RUHR UNIVERSITÄT BOCHUM

RUB

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

Lösungsblatt zur Vorlesung

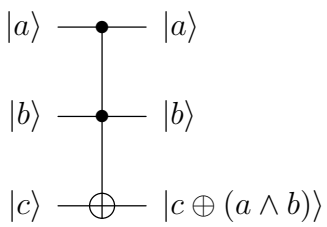
Quantenalgorithmen

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.



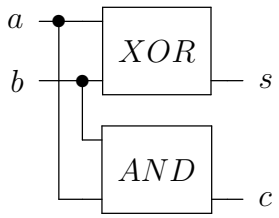
Beachten Sie, dass $c \oplus (a \wedge b)$ jeweils auf alle Basiszustände anzuwenden ist.

(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.

Lösungsvorschlag:

(a) Betrachte das Verhalten von $|c'\rangle := |c \oplus (a \wedge b)\rangle$ auf allen Basisvektoren. Offensichtlich ist das Toffoli-Gatter die Identität auf $|a\rangle$ und $|b\rangle$.

a	b	c	c'
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

Somit gilt für die Abbildungsmatrix des Toffoli-Gatters:

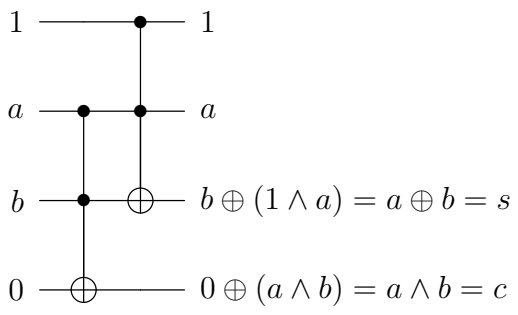
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(b) Offensichtlich ist die Abbildungsmatrix eine Permutationsmatrix und damit unitär.
Da das Toffoli-Gatter nach Vorlesung die reversible Einbettung $U_\wedge$ des $\wedge$ ist und reversible Einbettungen selbstinvers sind, d.h. $U_\wedge U_\wedge = id$, ist das Toffoli-Gatter reversibel.

(c) Schreibe das Toffoli-Gatter als $T(a, b, c) := (a \wedge b) \oplus c$. Dann gilt:

$T(a, b, 0) = (a \wedge b) \oplus 0 = a \wedge b$.
$T(a, 1, 1) = (a \wedge 1) \oplus 1 = a \oplus 1 = \neg a$.
$T(T(a, 1, 1), T(b, 1, 1), 1) = T(\neg a, \neg b, 1) = ((\neg a) \wedge (\neg b)) \oplus 1 = \neg((\neg a) \wedge (\neg b)) = \neg(\neg(a \vee b)) = a \vee b$.
Somit ist das Toffoli-Gatter universell, da $\{\vee, \neg, \wedge\}$ universell.

(d) Ein Halbaddierer lässt sich wie folgt durch Toffoli-Gatter realisieren:



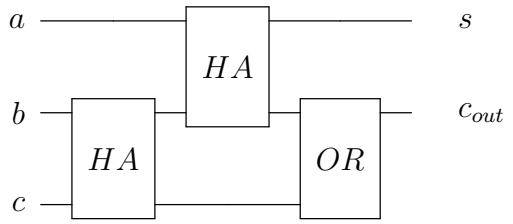
(e) Sei $|a\rangle = |b\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
Dann gilt:$|ab\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.
Betrachte nun die Anwendung des Halbaddierers auf $|ab\rangle$:

a	b	$0 \oplus (a \wedge b) = c$	$b \oplus (1 \wedge a) = s$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

Nach Anwendung des Halbaddierers befindet sich $|ab\rangle$ also im Zustand $|sc\rangle = \frac{1}{2}(|00\rangle + |10\rangle + |10\rangle + |01\rangle) =$

