RUHR UNIVERSITÄT BOCHUM RUB

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

Hausübungen zur Vorlesung

Quantenalgorithmen

WS 2013/2014

Blatt 5 / 9 January, 2014. 2 p.m.

Exercise 1 (4 Punkte)**:**
Let $f(x_1, x_2, x_3, x_4) = (x_1 + x_2, x_2 + x_3, x_3 + x_4, x_4 + x_1)$ be a $2:1$ mapping.

1. Run Simon's algorithm on f.
2. Assume that after the measurement you obtain $y_1 = (1, 1, 0, 0), y_2 = (1, 0, 1, 0), y_3 = (1, 0, 0, 1)$. Find the period s of f.
3. Show that $n - 1$ vectors from $\mathbb{F}_2^n$ are linearly independent over $\mathbb{F}_2$ with probability

$$\prod_{i=0}^{n-2} (1 - 2^{i-n}).$$

Exercise 2 (4 Punkte)**:**

1. Construct a matrix representation for QFT_{2^3}.
2. Calculate $\mathrm{QFT}_{2^3}\left(\frac{1}{\sqrt{2}}(|0\rangle + |4\rangle)\right)$.

Exercise 3 (4 Punkte)**:**

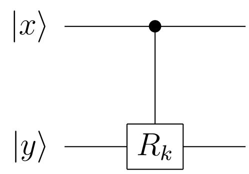
1. Show that QFT_{2^n} is unitary. *Hint: You might want to use the results from HW1.*
2. What is $(\mathrm{QFT}_{2^n})^2$?

Please turn over the page!

Exercise 4 (4 Punkte)**:**
Recall that the 1-qubit rotation is represented by a unitary matrix

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp(2\pi i/2^k) \end{bmatrix}.$$

During the phase estimation algorithms we use the use the controlled-R_k gate:



Show that the controlled-R_k circuit is equivalent to