Logik

Sets, Structures, Semantics: Pt. 3, Logics.

M.E.Müller

m.e.mueller@acm.org

— Version as of December 7, 2023—

Note

- These slides complement the notes "Sets, Structures, Semantics"
- Both depend on each other but are under constant construction
- They usually are not in sync w.r.t. numbering or even notation
- The slides, notes and any recorded material
  - may only be used for individual educational purposes
  - must not be copied, edited, distributed by any means
  - are copyright by the author and must always be indicated as such

Note

- Diese Folien ergänzen das Skript "Sets, Structures, Semantics"
- Beide sind u.U. in Notation und Numerierung nicht übereinstimmend.
- Das Skript, die Folien und alle Aufzeichnungen
  - dürfen nur zum individuellen Studium verwendet werden
  - dürfen nicht kopiert, verändert oder in irgendeiner Form verbreitet werden
  - sind urheberrechtlich geschützt und müssen als solche gekennzeichnet sein.

1.1.
WAS IST EINE LOGIK?

Log·ik(en)

- Logos ($\lambda\acute{o}\gamma o\varsigma$): Wort, Bedeutung, Schlußfolgerung
- [Techne] ($\tau\acute{\varepsilon}\chi\nu\eta$): Handwerk, Tun, Schaffen
- -ik(en) (): Menge von Wissen

Logik ist die Wissenschaft des geistvollen Umgangs mit Äußerungen

Man untersucht die Struktur von Argumenten ungeachtet derer konkreter “Interpretation”.

Logik

Def. 1: Logik

Eine Logik besteht aus:

1. einer wohldefinierten *Sprache* von *Äußerungen* (*Formeln*)
2. einer *Interpretation*, die jeder dieser Formeln
3. eine eindeutige *Bedeutung* zumißt, d.h. einen bestimmten "Umstand" in einem "*Modell*" beschreibt.

Hinweis

- Nicht jede Äußerung hat eine Bedeutung
- Jede Formel hat eine Bedeutung
- Keine Formel hat bzgl. einer Interpretation mehr als eine Bedeutung.
- Mehrere Formeln können dieselbe Bedeutung haben
- Ein und dieselbe Formel kann unter verschiedenen Interprationen oder in verschiedenen Modellen verschiedene Bedeutungen haben.

Äußerung und Bedeutung

Beispiele

- Nicht jede Äußerung hat eine Bedeutung
  Yakka foob mog. Hat obwohl schnell. Grüne Ideen schlafen wütend.
- Jede Formel hat eine Bedeutung
  Es ist kalt.
- Keine Formel hat mehr als eine Bedeutung.
  Es ist sonnig.
- Mehrere Formeln können dieselbe Bedeutung haben
  Es ist kalt und sonnig. Es ist kalt aber sonnig.
- Eine Formel kann unter verschiedenen Interprationen oder in verschiedenen Modellen verschiedene Bedeutungen haben.
  Es ist heiß.

Worum es in der Logik geht

Der Zweck von Logiken

- Logik befaßt sich *nicht* primär damit, ob etwas "wahr" ist, oder nicht.
- Es geht eher darum, *ob* etwas manchmal oder immer oder nie (wahr) ist oder sein kann.
- Worum es *hauptsächlich* geht:
  - Sind Äußerungen redundant/kompatibel/schlüssig?
  - Was passiert, wenn eine neue Aussage hinzukommt?
  - Gibt es folgerbare Äußerungern?
  - Gibt es dafür Schemata oder Algorithmen?

Von Sinn und Bedeutung

Nicht alles, was ich sage, ergibt Sinn.
Aber (fast) alles, was ich sage, hat eine Bedeutung

Grüner Schnee schlägt adipöse Einhörner.

Wenn wir uns über die Bedeutung von Wörtern *einig* sind, können Äußerungen wahr, sinnig oder "stimmig" sein — oder nicht.
Die "Einigkeit" wird durch eine geteilte *Semantik* und eine geteilte *Theorie* erreicht.

Dieser Text ist rot.
Dieser Text ist rot.

