RUHR UNIVERSITÄT BOCHUM RUB

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

Präsenzübungen zur Vorlesung

Quantenalgorithmen

WS 2013/2014

Blatt 5 / 19 December, 2013. 2 p.m.

Exercise 1:
Let

$$f : \mathbb{F}_2^2 \to \mathbb{F}_2$$
$$(x_1, x_2) \mapsto x_1 \oplus x_2.$$

Run Simon's algorithm to find $s_1, s_2 \neq 0$, such that $f(x_1 + s_1, x_2 + s_2) = f(x_1, x_2)$.

Exercise 2:
We denote $2^n = N$. Show the *shift property* of QFT: for $|z\rangle = \sum_{x \in \{0,1\}^n} \alpha_i |x\rangle$ it holds that

$$\text{if } \mathrm{QFT}_N \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1}, \end{pmatrix} \quad \text{then } \mathrm{QFT}_N \begin{pmatrix} \alpha_{N-1} \\ \alpha_0 \\ \vdots \\ \alpha_{N-2} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ w\beta_1 \\ \vdots \\ w^{N-1}\beta_{N-1}, \end{pmatrix}$$

where $w^N = 1$.

Exercise 3:
Suppose you have a quantum phase oracle $|x\rangle \mapsto (-1)^{f(x)}|x\rangle$, where $f : \{0,1\}^n \to \{0,1\}$, such that $\exists s \in \mathbb{F}_2^n : \ f(x) = f(x+s)$. Show how to find a vector $y \in \mathbb{F}_2^n$, such that $ys = 0 \mod 2$ using only n qubits.

Exercise 4:
Calculate $\mathrm{QFT}_2\Big(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\Big)$ and $\mathrm{QFT}_2\Big(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\Big)$.