# Eine bekannte Termalgebra (2023-04-17)

Die Signatur $\mathcal{S}$ bestehe aus den Operatoren: $o_{/0}$ und $s_{/1}$ .

Jede Variablenmenge $\mathcal{V}$ liefert einen kleinsten Fixpunkt $\boldsymbol{Term}(\mathcal{S},\mathcal{V})$ der BNF

$$\boldsymbol{T} ::= \mathcal{V} \mid o \mid s(\boldsymbol{T})$$

Von besonderem Interesse ist der Fall $\mathcal{V} = \emptyset$ ; die sog. Grundterme enthalten keine Variablen. Die Iteration nimmt dann folgende Form an:

$$\boldsymbol{T}_0 := \emptyset \quad , \quad \boldsymbol{T}_{n+1} := \{o\} \cup s(\boldsymbol{T}_n) \quad , \quad \text{konkret also}$$
$$\boldsymbol{T}_1 = \{o\} \ , \ \boldsymbol{T}_2 = \{o, s(o)\} \ , \ \boldsymbol{T}_3 = \{o, s(o), s(s(o))\} \ldots \ \text{bzw.}$$
$$\boldsymbol{T}_n = \{\, s^k(o) \, : \, k < n \,\} \ \text{also} \ \boldsymbol{Term}(\mathcal{S},\emptyset) = \bigcup_{n\in\mathbb{N}} \boldsymbol{T}_n = \{\, s^k(o) \, : \, k \in \mathbb{N} \,\}$$

was zu $\mathbb{N}$ isomorph ist, wobei $o$ als $0$ und $s$ als $\boldsymbol{succ}$ interpretiert wird.

# Teilmengen von $\mathbb{N}$ als Konsequenzen des Rekursionssatzes

Auf der Menge $\mathbb{B} = \{0, 1\}$ der Wahrheitswerte existieren 8 mögliche $\mathcal{S}$-Strukturen: die beiden Konstanten $c \in \mathbb{B}$ lassen sich mit den vier möglichen Abbildungen $\mathbb{B} \xrightarrow{f} \mathbb{B}$ kombinieren.

Die einzige Abbildung $\emptyset = \mathcal{V} \longrightarrow \mathbb{B}$ liefert in jedem dieser Fälle einen eindeutigen $\mathcal{S}$-Homomorphismus $\mathbb{N} \xrightarrow{\langle c, f \rangle} \mathbb{B}$, bzw. eine Teilmenge von $\mathbb{N}$:

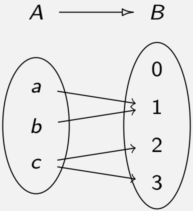
$$\begin{tikzcd}
1 \arrow[r, "0"] \arrow[d, dotted, "\langle c, f \rangle^0 = \boldsymbol{id}_1"'] & \mathbb{N} \arrow[d, dotted, "\langle c, f \rangle"] & \mathbb{N} \arrow[l, "\boldsymbol{succ}"'] \arrow[d, dotted, "\langle c, f \rangle"] \\
1 \arrow[r, "c"'] & \mathbb{B} & \mathbb{B} \arrow[l, "f"]
\end{tikzcd}$$

| $c$ | $f$ | Teilmenge von $\mathbb{N}$ |
|---|---|---|
| 0 | 0 | $\emptyset$ |
| 0 | 1 | $\{\, n \in \mathbb{N} \,:\, n > 0 \,\}$ |
| 0 | $\boldsymbol{tw}$ | $\{\, n \in \mathbb{N} \,:\, n$ ungerade $\}$ |
| 0 | $\boldsymbol{id}$ | $\emptyset$ |
| 1 | 0 | $\{0\}$ |
| 1 | 1 | $\mathbb{N}$ |
| 1 | $\boldsymbol{tw}$ | $\{\, n \in \mathbb{N} \,:\, n$ gerade $\}$ |
| 1 | $\boldsymbol{id}$ | $\mathbb{N}$ |

# Beweisen Teil 1: Objekte, Aussagen und Ergebnisse

Wir sprechen zumeist über

- ▷ Mengen und deren Elemente $x \in A$;
- ▷ Relationen $R \subseteq A \times B$




$R = \{\langle a, 1\rangle, \langle b, 1\rangle, \langle c, 2\rangle, \langle c, 3\rangle\}$

  Ist $A \,/\, B$ ein Singleton, fasst man $R$ als Teilmenge von $B \,/\, A$ auf.
- ▷ Funktionen $A \xrightarrow{f} B$, d.h. ganze und einwertige Relationen.

Im Prinzip sind Relationen und Funktionen auch bloß Mengen. (Solch Reduktionismus birgt die Gefahr, konzeptionelle Unterschiede zu verwischen).

