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

Hausübungen zur Vorlesung

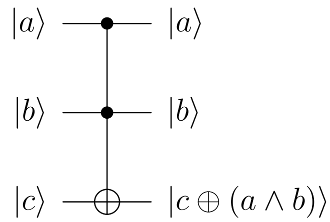
Quantenalgorithmen

WS 2011/2012

Blatt 3 / 14 November 2011

Abgabe bis 28. November 2011, 14 Uhr (vor der Übung)

AUFGABE 1 (13 Punkte)**:**
Das Toffoli-Gatter als Abbildung von $\mathbb{C}^8$ nach $\mathbb{C}^8$ sei durch folgenden Schaltkreis gegeben.



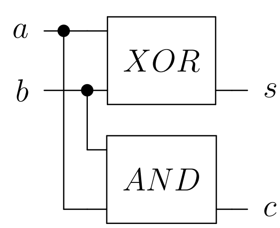
Beachten Sie, dass $c \oplus (a \wedge b)$ jeweils auf alle Basiszustände anzuwenden ist.

(a) Geben Sie die Abbildungsmatrix zum Toffoli-Gatter an.

(b) Zeigen Sie, dass die Abbildung unitär und reversibel ist.

(c) Beweisen Sie, dass das Toffoli-Gatter universell ist. Stellen Sie dazu die klassischen Operationen $\wedge, \vee$ und $\neg$ mit Hilfe des Toffoli-Gatters dar.

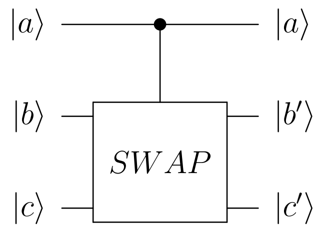
(d) Stellen Sie folgenden Halbaddierer mit Hilfe des Toffoli-Gatters dar.



(e) Wir belegen die Eingabebits des Toffoli-Halbaddierers in (d) mit den Werten $|a\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ und $|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Welches Ergebnis liefert die Berechnung?

(f) Geben Sie einen Toffoli-Volladdierer an, d.h. einen Schaltkreis bestehend aus Toffoli-Gattern, der $a + b + c$ berechnet.

AUFGABE 2 (8 Punkte)**:**
Das Fredkin-Gatter ist gegeben durch folgenden Schaltkreis.



Hierbei ist SWAP durch folgende unitäre Abbildung definiert.

$$\text{SWAP} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(a) Geben Sie die unitäre Matrix an, die das Fredkin-Gatter beschreibt.

(b) Beschreiben Sie mittels boolescher Formeln, wie sich die Basiszustände von $|b'\rangle$ und $|c'\rangle$ berechnen.

(c) Was ist die kleinste Anzahl an Fredkin-Gattern, die man benötigt um ein Toffoli-Gatter zu simulieren? Geben Sie dieses Gatter an.

(d) Was ist die kleinste Anzahl an Toffoli-Gattern, die man benötigt um ein Fredkin-Gatter zu simulieren? Geben Sie dieses Gatter an.