Simple Quantum Algorithms

Peter Høyer (hoyer@cpsc.ucalgary.ca)
University of Calgary
Department of Computer Science
Calgary, Alberta
T2N 1N4, Canada

Abstract.

What types of problems can we solve efficiently on a quantum computer? Why is it that factoring and finding discrete logarithms are simpler problems for a quantum computer than a traditional computer, but ordered searching and sorting are not? In this first and introductory talk on quantum algorithms, we take a set of simple problems and study how fast each of them can be solved on a quantum computer. The problems are simple toy versions of problems discussed in later talks by Harry Burhman, Alain Tapp, John Watrous, and the speaker.

We first define the most commonly used model for quantum computation, the so-called black box model. We then re-consider the algorithm Gilles Brassard just gave for Deutsch's problem, and eagerly move on to consider generalizations. For some natural generalizations, we can achieve fast quantum algorithms (such as constant versus balanced functions, unordered searching), for others, we cannot (such as parity, ordered searching, sorting). We finally introduce the so-called Simon's problem, ideas from which will be elaborated on by John Watrous on Wednesday.