Definition (r-universell): sei R eine Menge von reversieblen booleschen Funktionen, die auf einer konstanten Anzahl von Bits operieren. R heißt r-universell, falls jede reversible Funktion als Verknüpfung von Elementen aus R, Hilfsvariablen und Konstanten $0, 1$ dargestellt werden kann.

Satz: $\{\mathtt{T}\}$ ist r-universell.

Beweis: Da $S_u = \{\wedge, \neg, \mathtt{c}\}$ universell ist, kann insbesondere jede reversible Funktion mittels S_u dargestellt werden. Es genügt daher, jedes Element als Verknüpfung von $\mathtt{T}$, Hilfsvariablen und $0, 1$ zu schreiben. Rest: Übungsaufgabe.

9.2 Die Klassen $\mathcal{QP}$ und $\mathcal{BQP}$

Definition (einbettbar): Seien $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ und $U_f : \mathbb{F}_2^{n+l} \to \mathbb{F}_2^{m+k}$ boolesche Funktionen. Wir nennen f einbettbar in U_f, falls es ein $h \in \mathbb{F}_2^2$ gibt mit $U_f(x, h) = (h', f(x))$ für ein $h' \in \mathbb{F}_2^k$.

Satz: Jede boolesche Funktion $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ ist in eine reversible Funktion $U_f : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ einbettbar.

Beweis: Verwende reversible Einbettung aus 9.1: $U_f(x, y) \mapsto (x, f(x)+y)$. Damit ist f in U_f eingebettet, denn $u_f(x, 0^m) = x(f(x))$, d.h. $h = 0^m$ und $h' = x$.

Reversible boolesche Schaltkreise bestehen ausschließlich aus Gattern, die reversible boolesche Funktionen realisieren. Wir betten nun boolesche Schaltkreise in reversible Schaltkreise ein.

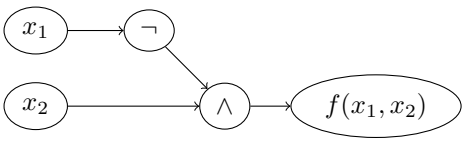
Satz: Sei $C = \{C_n\}_{n\in\mathbb{N}}$ eine uniforme Schaltkreisfamilie über $S = \{\wedge, \neg\}$ der Größe $\mathcal{O}(g(n))$, die $f_n, n \in \mathbb{N}$ berechnet. Dann gibt es eine uniforme reversible Schaltkreisfamilie C_r über $\{\mathtt{T}, 0, 1\}$ der Größe $\mathcal{O}(g(n))$, die $f_n^r : \mathbb{F}_2^{n+m+l} \to \mathbb{F}_2^{n+m+l}$ mit $(x, y, z \mapsto (x, f_n(x) + y, z')$ berechnet.
D.h. f_n und U_{f_n} sind in f_n^r eingebettet.

Beweis: Da C uniform ist, können wir für jedes n den Schatkrleis C_n auf einer DTM konstruieren. Wir ersetzen in C_n die

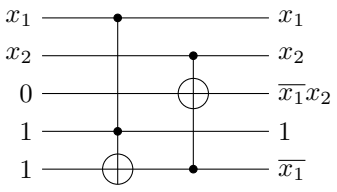
- $\wedge$-Gatter mit $\mathtt{T}(x_1, x_2, 0) = (x_1, x_2, x_1x_2)$
- $\neg$-Gatter mit $\mathtt{T}(x_1, 1, 1) = x_1, 1, 1 - x_1)$

Dazu verwenden wir höchstens dreimal soviele Eingabeknoten/Ausgabeknoten wie in C_n. D.h. die Größe von C_r ist höchstens dreimal die Größe von C, d.h die Größe von C_r ist $\mathcal{O}(g(n))$.

Beispiel:
$f(x_1, x_2) = \overline{x_1}x_2$
$U_f(x_1, x_2, 0) = (x_1, x_2, \overline{x_1}x_2)$



$f^r(x_1, x_2, 0, 1, 1) = (x_1, x_2, \overline{x_1}x_2, 1, \overline{x_1})$ ist Einbettung von f und U_f



Definition (Quantenschaltkreis-Familie): Eine QC-Familie $Q = \{Q_n\}_{n\in\mathbb{N}}$ heißt uniform, falls es eine DTM gibt, die für jedes $n \in \mathbb{N}$ bei Eingabe 1^n in Zeit und Platz poly(n) Q_n ausgibt. Eine boolesche Funktion $f_n, n \in \mathbb{N}$ hat uniforme Quanten-Schaltkreiskomplexität $\mathcal{O}(g(n))$ bezüglich S, falls es eine uniforme QC-Familie über S gibt, die f_n berechnet.

