Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Enrico Thomae

Hausübungen zur Vorlesung

Quantenalgorithmen

WS 2011/2012

Blatt 4 / 28 November 2011

Abgabe bis 12. Dezember 2011, 14 Uhr (vor der Übung)

AUFGABE 1 (6 Punkte)**:**
Wir definieren die Pauli-Gatter

$$\mathrm{Y} := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ und } \mathrm{Z} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

sowie die Rotationsgatter

$$\begin{aligned} R_y(\theta) &= \cos(\theta/2)I - i\sin(\theta/2)Y, \\ R_z(\theta) &= \cos(\theta/2)I - i\sin(\theta/2)Z. \end{aligned}$$

(a) Zeigen Sie, dass sich jede Matrix mit Spalten und Zeilen der Länge 1 in der Form

$$\mathrm{Y} := \begin{pmatrix} e^{i\alpha_{11}}\cos(\gamma/2) & -e^{i\alpha_{12}}\sin(\gamma/2) \\ e^{i\alpha_{21}}\sin(\gamma/2) & e^{i\alpha_{22}}\cos(\gamma/2) \end{pmatrix}$$

schreiben lässt. Hierfür nutzen Sie Ihr Wissen, dass eine Matrix genau dann unitär ist, wenn sowohl ihre Zeilen als auch ihre Spalten eine Orthonormalbasis von $H_2 = \mathbb{C}^2$ bilden.

(b) Zeigen Sie, dass für unitäre Matrizen der Darstellung in (a) mit $\gamma \neq k\pi, k \in \mathbb{Z}$ gilt

$$\begin{aligned} \alpha_{11} - \alpha_{12} &= \alpha_{21} - \alpha_{22} \pmod{2\pi}, \\ \alpha_{11} - \alpha_{21} &= \alpha_{12} - \alpha_{22} \pmod{2\pi}. \end{aligned}$$

(c) Schließen Sie aus der gefundenen Darstellung, dass sich jede unitäre Matrix, für die in obiger Darstellung $\gamma \neq k\pi, k \in \mathbb{Z}$ gilt, in folgender Form darstellen lässt.

$$e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$$

AUFGABE 2 (6 Punkte)**:**
Gegeben ist eine Funktion $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ im Orakel-Modell. Wir nennen für jeden Funktionswert $f(x) = f_1(x)\ldots f_m(x) \in \mathbb{F}_2^m$ die Summe $p(x) = f_1(x) + \ldots f_m(x) \bmod 2$ die *Parität* von x. Geben Sie einen QC an, der bei Eingabe $|0^n1^m\rangle$ die folgende Superposition berechnet

$$\frac{1}{2^{\frac{n}{2}}} \sum_{x\in\{0,1\}^n} (-1)^{p(x)}|x1^m\rangle.$$

AUFGABE 3 (7 Punkte)**:**
Ein n Qubit Toffoli-Gatter sei definiert durch die folgende Abbildung:

$$(x_1, \ldots, x_{n-1}, y) \mapsto (x_1, \ldots, x_{n-1}, y \oplus x_1 x_2 \ldots x_{n-1}).$$

(a) Zeigen Sie, dass ein n Qubit Toffoli-Gatter mittels 3 Qubit Toffoli-Gattern unter Benutzung von insgesamt $n+1$ Qubits simuliert werden kann. Wieviele 3 Qubit Toffoli-Gatter benötigen Sie?

(b) Wieviele 3 Qubit Toffoli-Gatter benötigen Sie in (a), falls Sie beliebig viele Hilfsqubits benutzen dürfen?