Quantum Cryptography (fall 2013) Prof. Dr. Dominique Unruh

Exercise Sheet 3

Out: September 24, 2013 Due: October 1, 2013

You will need 50% of all homeworks to qualify for the exam. (That is, if you get at least 50%, your final grade will be the exam grade. And if you do not get 50%, you do not pass the course.)

You may hand in your solutions in person or by email. If you submit by email, either scan a handwritten solution or typeset your solution readably. I do not consider ASCII formulas readable.

When submitting, indicate your name and your matriculation number. On your first submission, please also indicate a password, this password will be needed for accessing the solutions and your points online.

Problem 1: Deutsch-Jozsa Algorithm

Assume that $f : \{0,1\}^n \to \{0,1\}$ is a function that satisfies one of the following two properties:

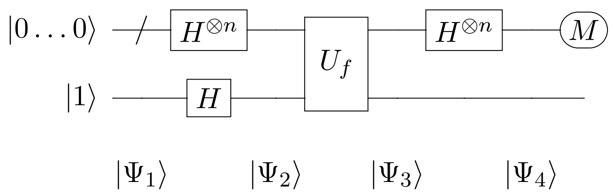
- f is constant (i.e., $f(x) = f(y)$ for all $x, y \in \{0,1\}^n$), or
- f is balanced (i.e., $|\{x : f(x) = 0\}| = |\{x : f(x) = 1\}| = 2^{n-1}$).

That is, we have the promise that f is constant or balanced, but we do not know which of the two holds.

Let U_f be the unitary transformation on $\mathbb{C}^{2^n}$ defined by

$$U_f|x, y\rangle = |x, y \oplus f(x)\rangle \qquad (x \in \{0,1\}^n, y \in \{0,1\}).$$

Consider the following circuit:



where M is a complete measurement in the computational basis.

The $|\Psi_i\rangle$ denote the intermediate states after the individual steps of the algorithm. E.g., $|\Psi_1\rangle = |0\dots01\rangle$.

(a) What is $|\Psi_2\rangle$?

(b) Show that

$$|\Psi_3\rangle = \sum_{x \in \{0,1\}^n} 2^{-n/2-1/2}|x, f(x)\rangle - 2^{-n/2-1/2}|x, \overline{f(x)}\rangle.$$

(Here $\overline{f(x)} := 1 - f(x)$.)

(c) Show that

$$|\Psi_3\rangle = \Big(2^{-n/2} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}|x\rangle\Big) \otimes |-\rangle$$

Here $|-\rangle$ is short for $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.

(d) Show that $H^{\otimes n}|x\rangle = 2^{-n/2}\sum_{z\in\{0,1\}^n}(-1)^{x\cdot z}|z\rangle$ where $x \cdot z := \sum_{i=1}^{n} x_i z_i$.

(e) What is $|\Psi_4\rangle$?

(f) Show that the probability P of measuring $0\dots0$ in the measurement is $\left(2^{-n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\right)^2$.

(g) Compute the probability P of measuring $0\dots0$ in the case that f is constant.

(h) Compute the probability P of measuring $0\dots0$ in the case that f is balanced.

Problem 2: Ensembles and Density Operators

(a) Consider the following quantum ensembles:

$$\begin{aligned} E_1 &= \{(|0\rangle, \tfrac{1}{2}), (|+\rangle, \tfrac{1}{2})\}, \\ E_2 &= \{(|0\rangle, \tfrac{1}{4}), (|1\rangle, \tfrac{3}{4})\}, \\ E_3 &= \{(|0\rangle, \tfrac{1}{4}), (|1\rangle, \tfrac{1}{4}), (|+\rangle, \tfrac{1}{4}), (|-\rangle, \tfrac{1}{4})\}. \end{aligned}$$

Compute the corresponding density operators ρ_1, ρ_2, ρ_3 as explicitly given matrices. (Note: $|+\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|-\rangle := \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.)

(b) Consider the following process: First, a random value $x \in \{0,1\}^n$ is chosen. Then an n-bit quantum register is prepared to have the value $|\Psi\rangle := |x\rangle$. Then a unitary transformation U is applied to Ψ. What is the density operator corresponding to the resulting ensemble?

Hint: As the first step, consider the case that U is the identity.

(c) Let a measurement M consisting of projectors $P_1, \dots, P_n$ be given. Let a quantum state $|\Psi\rangle$ be given. Assume that $|\Psi\rangle$ is measured using M but the measurement outcome is not recorded (i.e., it is forgotten, erased). What is the ensemble describing the state of the system after this experiment? What is the corresponding density operator?

(d) Assume a quantum system is in the state described by a density operator ρ. We apply a measurement M consisting of projectors $P_1, \dots, P_n$ to the system and forget the outcome. What is the density operator describing the resulting state of the system?

(e) In the lecture, we mentioned several times that a global phase, i.e., a factor $\varphi \in \mathbb{C}$ with $|\varphi| = 1$ in front of a quantum state, is physically irrelevant.

Demonstrate this by showing that the two states $|\Psi\rangle$ and $\varphi|\Psi\rangle$ are physically indistinguishable.[1]

[1] More precisely, the ensembles $\{(|\Psi\rangle, 1)\}$ and $\{(\varphi|\Psi\rangle, 1)\}$.