$y_1 = (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})$
$y_2 = x_1 \wedge x_2$

8.1 Universelle Mengen

Definition (universell): Sei S eine Menge von Booleschen Funktionen, die eine konstante Anzahl von Bits auf eine Konstante Anzahl von Bits abbilden. S ist universell, falls jede Boolesche Funktion $\mathbb{F}_2^n \to \mathbb{F}_2$ durch Verknüpfung von Elementen aus S realisiert werden kann.

Übung: Sei S universell. Dann kann jede Funktion $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ mittels S realisiert werden.

Satz: $S_U = \{\wedge, \neg, \mathtt{c}\}$ ist eine universelle Menge.

Beweis: Wir definieren die Funktion $M_a, a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$. Vermöge $M_a(x_1, \ldots, x_n) = \varphi_1(x_1) \wedge \varphi_2(x_2) \wedge \cdots \wedge \varphi_n(x_n)$ für $\varphi_i(x_i) = \begin{cases} x_i & \text{für } a_i = 1 \\ \overline{x_i} & \text{für } a_i = 0 \end{cases}$

D.h. M_a ist die charakteristische Funktion $M_a(x_1, \ldots, x_n) = \begin{cases} 1 & \text{falls } x = a \\ 0 & \text{sonst} \end{cases}$

Sei $\mathtt{T} = \{a \in \mathbb{F}_2^n | f(a) = 1\}$. Dann gilt $f = \bigvee_{a \in \mathtt{T}} M_a(x_1, \ldots, x_n) = \neg(\bigwedge_{a \in \mathtt{T}} \neg M_a(x_1, \ldots, x_n))$.

D.h. wir können f als $\neg, \wedge$-Verknüpfung von Kopien von $(x_1, \ldots, x_n)$ darstellen.

Beispiel (obiger Addierer): Für Ausgabebit y_1 gilt:
$\mathtt{T} = \{(0,1),(1,0)\} \Rightarrow y_1 = \bigvee_{a \in \mathtt{T}} M_a(x_1 x_2) = (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2}) = \neg(\neg((\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})))$
$= \neg(\overline{(\overline{x_1} \wedge x_2)} \wedge \overline{(x_1 \wedge \overline{x_2})})$

Beobachtung: Seien S_1, S_2 Mengen von booleschen Funktionen und S_1 universell.
Falls jedes $s \in S_1$ durch eine Verknüpfung aus S_2 darstellbar ist, dann ist S_2 universell.

Seien $\text{nand}(x_1, x_2) = \overline{x_1 \wedge x_2}$.

Satz: $S = \{\text{nand}, \mathtt{c}\}$ ist universell

Beweis: Wir stellen $\neg$ und $\wedge$ als Verknüpfung durch nand-Funktionen dar.
$\neg$: $\text{nand}(x, x) = \overline{x \wedge x} = \overline{x}$ (Anwendung von c, um x zu duplizieren)
$\wedge$: $\text{nand}(\text{nand}(x_1, x_2), \text{nand}(x_1, x_2)) = \text{nand}(\overline{x_1 \wedge x_2}, \overline{x_1 \wedge x_2}) = x_1 \wedge x_2$.

8.2 Uniforme / nicht-Uniforme Schaltkreisfamilien

Bezeichnung Wir bezeichnen mit C_n Schaltkreise mit n Eingabeknoten.
Wir nennen $C = \{C_n\}_{n \in \mathbb{N}}$ eine Schaltkreisfamilie.

Definition: Eine boolesche Funktion $f_n, n \in \mathbb{N}$ hat nicht-uniforme Schaltkreiskomplexität $\mathcal{O}(g(n))$ bzgl. einer universellen Menge S, falls es eine Schaltkreisfamilie $\{C_n\}_{n \in \mathbb{N}}$ über S mit Komplexität $\mathcal{O}(g(n))$ gibt, die f_n berechnet.