$$\frac{1}{\sqrt{2}}(|10\rangle) + \frac{1}{2}(|00\rangle + |01\rangle).$$

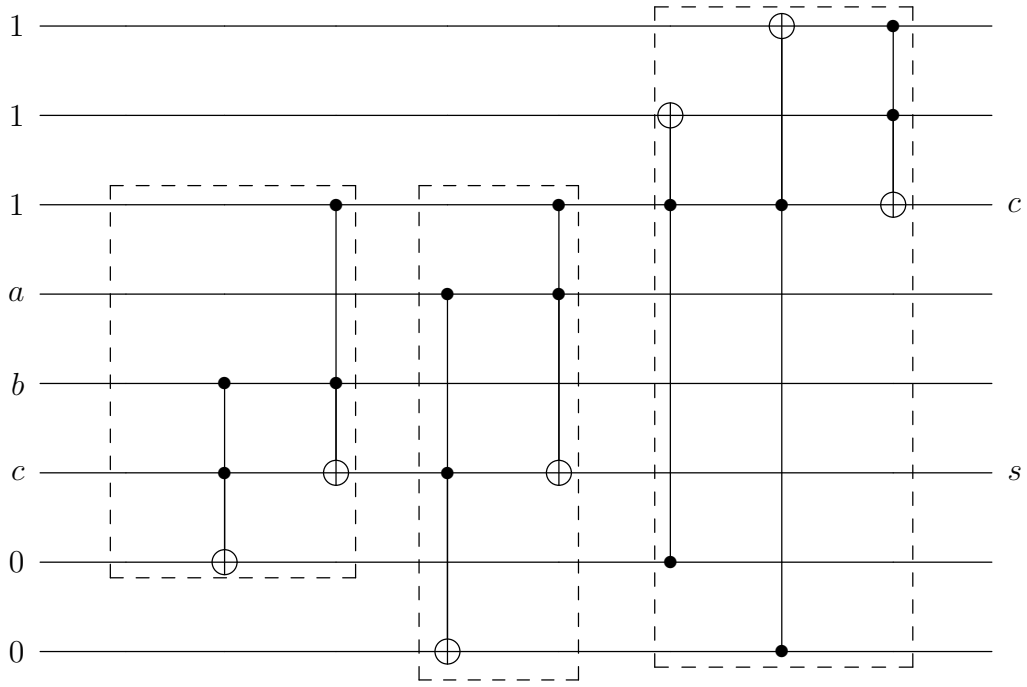
(f) Im Gegensatz zum Halbaddierer verfügt der Volladdierer noch über eine zusätzlich Eingangsleitung, die ein Carry-Bit c bereitstellt, das bei der Addition berücksichtigt wird.
Folgende Schaltung realisiert einen Volladdierer mittels Halbaddierern:



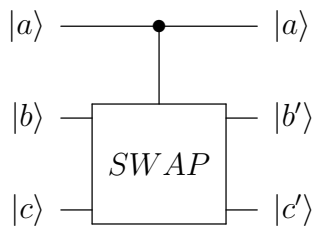
Dabei liefert der obere Ausgang eines HA das Summen-Bit s und der untere Ausgang das Carry-Bit c. Die Korrektheit lässt sich durch Auswerten der Schaltung in allen Basiszuständen einsehen. Dabei seien a', b', c' die Werte auf den Leitungen nach dem ersten HA, und a'', b'' die Werte der Leitungen nach dem zweiten HA:

a	b	c	a'	b'	c'	$a'' = s$	b''	c''	$b'' \vee c'' = c_{out}$
0	0	0	0	0	0	0	0	0	0
0	0	1	0	1	0	1	0	0	0
0	1	0	0	1	0	1	0	0	0
0	1	1	0	0	1	0	0	1	1
1	0	0	1	0	0	1	0	0	0
1	0	1	1	1	0	0	1	0	1
1	1	0	1	1	0	0	1	0	1
1	1	1	1	0	1	1	0	1	1

Man sieht, dass s die Summe von $a + b + c$ über $\mathbb{F}_2$ liefert, und c_{out} das korrekte Carry-Bit.
Ersetze nun die HA durch je zwei Toffoli-Gatter analog zu Teil (d) und das OR durch drei Toffoli-Gatter nach Teil (c):



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.

Lösungsvorschlag:

(a) Bei dem Fredkin-Gatter handelt es sich um ein kontrolliertes SWAP (CSWAP). Solange also $a = 0$ gilt, ist das CSWAP die Identität. CSWAP ist also auf den ersten vier Basisvektoren die Identität:

$$|0xy\rangle \xrightarrow{CSWAP} |0xy\rangle \forall x, y \in \{0, 1\}.$$

Für $|1xy\rangle$ wird ein SWAP auf $|xy\rangle$ angewendet, d.h.:

$$|1xy\rangle \xrightarrow{CSWAP} |1yx\rangle \forall x, y \in \{0, 1\}.$$

Somit wird das CSWAP beschrieben durch:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Offensichtlich ist diese Matrix unitär, da sie Permutationsmatrix ist.