Die zu beweisenden Aussagen sind in der Regel Aussagen über Mengen:

- Inklusionen: $A \subseteq B$, definitionsgemäß gdw.

$$\forall x.\, x \in A \to x \in B \ \text{(PL)} \quad \text{bzw.} \quad \forall x \in A.\, x \in B \ \text{(Praxis)}$$

- Gleichheiten: $A = B$ gdw. $A \subseteq B$ und $B \subseteq A$, s.o.
- Eigenschaften: es besteht eine bijektive Korrespondenz zwischen Teilmengen $P \subseteq A$ (oder $A \xrightarrow{P} 1$) und ihren charakteristischen Funktionen $A \xrightarrow{P} \boldsymbol{2} = \{0, 1\} =: \mathbb{B}$ (daher dasselbe Symbol $P$).

  Manche definieren $\mathbb{B}$ als $\{\boldsymbol{\mathit{false}}, \boldsymbol{\mathit{true}}\}$. Aussagen der Form „Alle Elemente von $A$ haben die Eigenschaft $P$“/„$P$ ist nicht leer“ kann man formal schreiben als

$$\forall x \in A.\ P(x) \quad \text{bzw.} \quad \exists x \in A.\ P(x)$$

Die erzielten Ergebnisse bezeichnet man gemäß ihrer Wichtigkeit als

- ▷ Lemma: einfache Aussage oder technische Hilfsaussage; beim Beweisen entsprechen Lemmata(!) den Prozeduren beim Programmieren.
- ▷ Proposition: Aussage von eigenständigem Interesse (aber nicht super wichtig)
- ▷ Satz: wichtige Aussage, der Beweis nutzt häufig vorher bewiesene Lemmata und Propositionen.
- ▷ Korollar: unmittelbare Folgerung aus einem Lemma/einer Proposition/einem Satz.

# Beweisen Teil 2: Beweistechniken

**Umgang mit** $\forall x \in A.\, P(x)$ . Man instantiiert die Variable $x$ durch ein generisches Element $v$ von $A$, über das wir sonst nichts wissen, etwa

$\boxed{\text{Sei } v \text{ aus } A \text{ gegeben.}}$ (von außen)

Gerade weil außer $v \in A$ nichts über $v$ bekannt ist, wird die folgende Argumentationskette für jedes ( $\forall$ ) Element von $A$ gelten

$\boxed{\text{zeigen, dass } P(v) \text{ gilt.}}$

**Umgang mit** $\exists x \in A.\, P(x)$ . Hier müssen Sie

$\boxed{\text{ein konkretes } v \text{ aus } A \text{ angeben}}$ (von innen)

Für dieses eine ( $\exists$ ) $v$ muss man in der folgenden Argumentationskette

$\boxed{\text{zeigen, dass } P(v) \text{ gilt.}}$

Dabei kann man alle speziellen Eigenschaften des gewählten $v$ ausnutzen.

**Zeigen, dass $P(v)$ gilt**:

- die Definition von $P(x)$ einsetzen;
- kleinschrittig argumentieren, so dass jeder Schritt leicht einsichtig aus dem vorherigen folgt.

**Zeigen, aus $P(v)$ folgt $Q(v)$, oder $P(v) \to Q(v)$**: (die Eigenschaft $P$ ist Teilmenge der Eigenschaft $Q$).

- direkt: Definition von $P(v)$ einsetzen, kleinschrittig umformen, bis $Q(v)$ erreicht ist;
- indirekt, durch sog. Kontraposition: Wenn $Q(v)$ falsch ist, darf $P(v)$ nicht wahr sein, also zeigt man anstelle der ursprünglichen Aussage stattdessen $\neg Q(v) \to \neg P(v)$.
- durch Widerspruch: Wäre die Implikation falsch, müsste $P(v) \wedge \neg Q(v)$ gelten. Ausgehend von dieser Annahme und den entsprechenden Definitionen einen Widerspruch finden (etwa $0 = 1$, oder $a \in \emptyset$, oder $\mathbb{N}$ ist endlich...) Dann war die Annahme falsch, die Implikation also richtig (gilt nur klassisch, nicht intuitionistisch!).

**Zeigen, dass Aussagen $A$, $B$ und $C$ äquivalent ($\leftrightarrow$) sind**: Man kann einen Ringschluss der Form $A \to B$ und $B \to C$ und $C \to A$ verwenden.

**Zeigen, dass eine Aussage $A$ nicht gilt**: Ein Gegenbeispiel angeben.

### Anmerkungen

- Beweisen ist ein Handwerk, das historisch gewachsen ist, im Lauf der Zeit verfeinert wurde, und dessen zulässige Werkzeuge (Schlussregeln) auf der Übereinkunft von Mathematikern und Logikern beruhen (Politiker und Juristen sind ausdrücklich ausgenommen).
- Mit formaler Beweistherorie werden wir uns ab Kapitel 4 befassen; “working mathematicians” kommunizieren meist informeller wie oben, was sich im Prinzip aber immer formalisieren lassen muss.
- Beweisen wird durch Übung leichter.
- Beweisen schult folgerichtiges Denken und Abstraktionsvermögen.