Worum es in der Logik geht

"The art of logic"

Anstelle über die Bedeutung von Äußerungen nachzudenken, kann man nicht einfach mechanisch die Struktur der Äußerungen selbst untersuchen?

$$1 + 1 = 1$$

Als Aussage über eine Gleichheit in $\mathbb{N}$ ist das "*falsch*", denn:

1. Die Auswertung von $1 + 1$ ergibt $2 \neq 1$.
2. Die Aussage "$x + x = x$" ist immer "*falsch*"

Die zweite Begründung basiert auf dem *Gesetz* der Isotonie von $+$ und $0 \notin \mathbb{N}$.

"$1 + 1 = 1$ oder $1 + 1 \neq 1$" erscheint *unsinnig*, aber ist *wahr* und sogar *gültig*.

Logik hat nichts mit Sinn zu tun — sondern mit Bedeutung.

Logiken je nach Bedarf

Jede formale Sprache mit Interpretation ist eine Logik!

- Schlußfolgern mit/aus Propositionen
- Schlußfolgern mit/aus prädikativen Aussagen
- Schlußfolgern über Ableitungen
- Wahrheit, Gültigkeit, Beweisbarkeit, Ableitbarkeit
- Schlußfolgern mit/unter Unsicherheit
- Nicht-monotones Schlußfolgern
- Schlußfolgern über Programme und deren Eigenschaften
- Schlußfolgern mit/unter zeitlichen Aspekten
- Schlußfolgern mit/unter Modalitäten
- Schlußfolgern mit Variablen Propositionen
- Schlußfolgern aus verschiedenen Perspektiven

2.
AUSSAGENLOGIK

Propositionale Logik (Aussagenlogik)

Wir beginnen mit einer einfachen Logik der *Aussagen*:

Propositionale Logik, PRL

Zusammen mit der Einführung der Aussagenlogik definieren wir wichtige Begriffe, die später für die Definition jeder weiterer Logik essentiell sind.

2.1.
SYNTAX DER AUSSAGENLOGIK

Proposition

Def. 2: Proposition

Eine *Proposition* oder *Aussage* ist eine Äußerung, der ein Wahrheitswert zugeordnet werden kann.

A bedeutet: *Gödel hat Recht*.

Man nennt A eine *Aussagenvariable*.

Def. 3: Wahrheitswerte Ω

Die Bedeutung einer Aussage ist ihr Wahrheitswert. Die Menge der Wahrheitswerte der Aussagenlogik ist $\Omega = \{\mathbf{0}, \mathbf{1}\}$.

PRL-Syntax

Def. 4: Propositionale Formeln $\mathrm{Prp}, \mathrm{Fml}_{(\mathsf{PRL})}$

1. Prp ist das Alphabet der *propositionalen/Aussagenvariablen*.
2. Fml ist die kleinste Menge mit:
   a. $\mathrm{Prp} \cup \{\mathsf{F}, \mathsf{T}\} \subseteq \mathrm{Fml}$ und
   b. Für jedes $p, q \in \mathrm{Fml}$ sind auch $\neg p$, $(p \vee q)$, $(p \wedge q)$, und $(p \longrightarrow q)$ in Fml.

- F und T heißen "*Falsum*" und "*Verum*"
- $\neg, \vee, \wedge, \rightarrow$ heißen *Negation*, *Disjunktion*, *Konjunktion*, *Subjunktion*
- Formeln werden gesprochen als:
  nicht p, p *oder/und* q, und *wenn* p, *dann* q.

$\mathrm{var}(p)$ bezeichnet die Menge aller Aussagenvariablen in p

$\mathrm{var}(A) := \{A\}$ für $A \in \mathrm{Prp}$
$\mathrm{var}(\neg p) := \mathrm{var}(p)$ und $\mathrm{var}((p \circledast q)) := \mathrm{var}(p) \cup \mathrm{var}(q)$.

