DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
ODENSE UNIVERSITY

COMPUTER SCIENCE COLLOQUIUM

An Introduction to Quantum Computation

Joan F. Boyar
Department of Mathematics and Computer Science
Odense University

Tuesday, April 4, 1995, at 2:15 PM
The Seminar Room

Abstract: The original idea of creating a computer based on the laws of quantum mechanics appears to be due to Feynman in 1982, and a formal model for such a computer was given by Deutsch in 1985. Since then, there has been more and more evidence that quantum computers are more powerful than classical probabilistic Turing machines, and thus, if they could be built, they have the potential of being significantly more powerful than any computer which exists today. The most exciting results so far are due to Shor (FOCS '94), and show that in the quantum model of computation there are polynomial time algorithms for both factoring and finding discrete logarithms. Both of these are generally assumed to be hard problems for classical computers, and much of modern cryptography is built on the assumption that one or both of these two problems is hard. Thus, if quantum computers could be built, not only would we be able to solve problems which we previously thought would never be solved, but, in addition, much of modern cryptography would become useless. Maybe quantum cryptography will take its place. Although there is much current research into the problems of actually building a quantum computer, it appears unlikely that we will see one on the market in the next few years. On the other hand, research on quantum cryptography is much further along; some experiments have actually been performed.

As the title says, this will only be an introduction to quantum computation. No previous knowledge is necessary, though some familiarity with Turing machines is probably essential. I will introduce the model of quantum computation which is used, mention some of the known results, and briefly introduce quantum cryptography. None of the work I will describe is my own.

Kim Skak Larsen