Nils Werner 108012219293 *Paul Rösler 108012225686* *Daniel Teuchert 108012214552*

Aufgabe 1

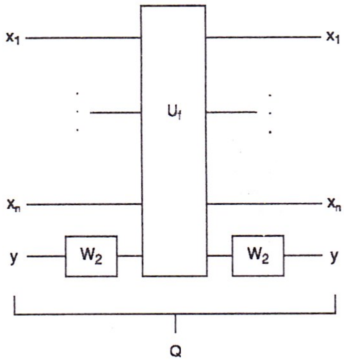


Abbildung 1: Quantenschaltkreis Q entspricht dem Schaltkreis aus Präsenzübung 4 Aufgabe 4

4/4

Gesucht ist ein Schaltkreis, welcher die reversieble Einbettung $U_f\ |\vec{x}y\rangle \rightarrow |\vec{x}\rangle \bigotimes |f(\vec{x}) \oplus y\rangle$ berechnet. Ein Bestandteil des Schaltkreises darf das Quantengate Q sein, welches dem Schaltkreis aus Aufgabe 4 der Präsenzübung 4 entspricht (Abb. 1). Das U_f dieser Aufgabe entspricht dabei dem U_f der Präsenzaufgabe. Um nun aus Q das Gate U_f zu erhalten muss jeweils die Auswirkung des Gates W_2 auf $|y\rangle$ ausgeglichen werden. Dazu kann man die Eigenschaft von W_2 nutzen, dass $|y\rangle \xrightarrow{W_2} \xrightarrow{W_2} |y\rangle$ ist.

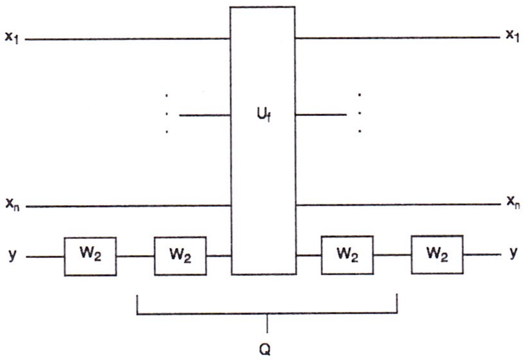


Abbildung 2: Schaltkreis aus W_2 und Q um U_f zu selektieren

Das voran und nachstellen von W_2 auf $|y\rangle$ sorgt nun dafür, dass auf $|\vec{x}y\rangle$ nur U_f wirkt und das der gesuchten Schaltung entspricht.

Aufg.	1	2	3	4	Σ
	4	5,5	3	6	18,5

Nils Werner 108012219293 — Paul Rösler 108012225686 — Daniel Teuchert 108012214552

Aufgabe 2

5,5

a)

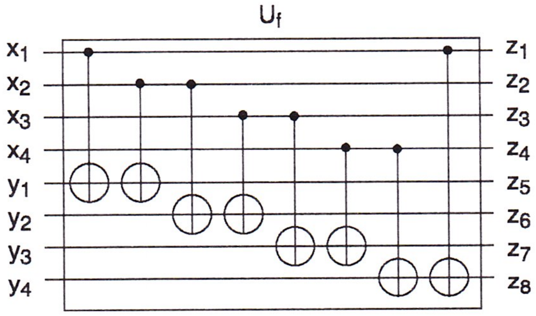
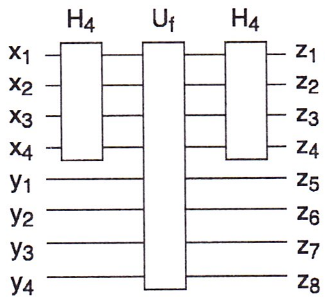


Abbildung 3: Quantenschaltkreis für die reversible Einbettung von f

b)



Messe.

