RUHR UNIVERSITÄT BOCHUM

RUB

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

Hausübungen zur Vorlesung

Quantenalgorithmen

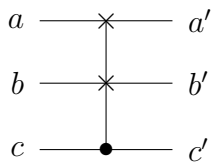
WS 2013/2014

Blatt 3 / 28 November, 2013. 2 p.m.

Exercise 1 (4 Punkte)**:**
The Fredkin gate is a 3-qubit gate that implements a controlled SWAP: if the third qubit is 1, the first and the second bit are swapped; if the third qubit is 0, all three bits are unchanged. The truth table is:

INPUT			OUTPUT		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	1	1

The quantum circuit is:



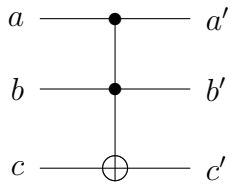
1. Find the matrix representation for the Fredkin gate;
2. Show that the Fredkin gate is self-inverse;
3. Show that the Fredkin gate is a universal set.

Please turn over the page!

Exercise 2 (4 Punkte)**:**
Another 3-bit gate is the Toffoli gate. It implements a controlled CNOT: the first two bits a, b are control bits, while c is the target bit. The truth table is:

INPUT			OUTPUT		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

The quantum circuit is:



1. Find the matrix representation;
2. Show how to build the following gates from the Toffoli gate: CNOT, NAND, NOT, AND, OR.

Exercise 3 (5 Punkte)**:**

1. Construct a binary half-adder using Toffoli gate. This adder accepts two bits a and b, outputs also two bits: a carry bit and $a + b \mod 2$.
2. Construct a full-adder which also accepts a carry bit c as the input. Such an adder output $a + b + c$ and a new carry bit.

Exercise 4 (4 Punkte)**:**
What is the smallest number of Fredkin gates needed to simulate a Toffoli gate? What is the samllest number of Toffoli gates needed to simulate a Fredkin gate?