(b) Betrachte die Auswertung des CSWAP auf allen Basiszuständen, so ergibt sich:

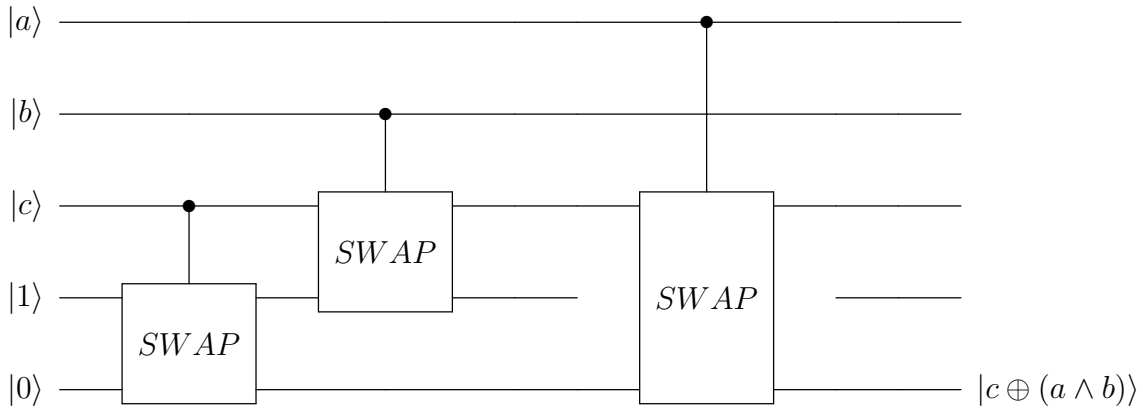
$$\begin{aligned} |b'\rangle &= \left|\overline{a}b\overline{c} + \overline{a}bc + a\overline{b}c + abc\right\rangle \\ &= \left|\overline{a}b(\overline{c} + c) + ac(\overline{b} + b)\right\rangle \\ &= |\overline{a}b + ac\rangle. \end{aligned}$$

Analog ergibt sich:

$$|c'\rangle = |\overline{a}c + ab\rangle.$$

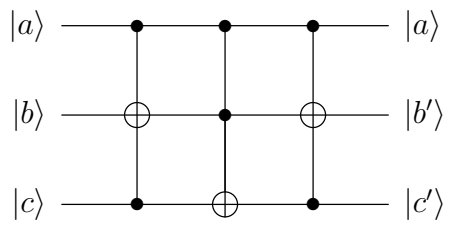
Hierbei wurde $\vee$ additiv und $\wedge$ multiplikativ geschrieben.

(c) Es werden drei Fredkin-Gatter benötigt, um ein Toffoli-Gatter zu simulieren:



Das Auswerten des Schaltkreises in allen Basiszuständen zeigt, dass dieser korrekt ein Toffoli-Gatter simuliert.

(d) Betrachte folgenden Schaltkreis:



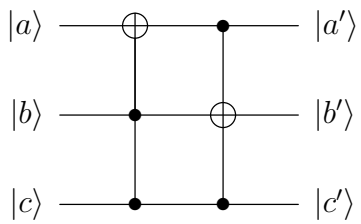
Für $a = 0$ wird kein Toffoli-Gatter angewendet und der Schaltkreis ist die Identität.
Somit ist der obige Schaltkreis für die ersten vier Basiszustände korrekt. Betrachte die übrigen Basiszustände:

$\|abc\rangle$	nach 1. Gatter	nach 2. Gatter	$\|ab'c'\rangle$
100	100	100	100
101	111	110	110
110	110	111	101
111	101	101	111

Es wird also korrekt ein Fredkin-Gatter simuliert.

Noch zu zeigen: Ein Fredkin-Gatter kann nicht mit zwei Toffoli-Gattern simuliert werden.

Da das Toffoli-Gatter selbstinvers ist, brauchen die Fälle nicht betrachtet zu werden, in denen bei beiden Toffoli-Gattern das NOT auf der gleichen Leitung liegt.
Alle übrigen Fälle, bei denen das NOT auf verschieden Leitungen liegt, lassen sich durch umordnen und umbenennen der Eingänge auf folgenden Schaltkreis reduzieren:



Annahme: Es handelt sich um ein korrekt simuliertes CSWAP.
Da für alle Belegungen $|c\rangle = |c'\rangle$ gilt, muss es sich bei $|c\rangle$ um das Kotrollbit handeln. Ausgewertet in $|111\rangle$ liefert der obige Schaltkreis jedoch $|011\rangle$, während ein CSWAP -insbesondere mit $|c\rangle$ als Kontrollbit - auf $|111\rangle$ die Identität ist.
Es handelt sich als um kein korrekt simuliertes CSWAP.

Somit sind mindestens drei Toffoli-Gatter nötig, um ein Fredkin-Gatter zu simulieren.