Abbildung 4: Quantenschaltkreis Q_S des Algorithmus von Simon für dieses f

c) $\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & 0 & 1 & 0\\ 1 & 0 & 0 & 1\\ 0 & 0 & 0 & 0\end{pmatrix}\begin{pmatrix}s_1\\ s_2\\ s_3\\ s_4\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix} \Leftrightarrow \begin{pmatrix}s_1\\ s_1\\ s_1\\ 0\end{pmatrix} = \begin{pmatrix}s_2\\ s_3\\ s_4\\ 0\end{pmatrix}$

$\Rightarrow (s_1, s_2, s_3, s_4) = (1,1,1,1) \vee (s_1, s_2, s_3, s_4) = (0,0,0,0)$

d) $Pr[n-1$ Vektoren aus $\mathbb{F}_2^n$ sind linear unabhängig$]$

$= \prod_{i=1}^{n-1} Pr[y_i \neq 0^n \wedge y_i$ ist l.u. von y_1 bis $y_{i-1}]$

$= \prod_{i=0}^{n-2} Pr[y_{i+1} \neq 0^n \wedge y_{i+1}$ ist l.u. von y_1 bis $y_i]$

$= \prod_{i=0}^{n-2} Pr[y_{i+1} \neq 0^n \wedge y_{i+1} \notin \{y_1, .., y_i\} \wedge y_{i+1}$ ist nicht Summe zweier oder mehr ungleicher Summanden aus $\{y_1, .., y_i\}]$

2^i Möglichkeiten.

$= \prod_{i=0}^{n-2} \frac{2^n - 1 - i - \binom{i}{2} - \binom{i}{3} - .. - \binom{i}{i}}{2^n} = \prod_{i=0}^{n-2} \frac{2^n - \sum_{j=0}^{i}\binom{i}{j}}{2^n} = \prod_{i=0}^{n-2} \frac{2^n - 2^i}{2^n} = \prod_{i=0}^{n-2}\left(\frac{2^n}{2^n} - \frac{2^i}{2^n}\right) = \prod_{i=0}^{n-2}(1 - 2^{i-n})$

$\prod_{i=0}^{2}(1 - 2^{i-4}) = (1-2^{-4})(1-2^{-3})(1-2^{-2}) = \frac{315}{512} \approx 62\%$

unnötig kompliziert...

Nein da y_i nicht gleichverteilt in $\mathbb{F}_2^4$ $(\langle y_i, s\rangle = 0)$

Aufgabe 3

Da $S_u = \{\wedge, \neg, c\}$ universell ist, kann insbesondere jede reversible Funktion mittels S_u dargestellt werden. Es genügt daher, jedes Element als Verknüpfung von T, Hilfsvariablen und 0, 1 zu schreiben (s. Script).
Sei $S'_q = \{T_\wedge, T_\neg, T_c\}$ das r-reversible Pendant zu S_u mit dem gezeigt wird, dass $S_q = \{T\}$ r-reversibel ist.
$T_\wedge = T(x_1, x_2, 0) = (x_1, x_2, x_1x_2)$
$T_\neg = T(x_1, 1, 1) = (x_1, 1, 1 + x_1) = (x_1, 1, -x_1)$
$T_c = T(x_1, 1, 0) = (x_1, 1, x_1)$
$S_u = \{\wedge, \neg, c\}$ kann also durch $S'_q = \{T_\wedge, T_\neg, T_c\}$ dargestellt werden, wobei lediglich das Toffoli-Gate T und 0, 1 verwendet werden. Daraus folgt, dass $S_q = \{T\}$ r-reversibel ist.

✓

3/3

Aufgabe 4

6/7

\langle, \rangle statt <, >

a) Nach dem Satz von Lagrange gilt: Die Ordnung jeder Untergruppe teilt die Ordnung der Gruppe.
Da $< a >$ in $\mathbb{Z}_{p_i}^*$ eine Untergruppe der Gruppe $< a >$ in $\mathbb{Z}_N^*$ mit a ist Generator ist, folgt $t_i | t \forall i \in \{1, ..., k\}$.
Daraus folgt, dass $t = kgV(t_1, .., t_k)$
Daraus folgt außerdem, das $s = max\{s_1, ..., s_k\}$, denn die maximale Potenz von 2 in einem der t_i muss auch in t vorkommen, da t das kgV von allen t_i ist.

