centers (JQI, QTC, CMTC, QMC)

More information at quics.umd.edu
Potential QuICS supervisors: quics.umd.edu/people/fellows

Quantum information courses:

- CMSC 657: **Introduction to quantum information processing**
  Offered every fall
- CMSC 858Q: **Quantum algorithms**
  Likely offered in spring 2021