Beweis: Es gilt

$$Ws(b=1) = Ws(b=1 \mid a=a') \cdot Ws(a=a') + Ws(b=1 \mid a\neq a') \cdot Ws(a\neq a')$$
$$= 0 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4},$$

denn im Fall $a=a'$ misst Bob stets den von Alice gesendeten Basiszustand ($b=0$), im Fall $a\neq a'$ misst Bob einen anderen Zustand mit Ws. $\frac{1}{2}$.

D.h. also, dass wir im Erwartungswert $4n$ Protokolldurchläufe benötigen, bis n Schlüsselbits generiert sind. Es bleibt zu zeigen, dass die erzeugten Schlüsselbits korrekt sind, d.h. $a=1-a'$.

<u>Satz</u>: $Ws(a=1-a' \mid b=1) = 1$

Beweis: Es gilt $Ws(a=1-a' \mid b=1) \cdot Ws(b=1) = Ws(b=1 \mid a=1-a') \cdot Ws(a=1-a')$

$$\Rightarrow Ws(a=1-a' \mid b=1) = \frac{Ws(b=1 \mid a=1-a') \cdot Ws(a=1-a')}{Ws(b=1)} = \frac{\frac{1}{2}\cdot\frac{1}{2}}{\frac{1}{4}} = 1$$

D.h. falls $b=1$, so müssen a und a' verschiedene Bits sein.

Damit erhalten Alice und Bob dasselbe Bit $a=1-a'$.

Boolesche Schaltkreise

Ziel: Berechne Boolesche Funktionen $f_n: \mathbb{F}_2^n \to \mathbb{F}_2^m$, $n\in\mathbb{N}$

Bsp.: Und $\wedge: \mathbb{F}_2^2 \to \mathbb{F}_2$, $(x_1,x_2) \xmapsto{\wedge} x_1\wedge x_2 = x_1x_2$ bzw. $\mathbb{F}_2^n \to \mathbb{F}_2$, $(x_1,\dots,x_n) \mapsto (((x_1\wedge x_2)\wedge x_3)\dots x_n)$

Oder $\vee: \mathbb{F}_2^2 \to \mathbb{F}_2$, $(x_1,x_2) \xmapsto{\vee} x_1\vee x_2 = x_1+x_2+x_1x_2$ bzw. $\mathbb{F}_2^n \to \mathbb{F}_2$, $(x_1,\dots,x_n) \mapsto (((x_1\vee x_2)\vee x_3)\dots x_n)$

Nicht $\neg: \mathbb{F}_2 \to \mathbb{F}_2$, $x \xmapsto{\neg} 1-x$ Schreibweise auch: $\bar{x}$

Kopierfunktion $c: \mathbb{F}_2 \to \mathbb{F}_2^2$, $x \xmapsto{c} (x,x)$

Entscheiden von Sprachen L: $\chi_L: \mathbb{F}_2^n \to \mathbb{F}_2$, $\chi_L(\omega) = \begin{cases} 1 & \text{falls } \omega\in L \\ 0 & \text{sonst} \end{cases}$

z.B. $SAT = \{\langle\phi\rangle \mid \phi \text{ ist erfüllbare Boolesche Formel}\}$, mit $\langle\phi\rangle$ n-Bit Kodierung von ϕ

<u>Def.</u> (Boolescher Schaltkreis): Sei S eine Menge von Booleschen Funktionen, die eine konstante Anzahl von Eingabebits auf eine konstante Anzahl von Ausgabebits abbildet (z.B. $S=\{\wedge,\vee,\neg\}$).

Ein Boolescher Schaltkreis über S ist ein azyklisches, gerichteter Graph $G=(V,E)$ mit:

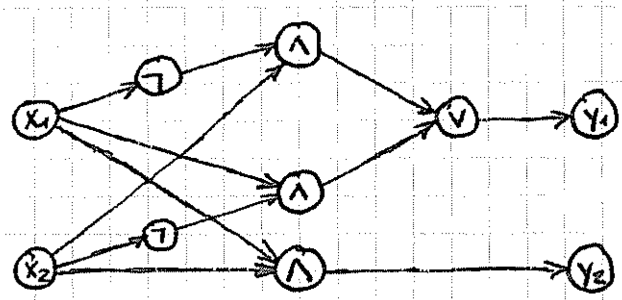
- Die Knoten V sind gelabelt mit Eingabe-/Ausgabevariablen oder Elementen aus S.

- Eingabeknoten haben Eingrad 0. Ausgabeknoten haben Eingrad 1, Ausgrad 0.
- Knoten mit Label $s \in S$, $s: \mathbb{F}_2^n \to \mathbb{F}_2^m$ haben Eingrad n und Ausgrad m.

Die Komplexität des Booleschen Schaltkreises ist definiert als $|V|+|E|$ (bezüglich S).

Bsp: Addierer $f(x_1,x_2)=(y_1,y_2)$ mit $y_1 = x_1 \oplus x_2$, y_2 Übertrag

x_1	x_2	y_1	y_2
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1



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

$y_2 = x_1 \wedge x_2$

Komplexität bezüglich $\{\wedge, \vee, \neg\}$: $|V|+|E| = 10 + 12 = 22$

Def (universell). Sei S eine Menge von Booleschen Fkt., die eine konstante Anzahl von Bits auf eine konstante Anzahl von Bits abbilden. S ist <u>universell</u>, 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 Fkt. $f: \mathbb{F}_2^n \to \mathbb{F}_2^m$ mittels S realisiert werden.

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

Beweis: Wir definieren die Fkt. M_a, $a = (a_1, \dots, a_n) \in \mathbb{F}_2^n$ vermöge

$$M_a(x_1,\dots,x_n) = \phi_1(x_1) \wedge \phi_2(x_2) \wedge \dots \phi_n(x_n) \qquad \text{für } \phi_i(x_i) = \begin{cases} x_i & \text{für } a_i = 1 \\ \overline{x_i} & \text{für } a_i = 0 \end{cases}$$

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

Sei $T = \{ a \in \mathbb{F}_2^n \mid f(a) = 1\}$. Dann gilt

$$f = \bigvee_{a \in T} M_a(x_1,\dots,x_n) = \neg\Big(\bigwedge_{a \in T} \neg M_a(x_1,\dots,x_n)\Big).$$

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

Bsp.: (obiger Addierer) Für Ausgabebit y_1 gilt:

$$T = \{(0,1),(1,0)\} \Rightarrow y_1 = \bigvee_{a \in T} M_a(x_1,x_2) = (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})$$
$$= \neg(\neg((\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2}))) = \neg(\overline{(\overline{x_1} \wedge x_2)} \wedge \overline{(x_1 \wedge \overline{x_2})})$$

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.

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

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

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

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

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

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

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

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

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