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

Hausübungen zur Vorlesung

Quantenalgorithmen

WS 2013/2014

Blatt 4 / 12 December, 2013. 2 p.m.

Exercise 1 (3 Punkte)**:**
You are given an oracle that simulates a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. For every image $f(x) = f_1(x) \dots f_m(x) \in F_2^m$ we define the *parity* of x as the function $p(x) = f_1(x) + \dots f_m(x) \mod 2$. Construct a QC such that on the input $|0^n 1^m\rangle$ it outputs the superposition

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

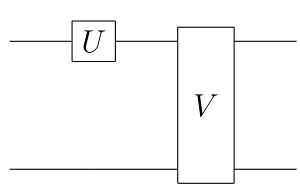
Exercise 2 (4 Punkte)**:**
The 1-qubit Pauli Operators are give by

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & -0 \\ 0 & -1 \end{bmatrix}.$$

You are given an access to a black box U which implements one of the four Pauli operators, but you are allowed to use U only once. The goal of the exercise is to construct a QC that distinguishes which one of the four unitary gates is implemented in the black box.

1. Show that $(P \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where $P \in \{I, X; Y, Z\}$, are orthogonal for all possible P's. This proves that the set $\{(P \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\}$ forms a basis in $\mathbb{C}^4$.

2. Show that the QC below, where V is an arbitrary two-qubit unitary, distinguishes all four 1-qubit Paulis from each other by choosing the appropriate two-qubit state as input and two-qubit unitary V:



Exercise 3 (4 Punkte)**:**
Suppose our function $f : \{0,1\}^n \to \{0,1\}$ satisfies the following promise: either

1. f evaluates to 0 on the first 2^{n-1} inputs and to 1 on the second 2^{n-1} inputs (inputs are in lexicographical order), or

2. the number of evaluations to 0 in the first 2^{n-1} inputs equals 2^{n-2} and the number of evaluations to 1 on the second 2^{n-1} input bits equals to 2^{n-2}.

Modify the Deutsch-Jozsa algorithm to efficiently distinguish between the two cases.