Beobachtung Nach 8.1 können alle Funktionen $\mathbb{F}_2^n \to \mathbb{F}_2$ mittels einer nicht-uniformen Schaltkreisfamilie $C = \{C_n\}_{n \in \mathbb{N}}$ berechnet werden.

Insbesondere existiert C mit: $C_n = \begin{cases} 1 & \text{falls DTM } M_n \text{ auf Eingabe } M_n \text{ hält} \\ 0 & \text{sonst} \end{cases}$

D.h. C_n entscheidet das im Touringmaschinen-Modell nicht entscheidbare Halteproblem.
Problem: Konstruktion von C_n erfordert die Kenntnis der Funktionswerte der f_n.

Definition (uniformes Modell): Eine Schaltkreisfamilie $\{C_n\}_{n \in \mathbb{N}}$ heißt uniform, falls es eine DTM gibt, die für alle $n \in \mathbb{N}$ bei Eingabe 1^n in Zeit und Platz $\text{poly}(n)$ C_n ausgibt. Eine boolesche Funktion $f_n, n \in \mathbb{N}$ hat uniforme Schaltkreiskomplexität $\mathcal{O}(g(n))$, falls es eine uniforme Schaltkreisfamilie $\{C_n\}_{n \in \mathbb{N}}$ gibt, die f_n berechnet.

8.3 Die Klasse $\mathcal{P}$

Bezeichnung: $\text{poly}(n) = \mathcal{O}(n^c)$ für konstantes c.

Definition ($\mathcal{P}$): Die Klasse $\mathcal{P}$ besteht aus allen booleschen Funktionen $f_n, n \in \mathbb{N}$ mit uniformer Schaltkreiskomplexität $\text{poly}(n)$

Beispiel: $f_n = \bigwedge_{i=1}^{n} x_i$ hat uniforme Schaltkreiskomplexität $\mathcal{O}(n)$ bezüglich $S_u = \{\wedge, \neg, \text{c}\}$.
$f_n = \bigvee_{i=1}^{n} x_i$ hat uniforme Schaltkreiskomplexität $\mathcal{O}(n)$ bezüglich $S_u = \{\wedge, \neg, \text{c}\}$.

8.4 Die Klasse $\mathcal{BPP}$

Definition ($\mathcal{BPP}$): Die Klasse $\underline{\mathcal{BPP}}$ besteht aus allen booleschen Funktionen $f_n, n \in \mathbb{N}$, für die es eine uniforme Schaltkreisfamile $\{C_n\}_{n\in\mathbb{N}}$ gibt mit:

- C_n hat Größe $\text{poly}(n)$
- $\exists m \in \text{poly}(n) : y \in_R \mathbb{F}_2^m \; \forall \; x \in \mathbb{F}_2^n : \text{Ws.}_y(C(x,y) = f_n(x)) \geq \frac{2}{3}$

Beispiel: Sei x eine n-bit Zahl, $f_n(x) = \begin{cases} 1 & \text{falls } x \text{ prim} \\ 0 & \text{sonst} \end{cases}$
Miller-Rabin Test liefert uniforme Schaltkreisfamilie mit Ws. $(C(x,y) = f_n(x)) \geq \frac{3}{4}$

8.5 Die Klasse $\mathcal{NP}$

Definition ($\mathcal{NP}$): Die Klasse $\mathcal{NP}$ besteht aus allen booleschen Funktionen $f_n, n \in \mathbb{N}, \mathbb{F}_2^n \to \mathbb{F}_2$, für die es eine uniforme Schaltkreisfamilie $\{C_n\}_{n\in\mathbb{N}}$ gibt mit:

- C_n hat Größe $\text{poly}(n)$
- $\exists m \in \text{poly}(n) \; \forall x \in \mathbb{F}_2^n : f_n(x) = 1 \Leftrightarrow \exists \; y \in \mathbb{F}_2^m : C(x,y) = 1$