# Beweisen Teil 3: ein Beispiel (2023-04-24)

## Lemma

*Jede Formelmenge* $\Gamma \subseteq \mathcal{F}[\mathcal{A}]$ *ist in ihrer Folge-Hülle* $\Gamma^{\rhd\lhd}$ *enthalten.*

## Beweis.

Um $\Gamma \subseteq \Gamma^{\rhd\lhd}$ zu zeigen,

brauchen wir die Definition von $\subseteq$ .

$$\forall A \in \Gamma.\, A \in \Gamma^{\rhd\lhd}$$

Der All-Quantor motiviert den nächsten Satz.

Sei eine (generische) Formel $B \in \Gamma$ gegeben. Nachzuweisen ist $B \in \Gamma^{\rhd\lhd}$ .

Nun brauchen wir die Definition von $\Gamma^{\rhd\lhd}$ .

$$\begin{aligned}
\Gamma^{\rhd\lhd} &= \{\, \varphi \in \mathbb{B}^{\mathcal{A}} : \forall A \in \Gamma.\, \hat{\varphi}(A) = 1 \,\}^{\lhd} \\
&= \Big\{\, C \in \mathcal{F}[\mathcal{A}] : \forall \varphi \in \mathbb{B}^{\mathcal{A}}.\, \big(\forall A \in \Gamma.\, \hat{\varphi}(A) = 1\big) \to \hat{\varphi}(C) = 1 \,\Big\}
\end{aligned}$$

## Beweis, Fortsetzung.

Damit $B \in \Gamma^{\rhd\lhd}$ gilt, muß $B$ die definierende Bedingung erfüllen:

$$\forall \varphi \in \mathbb{B}^{\mathcal{A}}.\, \big(\forall A \in \Gamma.\, \hat{\varphi}(A) = 1\big) \to \hat{\varphi}(B) = 1\big)$$

Der All-Quantor motiviert wieder den nächsten Satz.

Sei (ein generisches) $\psi \in \mathbb{B}^{\mathcal{A}}$ gegeben.

Um eine Implikation zu zeigen, gab es drei Möglichkeiten.

**Direkt**: Falls $\forall A \in \Gamma.\, \hat{\psi}(A) = 1$, müssen wir $\hat{\psi}(B) = 1$ zeigen.

Jetzt ist zum ersten Mal ein eigener Schluss zu ziehen;
der bisherige Beweis war rein mechanisch.

Wegen $B \in \Gamma$ gilt nach Voraussetzung $\hat{\psi}(B) = 1$.

**Kontraposition**: Falls $\hat{\psi}(B) = 0$, existiert wegen $B \in \Gamma$ eine Formel in $\Gamma$, die $\psi$ nicht erfüllt, was linke Seite der Implikation negiert.

**Durch Widerspruch**: Annahme: $\forall A \in \Gamma.\, \hat{\psi}(A) = 1$ und $\hat{\psi}(B) = 0$.
Wegen $B \in \Gamma$ muss aber auch $\hat{\psi}(B) = 1$ gelten, Widerspruch.

# $\mathcal{J}$ ist funktional vollständig (2023-05-08)

Für $n \in \mathbb{N}$ soll jede der $2^{2^n}$ Boole'schen Funktionen durch eine Formel in $\mathcal{F}[\mathcal{A}]$ realisiert werden. Wegen $\neg$ genügt die Betrachtung von $2^{2^{n-1}}$ Boole'schen Funktionen, von denen keine ein Komplement einer anderen ist.

0 $\perp$ und $\top$ liefern die konstanten Funktionen 0 bzw. 1 .

1

| $p$ | $\perp$ | $p$ | $\top$ | $\neg p$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 1 | 1 | 0 |

2

| $p$ | $q$ | $\perp$ | $p \wedge q$ | $p \wedge \neg q$ | $\neg p \wedge q$ | $\neg p \wedge \neg q$ | $p$ | $q$ | $p \leftrightarrow q$ | $\top$ | $\neg p \vee \neg q$ | $\neg p \vee q$ | $p \vee \neg q$ | $p \vee q$ | $\neg p$ | $\neg q$ | $\neg p \leftrightarrow q$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |

Was passiert für $n > 2$ ? Man beachte, dass die Anzahl der Boole'schen Funktionen sich in jedem Schritt quadradriert:

$$2^{2^{n+1}} = 2^{2\cdot 2^n} = \left(2^2\right)^{2^n} = 4^{2^n} = 2^{2^n} \cdot 2^{2^n} = \left(2^{2^n}\right)^2$$

Für $n = 3$ sind das $16^2 = 256$ Boole'sche Funktionen, was eine direkte Verifikation ausschließt.

Stattdessen verwenden wir natürliche Induktion über die Stelligkeit der Boole'schen Funktionen, d.h., wir nehmen an, die Behauptung sei korrekt für $k \in \mathbb{N}$ und weisen sie dann für $k + 1$ nach.