2.2. SEMANTIK DER AUSSAGENLOGIK

PRL-Semantik

Def. 5: Interpretation $\mathcal{I} = \langle \mathfrak{i}, \alpha \rangle$

Eine *Interpretation* $\mathcal{I}$ weist Ausdrücken aus Fml eine Bedeutung in einer Struktur (Algebra) $\mathfrak{A}$ zu:

- α interpretiert die atomaren Elemente, d.h. *Aussagen* aus Prp.
- $\mathfrak{i}$ interpretiert die *strukturellen* Elemente aus Fml.

$\mathcal{I}$ besteht aus zwei Teilen: $\mathcal{I} = \langle \mathfrak{i}, \alpha \rangle$. Wir schreiben $\mathfrak{i}(\circledast) = \circledast_{\mathfrak{i}}$.

$$\mathrm{Fml}_{\Sigma} \xrightarrow{\qquad\qquad\mathcal{I}\qquad\qquad} \mathfrak{A} = \langle \mathcal{U}, \ldots \rangle$$

$$\begin{tikzcd}
A \arrow[rrr, bend left, "\alpha"] & \circledast \arrow[rrr, bend left, "\mathfrak{i}"] & B \arrow[rrr, bend left, "\alpha"] & a & \circledast_{\mathfrak{i}} & b \\
\in & \in & \in & \in & \in & \in \\
\mathrm{Prp} & \Sigma & \mathrm{Prp} & \mathcal{U} & \mathfrak{A} & \mathcal{U}
\end{tikzcd}$$

PRL-Semantik

Def. 6: Belegung oder Wahrheitswertzuweisung α

Eine *Belegung* α ist eine Funktion $\alpha : \mathrm{Prp} \to \Omega$.

Standard Definition der PRL-**Interpretation** $\mathcal{I}^\alpha.p$

Die übliche Definition der PRL -Semantik basiert auf $\Omega = \{\mathbf{0}, \mathbf{1}\}$ und einer Interpretation $\mathcal{I}^\alpha : \mathrm{Fml} \to \Omega$ mit:

$$
\begin{array}{lllll}
1. & \mathcal{I}^\alpha.p & \stackrel{\alpha}{=\!=} & \alpha(p) & \text{gdw.} \quad p \in \mathrm{Prp} \\
2. & \mathcal{I}^\alpha.\neg p & \stackrel{i}{=\!=} & \mathbf{1} & \text{gdw.} \quad \mathcal{I}^\alpha.p = \mathbf{0} \\
3. & \mathcal{I}^\alpha.(p \wedge q) & \stackrel{i}{=\!=} & \mathbf{1} & \text{gdw.} \quad \mathcal{I}^\alpha.p = \mathbf{1} \text{ und } \mathcal{I}^\alpha.q = \mathbf{1} \\
4. & \mathcal{I}^\alpha.(p \vee q) & \stackrel{i}{=\!=} & \mathbf{1} & \text{gdw.} \quad \mathcal{I}^\alpha.p = \mathbf{1} \text{ oder } \mathcal{I}^\alpha.q = \mathbf{1} \\
5. & \mathcal{I}^\alpha.(p \longrightarrow q) & \stackrel{i}{=\!=} & \mathbf{1} & \text{gdw.} \quad \text{Wenn } \mathcal{I}^\alpha.p = \mathbf{1}, \\
 & & & & \qquad\qquad \text{dann } \mathcal{I}^\alpha.q = \mathbf{1}
\end{array}
$$

"und", "oder" und "wenn... dann" haben die intuitive Bedeutung.
Außerdem gilt: $\mathcal{I}^\alpha.\mathsf{T} = \mathbf{1}$ und $\mathcal{I}^\alpha.\mathsf{F} = \mathbf{0}$.

PRL-Semantik mit (Operator-) Tabellen

Def. 7: Wahrheitstabellen für die PRL-Operator Semantik

	$\neg p$
$\mathbf{1}$	$\mathbf{0}$
$\mathbf{0}$	$\mathbf{1}$

$\vee$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$

$\wedge$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$

$\longrightarrow$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$

Kor.

