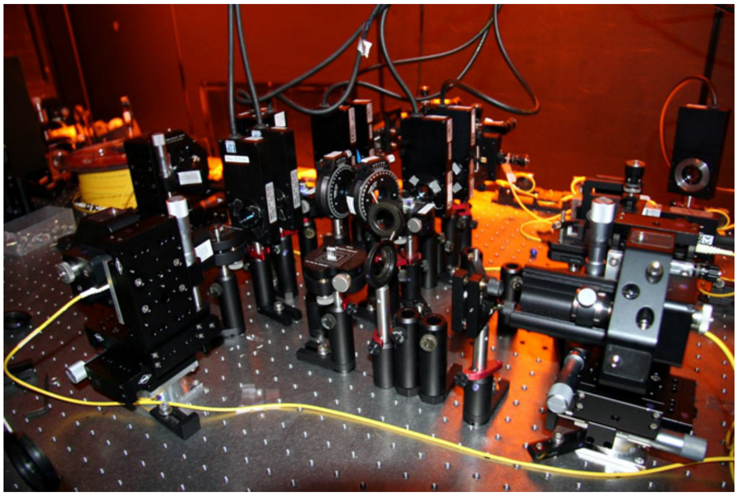
Introduction to Quantum Computing

Part I

Emma Strubell

http://cs.umaine.edu/~ema/quantum_tutorial.pdf

April 12, 2011



Overview

What is quantum computing?

- Background
- Caveats

Mathematical representation

- Fundamental differences
- Hilbert spaces and Dirac notation
- The qubit
- Quantum Registers
- Quantum logic gates
- Computational complexity

Origins of fame

- Quantum computer first proposed by Richard Feynman in 1981
  - Problem: efficiently simulating quantum systems inherently impossible on a classical computer
  - Solution: new machine "built of quantum mechanical elements which obey quantum mechanical laws"
- Daniel Simon demonstrates exponential speedup in 1994
  - nobody cares; algorithm too abstract
- Peter Shor demonstrates *exciting* exponential speedup in 1997
  - based on Simon's algorithm
  - efficiently factors integers into primes
  - this breaks RSA

© Copyright California Institute of Technology. All rights reserved. Commercial use or modification of this material is prohibited.

Unfortunately, scalable QCs still don't exist

- As of 2009, quantum computers able to factor 15 into 5 and 3
- The problem is *decoherence*
  - Man-made quantum system wants to interact with surrounding systems
  - Sources of interference include electric and magnetic fields required to power machine itself

Overview

What is quantum computing?

- Background
- Caveats

Mathematical representation

- Fundamental differences
- Hilbert spaces and Dirac notation
- The qubit
- Quantum Registers
- Quantum logic gates
- Computational complexity

Three main differences from classical computers

1. Superposition
   - quantum system exists in all possible states at all times
2. Probabilities
   - fortunately, a probability can be associated with each of those states
3. Entanglement
   - probabilities of different states can depend on each other
   - quantum teleportation uses this property for cryptographic purposes