Quantum Searching and Applications

Alain Tapp (tappa@iro.umontreal.ca)
Université de Montréal
Département d'informatique et de recherche opérationnelle
C.P. 6128, Succ. Centre-ville
Montréal, Québec
H3C 3J7, Canada

Abstract.

In 1996, Lov Grover gave the foundation of an exciting new algorithm for quantum computers. One of the most important classes of problems in computer science is the class **NP**. Roughly speaking, it addresses all the problems that can be stated as follows: we have a function $F : \{0,1\}^n \rightarrow \{0,1\}$ and an efficient classical algorithm that computes it. The problem is to find an x such that $F(x) = 1$, provided such an x exists. Sometimes, an efficient solution is known for this problem, but in general it seems to be very hard. There are literally hundreds of problems that can be put in this hard class, from areas including optimization, scheduling, cryptography, theorem proving, combinatorics, etc. The most efficient algorithms known in general that can solve these problems have a running time proportional to the number of possible inputs x. Grover sketched an algorithm that solves the general problem in a time proportional to the square root of that number, which is in $O(2^{n/2})$. In this talk, I will present Grover's original idea and then its analysis and generalization as discussed by Boyer, Brassard, Høyer and Tapp.