Die Klassen QP und BQP

Def: 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 $h\in\mathbb{F}_2^l$ gibt mit

$$U_f(x,h)=(h',f(x)) \quad \text{für ein } h'\in\mathbb{F}_2^k.$$

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 von S. 21: $U_f:(x,y)\mapsto(x,f(x)+y)$

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 $O(g(n))$, die f_n, $n\in\mathbb{N}$, berechnet. Dann gibt es eine uniforme reversible Schaltkreisfamilie C_r über $\{T,0,1\}$ der Größe $O(g(n))$, die

$$f_n^r:\mathbb{F}_2^{n+m+l}\to\mathbb{F}_2^{n+m+l} \text{ mit } (x,y,z)\mapsto(x,f_n(x)+y,z') \text{ berechnet.}$$

D.h. f_n und U_{f_n} sind in f_n^r eingebettet.

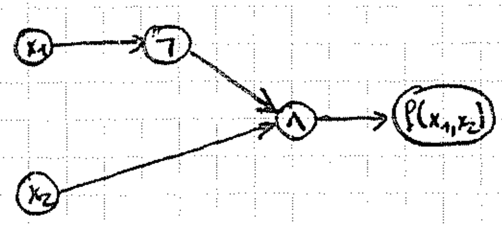
Beweis: Da C uniform ist, können wir für jedes n den Schaltkreis C_n auf einer DTM konstruieren. Wir ersetzen in C_n die $\wedge$-Gatter mit $T(x_1,x_2,0)=(x_1,x_2,x_1x_2)$

$\neg$-Gatter mit $T(x,1,1)=(x,1,1-x)$

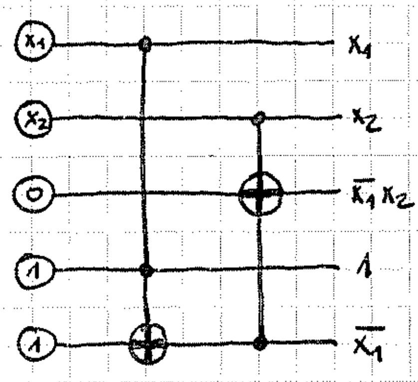
Dazu verwenden wir höchstens dreimal soviele Eingabeknoten /Ausgabeknoten wie in C_n. D.h. die Größe von C_r ist höchstens dreimal die Größe von C, d.h. die Größe von C_r ist $O(g(n))$.

Bsp.: $f(x_1,x_2)=\overline{x_1}\cdot x_2$

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



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



Def.: 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 boolsche Funktion $f_n, n \in \mathbb{N}$, hat uniforme Quanten-Schaltkreiskomplexität $O(g(n))$ bzgl. S, falls es eine uniforme QC-Familie über S gibt, die f_n berechnet.

Def.: Die Klasse QP ist die Klasse aller boolschen Fkt. $f_n, n \in \mathbb{N}$, für die es ein $g(n) = poly(n)$ und eine uniforme QC-Familie $Q_{g(n)}$ bzgl. $S_2 = \{H, CNOT, T\}$ 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: $P \subseteq QP$

Beweis: Sei $f_n \in P$. Dann gibt es eine uniforme Schaltkreisfamilie C mit Größe $poly(n)$, die f_n berechnet.
$\overset{\text{Satz S.28}}{\Longrightarrow}$ $\exists$ 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 $\{T, 0, 1\}$ definiert.
Ersetzung der boolschen Gatter T durch unitäre Gatter, die T beschreiben, transformiert C_r in einen Quantenschaltkreis. Damit ist die Funktion $f_n \in QP$.

Def.: Die Klasse BQP ist die Klasse aller boolschen Fkt. $f_n, n \in \mathbb{N}$, für die es ein $g(n) = poly(n)$ und eine uniforme QC-Familie $Q_{g(n)}$ bzgl. $\{H, CNOT, T\}$ gibt mit:
- $Q_{g(n)}$ hat Größe $poly(n)$.
- $\exists k = poly(n): y \in_R \mathbb{F}_2^k \; \forall x \in \mathbb{F}_2^n: Ws_y(Q_{g(n)}(x,y) = f_n^r(x)) \geq \frac{2}{3}$, wobei f_n^r eine Einbettung von f_n ist.

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

Def. (H_k): Sei $x = |x_0 x_1 \ldots x_{k-1}\rangle$. Dann ist $H_k|x\rangle = H_k|x_0 \ldots x_{k-1}\rangle = H|x_0\rangle \otimes H|x_1\rangle \otimes \ldots \otimes H|x_{k-1}\rangle$ die Hadamard-Abbildung auf einem k-Qubit.

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

Bew.: $k = 1, 2$: s. Vorlesung $k = 3$: s. Übung
beliebiges k: induktiv

<u>Korollar</u>: $H_k|0^k\rangle = \frac{1}{2^{k/2}} \sum_{y\in\{0,1\}^k} |y\rangle$ liefert gleichmäßige Überlagerung der Basiszustände.

