Seminar on Quantum Computation

André Berthiaume
CWI

Computer science has a classical soul; many definitions implicitly contain ideas from the time we believed the world evolved according to newtonian physics. Ideas such as: an object's state is well defined, instantaneous actions at a distance are impossible, etc. Modern physics and more specifically quantum physics tells us that Nature is not as straightforward as Newton originally believed. One can prepare systems such that the state is completely undefined in any classical sense. Instantaneous actions at a distance have been observed and sometimes having *less* alternatives to produce a given outcome may *improve* the probability of getting this outcome! What would happen computing models are allowed to operate within the rules of quantum physics? What are the advantages offered by a *quantum computer*?

In this mini-course, I will introduce the quantum computer and present some of the milestone results in quantum complexity theory leading up to Shor's famous polynomial time quantum factoring algorithm. Foreknowledge of quantum physics is useful but not necessary as the relevant notions will be introduced when needed. A fascinating aspect of quantum computation is the possibility of building such devices. I will briefly address some of the problems still to be overcome, but it is worth mentioning that some ongoing experiments have shown some very positive results. Quantum computers may well be available sooner than we think.

Session I: Introduction

We present the basic elements of quantum physics and introduce the qubit, the quantum gate, the quantum register, quantum gate arrays and observables.

Session II: Quantum Complexity, Part I

We define the Deutsch-Jozsa problem and show how a quantum gate array can solve it exponentially faster than a classical computer. Using this problem in a relativised setting, we extend the result to complexity classes.

Session III: Quantum Complexity, Part II

We show how Bernstein & Vazirani (1993) and Simon (1994) seperated (relative to oracles) the classe BPP from its quantum version, BQP.

Session IV: Factoring

We present Shor's factoring algorithm and review some issues concerning the construction of a quantum computer.