Original AMS Short Course Announcement

Quantum Computation
A Grand Mathematical Challenge
for the
Twenty-First Century and the Millennium
AMS Short Course

Overview

The Nobel Laureate Richard Feynman was one of the first individuals to observe that there is an exponential slow down when computers based on classical physics, i.e., classical computers, are used to simulate quantum systems. Richard Feynman then went on to suggest that it would be far better to use computers based on quantum mechanical principles, i.e., quantum computers, to simulate quantum systems. Such quantum computers should be exponentially faster than their classical counterparts.

Interest in quantum computation suddenly exploded when Peter Shor devised an algorithm for quantum computers that could factor integers in polynomial time. The fastest known algorithm for classical computers factors much more slowly, i.e., in superpolynomial time. Shor's algorithm meant that, if quantum computers could be built, then cryptographic systems based on integer factorization, e.g., RSA, could easily be broken. These cryptographic systems are currently extensively used in banking and in many other areas. Lov Grover then went on to create a quantum algorithm that could search databases faster than any thing possible on a classical computer. These algorithms are based on physical principles not implementable on classical computers, quantum superposition and quantum entanglement.

As a result, the race to build a quantum computer is on. But the mathematical, physical, and engineering challenges to do so are formidable, and are a worthy challenge for the best scientific minds. One of the chief obstacles to creating a quantum computer is quantum decoherence. By this we mean that quantum systems want to wander from their computational paths and quantum entangle with the rest of the environment.

This short course focuses on the mathematical challenges involved in the development of quantum computers and quantum algorithms, challenges worthy of the best mathematical minds. It is hoped that, as a result of this course, many

©0000 (copyright holder)

mathematicians will be enticed into working on the grand challenge of quantum computation.

The Short Course will begin with an overview of quantum computation, given in an intuitive and conceptual style. No prior knowledge of quantum mechanics will be assumed.

In particular, the Short Course will begin with an introduction to the strange world of the quantum. Such concepts as quantum superposition, Heisenberg's uncertainty principle, the "collapse" of the wave function, and quantum entanglement (i.e., EPR pairs) will be introduced. This will also be interlaced with an introduction to Dirac notation, Hilbert spaces, unitary transformations, and quantum measurement.

Some of the topics covered in the course will be:

- Quantum teleportation
- Shor's quantum factoring algorithm
- Grover's algorithm for searching a database
- Quantum error-correcting codes
- Quantum cryptography
- Quantum information theory
- Quantum complexity theory, including the quantum Turing machine
- The problems of quantum entanglement and locality
- Implementation issues from a mathematical perspective

Each topic will be explained and illustrated with simple examples.