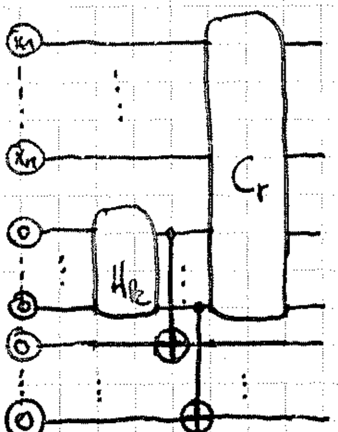
<u>Satz</u>: $BPP \subseteq BQP$

Beweis: Sei $f \in BPP$ und C die Schaltkreisfamilie polyn. Größe mit $Ws_y(C(x,y)=f_n) \geq \frac{2}{3}$.

Analog zum Beweis $P \subseteq QP$:

- Transformiere C in reversible Familie C_r über $\{T,0,1\}$ polyn. Größe, die $\hat{f}_n$ berechnet.
- Transformiere 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:



$|x0^{2k}\rangle \xrightarrow{H_k} \frac{1}{2^{k/2}} \sum_{y\in\{0,1\}^k} |xyy\rangle \xrightarrow{C_r} \frac{1}{2^{k/2}} \sum_{y\in\{0,1\}^k} C_r|xy\rangle \otimes |y\rangle$

Aber $C_r|xy\rangle = f(x)$ für alle x und mind. $2/3$ aller y.

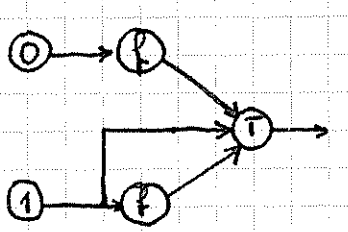
Messung der letzten k Qubits liefert $C_r|xy\rangle \otimes |y\rangle$ für jedes $y \in \{0,1\}^k$ mit Ws $\frac{1}{2^k}$. Messung der restlichen Qubits liefert $f(x)$ mit Ws $\geq \frac{2}{3}$.

<u>Deutsch-Josza Problem</u>

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

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

Boolescher Schaltkreis C:

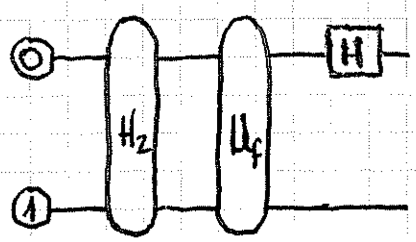


$C(0,1) = T(f(0),1,f(1)) = f(0)+f(1)$

$\Rightarrow C(0,1)=0 \Leftrightarrow f(0)=f(1)$

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!

<u>Satz</u>: Q entscheidet das Deutsch-Josza Problem.

Beweis: $|01\rangle \xmapsto{H_2 = H\otimes H} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$

$$= \frac{1}{2}\Big(|0\rangle \otimes (|0\rangle-|1\rangle) + |1\rangle(|0\rangle-|1\rangle)\Big)$$

$$\xmapsto{U_f} \frac{1}{2}\Big(|0\rangle \otimes (|0+f(0)\rangle - |1+f(0)\rangle) + |1\rangle(|0+f(1)\rangle - |1+f(1)\rangle)\Big)$$

$$= \frac{1}{2}\Big(|0\rangle \otimes (-1)^{f(0)}(|0\rangle-|1\rangle) + |1\rangle \otimes (-1)^{f(1)}(|0\rangle-|1\rangle)\Big)$$

$$= \frac{1}{2}\Big(\big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\big) \otimes (|0\rangle-|1\rangle)\Big)$$

$$\xmapsto{H\otimes I} \frac{1}{2^{3/2}}\Big(\big((-1)^{f(0)}+(-1)^{f(1)}\big)|0\rangle + \big((-1)^{f(0)}-(-1)^{f(1)}\big)|1\rangle\Big) \otimes (|0\rangle-|1\rangle)$$

Für $f(0)=f(1)$: $(-1)^{f(0)} \cdot \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle-|1\rangle)$

$\Rightarrow$ Messung liefert 0 im 1. Qubit.

Für $f(0)\neq f(1)$: $(-1)^{f(0)} \cdot \frac{1}{\sqrt{2}}|1\rangle \otimes (|0\rangle-|1\rangle)$

$\Rightarrow$ Messung liefert 1 im 1. Qubit

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

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

<u>Verallgemeinertes Deutsch-Josza Problem</u>

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

Promise-Problem: f ist entweder

- konstant, d.h. $f(x)=c$ für ein festes $c\in\mathbb{F}_2$ und alle x oder
- 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:
  - Setze $c = f(0^n)$
  - FOR $i=1$ TO 2^{n-1}
    - Falls $f(i)\neq c$, Ausgabe „balanciert" und EXIT.
  - Ausgabe „konstant"

Anzahl f-Aufrufe $\le 2^{n-1}+1$ (genau $2^{n-1}+1$ für konstante f)

Erfolgswahrscheinlichkeit: 1.