Definition ($\mathcal{QP}$): Die Klasse $\mathcal{QP}$ ist die Klasse aller booleschen Funktionen $f_n, n \in \mathbb{N}$, für die es ein $g(n) \in$ poly(n) und eine uniforme QC-Familie $Q_{g(n)}$ bezüglich $S_2 = \{\mathtt{H}, \mathtt{CNOT}, \mathtt{T}\}$ gibt mit:

- $Q_{g(n)}$ hat Größe poly(n)
- $Q_{g(n)}$ berechnet $f_n^r : \mathbb{F}_2^{g(n)} \to \mathbb{F}_2^{g(n)}$, wobei f_n in f_n^r eingebettet ist für alle $n \in \mathbb{N}$.

Satz: $\mathcal{P} \subseteq \mathcal{QP}$

Beweis: Sei $f_n \in \mathcal{P}$. Dann gibt es eine uniforme Schaltkreisfamile C mit Größe poly(n) die f_n berechnet.
$\overset{9.2}{\Rightarrow} \exists$ uniforme reversible Schaltkreisfamilie C_r der Größe poly(n), die f_n^r berechnet, so dass f_n in f_n^r eingebettet ist. C_r ist über $\{\mathtt{T}, 0, 1\}$ definiert.
Ersetzung der booleschen Gatter `T` durch unitäre Gatter, die `T` beschreiben, transformiet C_r in einen Quantenschaltkreis. Damit ist die Funktion $f_n \in \mathcal{QP}$.

Definition ($\mathcal{BQP}$): Die Klasse $\mathcal{BQP}$ ist die Klasse aller booleschen Funktionen $f_n, n \in \mathbb{N}$, für die es ein $g(n) \in$ poly(n) und eine uniforme QC-Familie $Q_{g(n)}$ bezüglich $\{\mathtt{H}, \mathtt{CNOT}, \mathtt{T}\}$ gibt mit:

- $Q_{g(n)}$ hat Größe poly(()n)
- $\exists k \in$ poly$(n) : y \in_R \mathbb{F}_2^k \; \forall \; x \in \mathbb{F}_2^n :$ Ws.$_y(Q_{g(n)}(x, y) = f_n^r(x)) \geq \frac{2}{3}$, wobei f_n^r eine Einbettung von f_n ist.

Problem: Erzeugung zufälliger Eingaben $y \in \mathbb{F}_2^k$ mit QC.

Definition (H_k): Sei $x = |x_0 x_1 \dots x_{k-1}\rangle$. Dann ist
$H_k|x\rangle = H_k|x_0 \dots x_{k-1}\rangle = H|x_0\rangle \otimes H|x_1\rangle \otimes \dots \otimes H|X_{k-1}\rangle$ die Hadamard-Abbildung auf ein k-Qubit-Register.

Satz: $H_k|x\rangle = \frac{1}{2^{\frac{k}{2}}} \sum\limits_{y \in \{0,1\}^k} (-1)^{xy}|y\rangle$, wobei xy das innere Produkt von x, y ist.

Beweis: $k = 1, 2$: siehe 5.3, $k = 3$: siehe Übung. Beliebiges k: induktiv.

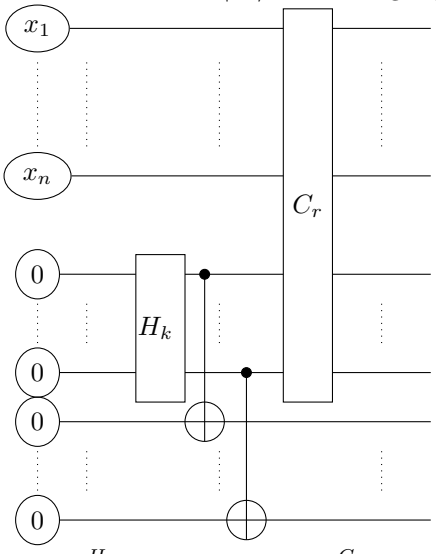
Korollar: $H_k|0^k\rangle = \frac{1}{2^{\frac{k}{2}}} \sum\limits_{y \in \{0,1\}^k} |y\rangle$ liefert gleichmäßige Überlagerung der Basiszustände.

