RUHR UNIVERSITÄT BOCHUM

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Elena Kirshanova

**Präsenzübungen zur Vorlesung**

# Quantenalgorithmen

**WS 2013/2014**

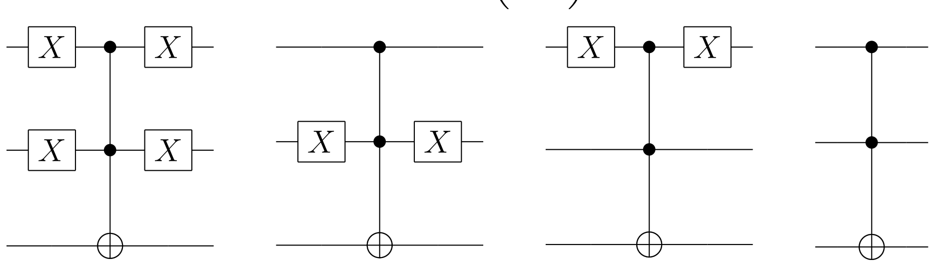
Blatt 7 / 5 February, 2014. 2 p.m.

**Exercise 1:**
The goal of this exercise is to construct the operator $\mathbf{W}$ – 'rotation about mean'. We denote $|\psi\rangle = H|0^n\rangle$ – the uniform superposition of all possible inputs.

1. Given an embedding $U_g$ for
$$g : \{0,1\}^n \to \{0,1\}$$
$$g(x) = \begin{cases} 0 & \text{if } x = 0^n \\ 1 & \text{if } x \neq 0^n. \end{cases}$$
construct a QC that
   - on input $|\psi\rangle$ outputs $|\psi\rangle$,
   - on input $H|x\rangle$ outputs $-H|x\rangle$ for $x \neq 0^n$.
2. Consider an arbitrary superposition $|\phi\rangle = \sum_x \alpha_x |x\rangle$ with $\mu = \frac{1}{N}\sum \alpha_x$ – the mean of the amplitudes. Using the QC constructed above show that it transforms
$$|\phi\rangle \to \sum (2\mu - \alpha_x)|x\rangle.$$
3. Finally, show that for an arbitrary $|\phi\rangle = \sum_x \alpha_x |x\rangle$
$$\mathbf{W} = (2|\psi\rangle\langle\psi|)(\sum_x \alpha_x |x\rangle) = \sum (2\mu - \alpha_x)|x\rangle.$$

**Exercise 2:**
**Searching for one item out of four**.
We consider a function $f : \{0,1\}^2 \to \{0,1\}$ such that $f(x) = 1$ if and only if $x = a$. We show that using Grover's algorithm we need only one query to determine $a$.

1. What is the mean number of queries of the classical oracle required to determine $a$?
2. We have only 4 possibilities for a quantum oracle $U_f$. Label which circuit below corresponds to which value of $a$ (recall that $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$).



3. Show that after applying a $U_f$ oracle the resulting states are orthonormal for different $a$.

4. Since the states are orthonormal, there should be a unitary transformation that distinguishes between the four cases. Find this transformation and construct a QC for such a distinguisher using Hadamard and CNOT.

**Exercise 3:**
**Collision finding**
You are given a two-to-one function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Classically you can find a collision (i.e. a pair $x, y$ s.t. $f(x) = f(y)$) in time $\mathcal{O}(2^{n/2})$ using birthday-paradox. Devise a quantum algorithm that finds a collision in time $\mathcal{O}(2^{n/3})$ with Grover's algorithm as black-box.

**Exercise 4:**
**Phase-error correcting code**. In order to being able to correct a phase-error (represented by the Pauli operator $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$) in addition to repeating the initial qubit we apply Hadamard transformation. That is, the phase error-correcting code is:

$$|0\rangle \to \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle),$$

$$|1\rangle \to \frac{1}{2}(|111\rangle + |001\rangle + |010\rangle + |100\rangle).$$

Give a QC that corrects a single phase-error in this code.