- Jede Spalte der systematischen Auflistung der Boole'schen Funktionen in den Atomen $p_i$ , $i \leq k$ , zerfällt in eine obere und eine untere Hälfte.
- Die entsprechenden Boole'schen Funktionen in den Atomen $p_i$ , $i < k$ lassen sich mit Formeln $F(p_0, \ldots, p_{k-1})$ bzw. $G(p_0, \ldots, p_{k-1})$ realisieren, in denen *höchstens* die Atome von $p_0$ bis $p_{k-1}$ vorkommen.

- ▷ Damit lässt sich die ursprüngliche Boole'sche Funktion mit Hilfe des *if-then-else* Junktors $[\_,\_,\_]$ realisieren als

$$[p_k, G(p_0, \ldots, p_{k-1}), F(p_0, \ldots, p_{k-1})]$$

- ▷ Somit bleibt nachzuweisen, dass sich $[\_,\_,\_]$ mit Hilfe der Junktoren aus $\mathcal{J}$ simulieren lässt. Ein Vergleich der Wahrheitstabellen zeigt

$$[p, q, r] \mathrel{\models\!\!\!\dashv} (p \to q) \wedge (\neg p \to r) \qquad (*)$$

- ▷ Die ursprüngliche Boole'sche Funktion wird somit realisiert durch

$$(p_k \to G) \wedge (\neg p_k \to F) \qquad \square$$

Aus $(*)$ lässt sich auch leicht herleiten:

$$p \wedge q \mathrel{\models\!\!\!\dashv} [p, q, \bot] \quad p \vee q \mathrel{\models\!\!\!\dashv} [p, \top, q] \quad p \to q \mathrel{\models\!\!\!\dashv} [p, q, \top] \quad \neg p \mathrel{\models\!\!\!\dashv} [p, \bot, \top]$$

# AL versus $PL_1$: Syntax (2023-05-22)

| | Aussagenlogik | Logik der ersten Stufe |
|---|---|---|
| Signatur | – | $\boldsymbol{Fun} + \boldsymbol{Pred} \xrightarrow{\mathcal{S}} \mathbb{N}$ |
| Variablen | – | $\mathcal{V} = \{\, x_i \;:\; i \in \mathbb{N} \,\}$ |
| Terme | – | $\boldsymbol{Term}\,(\boldsymbol{Fun}, \mathcal{V})$ |
| Atome | $\mathcal{A} = \{\, p_i \;:\; i \in \mathbb{N} \,\}$ | $\boldsymbol{AT} := \boldsymbol{Atm}\,(\boldsymbol{Pred} + \{\doteq\}, \boldsymbol{Term}\,(\boldsymbol{Fun}, \mathcal{V}))$ |
| Junktoren | $\mathcal{J} \xrightarrow{\boldsymbol{ar}} \mathbb{N}$ | $\mathcal{J} + \{\, \forall x, \exists x \;:\; x \in \mathcal{V} \,\} \xrightarrow{\boldsymbol{ar'}} \mathbb{N}$ |
| Formeln | $\boldsymbol{F} ::= \mathcal{A} \mid \bot \mid \top \mid \neg \boldsymbol{F} \mid (\boldsymbol{F} \star \boldsymbol{F})$<br>Termalgebra $\mathcal{F}[\mathcal{A}]$ bzgl. $\boldsymbol{ar}$ auf $\mathcal{A}$ | $\boldsymbol{F} ::= \boldsymbol{AT} \mid \bot \mid \top \mid \neg \boldsymbol{F} \mid (\boldsymbol{F} \star \boldsymbol{F}) \mid (\forall x\, \boldsymbol{F}) \mid (\exists x\, \boldsymbol{F})$<br>Termalgebra $\boldsymbol{FO}(\mathcal{S})$ bzgl. $\boldsymbol{ar'}$ auf $\boldsymbol{AT}$ |

