Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Hausübungen zur Vorlesung

Quantenalgorithmen

SS 2016

Blatt 5 / 16. Juni 2016

Abgabe: 27. Juni 2016, 10.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (4 Punkte)**:**

Führen Sie die QFT auf folgendem Zustand aus.

$$|z\rangle = \frac{1}{2}\sum_{j=0}^{7} \cos\left(\frac{2\pi j}{8}\right)|j\rangle$$

AUFGABE 2 (5 Punkte)**:**

Wir betachten QFT_8^{-1} auf 3 Qubits.

(a) Geben Sie die Matrizen R_k für die Rotationen, die der Schaltkreis benötigt, explizit an.

(b) Schreiben Sie den Quantenschaltkreis explizit auf.

(c) Geben Sie die unitäre 8×8 Matrix, die QFT_8^{-1} beschreibt, explizit an.

Bemerkung: Die in den Matrizen vorkommenenden komplexen Zahlen sollen dabei in der Form $a + bi$ geschrieben werden (und nicht als $e^{2\pi i\alpha}$). Für (a), (b) is jeweil keine Begründung erforderlich. Für (c) soll nachvollziehbar sein, wie Sie Ihr Ergebnis erhalten haben (Referenz oder Rechnung).

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Geben Sie den Quantenschaltkreis für QFT_4^{-1} explizit an.

Gegeben sei nun der Zustand

$$|z\rangle = \frac{1}{2}\sum_{y=0}^{2^2-1}(-1)^{xy}|y\rangle = \frac{1}{2}(|0\rangle + |1\rangle - |2\rangle - |3\rangle).$$

Wenden Sie Ihren Schaltkreis für QFT_4^{-1} auf diesen Zustand an. Geben Sie die Zwischenzustände nach jedem Gate an sowie das Ergebnis.

AUFGABE 4 (6 Punkte)**:**

Sei $|z\rangle = \sum_{i=0}^{2^n-1} z_i|i\rangle$ ein beliebiger Zustand mit Amplituden $z_i \in \mathbb{C}$. Betrachte die QFT $|x\rangle = \mathrm{QFT}|z\rangle$ und schreibe diese als $\sum_{i=0}^{2^n-1} x_i|i\rangle$ für $x_i \in \mathbb{C}$.

Für beliebigen Shift $b \in \mathbb{Z}$ betrachte $|z'\rangle := \sum_{i=0}^{2^n-1} z_{i+b \bmod 2^n}|i\rangle$. Die dazuzugehörige QFT sei $|x'\rangle = \mathrm{QFT}|z'\rangle$. Schreibe $|x'\rangle$ als $\sum_{i=0}^{2^n-1} x'_i|i\rangle$.

(a) Zeigen Sie: Es gilt $|x_i| = |x'_i|$ für alle i. Insbesondere haben Messungen an $|x'\rangle$ und $|x\rangle$ in der Standardbasis dieselbe Wahrscheinlichkeitsverteilung.

(b) Betrachten Sie nun konkret $n = 4$ und den periodischen Zustand $|z\rangle = \frac{1}{\sqrt{3}}\big(|2\rangle + |7\rangle + |12\rangle\big)$ mit zugehöriger QFT $|x\rangle = \mathrm{QFT}|z\rangle$.
Was sind die beiden wahrscheinlichsten Messergebnisse bei Messung von $|x\rangle$ in der Standardbasis und mit welchen Wahrscheinlichkeit treten diese jeweils auf?

Hinweis: Die Rechnung in (b) wird etwas einfacher, wenn Sie (a) verwenden: Sie können an Stelle von $|z\rangle$ die QFT von $|z'\rangle = \frac{1}{\sqrt{3}}\big(|11\rangle + |0\rangle + |5\rangle\big)$ bestimmen. ($|11\rangle$ entspricht $|-5\rangle$; die Symmetrie um 0 vereinfacht die Rechnung, insbesondere hat $|x'\rangle$ relle Koeffizienten.)

Die Ergebnisse in (b) sollen numerisch ermittelt werden, nicht exakt. Sie benötigen also einen Taschenrechner/Computer o.ä. Wegen $\sum_i |x'_i|^2 = 1$ kann man $|x'_i|^2 \leq 1 - |x_{i_1}|^2 - \ldots |x_{i_k}|^2$ abschätzen, wenn man $x_{i_1}, \ldots, x_{i_k}$ bereits berechnet hat. Wer also die größten $|x'_i|^2$ zuerst berechnet muss nicht unbedingt alle x'_i berechnen.