RUHR UNIVERSITÄT BOCHUM RUB

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

Präsenzübungen zur Vorlesung

Quantenalgorithmen

WS 2013/2014

Blatt 3 / 21 Novermber, 2013

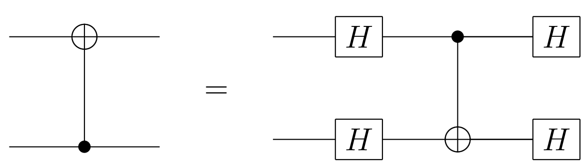
Exercise 1:
Show that the set NOR, COPY is a universal set. The truth table for NOR:

a	b	$\overline{a \vee b}$
0	0	1
0	1	0
1	0	0
1	1	0

Exercise 2:
Show that no set of two-bit gates is universal for classical reversible computation.
Conclusion: the smallest gate which is universal for reversible classical circuits requires three bits input and output. You will see two examples in the next homework.

Exercise 3:

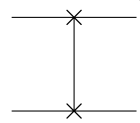
1. Show that control and target qubits of CNOT can be swapped by conjugating both qubits with the Hadamard transform:



Please turn over the page!

2. A SWAP gate interchanges two qubits $|a, b\rangle \mapsto |b, a\rangle$. Matrix and circuit representations for SWAP are:

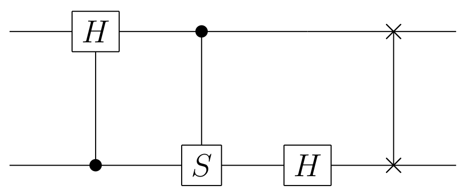
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$



Implement a SWAP gate using a few CNOTs.

Exercise 4:

1. Let $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. Give a 4×4 matrix that corresponds to the following quantum circuit:



2. Describe a two-qubit quantum circuit consisting of one CNOT gate and two Hadamard gates that implements the following unitary transformation:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Exercise 5:
Let

$$Z = \{|0\rangle, |1\rangle\}$$

be an orthonormal basis in $\mathbb{C}^2$ (this basis corresponds to horizontal and vertical polarization of a photon). The second orthonormal basis in $\mathbb{C}^2$ is

$$X = \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\},$$

which corresponds to the $45°$ and $-45°$ polarization. Alice, according to the BB84 protocol sends photons randomly prepared in one of the bases Z or X to Bob. Bob then randomly chooses a basis Z or X to measure the received photons. Alice and Bob interpret $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ as binary 0, $|1\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ as binary 1.

1. What is the probability that the binary interpretation is identical for Alice and Bob?

2. Assume that an eavesdropper Eve intercepts the photons send to Bob, measures the photon polarization in one of the bases Z or X, and then resends them to Bob. What is the probability that the binary interpretation is identical for Alice and Bob?