


Seien α , β aussagenlogische Formeln.

α heißt **erfüllbar**,
falls $\alpha^I = 1$ für wenigstens eine Belegung I .

α heißt **gültig** oder **Tautologie**,
falls $\alpha^I = 1$ für alle Belegungen I .

α und β heißen **äquivalent**, i.Z. $\alpha \equiv \beta$,
falls $\alpha^I = \beta^I$ für alle Belegungen I .

α heißt **logische Folgerung** von β , i.Z. $\beta \Vdash \alpha$,
falls $\alpha^I \geq \beta^I$ für alle Belegungen I .

Spieler **A**  ...  Spieler **B**
 n Streichhölzer

$n \in \mathbb{N}$
 $n \geq 1$

- Spieler ziehen abwechselnd, beginnend mit Spieler **A**
- pro Spielzug: entferne **1** oder **2** Streichhölzer
- Verlierer ist, wer das letzte Streichholz entfernt

gesucht: Gewinnstrategie für Spieler **A** (falls existent)

verwende Aussagensymbole x_1, x_2, x_3, \dots

$x_n \hat{=}$ "es gibt eine Gewinnstrategie für n Streichhölzer"

Spieler **A**  ...  Spieler **B**
 n Streichhölzer

$n \in \mathbb{N}$
 $n \geq 1$

- Spieler ziehen abwechselnd, beginnend mit Spieler **A**
- pro Spielzug: entferne **1** oder **2** Streichhölzer
- Verlierer ist, wer das letzte Streichholz entfernt

Spieler **A** hat Gewinnstrategie genau dann, wenn

$$\neg x_1 \wedge x_2 \wedge \bigwedge_{3 \leq i \leq n} (x_i \leftrightarrow \neg x_{i-1} \vee \neg x_{i-2}) \Vdash x_n$$

Spieler **A** zieht so, dass **B**
keine Gewinnstrategie hat

$$\alpha_n = \neg x_1 \wedge x_2 \wedge \bigwedge_{3 \leq i \leq n} (x_i \leftrightarrow \neg x_{i-1} \vee \neg x_{i-2})$$

Spieler **A** hat Gewinnstrategie für n Streichhölzer } $\Leftrightarrow \alpha_n \Vdash x_n \Leftrightarrow n \bmod 3 \neq 1$

$$\alpha_3 = \neg x_1 \wedge x_2 \wedge (x_3 \leftrightarrow \neg x_2 \vee \neg x_1) \Vdash x_3$$

$$\alpha_4 = \alpha_3 \wedge (x_4 \leftrightarrow \neg x_3 \vee \neg x_2) \Vdash \neg x_4$$

$$\alpha_5 = \alpha_4 \wedge (x_5 \leftrightarrow \neg x_4 \vee \neg x_3) \Vdash x_5$$

Gewinnstrategie für n Streichhölzer mit $n \bmod 3 \neq 1$:
entferne $i \in \{1, 2\}$ Streichhölzer, so dass $n - i \bmod 3 = 1$

$$\neg x \wedge ((\neg x \vee z) \leftrightarrow y) \Vdash y$$

richtig. Sei \mathbf{I} ein Modell für $\neg x \wedge ((\neg x \vee z) \leftrightarrow y)$.

$$\left. \begin{array}{l} x^{\mathbf{I}} = 0 \\ ((\neg x \vee z) \leftrightarrow y)^{\mathbf{I}} = 1 \end{array} \right\} \implies 1 = (\neg x \vee z)^{\mathbf{I}} = y^{\mathbf{I}}$$

$$x \wedge \neg y \Vdash (x \vee y) \wedge (\neg x \vee \neg y)$$

richtig, da stets gilt:

$$x \wedge \neg y \Vdash (x \vee \dots) \wedge (\dots \vee \neg y)$$

$x \wedge (x \rightarrow y) \wedge \neg y \Vdash \text{false}$

richtig, da $x \wedge (x \rightarrow y) \wedge \neg y$ unerfüllbar

für jede Formel α gilt:

α unerfüllbar gdw $\alpha \Vdash \text{false}$

gdw $\alpha \Vdash \beta$ für jede Formel β

gdw $\alpha \equiv \text{false}$

gdw $\neg\alpha$ ist gültig

Für jede Formelmenge \mathcal{F} und Formel α gilt:

$$\mathcal{F} \Vdash \alpha \text{ gdw } \mathcal{F} \cup \{\neg\alpha\} \text{ ist unerfüllbar}$$

Für endliche Formelmengen gilt:

$$\{\beta_1, \dots, \beta_n\} \Vdash \alpha$$

$$\text{gdw } \{\beta_1, \dots, \beta_n, \neg\alpha\} \text{ ist unerfüllbar}$$

$$\text{gdw } \beta_1 \wedge \dots \wedge \beta_n \wedge \neg\alpha \text{ ist unerfüllbar}$$

$$\text{gdw } \beta_1 \wedge \dots \wedge \beta_n \rightarrow \alpha \text{ ist gültig}$$

$$\neg(\beta \wedge \neg\alpha) \equiv \neg\beta \vee \neg\neg\alpha \equiv \neg\beta \vee \alpha = \beta \rightarrow \alpha$$