# AL versus $PL_1$: Semantik

| | Aussagenlogik | Logik der ersten Stufe |
|---|---|---|
| Struktur | $\mathbb{B}$ mit kanonischer ***ar***-Interpretation | $\mathcal{M} = \langle$Datenbereich $D$, Interpretation $I$ von $\mathcal{S}$ in $D\rangle$ |
| Belegung | $\mathcal{A} \xrightarrow{\varphi} \mathbb{B}$ | $\mathcal{V} \xrightarrow{\sigma} D$ sowie $\boldsymbol{Term}\,(\boldsymbol{Fun}, \mathcal{V}) \xrightarrow{\check{\sigma}} D$<br>$\boldsymbol{AT} \xrightarrow{\overline{\sigma}} \mathbb{B}$ , hängt von $\mathcal{M}$ ab |
| Bewertung | $\mathcal{F}[\mathcal{A}] \xrightarrow{\hat{\varphi}} \mathbb{B}$ | $\boldsymbol{FO}(\mathcal{S}) \xrightarrow{\hat{\sigma}} \mathbb{B}$ |
| Auswertung | $\mathcal{F}[\mathcal{A}] \times \mathbb{B}^{\mathcal{A}} \xrightarrow{\boldsymbol{E}} \mathbb{B}$ | $\boldsymbol{Term}\,(\boldsymbol{Fun}, \mathcal{V}) \times D^{\mathcal{V}} \xrightarrow{\mathcal{M}[\![-]\!](-)} D$<br>$\boldsymbol{FO}\,(\mathcal{S}) \times D^{\mathcal{V}} \xrightarrow{\boldsymbol{E}_{\mathcal{M}} := \mathcal{M}[\![-]\!](-)} \mathbb{B}$ |
| Hüllenop. | $(\ )^{\triangleright\triangleleft} := \boldsymbol{E}^{\triangleleft} \circ \boldsymbol{E}^{\triangleright}$ auf $\boldsymbol{P}(\mathcal{F}[\mathcal{A}])$ | $(\ )^{\triangleright\triangleleft}_{\mathcal{M}} := \boldsymbol{E}^{\triangleleft}_{\mathcal{M}} \circ \boldsymbol{E}^{\triangleright}_{\mathcal{M}}$ auf $\boldsymbol{P}(\boldsymbol{FO}(\mathcal{S}))$ |
| Erfüller von $A$ | $\varphi \in \mathbb{B}^{\mathcal{A}}$ mit $\hat{\varphi}(A) = 1$ | $\langle \mathcal{M}, \sigma \in \mathcal{M}^{\mathcal{V}} \rangle$ mit $\mathcal{S}$-Struktur $\mathcal{M}$ und $\hat{\sigma}(A) = 1$ |

### Beispiel (Gerichtete Graphen)

Laut Vereinbarung sind die Datenbereiche $D$ der $\mathcal{S}$-Strukturen $\mathcal{M}$ nicht leer. Das begrüßen nicht alle Mathematiker.

Für die Theorie der nichtleeren gerichteten Graphen genügt also die Signatur $\mathcal{G}_0 = \{R_{/2}\}$. Trotzdem kann es sinnvoll sein, zusätzlich noch eine Konstante zu postulieren, also $\mathcal{G}_1 = \{c_{/0}; R_{/2}\}$ zu setzen. Der Unterschied betrifft die Anzahl der möglichen Graph-Homomorphismen: Ist $\boldsymbol{1}$ der Graph mit einem Knoten und ohne Kanten, so gibt es

- $n$ $\mathcal{G}_0$-Homomorphismen von $\boldsymbol{1}$ in jeden Graphen mit $n$ Knoten;
- nur einen $\mathcal{G}_1$-Homomorphismus von $\boldsymbol{1}$ in jeden Graphen mit $n$ Knoten, da der duch $c$ ausgewählte Knoten erhalten bleiben muß.

HA: Ist $\boldsymbol{L}$ der Graph mit einem Knoten und einer Kante (genannt Schleife oder Loop), wieviele $\mathcal{G}_0$- bzw. $\mathcal{G}_1$-Homomorphismen gibt es von $\boldsymbol{L}$ in einen Graphen mit $n$ Knoten?

## Beispiel (Gerichtete Graphen, Forsetzung)

Geben Sie eine $\mathcal{G}_0$-Formel an, die genau von den Graphen erfüllt wird,

- die höchstens vier Knoten und mindestens zwei Kanten haben.

▷ Die Begrenzung auf höchstens vier Knoten erreicht man mit

$$\exists x\, \exists y\, \exists z\, \exists w\, \forall u\, (x \doteq u \lor y \doteq u \lor z \doteq u \lor w \doteq u)$$

Die Interpretationen von $x$, $y$, $z$ und $w$ müssen nicht verschieden sein, aber es gibt auch keine anderen Knoten.

▷ Verlangt man Kanten vermöge $R(x, y)$ und $R(z, w)$, so konnen diese evtl. auch zusammenfallen. Damit dies nicht passiert, müssen die Interpretationen der Startknoten $x$ und $z$, oder der Zielknoten $y$ und $w$ verschieden sein, also $\neg(x \doteq z) \lor \neg(y \doteq w)$.

$$\exists x\, \exists y\, \exists z\, \exists w\, \Big(R(x, y) \land R(z, w) \land (\neg(x \doteq z) \lor \neg(y \doteq w)) \\ \land \forall u\, (x \doteq u \lor y \doteq u \lor z \doteq u \lor w \doteq u)\Big)$$

## Beispiel (Gerichtete Graphen, Forsetzung)

Geben Sie eine $\mathcal{G}_0$-Formel an, die genau von den Graphen erfüllt wird,

- für die in jedem Knoten ein Pfad mit mindestens drei verschiedenen Kanten startet.