b) $s_i = r_i$ gilt gdw. a ein quadratischer Rest modulo p_i ist.
Da a uniform aus $\mathbb{Z}_N^*$ gezogen wird, gilt für jedes i unabhängig: $a \in_R \mathbb{Z}_{p_i}^*$
Außerdem gilt für $\mathbb{QR} = \{x \in \mathbb{Z}_{p_i}^* | x$ ist Quadratischer Rest modulo $p_i\}$: $|\mathbb{QR}| = \frac{|\mathbb{Z}_N^*|}{2}$. Dies liegt daran, dass $x \to x^2$ eine 2 zu 1 Abbildung ist ($x^2 = (-x)^2$).
Somit gilt Ws[a ist quadratischer Rest modulo p_i]$= \frac{1}{2}, \forall a \in_R \mathbb{Z}_N^*$

c) Fall 1: $r_j = r_i$
Ws$[s_i \neq s_j] \geq$ Ws$[s_i = r_i \wedge s_j \neq r_j] = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$

Fall 2: $r_j \neq r_i$
Ws$[s_i \neq s_j] \geq$ Ws$[s_i = r_i \wedge s_j = r_j] = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$

unnötig

Insgesamt:
Ws$[s_i \neq s_j] =$ Ws$[s_i \neq s_j | r_j = r_i]Ws[r_j = r_i] +$ Ws$[s_i \neq s_j | r_j \neq r_i]Ws[r_j \neq r_i] \geq \frac{1}{4}Ws[r_j = r_i] + \frac{1}{4} \cdot (1-Ws[r_j = r_i]) = \frac{1}{4}(Ws[r_j = r_i] + 1 -Ws[r_j = r_i]) = \frac{1}{4}$
$\Rightarrow$ Ws$[s_i \neq s_j] \geq \frac{1}{4}$

d) $a^{2^{s_i-1}u} = a^{\frac{2^s u}{2}} \bmod p_i$
Es gilt: $\text{ord}_{\mathbb{Z}_N^*}(a) = t = 2^s u$ und $\text{ord}_{\mathbb{Z}_{p_i}^*}(a) = t_i = 2^{s_i} u_i$
Wie in a) gezeigt, gilt $t = \text{kgV}(t_1, ..., t_k)$ und somit auch $s = \max\{s_1, ..., s_k\}$
Daraus folgt, das u_i u teilt, denn t_i teilt t
$\Rightarrow u_i \cdot K = u$ für K ungerade
$\Rightarrow a^{2^{s_i-1}u} = a^{\frac{2^{s_i} u_i \cdot K}{2}} \bmod p_i$ Es gilt: $t_i = \text{ord}(a) \bmod p_i$: (Schritt war im $\mathbb{Z}_p$: so nicht)
$\Rightarrow 1^{\frac{K}{2}} = 1^{\frac{1}{2}} \bmod p_i$ Hierfür gibt es nur 2 Lösungen: 1 und -1
In diesem Fall bleibt jedoch nur die Lösung $a^{2^{s-1}u} = -1 \bmod p_i$, da $a^{\frac{2^{s_i-1}u_i}{2}}$ nicht 1 sein kann, da $\frac{2^{s_i-1}u_i}{2} < t_i =$ ord$(a) \bmod p_i$, also muss gelten $a^{\frac{2^{s_i-1}u_i}{2}} = -1 \bmod p_i$ und weil K ungerade ist, kann auch $a^{(\frac{2^{s_i-1}u_i}{2})^K} \bmod p_i$ nicht 1 werden.

e) Wie bereits in d) gezeigt, gilt: $a^{2^{s_i-1}u} \bmod p_i = -1$, falls $s_i \geq 1$
Fall 1: $s_i = s$
$\Rightarrow a^{2^{s-1}u} = a^{2^{s_i-1}u} = -1 \bmod p_i$
$\Rightarrow a^{2^{s-1}u} = -1 \bmod p_i$, falls $s_i = s$

Fall 2: $s_i < s \Rightarrow s = s_i + k$, mit $k \geq 1$
$\Rightarrow a^{2^{s-1}u} = a^{2^{s_i+k-1}u} = a^{2^{s_i-1}2^k u} = (a^{2^{s_i-1}u})^{2^k} = (-1)^{2^k} = 1^{2^{k-1}} = 1 \bmod p_i$
$\Rightarrow a^{2^{s-1}u} = 1 \bmod p_i$, falls $s_i < s$. Daraus folgt auch: u_i teilt u, da beide Zahlen ungerade sind und somit nicht

in 2^{s_i} bzw. 2^s enthalten sind.

f) Falls gilt: $a^{2^{s-1}u} \bmod p_i = -1 \Rightarrow a^{2^{s-1}u} + 1 = K \cdot p_i$, für ein $K \in \mathbb{Z}$
Fall 1: $\text{ggT}(N, K) = 1$
$\Rightarrow \text{ggT}(N, a^{2^{s-1}u} + 1) = p_i$, also ein nicht-trivialer Teiler von N.

nutzlos.

