Quantum Information Theory

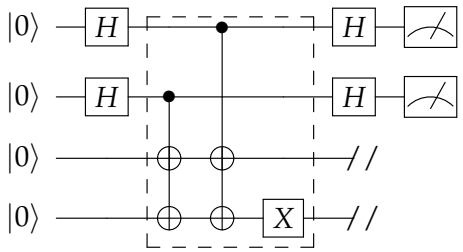
David Gross, Mateus Araújo

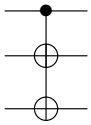
Exercise sheet 7

(there will be no exercise class, the purpose of this sheet is to help you prepare for the exam. I will correct any sheets sent to me via email.)

1 Simon's algorithm

The following circuit implements Simon's algorithm for $n = 2$ bits for a concrete implementation of the oracle, highlighted by the dashed box:



X is the NOT gate, H is the Hadamard gate, and the gate  applies X to the second and the third qubits if the state of the first qubit is $|1\rangle$.

a) The oracle in the dashed box implements the unitary transformation $U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, where $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ is a function such that $f(x) = f(x \oplus s)$ for all bitstrings x and some secret bitstring s. Compute the value of f for all possible inputs, and the secret s.

b) Compute the quantum state produced by this circuit just before the measurement, and which measurement outcomes can happen with which probabilities.

c) Compute the unique nonzero bitstring s such that $s \cdot y = 0$ for all outcomes y found in item **b)**, and check whether it matches with the answer from item **a)**.

Reminder: The dot product is modulo 2.

d) Let $g : \mathbb{Z}_2^{\times 3} \to \mathbb{Z}_2^{\times 3}$ be a function such that $g(x) = g(x \oplus 010)$ with values given by the table

x	$g(x)$
000	000
001	011
010	000
011	011
100	101
101	110
110	101
111	110

Write a quantum circuit that implements the unitary $V|x\rangle|y\rangle = |x\rangle|y \oplus g(x)\rangle$.

e) Suppose you ran Simon's algorithm for $n = 10$ bits, and got outcomes

y_1	1100000000
y_2	0010010000
y_3	1101100110
y_4	1001000000
y_5	0001000100
y_6	0001100000
y_7	0110000100
y_8	0101000000
y_9	0000100100
y_{10}	0000000101
y_{11}	1010000010
y_{12}	0011101101

What is the unique bitstring s such that $s \cdot y_i = 0$ for all i? This can be done by hand, but I recommend using a computer.