LABORATORY FOR COMPUTER SCIENCE

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

PHYSICS OF COMPUTATION THEORY OF COMPUTATION JOINT SEMINAR

Date: Tuesday, May 17, 1994
Time: Refreshments at 4:00pm
Talk at **4:15pm**
Place: 34-101

A Polynomial Time Algorithm for Factoring Integers on a Quantum Computer

Peter W. Shor
AT&T Bell Labs

A computer is generally considered to be a universal computational device, in other words, it is able to simulate any physical computational device with a cost of at most a polynomial factor in the computation time. It is not clear that this is still true if quantum mechanics is taken into account. Several researchers, starting with D. Deutsch, have developed mathematical models for quantum mechanical computers and investigated their computational properties. We show that these computers can factor integers and find discrete logarithms in polynomial time.

Hosts: Norm Margolus, Bonnie Berger

This talk is part of a seminar series on adapting computers and computations to the constraints of, and opportunities afforded by, microphysics; and on the development and application of the physical theory of computation and information. If you would like to receive electronic notice of these seminars, send email to "poc@im.lcs.mit.edu."