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

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

Beweis: Wir stellen $\neg$ und $\wedge$ als Verknüpfung durch nand-Funktionen dar.

$\neg$: $nand(x, x) = \overline{x \wedge x} = \overline{x}$ (Anwendung von c, um x zu duplizieren)

$\wedge$: $nand(nand(x_1, x_2), nand(x_1, x_2)) = nand(\overline{x_1 \wedge x_2}, \overline{x_1 \wedge x_2}) = x_1 \wedge x_2$

Bezeichnung: Wir bezeichnen mit C_n Schaltkreise mit n Eingabeknoten.

Wir nennen $C = \{C_n\}_{n \in \mathbb{N}}$ eine Schaltkreisfamilie.

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

Beobachtung: Nach Satz S. 19 können alle Fkt. $\mathbb{F}_2^n \to \mathbb{F}_2$ 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 Turingmaschinen-Modell nicht entscheidbare Halteproblem.

Problem: Konstruktion von C_n erfordert die Kenntnis der Funktionswerte der f_n.

Def. (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 $poly(n)$ C_n ausgibt.

Eine boolesche Fkt. f_n, $n \in \mathbb{N}$, hat uniforme Schaltkreiskomplexität $O(g(n))$, falls es eine uniforme Schaltkreisfamilie $\{C_n\}_{n \in \mathbb{N}}$ mit Größe $O(g(n))$ gibt, die f_n berechnet.

Bezeichnung: $poly(n) = O(n^c)$ für konstantes c.

Def. (P): Die Klasse P besteht aus allen booleschen Fkt. f_n, $n \in \mathbb{N}$, mit uniformer Schaltkreiskomplexität $poly(n)$.

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

$f_n = \bigvee_{i=1}^{n} x_i$ ——— " ———

Def.: Die Klasse BPP besteht aus allen booleschen Funktionen $f_n, n\in\mathbb{N}$, für die es eine uniforme Schaltkreisfamilie $\{C_n\}_{n\in\mathbb{N}}$ gibt mit:

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

Bsp.: 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 $\mathrm{Ws}(C(x,y) = f_n(x)) \geq \frac{3}{4}$.

Def. (NP): Die Klasse NP besteht aus allen booleschen Fkt. 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 poly(n)
- $\exists m = \mathrm{poly}(n)\ \forall x\in\mathbb{F}_2^n: f_n(x) = 1 \Leftrightarrow \exists y\in\mathbb{F}_2^m: C(x,y) = 1$.

Bsp.: $f_n = \chi_{SAT}(\langle\phi\rangle) = \begin{cases} 1 & \text{falls } \langle\phi\rangle\in SAT \\ 0 & \text{sonst}\end{cases}$

$\chi_{SAT}\in NP$, denn für jedes $\langle\phi\rangle\in SAT$ mit m Variablen gibt es eine erfüllbare Belegung $y\in\mathbb{F}_2^m$.
Der Schaltkreis C_n wertet ϕ mit Belegung y aus.

Reversible Schaltkreise

Def. (reversibel): Sei $f: \mathbb{F}_2^n \to \mathbb{F}_2^m$ eine beliebige boolesche Funktion.

Die reversible Einbettung $\mathcal{U}_f$ von f ist definiert als $\mathcal{U}_f: \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$, $(x,y) \mapsto (x, f(x)+y)$

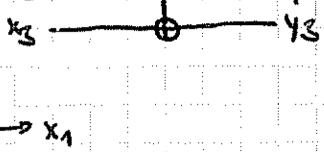
Beachte: $\mathcal{U}_f(\mathcal{U}_f(x,y)) = \mathcal{U}_f(x, f(x)+y) = (x, f(x)+f(x)+y) = (x,y)$, d.h. $\mathcal{U}_f$ ist Permutation.

Wir bezeichnen Permutationen auch als reversible Fkt. Sie werden durch Perm.-Matrizen beschrieben

Bsp.: $\wedge: \mathbb{F}_2^2 \to \mathbb{F}_2$, $(x_1,x_2)\mapsto x_1x_2$

$T = \mathcal{U}_\wedge: \mathbb{F}_2^3 \to \mathbb{F}_2^3$, $(x_1,x_2,x_3) \longmapsto (x_1, x_2, x_1x_2 + x_3) = (x_1, x_2, x_1\wedge x_2 \oplus x_3)$

Toffoli-Funktion T



NOT auf x_3 gdw. $x_1 = x_2 = 1$

$I: \mathbb{F}_2 \to \mathbb{F}_2$, $x_1 \longmapsto x_1$

$CNOT = \mathcal{U}_I: \mathbb{F}_2^2 \to \mathbb{F}_2^2$, $(x_1,x_2) \longmapsto (x_1, x_1+x_2)$

Man beachte: $CNOT(x_1, 0) \longmapsto (x_1,x_1)$ liefert Kopierfkt. c für $x_1\in\mathbb{F}_2$

Def (r-universell): Sei R eine Menge von reversiblen Booleschen Fkt, die auf einer konstanten Anzahl von Bits operieren. R heißt <u>r-universell</u>, falls jede reversible Fkt. als Verknüpfung von Elementen aus R, Hilfsvariablen und Konstanten 0, 1 dargestellt werden kann.

<u>Satz</u>: $\{T\}$ ist r-universell.

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