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

SS 2015

Quantum Computing — Assignment 5

Due: Wednesday, 03.06., 14:15

Geben Sie bitte Namen, Matrikelnummer und die Übungsgruppe an.

Exercise 1 5 Points

Let $y \in \{0,1\}$ be an unknown bit and U_y the unitary operation $|\varphi\rangle \mapsto (-1)^y |\varphi\rangle$. Design a network consisting of one conditional U_y gate and two Hadamard gates which can be used to determine y.

Exercise 2 10 Points

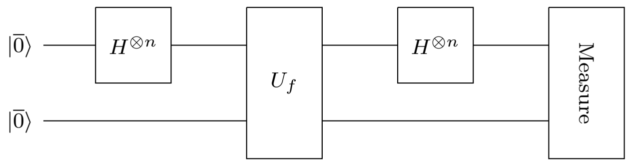
For $y \in \{0,1\}^n$ let the function $f_y : \{0,1\}^n \to \{0,1\}$ be defined by $f_y(x) = x \cdot y$. Show that there is a quantum algorithm that determines y by evaluating the function f only once.

Exercise 3 15 Points

Let U_f be a quantum gate that computes a function $f : \{0,1\}^n \to \{0,1\}^n$ (i.e. $U_f : H^{2^{2n}} \to H^{2^{2n}}$ computes the unique function which maps $|\overline{x}\rangle |\overline{y}\rangle$ to $|\overline{x}\rangle |\overline{y} \oplus f(\overline{x})\rangle$) with the promise that either f is one-to-one or there exists an $s \in \{0,1\}^n$ such that for all $x, x' \in \{0,1\}^n$ with $x \neq x'$

$$f(x) = f(x') \Leftrightarrow x = x' \oplus s.$$

The task is to determine which of the above conditions holds for f and, in the second case, also determine s. In this exercise we want to develop a solution for this problem. Consider the following circuit:



(a) show that right before measurement the registers are in the state

$$\frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle |f(x)\rangle .$$

(b) We apply the gate independently $(n-1)$ times and obtain, through the measurement, pairs $(y_1, f(x_1)), \ldots, (y_{n-1}, f(x_{n-1}))$.

  (i) Show that if f is one-to-one then the possible outcomes of the above measurements are distributed uniformly over all possible tuples.

  (ii) Show that in the other case the possible outcomes of the above measurements are distributed uniformly over all tuples with $y_i \cdot s \equiv 0 \mod 2$.

(c) Show that $y_1, \ldots, y_{n-1}$ (as vectors over $\mathbb{Z}_2$) are linearly independent with probability at least $\frac{1}{4}$.

(d) Under the assumption that the measurement yields linearly independent $y_1, \ldots, y_{n-1}$ develop an algorithm that solves the problem.

Hint: Compute $f(x)$ for the solutions x of a suitable system of linear equations.

(e) Combine the ideas of Items (a)-(d) to an algorithm that solves the problem with (expected) $\mathcal{O}(n)$ many applications of the depicted gate.