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

Präsenzübungen zur Vorlesung

Quantenalgorithmen

SS 2016

Blatt 5 / 20. Juni 2016

AUFGABE 1:

In dieser Aufgabe wollen wir die Periode von $f(x) = 3^x \bmod 10$ mit Hilfe des in der Vorlesung angegebenen Quanten-Algorithmus bestimmen und gehen dazu die einzelnen Schritte des Algorithmus genau durch. Wir wählen als Definitionsbereich für f die Menge $\{0, \ldots, 2^7 - 1\}$.

Wir nehmen an, dass wir zunächst eine Messung an den $f(x)$ entsprechenden Bits vornehmen und diese $|3\rangle$ liefern.

Geben Sie den (periodischen) Zustand des Systems nach dieser Messung an. Was ist der Zustand nach QFT? Was ist die Wahrscheinlichkeit, in der dann folgenden Messung einen der Werte $y = 32i$, $i = 0, \ldots, 3$ zu erhalten? Wie gross ist die Wahrscheinlichkeit, dass sich aus zwei durch unabhänge Durchläufe des Algorithmus erhaltenen Werte y_1 und y_2 die Periode von f ermitteln lässt?

AUFGABE 2:

Zeigen Sie, dass für $m \nmid y$ gilt

$$\sum_{k=0}^{m-1} (\zeta_m^y)^k = 0,$$

wobei $\zeta_m := e^{\frac{2\pi i}{m}}$

Hinweis: Betrachten Sie $f(x) = X^m - 1$. Was sind die Nullstellen von f?
Können Sie f faktorisieren?

Bitte wenden!

AUFGABE 3:

Sei $M \in \mathbb{Z}$ mit $M > 1$ und $\zeta_M = e^{2\pi i/M}$. Zeigen Sie, dass die Vektoren

$$\vec{v}_n = \frac{1}{\sqrt{M}}(\zeta_M^{nk})_{k=0,\ldots,M-1}$$

eine Orthonormalbasis des $\mathbb{C}^M$ bilden (mit dem üblichen Skalaprodukt $\langle x, y\rangle = \sum_i x_i^* y_i$). Folgern Sie daraus, dass die Matrix

$$U = \frac{1}{\sqrt{M}}(q^{nk})_{n,k=0,\ldots,M-1}$$

unitär ist. Was für eine Rolle spielt U für die QFT bzw. DFT?

Zeigen Sie weiterhin, dass

$$Uv = U^*\rho(v),$$

wobei der Reversionsoperator $\rho(v)$ wie folgt definiert ist:

$$\rho\colon \mathbb{C}^M \to \mathbb{C}^M, (v_0, v_1, \ldots, v_{M-1}) \mapsto (v_0, v_{M-1}, v_{M-2}, \ldots, v_1).$$

Folgern sie, dass $U^4 = \mathrm{id}$ gilt.