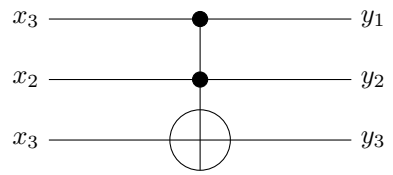
Beispiel: $f_n = X_{\texttt{SAT}}(\langle\phi\rangle) = \begin{cases} 1 & \text{falls } \langle\phi\rangle \in \texttt{SAT} \\ 0 & \text{sonst} \end{cases}$
$X_{\texttt{SAT}} \in \mathcal{NP}$, denn für jedes $\langle\phi\rangle \in \texttt{SAT}$ mit m Variablen gibt es eine erfüllbare Belegung $y \in \mathbb{F}_2^m$. Der Schaltkreis C_n wertet ϕ mit Belegung y aus.

9 Quantenschaltkreiskomplexitäten

9.1 Reversible Schaltkreise

Definition (Reversibel): Sei $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ eine beliebige boolesche Funktion.
Die reversible Einbettung U_f von f ist definiert als $U_f : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}, (x,y) \mapsto (x, f(x)+y)$
Beachte: $U_f(U_f(x,y)) = U_f(x, f(x)+y) = (x, f(x)+f(x)+y) = (x,y)$, d.h. U_f ist Permutation.
Wir bezeichnen Permutationen auch als reversible Funktion. Sie werden durch Permutationsmatrizen beschrieben.

Beispiel: $\wedge : \mathbb{F}_2^2 \to \mathbb{F}_2, (x_1, x_2) \mapsto x_1 x_2$
$\texttt{T} = U_\wedge : \mathbb{F}_2^3 \to \mathbb{F}_2^3, (x_1, x_2, x_3) \mapsto (x_1, x_2, x_1 x_2 + x_3) = (x_1, x_2, x_1 \wedge x_2 \oplus x_3)$
Toffoli-Funktion T



NOT auf $x_3 \Leftrightarrow x_1 = x_2 = 1$

$I : \mathbb{F}_2 \to \mathbb{F}_2, x_1 \mapsto x_1$
$\texttt{CNOT} = U_I : \mathbb{F}_2^2 \to \mathbb{F}_2^2, (x_1, x_2) \mapsto (x_1, x_1 + x_2)$
Man beachte: $\texttt{CNOT}(x_1, 0) \mapsto (x_1, x_1)$ liefert Kopierfunktion c für $x_1 \in \mathbb{F}_2$

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.

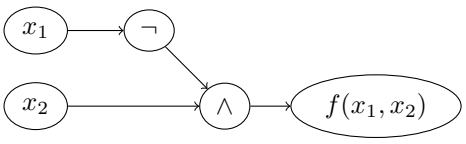
Satz: Sei $C = \{C_n\}_{n\in\mathbb{N}}$ eine uniforme Schaltkreisfamilie über $S = \{\wedge, \neg\}$ der Größe $\mathcal{O}(g(n))$, die $f_n, n \in \mathbb{N}$ berechnet. Dann gibt es eine uniforme reversible Schaltkreisfamilie C_r über $\{\mathtt{T}, 0, 1\}$ der Größe $\mathcal{O}(g(n))$, die $f_n^r : \mathbb{F}_2^{n+m+l} \to \mathbb{F}_2^{n+m+l}$ 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

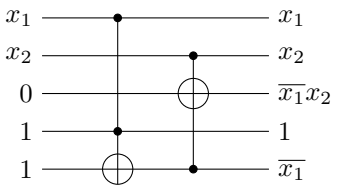
- $\wedge$-Gatter mit $\mathtt{T}(x_1, x_2, 0) = (x_1, x_2, x_1x_2)$
- $\neg$-Gatter mit $\mathtt{T}(x_1, 1, 1) = x_1, 1, 1 - x_1)$

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