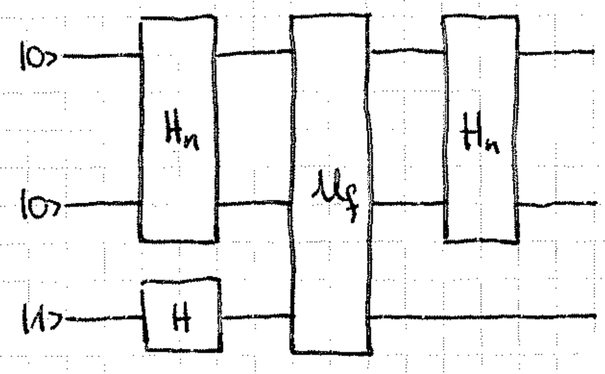
- Probabilistische Algorithmus
  - Setze $c = f(0^n)$.
  - Für i-1 zufällige Werte $x_j \in \{1,2,\dots,2^n-1\}$
    - Falls $f(x_j) \neq c$, Ausgabe „balanciert" und EXIT.
  - Ausgabe „konstant"

Fehlerwahrscheinlichkeit: $\underbrace{Ws(\text{Ausgabe „balanciert"} \mid f \text{ konstant})}_{=0} + Ws(\text{Ausgabe „konst"} \mid f \text{ bal.})$

$$= Ws(x_1 = x_2 = \dots = x_{i-1} = f(0) \mid f \text{ balanciert}) = \prod_{j=1}^{i-1} \frac{2^{n-1}-j}{2^n} \le \left(\frac{1}{2}\right)^{i-1}$$

D.h. für i=3 f-Aufrufe ist die Ausgabe korrekt mit Ws. $\geq \frac{3}{4}$.

- 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!

<u>Satz</u>: Q_{DJ} entscheidet das verallgemeinerte Deutsch-Josza Problem.

Beweis:
$$|0^n 1\rangle \xrightarrow{H_n \otimes H} \frac{1}{2^{\frac{n}{2}}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\xrightarrow{U_f} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes (|0+f(x)\rangle - |1+f(x)\rangle)$$
$$= \frac{1}{2^{\frac{n+1}{2}}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes (|0\rangle - |1\rangle)$$
$$\xrightarrow{H_n} \frac{1}{2^{\frac{2n+1}{2}}} \sum_{y \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)+xy} |y\rangle \otimes (|0\rangle - |1\rangle) = |z\rangle$$

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
$$\frac{1}{2^{\frac{2n+1}{2}}} \sum_{y \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \cdot (-1)^{xy} |y\rangle = \frac{1}{2^{\frac{2n+1}{2}}} (-1)^{f(0)} \Big(2^n |0^n\rangle + \underbrace{\sum_{\substack{y \in \{0,1\}^n \\ y \neq 0^n}} \sum_{x \in \{0,1\}^n} (-1)^{xy} |y\rangle}_{0}\Big)$$
$$\Rightarrow |z\rangle = \frac{1}{\sqrt{2}} (-1)^{f(0^n)} |0^n\rangle \otimes (|0\rangle - |1\rangle)$$

D.h. für konstantes f liefert die Messung der ersten n Qubits 0^n.

2. Fall: f balanciert:

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

$\Rightarrow$ 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

Das Bernstein-Vazirani Problem (1983)

Gegeben: Funktion $f_a: \mathbb{F}_2^n \to \mathbb{F}_2$ mit $a\in\{0,1\}^n$ im Orakel-Modell

$$x \mapsto ax = \sum_{i=1}^n a_i x_i \mod 2$$

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

- Klassisch:

Untere Schranke: Jeder Aufruf von f liefert 1 Bit an Information.

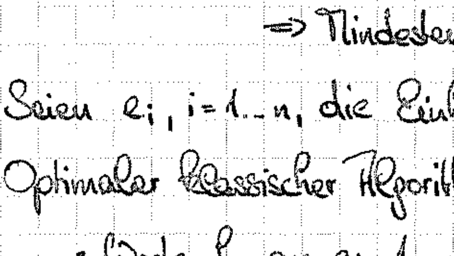
$\Rightarrow$ Mindestens n Aufrufe von f zur Bestimmung von a notwendig.

Seien e_i, $i=1..n$, die Einheitsvektoren.

Optimaler klassischer Algorithmus:

- Werte f_a an e_i, $1..n$, 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: $|0^n 1\rangle \xmapsto{H_n \otimes H} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes (|0\rangle - |1\rangle)$

$$\xmapsto{U_{f_a}} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes (|0\rangle - |1\rangle)$$

$$\xmapsto{H_n \otimes I_2} \frac{1}{2^{n+\frac{1}{2}}} \sum_{y \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} (-1)^{xa} \cdot (-1)^{xy} |y\rangle \otimes (|0\rangle - |1\rangle) = |\varphi\rangle$$

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

D.h. $|\varphi\rangle = \frac{1}{\sqrt{2}} |a\rangle \otimes (|0\rangle - |1\rangle)$

Messung der ersten n Qubits liefert a mit Wahrscheinlichkeit 1. ∎

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

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 $x_1, \dots, x_k$ 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 $X_{i,j} = \begin{cases} 1 & \text{falls } f(x_i) = f(x_j) \\ 0 & \text{sonst} \end{cases}$ $\quad Pr(X_{i,j} = 1) = \frac{1}{2^n - 1}$

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

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