Fall 2: $\text{ggT}(N, K) = q$, aber p_i teilt nicht K

$\Rightarrow \text{ggT}(N, a^{2^{s-1}u} + 1) = p_i \cdot q$, also ein nicht-trivialer Teiler von N. (könnte $= N$ sein)

Fall 3: $\text{ggT}(N, K) = q$ und p_i teilt $K \Rightarrow p_i$ teilt q
$\Rightarrow \text{ggT}(N, a^{2^{s-1}u} + 1) = q$, also ein nicht-trivialer Teiler von N.

$\Rightarrow$ wenn $\exists i$, mit $a^{2^{s-1}u} \bmod p_i = -1$, gilt $\text{ggT}(N, a^{2^{s-1}u})$ ist ein nicht-trivialer Teiler.
Dieser Fall tritt genau dann ein, wenn es ein j gibt mit $s_j \geq 1$, denn dann gibt es ein i mit $s_i = \max\{s_1, ..., s_k\} = s \geq 1$ und es gilt $a^{2^{s_i-1}u} = -1 = a^{2^{s-1}u} \bmod p_i$. Ws[$s \geq 1$]=Ws[$\exists i \neq j$ mit $s_i \neq s_j$]$\geq \frac{1}{4}$ (siehe c))
$\Rightarrow$ Mit Ws $\frac{1}{4}$ ist $\text{ggT}(N, a^{2^{s-1}u})$ ein nicht-trivialer Teiler.

Benötige: $\exists i$ mit $a^{2^{s-1}u} \bmod p_i = -1$
$\Rightarrow \text{ggT}(\ldots) \neq 1$
$\exists j$ mit $a^{2^{s-1}u} \bmod p_j = +1$
$\Rightarrow \text{ggT}(\ldots) \neq N$.
↯.

g) Algorithmus:

1. Wähle $a \in_R \mathbb{Z}_N^*$ uniform
2. Berechne `PERIODE`(N, a) und erhalte so $t = \text{ord}_{\mathbb{Z}_N^*}(a)$ mit $t = 2^s \cdot u$
3. Berechne $\frac{a^t}{a^2} + 1 = x$
4. Berechne $\text{ggT}(N, x) = p$
5. Falls gilt: $p|N$ gebe p aus, sonst gehe zu Schritt 1

Potenzgesetze...

$\frac{a^{2^s \cdot u}}{a^2} = a^{(2^s \cdot u) - 2}$

Korrektheit: $x = \frac{a^t}{a} + 1 = \frac{a^{2^s \cdot u}}{a^2} + 1 \neq a^{2^{s-1} \cdot u} + 1$
Es gilt mit Ws $\geq \frac{1}{4}$ dass $\text{ggT}(N, x) = p$ ein nicht-trivialer Teiler von N ist und das somit gilt $p|N$ Bei dem zweifachen durchlaufen von den Schritten 1-4 ist die Wahrscheinlichkeit einen nicht-trivialen Teiler gefunden zu haben schon bei ? $1 - (\frac{3}{4})^2 = 0,4375 = 43,75\%$
Laufzeit: `PERIODE`(N, a): $O(T(N))$, $\text{ggT}(N, x)$: $O(log(Nx)^{\cancel{3}\,2}) = O(log(N)^{\cancel{3}\,2})$
Gesamt: $O(max\{T(N), log(N)^3)\}) = O(T(N) + log(N)^3) = O(T(N)log(N)^3)$.

ggT geht in $\log^2(N)$
(Berechnen von a^t ~~$a^{...}$~~ mod N
benötigt $\log^3 N$)

2/2