Für alle Formeln α, β gilt:

$\beta \Vdash \alpha$ gdw $\beta \rightarrow \alpha$ ist gültig

gdw $\beta \rightarrow \alpha \equiv \mathbf{true}$

gdw $\beta \wedge \neg \alpha$ unerfüllbar

$\beta \rightarrow \alpha \stackrel{\text{def}}{=} \neg \beta \vee \alpha$ Def. des Implikationsoperators

$\neg(\neg \beta \vee \alpha) \equiv \neg \neg \beta \wedge \neg \alpha \equiv \beta \wedge \neg \alpha$

Für alle Formeln α, β gilt:

$$\begin{aligned} \alpha \equiv \beta & \quad \text{gdw} \quad \alpha \leftrightarrow \beta \text{ ist gültig} \\ & \quad \text{gdw} \quad \alpha \Vdash \beta \text{ und } \beta \Vdash \alpha \\ & \quad \text{gdw} \quad \alpha \oplus \beta \text{ unerfüllbar} \end{aligned}$$

Paritätsoperator \oplus (XOR)

$$\alpha \oplus \beta \stackrel{\text{def}}{=} (\alpha \wedge \neg \beta) \vee (\neg \alpha \wedge \beta) \equiv \neg(\alpha \leftrightarrow \beta)$$

Erfüllbarkeitsproblem (SAT “satisfiability problem”)

- gegeben: aussagenlogische Formel α
- gefragt: ist α erfüllbar ?

Gültigkeitsproblem (VALID “validity problem”)

- gegeben: aussagenlogische Formel α
- gefragt: ist α gültig ?

Folgerungsproblem

- gegeben: aussagenlogische Formeln α und β
- gefragt: gilt $\beta \Vdash \alpha$?

zentrale Fragestellung, z.B. für Verifikation,
deduktive Datenbanken, Logikprogrammierung

Erfüllbarkeitsproblem (SAT “satisfiability problem”)

⋮

Gültigkeitsproblem (VALID “validity problem”)

⋮

Folgerungsproblem

⋮

Äquivalenzproblem

- gegeben: aussagenlogische Formeln α und β
- gefragt: gilt $\alpha \equiv \beta$?

naive Lösung: Inspektion der Wertetafeln

Folgerungsproblem via SAT

312B

Eingabe für das Folgerungsproblem:
zwei Formeln α und β

Eingabe für Erfüllbarkeitsproblem: Formel $\beta \wedge \neg\alpha$

SAT-Beweiser
"ist $\beta \wedge \neg\alpha$ erfüllbar?"

nein, $\beta \wedge \neg\alpha$ unerfüllbar

ja, $\beta \wedge \neg\alpha$ erfüllbar

ja, $\beta \Vdash \alpha$

nein, $\beta \not\Vdash \alpha$

gegeben: aussagenlogische Formel α ,
Belegung \mathbf{I}

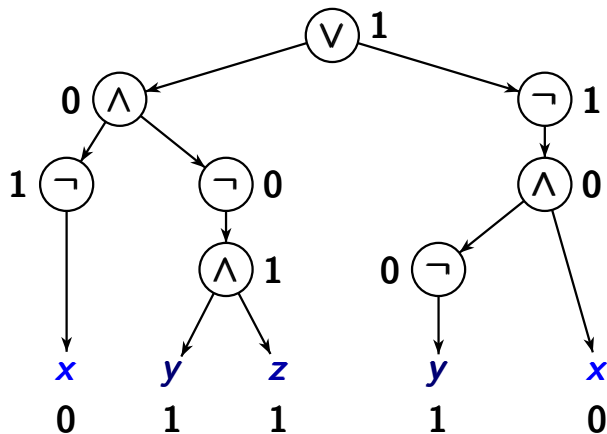
gefragt: ist \mathbf{I} ein Modell für α , d.h., ist $\alpha^{\mathbf{I}} = \mathbf{1}$?

Evaluierungsalgorithmus:

1. erstelle den **Syntaxbaum** für α
2. **bewerte** die Knoten des Syntaxbaums gemäß \mathbf{I} in Bottom-up-Manier
3. prüfe, ob die **Wurzel** des Syntaxbaums mit $\mathbf{1}$ (“wahr”) bewertet wurde

Formel $\alpha = (\neg x \wedge \neg(y \wedge z)) \vee \neg(\neg y \wedge x)$

Belegung I mit $x^I = 0$, $y^I = 1$, $z^I = 1 \rightsquigarrow \alpha^I = 1$



Syntaxbaum \cong Schaltnetz

341

$$\text{Formel } \alpha = (\neg x \vee (y \wedge z)) \wedge \neg z$$

nicht-atomare Teilformel \cong innerer Knoten \cong Gatter im Schaltnetz