▷ Ketten von drei aufeinanderfolgenden Kanten aus $x$ erhält man mit

$$\forall x\, \exists y\, \exists z\, \exists w\, \big(R(x,y) \wedge R(y,z) \wedge R(z,w)\big)$$

▷ Damit keine zwei dieser Kanten zusammenfallen, ist das Auftreten von Schleifen der Länge 1 bzw. 2 zu kontrollieren, wobei aufgrund von Kontraposition jeweils nur eine Formel nötig ist:

$$\begin{aligned} A(x,y,z,w) &= \big((x \doteq y) \vee (z \doteq w)\big) \to \neg(y \doteq z) \\ B(x,y,z,w) &= (x \doteq z) \to \neg(w \doteq y) \end{aligned}$$

$$\forall x\, \exists y\, \exists z\, \exists w\, \big(R(x,y) \wedge R(y,z) \wedge R(z,w) \wedge A(x,y,z,w) \wedge B(x,y,z,w)\big)$$

## Beispiel (Arithmetik)

Die Signatur $\mathcal{S}_{\mathrm{arith}} = \{0_{/0}, 1_{/0}, +_{/2}, *_{/2}; <_{/2}\}$ der Arithmetik möge die kanonische Interpretation in den natürlichen Zahlen $\mathbb{N}$ haben.

- Finden Sie eine Formel, die besagt, dass je zwei Zahlen ein kleinstes gemeinsames Vielfaches haben.

▷ Ein gemeinsames Vielfaches läßt sich wie folgt ausdrücken:

$$\forall x\, \forall y\, \exists u\, \exists v\, (x * u \doteq y * v)$$

▷ Damit die Interpretation von $x * u$ in $\mathbb{N}$ das kgV ist, muss jedes andere gemeinsame Vielfache mindestens so groß sein:

$$\forall x\, \forall y\, \exists u\, \exists v \Big( x * u \doteq y * v \\ \wedge \forall z\, \forall w\, (x * z \doteq y * w \to \neg(z < u) \wedge \neg(w < v))\Big)$$

Beachte, dass $\neg(z < u)$ in $\mathbb{N}$ dasselbe bedeutet wie $u \leq z$ .

# Elimination des $\doteq$-Symbols aus Formeln (2023-06-26)

**Motivation**: Folgendes Verfahren konstruiert zu jeder $\boldsymbol{FO}$-Formel $A$ eine erfüllungsäquivalente Formel $A^{(E)}$ *ohne formales Gleichheitszeichen* $\doteq$, so dass Folgendes gilt:

wenn $A^{(E)}$ ein abzählbares Modell besitzt, hat auch $A$ ein solches.

ObdA möge $A$ in bereinigter Skolem-Normalform vorliegen.

Wir erweitern die endliche(!) Minimalsignatur $\mathcal{S}_A$ für $A$ um ein neues 2-stelliges Prädikat $E_{/2}$ zu einer Signatur $\mathcal{S}'_A$. Dann ersetzen wir in einem **ersten Schritt** jedes Auftreten von $\doteq$ in $A$ durch $E$:

$$A_1 := A\{\doteq /E\}$$

Jedes Model $\mathcal{M} = \langle D, I\rangle$ für $A$ lässt sich zu einem Model $\mathcal{M}' = \langle D, I'\rangle$ für $A_1$ erweitern indem man das neue Prädikat als Gleichheit interpretiert.

**Zweiter Schritt**: $A_1$ so zu einer Formel $A^{(E)}$ zu erweitern, dass $A^{(E)}$ in einer $\mathcal{S}'_A$-Struktur $\mathcal{N} = \langle D, J \rangle$ nur dann erfüllbar ist, wenn $E^{\mathcal{N}}$ eine Kongruenzrelation $\equiv$ auf $D$ bzgl. $\mathcal{S}_A$ ist, sowohl bezüglich der Operatoren in ***Fun***$_A$, als auch bzgl. der Prädikate in der ursprünglichen Menge ***Pred***$_A$.

Da $\mathcal{S}_A$ endlich ist, sind nur endlich viele Bedingungen zu $A_1$ hinzuzufügen.

Gelingt das, kann man den Datenbereich eines $A^{(E)}$-Models $\mathcal{N} = \langle D, J \rangle$ nach $\equiv$ faktorisieren (d.h., die Äquivalenzklassen im Datenbereich bilden) und erhält so eine neue $\mathcal{S}'_A$-Struktur $\mathcal{N}' := \mathcal{N}/_{\equiv} = \langle D/_{\equiv}, J' \rangle$ mit $E^{\mathcal{N}'}$ als Gleichheit. Ist $D$ abzählbar, so auch $D/_{\equiv}$.

$J'$ interpretiert die $\mathcal{S}_A$-Symbole, indem die $J$-Interpretationen auf Repräsentanten der zu bearbeitenden Äquivalenzklassen angewendet werden. Aufgrund der Kongruenzeigenschaften von $E^{\mathcal{N}}$ ist dieses Vorgehen unabhängig von der Wahl dieser Repräsentanten und somit wohldefiniert.

**Konstruktion von** $A^{(E)}$: Zu $A_1$ fügen wir per Konjunktion folgende Bedingungen an $E$ hinzu:

- ▷ $\forall x\, E(x,x)$ ( $E$ ist reflexiv);
- ▷ $\forall x\, \forall y\, \forall z \big(E(x,y) \wedge E(y,z) \to E(x,z)\big)$ ( $E$ ist transitiv);
- ▷ $\forall x\, \forall y\, \big(E(x,y) \to E(y,x)\big)$ ( $E$ ist symmetrisch);

Nun muss $E$ als Äquivalenzrelation interpretiert werden.

