In jedem Durchlauf wird ein Schlüsselbit generiert gdw. $b = 1$ gilt.

Satz: Ws. $(b = 1) = \frac{1}{4}$

Beweis: Es gilt

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

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 $a = 1 - a'$.

Satz: Ws. $(a = 1 - a'|b = 1) = 1$

Beweis: Es gilt Ws. $(a = 1 - a'|b = 1 \cdot$ Ws. $(b = 1) =$ Ws. $(b = 1|a = 1 - a') \cdot$ Ws. $(a = 1 - a')$
$\Rightarrow$ Ws. $(a = 1 - a'|b = 1) = \frac{\text{Ws.}\,(b=1|a=1-a')\cdot\text{Ws.}\,(a=1-a')}{\text{Ws.}\,(b=1)} = \frac{\frac{1}{2}\cdot\frac{1}{2}}{\frac{1}{4}} = 1$
D.h. falls $b = 1$, so müssen a und a' verschiedene Bits sein. Damit erhalten Alice und Bob dasselbe Bit $a = 1 - a'$

8 Boolesche Schaltkreise, Schaltkreiskomplexitäten

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

Beispiel: Und $\wedge : \mathbb{F}_2^2 \to \mathbb{F}_2, (x_1, x_2) \overset{\wedge}{\longmapsto} x_1 \wedge x_2 = x_1x_2$ bzw. $\mathbb{F}_2^n \to \mathbb{F}_2$,
$(x_1, \ldots, x_n) \mapsto (((x_1 \wedge x_2) \wedge x_3) \ldots x_n)$

Oder $\vee : \mathbb{F}_2^2 \to \mathbb{F}_2, (x_1, x_2) \overset{\vee}{\longmapsto} x_1 \vee x_2 = x_1 + x_2 + x_1x_2$ bzw. $\mathbb{F}_2^n \to \mathbb{F}_2$,
$(x1, \ldots, x_n) \mapsto (((x_1 \vee x_2) \vee x_3) \ldots x_n)$

Nicht $\neg : \mathbb{F}_2 \to FZ, x \overset{\neg}{\longmapsto} 1 - x$ Schreibweise auch: $\overline{x}$

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

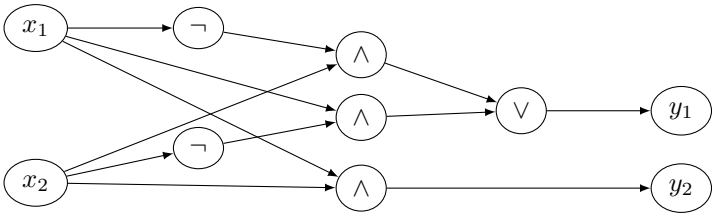
Entscheiden von Sprachen $\mathtt{L} : X_{\mathtt{L}} : \mathbb{F}_2^n \to \mathbb{F}_2, X_{\mathtt{L}}(\omega) = \begin{cases} 1 & \text{falls } \omega \in \mathtt{L} \\ 0 & \text{sonst} \end{cases}$

Definition (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 azyklischer, 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).

Beispiel: 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	1	1



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

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

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.