Quantum Computing Seminar

Departments of Computer Science, Electrical Engineering,
Mathematics, and Physics

Agenda

- When will we meet?
- Schedule of Talks
- Brief Historical Overview

Reversible Computing

- Bennett (1973)
  (universal reversible Turing machines exist)

- Toffoli, Fredkin (1980-1982)
  (universal classical reversible gates exist)

Quantum Computing

- Feynman (1982)
  (Is it possible to simulate quantum physics on a classical computer in an efficient way?)
  Conjecture: The simulation of a general quantum system on a classical computer requires exponential time.

- Feynman (1985, 1986)
  (quantum circuit notation)

- Deutsch (1985)
  (universal quantum Turing machine)

Complexity Theory

- Bernstein, Vazirani (1993)
  (universal quantum Turing machine capable to simulate other quantum Turing machines with polynomial overhead)
  Beginning of quantum complexity theory

- Yao (1993)
  (Universal Turing machine model is equivalent to uniform families of quantum circuits)

Early Results in Complexity Theory

- Deutsch, Jozsa (1993)
  (There exist problems unknown to be in $\mathbf{P}$ that are in $\mathbf{QEP}$)
- Bertiaume, Brassard (1992-1994)
  (There exists an oracle A such that $\mathbf{QEP}^A \not\subseteq \mathbf{ZPP}^A$)
  There exists an oracle for which there are computational problems that can be solved on a QTM in polynomial time with certainty but each PTM needs exponential time to solve these problems with certainty.
- Simon (1994)
  There exists an oracle relative to which there is a problem solvable in polynomial time with bounded error probability on a QTM, but any PTM with bounded error probability solving this problem with bounded error probability (using the oracle) will require at least $2^{n/2}$ steps on infinitely many inputs of length n

The Breakthrough

- Shor (1994)
  - Factoring integers can be done in polynomial time on a QTM
  - Computing the discrete logarithm can be done in polynomial time on a QTM

Some Areas of Quantum Computing

- Quantum Complexity Theory
- Design of Quantum Algorithms
- Quantum Information Theory
- Quantum Cryptography
- Experimental Studies