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

SS 2015

Quantum Computing — Assignment 2

Due: Wednesday, 29.04., 14:15

Geben Sie bitte Namen, Matrikelnummer und die Übungsgruppe an.

Exercise 1 10 Points

In this excercise we consider reversible gates for classical computations.

(a) Give a complete description of all functions $f : \{0,1\}^3 \to \{0,1\}$ such that the function $(x, y, z) \mapsto (x, y, f(x, y, z))$ is reversible.

(b) Construct a reversible version of a two-bit adder (i.e. $a(x, y) = (x \oplus y, xy)$) using controlled negation and Toffoli gates.

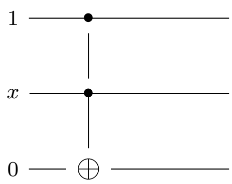
Hint: First find a suitable function $g(x, y)$ such that $a'(x, y) = (g(x, y), x \oplus y, xy)$ is injective. Then implement a' with the help of additional (constant) input bits.

(c) The gate $F : \{0,1\}^3 \to \{0,1\}^3$ is given by $(x, y, z) \mapsto \begin{cases} (x, y, z) & \text{, if } x = 1 \\ (x, z, y) & \text{, else} \end{cases}$

Show that $\{F\}$ is universal for reversible computation.

Exercise 2 10 Points

(a) Consider the branching gate B from the lecture.



We have seen that B can be used to copy classical bits. What is computed by B if the input x is an arbitrary qubit?

(b) The No-Cloning Theorem states that there is no unitary U such that, for *some fixed* $|\varphi\rangle \in H^2$ and *all* $|\psi\rangle \in H^2$

$$U |\psi\rangle |\varphi\rangle = |\psi\rangle |\psi\rangle .$$

Show that, in fact, for all U and $|\varphi\rangle$ the following is true: if for $|\psi\rangle \neq |\gamma\rangle$ with

$$U |\psi\rangle |\varphi\rangle = |\psi\rangle |\psi\rangle \text{ and}$$
$$U |\gamma\rangle |\varphi\rangle = |\gamma\rangle |\gamma\rangle$$

then $|\psi\rangle$ and $|\gamma\rangle$ must be orthogonal.

Hint: use that $\langle \vartheta \otimes \nu \mid \vartheta' \otimes \nu' \rangle = \langle \vartheta \mid \vartheta' \rangle \langle \nu \mid \nu' \rangle$.

Exercise 3 5 Points

Prove that any unitary matrix $U \in \mathbb{C}^{n \times n}$ has a square root, that means, there is a unitary matrix V such that $V \cdot V = U$.
Hint: Recall that by the spectral theorem from linear algebra U is diagonalizable via a basis-transformation to an orthonormal basis of $\mathbb{C}^n$, consisting of eigenvectors of U.