Technische Universität Darmstadt
Fachgebiet Kryptographische Protokolle
Alexander May, Ulrich Vollmer
Maike Ritzenhofen

Hausübungen zur Vorlesung

Quantenalgorithmen

WS 2006/07

Blatt 6 / 18. Januar 2007 / Abgabe 07. Februar 2007

AUFGABE 1 (5 Punkte)**:**
Berechnen Sie die diskrete Fourier-Transformation auf $\mathbb{C}^M$ der folgenden Funktionen.

(a) v mit $v_n = a^n$ für ein festes $a \in \mathbb{C}$ mit $a \neq 1$, spezialisieren Sie die erhaltene Formel für $\hat{v}$ auf den Fall $a = q^j$ für $j \in \mathbb{Z}$. Dabei ist $q = e^{\frac{2\pi i}{M}}$.

(b) w mit

$$w_n = \begin{cases} 1 & \text{falls } (M/2) \mid n \\ 0 & \text{sonst} \end{cases}$$

unter der Annahme, daß $2 \mid M$.

(c) Sei $S[x,r] = \{\, y \mid 0 \leq y < M, r \mid (y-x) \,\}$ und $\delta[x,r]$ die charakteristische Funktion von $S[x,r]$, also

$$\delta[x,r](y) = \begin{cases} 1 & \text{falls } r \mid (y-x) \\ 0 & \text{sonst.} \end{cases}$$

unter der Annahme, daß $r \mid M$. Finden Sie den fehlenden Exponenten "?" in der Beziehung $\widehat{\delta[x,r]}_k = e^{?}\ \widehat{\delta[0,r]}_k$ zwischen den Fourier-Transformierten von $\delta[x,r]$ und $\delta[0,r]$ und beweisen sie dieses.

AUFGABE 2 (5 Punkte)**:**
Berechnen Sie die Periode von $f(a) = 7^a \bmod 10$ mit Hilfe des in der Vorlesung angegebenen Quanten-Algorithmus. Wählen Sie dabei $M = 2^7$ und nehmen Sie an, daß Sie in der ersten Messung den Wert 7 erhalten haben.
Geben Sie die im Zuge des Algorithmus auftretenden Zwischenzustände an und berechnen Sie die Wahrscheinlichkeit, in der zweiten Messung einen der Werte $y = 32i$, $i = 0, \ldots, 3$ zu erhalten.
Wie groß ist die Wahrscheinlichkeit, daß für die aus zwei Durchläufen des Algorithmus erhaltenen Werte y_1 und y_2 gilt, daß

1. $y_1 y_2 \neq 0$, und
2. das kleinste gemeinsame Vielfache von M/y_1 und M/y_2 ist die Periode von f?

AUFGABE 3 (5 Punkte)**:**
Verifizieren Sie, daß die Quanten-Fourier-Transformation auf m Qubits (also auf $\mathbb{C}^M$ mit $M = 2^m$) einen Basiszustand $|x\rangle$ auf folgenden unverschränkten Zustand abbildet:

$$\frac{1}{\sqrt{M}}\big(|0\rangle + e^{2\pi i(2^{-m}x)}|1\rangle\big) \otimes \big(|0\rangle + e^{2\pi i(2^{1-m}x)}|1\rangle\big) \otimes \cdots \otimes \big(|0\rangle + e^{2\pi i(2^{-1}x)}|1\rangle\big)\ .$$

AUFGABE 4 (5 Punkte)**:**
Sei R_k das 1-Qubit-Gatter, welches $|0\rangle$ auf $|0\rangle$ abbildet und $|1\rangle$ auf

$$e^{2^{-k}\pi i}|1\rangle\ .$$

Beweisen Sie für $k \geq 0$, daß die Operator-Norm von $R_k - I$ kleiner ist als $2^{1-k}\pi$. Zur Erinnerung: Die Norm eines linearen Operators V ist definiert als

$$\|V\| = \max(\,|Vv| \mid |v| = 1\,)\ .$$