Weiter soll für jedes $f_{/n} \in \boldsymbol{Fun}_A$ in jeder Position $i < n$ die Ersetzung eines Arguments durch ein $E$-äquivalentes ein $E$-äquivalentes Ergebnis liefern:

- ▷ $\forall z_0, \ldots, z_{i-1}\, \forall x\, \forall y\, \forall z_{i-1}, y, z_{i+1}, \ldots, z_{n-1}. \big(E(x,y) \to E(f(z_0, \ldots, z_{i-1}, x, z_{i+1}, \ldots, z_{n-1}), f(z_0, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_{n-1}))\big)$

Und für jedes $P_{/n} \in \boldsymbol{Pred}_A$ soll in jeder Position $i < n$ die Ersetzung eines Arguments durch ein $E$-äquivalentes die Gültigkeit des Prädikats erhalten:

- ▷ $\forall z_0, \ldots, z_{i-1}\, \forall x\, \forall y\, \forall z_{i-1}, y, z_{i+1}, \ldots, z_{n-1}. \big(E(x,y) \wedge P(z_0, \ldots, z_{i-1}, x, z_{i+1}, \ldots, z_{n-1}) \to P(z_0, \ldots, z_{i-1}, y, z_{i+1}, \ldots, z_{n-1})\big)$

# Connie Booth ist vermutlich keine Hexe!

Im Film “Monty Python and the Holy Grail” von 1975 wird „nachgeweisen“, , dass die von Conny Booth, damalige Ehefau von John Cleese, dargestellte junge Frau eine Hexe ist (vergl. Aufgabe 6, Blatt 0).

Ist der hier dargestellte mittelalterliche Gebrauch von Logik korrekt?

# Das logische Argument des Films

1. Was macht man mit Hexen? Man verbrennt sie!
2. Was sonst verbrennt man? Holz!
3. Was zeichnet Holz aus? Es schwimmt.
4. Was schwimmt noch? Eine Ente.
5. Implizit verwendet: Alles, was dasselbe Gewicht hat, wie etwas das schwimmt, schwimmt ebenfalls.
6. Experimentell nachgeweisen: Connie wiegt genausoviel wie eine Ente.

---

7. Daher ist Connie eine Hexe!

# Logische Formalisierung

Prädikate: $W_{/1}$ / $V_{/1}$ / $H_{/1}$ / $S_{/1}$ für Hexe / Verbrennen / Holz / Schwimmen
Operatoren: $c_{/0}$ für Connie, $e_{/0}$ für eine Ente, $g_{/1}$ für Gewicht

1. $\forall x.\, \big(W(x) \to V(x)\big)$
2. $\forall x.\, \big(H(x) \to V(x)\big)$
3. $\forall x.\, \big(H(x) \to S(x)\big)$
4. $S(e)$
5. $\forall x\, \forall y.\, \big(S(x) \wedge g(x) \doteq g(y) \to S(y)\big)$
6. $g(c) \doteq g(e)$

---

7. $W(c)$

# Übergang zur KNF

1. $\forall x.\, \big(\neg W(x) \vee V(x)\big)$
2. $\forall x.\, \big(\neg H(x) \vee V(x)\big)$
3. $\forall x.\, \big(\neg H(x) \vee S(x)\big)$
4. $S(e)$
5. $\forall x\, \forall y.\, \big(\neg S(x) \vee \neg(g(x) \doteq g(y)) \vee S(y)\big)$
6. $g(c) \doteq g(e)$

---

7. $W(c)$

Die Schlußfolgerung

$$\{(1), (2), (3), (4), (5), (6)\} \models (7)$$

ist äquivalent zur Unerfüllbarkeit von

$$E\big(\{(1), (2), (3), (4), (5), (6), \neg(7)\}\big) \qquad (*)$$

# Anwendung der Resolventenmethode

$\neg W(x), V(x) \quad \neg H(x), V(x) \quad \neg H(x), S(x) \quad S(e) \quad \neg S(x), \neg(g(x) \doteq g(y)), S(y) \quad g(c) \doteq g(e) \quad \neg W(c)$

$\{\}$ $\quad$ $\{x/e\}$

$S$ $\qquad \neg H(x), \neg(g(x) \doteq g(y)), S(y) \quad \neg(g(e) \doteq g(y)), S(y)$

$\{x/e\}\{y/c\}$ $\quad$ $\{x/e\}\{y/c\}$ $\quad$ $\{y/c\}$

$\doteq$ $\qquad \neg H(c), S(e) \quad \neg H(e), S(c) \quad S(c)$

Damit kann die leere Resolvente nicht auftreten, und $(*)$ ist erfüllbar. Also ist die Schußfolgerung, Connie sei eine Hexe, aus den gegebenen Prämissen nicht korrekt. Sie könnte aber natürlich trotzdem eine Hexe sein…

# Hintergrund zur Tseitin-Transformation

Die ursprüngliche Tseitin-Transformation sollte Boole'sche Schaltkreise in KNF umzuformen, und ist auf beliebige Formeln in $\mathcal{F}[\mathcal{A}]$ anwendbar.