Satz: $\mathcal{BPP} \subseteq \mathcal{BQP}$

Beweis: Sei $f \in \mathcal{BPP}$ und C die Schaltkreisfamilie polynomieller Größe mit Ws.$_y(C(x, y) = f_n) \geq \frac{2}{3}$.
Analog zum Beweis $\mathcal{P} \subseteq \mathcal{QP}$:

- Transformiere C in reversible Familie C_r über $\{\mathtt{T}, 0, 1\}$ polynomieller Größe, die f_n^r berechnet.
- Transformire C_r in QC-Familie Q durch Ersetzung von `T` durch seine unitäre Variante.

Wir verwenden $H_k|0^k\rangle$ zur Erzeugung von y:



$|x0^{2k}\rangle \overset{H_k}{\longmapsto} \frac{1}{2^{\frac{k}{2}}} \sum\limits_{y \in \{0,1\}^k} |xyy\rangle \overset{C_r}{\longmapsto} \frac{1}{2^{\frac{k}{2}}} \sum\limits_{y \in \{0,1\}^k} C_r|xy\rangle \otimes |y\rangle$

Aber $C_r|xy\rangle = f(x) \; \forall x$ und mindestens $\frac{2}{3}$ aller y.
Messung der letzten k Qubits liefert $C_r|xy\rangle \otimes |y\rangle$ für jedes $y \in \{0,1\}^k$ mit Ws. $\frac{1}{2^k}$. Messung der restlichen Qubits liefert $f(x)$ mit Ws. $\geq \frac{2}{3}$

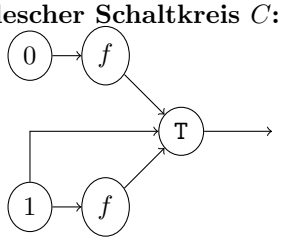
10 Quanten -schaltkreise und -algorithmen

10.1 Deutsch-Josza Problem

Gegeben: Gatter $f : \mathbb{F}_2 \to \mathbb{F}_2$

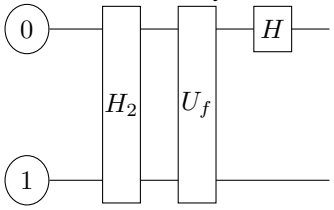
Gesucht: Schaltkreis, der entscheidet ob $f(0) = f(1)$ mit minimaler Anzahl von f-Gattern

Boolescher Schaltkreis C:



$C(0,1) = \mathtt{T}(f(0), 1, f(1)) = f(0) + f(1) \Rightarrow C(0,1) = 0 \Leftrightarrow f(0) = f(1)$. Minimale Anzahl von f-Gattern für boolesche Schaltkreise, da $f(0)$ keine Information über $f(1)$ liefert.

Quantenschaltkreis Q:



$U_f|xy\rangle = |x\rangle \otimes |f(x)+y\rangle$ ist die reversible Einbettung von f. Beachte: Q verwendet nur ein f-Gatter!

Satz: Q entscehidet das Deutsch-Josza Problem.

Beweis:

$$
\begin{aligned}
|01\rangle &\overset{H_2 = H \otimes H}{\longmapsto} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&= \frac{1}{2}(|0\rangle \otimes (|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle) \\
&\overset{U_f}{\longmapsto} \frac{1}{2}(|0\rangle \otimes (|0 + f(0)\rangle - |1 + f(0)\rangle) + |1\rangle(|0 + f(1)\rangle - |1 + f(1)\rangle)) \\
&= \frac{1}{2}(|0\rangle \otimes (-1)^{f(0)}(|0\rangle - |1\rangle) + |1\rangle \otimes (-1)^{f(1)}(|0\rangle - |1\rangle)) \\
&= \frac{1}{2}(((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle)) \\
&\overset{H \otimes I}{\longmapsto} \frac{1}{2^{\frac{3}{2}}}(((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle) \otimes (|0\rangle - |1\rangle)
\end{aligned}
$$

Für $f(0) = f(1)$: $(-1)^{f(0)} \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle - |1\rangle)$
$\Rightarrow$ Messung liefert 0 im 1. Qubit

Für $f(0) \neq f(1)$: $(-1)^{f(0)} \frac{1}{\sqrt{2}}|1\rangle \otimes (|0\rangle - |1\rangle)$
$\Rightarrow$ Messung liefert 1 im 1. Qubit.

D.h. die Messung des 1. Qubits entscheidet das Deutsch-Josza Problem.

Orakel-Modell: Information über $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ durch Auswerten von f.

