Lehr- und Forschungsgebiet
Mathematische Grundlagen der Informatik
RWTH Aachen
Prof. Dr. E. Grädel, F. Abu-Zaid, S. Schalthöfer

SS 2015

Quantum Computing — Assignment 6

Due: Wednesday, 10.06., 14:15

Exercise 1 5 Points

Find a number $m < \frac{3}{4}2^n$ such that, for any function $f : \{0,1\}^n \to \{0,1\}$ with $|\{x \in \{0,1\}^n \mid f(x) = 1\}|$, a value y with $f(y) = 1$ can be found by a single application of the Grover operator with probability 1.

Exercise 2 10 Points

Let $\mathcal{F}$ be a family of functions $F : \{0,1\}^n \to \{0,1\}$. A *heuristic* is a function $G : \mathcal{F} \times R \to \{0,1\}^n$, for an appropriate finite set R.

For every function $F \in \mathcal{F}$, let $h_F = |\{r \in R \mid F(G(F,r)) = 1\}|$.

Let $F \in \mathcal{F}$ be a search problem chosen according to some probability distribution, and let G be a heuristic such that a value y with $F(y) = 1$ is found in expected time T when choosing $r \in R$ uniformly at random. Combine Grover's search algorithm with the heuristic to prove that there is a quantum algorithm that finds such a y in expected time $\mathcal{O}(\sqrt{T})$.

Exercise 3 10 Points

In this exercise, we develop a search algorithm for an unknown number of solutions.

In the following, let $f : \{0,1\}^n \to \{0,1\}$ with $m = |\{x \in \{0,1\}^n \mid f(x) = 1\}| \leq \frac{3}{4}2^n$, and choose ϑ_0 such that $\sin^2 \vartheta_0 = \frac{m}{2^n}$.

(a) Determine the probability of finding some y with $f(y) = 1$ with r applications of the Grover operator if $r \in [0, k-1]$ is chosen uniformly. You may use the fact that for any real α and any positive integer k,

$$\sum_{r=0}^{k-1} \cos((2r+1)\alpha) = \frac{\sin(2k\alpha)}{2\sin\alpha}.$$

(You may also prove that fact and get two extra points.)

(b) Show that if $k \geq \frac{1}{\sin(2\vartheta_0)}$, then $\frac{\sin(4k\vartheta_0)}{4k\sin(2\vartheta_0)} \leq \frac{1}{4}$, and conclude that in this case, a solution is found in r steps with probability $\geq \frac{1}{4}$.

(c) Describe an algorithm that, given a QGA U_f for a function f as defined above, determines a y with $f(y) = 1$ with probability $\geq \frac{1}{4}$ using U_f only $\mathcal{O}(\sqrt{2^n})$ times. In the analysis of your algorithm, consider the cases $m \leq \frac{3}{4}2^n$ and $m > \frac{3}{4}2^n$ separately.