CORR 2000-44

Quantum Apmplitude Amplification and Estimation

Gilles Brassard*, Peter Høyer*, Michele Mosca, & Alain Tapp

Abstract Consider a Boolean function $\mathcal{X} : X \to \{0,1\}$ that partitions set X between its *good* and *bad* elements, where x is good if $\mathcal{X}(x) = 1$ and bad otherwise. Consider also a quantum algorithm $\mathcal{A}$ such that $\mathcal{A}|n0\rangle = \sum_{x \in X} \alpha_x |x\rangle$ is a quantum superposition of the elements of X, and let a denote the probability that a good element is produced if $\mathcal{A}|0\rangle$ is measured. If we repeat the process of running $\mathcal{A}$, measuring the output, and using $\mathcal{X}$ to check the validity of the result, we shall expect to repeat $1/a$ times on the average before a solution is found. *Amplitude amplification* is a process that allows to find a good x after an expected number of applications of $\mathcal{A}$ and its inverse which is proportional to $1/\sqrt{a}$, assuming algorithm $\mathcal{A}$ makes no measurements. This is a generalization of Grover's searching algorithm in which $\mathcal{A}$ was restricted to producing an equal superposition of all members of X and we had a promise that a single x existed such that $\mathcal{X}(x) = 1$. Our algorithm works whether or not the value of a is known ahead of time. In case the value of a is known, we can find a good x after a number of applications of $\mathcal{A}$ and its inverse which is proportional to $1/\sqrt{a}$ even in the worst case. We show that this quadratic speedup can also be obtained for a large family of search problems for which good classical heuristics exist. Finally, as our main result, we combine ideas from Grover's and Shor's quantum algorithms to perform *amplitude estimation*, a process that allows to estimate the value of a. We apply amplitude estimation to the problem of *approximate counting*, in which we wish to estimate the number of $x \in X$ such that $\mathcal{X}(x) = 1$. We obtain optimal quantum algorithms in a variety of settings.

Keywords Quantum computation. Searching. Counting. Lower bound.