10.2 Verallgemeinertes Deutsch-Josza Problem

Gegeben: $f : \mathbb{F}_2^n \to \mathbb{F}_2$ im Orakel-Modell
Promise-Problem: f ist entweder

- konstant, d.h. $f(x) = c \; \forall c \in \mathbb{F}_2, \; \forall x \in \mathbb{F}_2^n$
- balanciert, d.h $f(x) = 0$ für genau die Hälfte aller $x \in \mathbb{F}_2^n$

Ziel: Entscheide, ob f konstant oder balanciert ist mit minimaler Zahl von f-Aufrufen.

Klassischer deterministischer Algorithmus:

1. `Setze` $c = f(0^n)$
2. `FOR i = 1 TO` 2^{n-1}
   - `Falls` $f(i) \neq c$, `Ausgabe ‘‘balanciert’’ und EXIT.`
3. `Ausgabe: ‘‘Konstant’’`

Anzahl f-Aufrufe $\leq 2^{n-1}+1$ (genau $2^{n-1}+1$ für konstante f)
Erfolgswahrscheinlichkeit: 1.

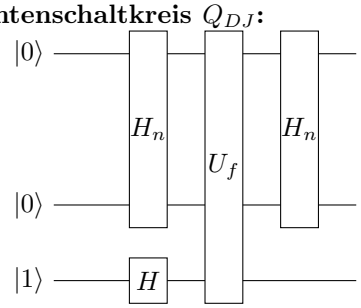
Probalistischer Algorithmus:

1. `Setze` $c = f(0^n)$
2. `FOR i-1 zufällige Werte` $x_j \in \{1, 2, \ldots, 2^{n-1}\}$
   - `Falls` $f(x_i) \neq c$, `Ausgabe ‘‘balanciert’’ und EXIT.`
3. `Ausgabe: ‘‘Konstant’’`

Fehlerwahrscheinlichkeit: $\underbrace{\text{Ws. (Ausgabe “balanciert”}|f \text{ konstant)}}_{=0} + \text{Ws. (Ausgabe “konstant”}|f \text{ balanciert)}$

$= \text{Ws.}\,(x_1 = x_2 = \cdots = x_{i-1} = f(0)|f \text{ balanciert}) = \prod_{j=1}^{i-1} \frac{2^{n-1}-j}{2^n} \leq \left(\frac{1}{2}\right)^{i-1}$

Quantenschaltkreis Q_{DJ}:



U_f ist reversible Einbettung von $f : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{n+1}, |xy\rangle \mapsto |x\rangle \otimes |f(x)+y\rangle$ für $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2$.
Q_{DJ} besitzt nur ein U_f-Gatter und damit nur ein f-Gatter!

Satz: Q_{DJ} entscheidet das verallgemeinerte Deutsch-Josza Problem.

Beweis:

$$
\begin{aligned}
|0^n 1\rangle &\overset{H_n \otimes H}{\longmapsto} \frac{1}{2^{\frac{n}{2}}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&\overset{U_f}{\longmapsto} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x\in\{0,1\}^n} |x\rangle(|0+f(x)\rangle - |1-f(x)\rangle) \\
&= \frac{1}{2^{\frac{n+1}{2}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle \otimes (|0\rangle - |1\rangle) \\
&\overset{H_n}{\longmapsto} \frac{1}{2^{\frac{2n+1}{2}}} \sum_{x\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+xy}|y\rangle \otimes (|0\rangle - |1\rangle) = |z\rangle
\end{aligned}
$$

Lemma: $\sum_{x\in\{0,1\}^n} (-1)^{xy} = \begin{cases} 2^n & \text{für } y = 0^n \\ 0 & \text{sonst} \end{cases}$ Beweis: Übungsaufgabe.

1. Fall: f konstant: Für die ersten n Qubits von $|z\rangle$ gilt:
$\frac{1}{2^{\frac{2n+1}{2}}} \sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}(-1)^{xy}|y\rangle = \frac{1}{2^{\frac{2n+1}{2}}}(-1)^{f(0^n)}(2^n|0^n\rangle + \sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{xy}|y\rangle$
$\Rightarrow |z\rangle = \frac{1}{\sqrt{2}}(-1)^{f(0^n)}|0^n\rangle \otimes (|0\rangle - |1\rangle)$
D.h für konstantes f liefert die Messung der ersten n Qubits 0^n.

