Quantum Lower Bounds (Polynomial Method)

Harry Buhrman (buhrman@cwi.nl)
CWI & University of Amsterdam
CWI INS 4 Kruislaan 413 1098 SJ
Amsterdam
The Netherlands

Abstract.

In this lecture, we will study the limitations of quantum computation. After the successful quantum algorithms culminating in the factoring algorithm of Shor, this lecture will discuss to what extent quantum computation is more powerful than classical computation. In particular, we will describe a general technique, called the polynomial method, that enables one to prove impossibility results even for quantum computers. In particular, we will show that certain functions cannot be computed faster on a quantum computer than on a classical computer. We will also show that a whole group of problems, the total Boolean functions, cannot be computed significantly faster on a quantum computer.