**Idee**: für jede Teilformel $B$ von $A$ (vergl. ▸ Folie 47), die kein Literal ist, ein frisches Atom $p$ einführen, dann $p \leftrightarrow B$ in KNF umformen, und alle resultierenden Klauseln zu einer KNF zusammenfassen:

| $B$ | $p \leftrightarrow B$ | KNF($p \leftrightarrow B$) in Mengendarstellung |
|---|---|---|
| $\neg C$ | $(\neg C \to p) \wedge (p \to \neg C)$ | $\{C, p\}, \{\neg p, \neg C\}$ |
| $C \wedge D$ | $(C \wedge D \to p) \wedge (p \to C \wedge D)$ | $\{\neg C, \neg D, p\}, \{\neg p, C\}, \{\neg p, D\}$ |
| $C \vee D$ | $(C \vee D \to p) \wedge (p \to C \vee D)$ | $\{\neg C, p\}, \{\neg D, p\}, \{\neg p, C, D\}$ |
| $C \to D$ | $(\neg C \vee D \to p) \wedge (p \to \neg C \vee D)$ | $\{C, p\}, \{\neg D, p\}, \{\neg p, \neg C, D\}$ |
| $C \leftrightarrow D$ | $((\neg C \vee D) \wedge (\neg D \vee C) \to p)$ <br> $\wedge (p \to (\neg C \vee D) \wedge (\neg D \vee C))$ | $\{C, D, p\}, \{\neg C, \neg D, p\}, \{\neg p, \neg C, D\}, \{\neg p, C, \neg D\}$ |

Liegt $A$ schon in NNF vor (1. Schritt bei der konventionellen Umwandlung in KNF), kommen nur die blauen Zeilen zum Tragen.

Die Umwandlung in NNF eliminiert erst $\leftrightarrow$, dann $\rightarrow$, bevor ggf. Negationen mit Hilfe der de Morganschen Regeln nach innen befördert werden.

Sofern keine führende Negation vorliegt, kann man sofort mit der Tseitin-Transformation beginnen und sich dabei auf die echten binären Teilformeln beschränken. Falls der Hauptjunktor eine Konjunktion ist, kann man weitere Schritte einsparen.

**Beispiel** ( $A = (\neg s \wedge p) \leftrightarrow ((q \to r) \vee \neg p)$ )

$$\Big((\neg s \wedge p) \to ((q \to r) \vee \neg p)\Big) \wedge \Big(((q \to r) \vee \neg p) \to (\neg s \wedge p)\Big)$$

$$(\neg(\neg s \wedge p) \vee (\neg q \vee r \vee \neg p) \wedge (\neg(\neg q \vee r \vee \neg p) \vee (\neg s \wedge p))$$

$$\begin{aligned} (\neg t_0 \vee t_1) \wedge (\neg t_1 \vee t_0) &: \{\neg t_0, t_1\}, \{\neg t_1, t_0\} \\ t_0 \leftrightarrow (\neg s \wedge p) &: \{s, \neg p, t_0\}, \{\neg t_0, \neg s\}, \{\neg t_0, p\} \\ t_1 \leftrightarrow (\neg q \vee r \vee \neg p) &: \{q, t_1\}, \{\neg r, t_1\}, \{p, t_1\}, \{\neg t_1, \neg q, r, \neg p\} \end{aligned}$$

***Tse***$(A)$ besteht dann aus allen blauen Klauseln.

## Beispiel (Hauptjunktor $\vee$ statt $\wedge$)

$$\big(\neg(\neg s \wedge p) \wedge (\neg q \vee r \vee \neg p)\big) \vee \big(\neg(\neg q \vee r \vee \neg p) \vee (\neg s \wedge p)\big) = B$$

$$\begin{aligned}
w_0 \vee w_1 &: \{w_0, w_1\} \\
w_0 \leftrightarrow \neg t_0 \wedge t_1 &: \{t_0, \neg t_1, w_0\}, \{\neg w_0, \neg t_0\}, \{\neg w_0, t_1\} \\
w_1 \leftrightarrow \neg t_1 \wedge t_0 &: \{t_1, \neg t_0, w_1\}, \{\neg w_1, \neg t_1\}, \{\neg w_1, t_0\} \\
t_0 \leftrightarrow (\neg s \wedge p) &: \{s, \neg p, t_0\}, \{\neg t_0, \neg s\}, \{\neg t_0, p\} \\
t_1 \leftrightarrow (\neg q \vee r \vee \neg p) &: \{q, t_1\}, \{\neg r, t_1\}, \{p, t_1\}, \{\neg t_1, \neg q, r, \neg p\}
\end{aligned}$$

***Tse***$(B)$ besteht dann aus allen orangen und blauen Klauseln.