2. Fall: f balanciert: $\sum_{y\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+xy}|y\rangle = \underbrace{\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|0^n\rangle}_{=0} + \sum_{\substack{y\in\{0,1\}^n\\ y\neq 0^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+xy}|y\rangle$

$\Rightarrow$ Messung der ersten n Qubits von z liefert 0^n mit Ws. 0

Entscheiden des DJ-Problems durch Messung der ersten n Qubits von $|z\rangle$:
Falls 0^n, Ausgabe "f konstant"
Sonst Ausgabe "f balanciert"

Vergleich:

	f-Aufrufe	Ws.
Deterministisch	$2^{n-1}+1$	1
Probabilistisch	3	$\geq \frac{3}{4}$
Quanten	1	1

10.3 Bernstein-Vazirani Problem (1983)

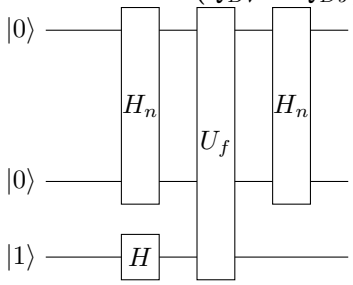
Gegeben: Funktion $f_a : \mathbb{F}_2^n \to \mathbb{F}_2, x \mapsto ax = \sum_{i=1}^{n} a_i x_i \bmod 2$ mit $a \in \{0,1\}^n$ im Orakel-Modell

Gesucht: $a \in \{0,1\}^n$ mit minimaler Anzahl von f-Aufrufen

Klassisch: Untere Schranke: Jeder Aufruf von f liefert 1 Bit an Information.
$\Rightarrow$ Mindestens n Aufrufe von f zur Bestimmung von a notwendig.
Seien $e_i, i = 1 \ldots n$ die Einheitsvektoren.
Optimaler klassischer Algorithmus:

- `Werte` f_a `an` $e_i, i = 1 \ldots n$ `aus und gib die entsprechenden` a_i `aus.`

Quantenschaltkreis ($Q_{BV} = Q_{DJ}$):



U_f ist reversible Einbettung von f_a

Satz: Q_{BV} berechnet a mit einem Aufruf von f.

Beweis:

$$
\begin{aligned}
|0^n 1\rangle &\overset{H_n\otimes H}{\longmapsto} \frac{1}{2^{\frac{n+1}{2}}}\sum_{x\in\{0,1\}^n}|x\rangle\otimes(|0\rangle-|1\rangle)\\
&\overset{U_{f_a}}{\longmapsto} \frac{1}{2^{\frac{n+1}{2}}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle\otimes(|0\rangle-|1\rangle)\\
&\overset{H_n\otimes I_2}{\longmapsto} \frac{1}{2^{\frac{n+1}{2}}}\sum_{y\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}(-1)^{xa}(-1)^{xy}|y\rangle\otimes(|0\rangle-|1\rangle) = |z\rangle
\end{aligned}
$$

Beobachtung: $\sum_{x\in\{0,1\}^n}(-1)^{x(y+a)} = \begin{cases} 2^n & \text{für } y+a=0^n, \text{d.h. } y=a \\ 0 & \text{sonst} \end{cases}$
Messung der ersten n Qubits liefert a mit Wahrscheinlichkeit 1.

Für das Berstein-Vazirani Problem liefern Quantenschaltkreise einen Speedup von n, d.h. einen polynomiellen Faktor.

10.4 Das Problem von Simon (1994):

Gegeben: Funktion $f : \mathbb{F}_2^n \to \mathbb{F}_2^m, m \geq n$ im Orakel-Modell
Promise-Problem: $\exists s \in \mathbb{F}_2^n : f(x) = f(y) \Leftrightarrow x = y + s$
D.h. insbesondere die Funktion f ist eine 2:1-Abbildung: Je zwei Urbilder x und $x + s$ werden auf dasselbe Bild abgebildet.

Gesucht: $s \in \mathbb{F}_2^n$

Klassischer Algorithmus: Werte verschiedene $x_1, \ldots, x_k$ aus, bis Kollision $f(x_i) = f(x_j)$ gefunden. Ausgabe: $x_i + x_j$

Deterministisch: $k \leq 2^{n-1} + 1$ Auswertungen notwendig

Probabilistisch: Wie groß muss k gewählt werden, damit Kollision erwartet wird?

Definiere: $x_{ij} = \begin{cases} 1 & \text{falls } f(x_i) = f(x_j) \\ 0 & \text{sonst} \end{cases}$, $\text{Ws.}\,(x_{ij} = 1) = \frac{1}{2^n - 1}$

$$E(\#\text{ Kollisionen}) = \sum_{1 \leq i < j \leq n} \text{Ws.}\,(x_{ij} = 1) = \binom{k}{2} \frac{1}{2^n - 1} \approx \frac{k^2}{2^n - 1}$$

Der Erwartungswert ist konstant für $k = \Omega(2^{\frac{n}{2}})$, d.h k ist exponentiell in n.