$\wedge$ und $\vee$ sind kommutativ, idempotent und assoziativ. $\neg$ ist involutiv. $\mathbf{1}$ ist $\wedge$-neutral. $\mathbf{0}$ ist $\vee$-neutral. $\mathbf{0}$ ist ein $\wedge$-Annihilator.

PRL-Semantik: Boole'sche Algebra / Verbände

Def. 8: PRL-Semantik via BA $\mathcal{I}^{\alpha}_{\mathcal{B}}.p$

Man wählt $\mathfrak{A} = \mathcal{B} = \langle \Omega, \sqcap, \sqcup, \backslash, \bar{\ }, \top, \bot \rangle$ mit $\Omega = \{\bot, \top\}$ und definiert:

$$
\begin{array}{lllll}
1. & \mathcal{I}^{\alpha}_{\mathcal{B}}.p & = & \alpha(p) \text{ for } p \in \mathrm{Prp} \\
2. & \mathcal{I}^{\alpha}_{\mathcal{B}}.\neg p & = & \overline{\mathcal{I}^{\alpha}_{\mathcal{B}}.p} \\
3. & \mathcal{I}^{\alpha}_{\mathcal{B}}.(p \wedge q) & = & \mathcal{I}^{\alpha}_{\mathcal{B}}.p \sqcap \mathcal{I}^{\alpha}_{\mathcal{B}}.q \\
4. & \mathcal{I}^{\alpha}_{\mathcal{B}}.(p \vee q) & = & \mathcal{I}^{\alpha}_{\mathcal{B}}.p \sqcup \mathcal{I}^{\alpha}_{\mathcal{B}}.q \\
5. & \mathcal{I}^{\alpha}_{\mathcal{B}}.(p \longrightarrow q) & = & \overline{\mathcal{I}^{\alpha}_{\mathcal{B}}.p} \sqcup \mathcal{I}^{\alpha}_{\mathcal{B}}.q = \mathcal{I}^{\alpha}_{\mathcal{B}}.p \backslash \mathcal{I}^{\alpha}_{\mathcal{B}}.q
\end{array}
$$

sowie $\mathcal{I}^{\alpha}_{\mathcal{B}}.\mathsf{T} = \top$, $\mathcal{I}^{\alpha}_{\mathcal{B}}.\mathsf{F} = \bot$.

Kurz gesagt, $\mathfrak{i} : (\neg, \wedge, \vee, \longrightarrow, \mathsf{F}, \mathsf{T}) \mapsto (\bar{\ }, \sqcap, \sqcup, \backslash, \bot, \top)$

PRL-Semantik: $\mathbb{N}_0$-Arithmetik

Def. 9: PRL-Semantik in $\mathbb{N}_0$-Arithmetik $\mathcal{I}^{\alpha}_{\mathbb{N}_0}.p$

Man wählt die natürliche Arithmetik mit $\leq$ auf $\Omega = \{0,1\} \subseteq \mathbb{N}_0$:

$$
\begin{array}{lll}
1. & \mathcal{I}^{\alpha}_{\mathbb{N}_0}.p & = & \alpha(p) \text{ für } p \in \mathrm{Prp} \\
2. & \mathcal{I}^{\alpha}_{\mathbb{N}_0}.\neg p & = & 1 - \mathcal{I}^{\alpha}_{\mathbb{N}_0}.p \\
3. & \mathcal{I}^{\alpha}_{\mathbb{N}_0}.(p \wedge q) & = & \min(\{\mathcal{I}^{\alpha}_{\mathbb{N}_0}.p, \mathcal{I}^{\alpha}_{\mathbb{N}_0}.q\}) \\
4. & \mathcal{I}^{\alpha}_{\mathbb{N}_0}.(p \vee q) & = & \max(\{\mathcal{I}^{\alpha}_{\mathbb{N}_0}.p, \mathcal{I}^{\alpha}_{\mathbb{N}_0}.q\}) \\
5. & \mathcal{I}^{\alpha}_{\mathbb{N}_0}.(p \longrightarrow q) & = & \max(\{1 - \mathcal{I}^{\alpha}_{\mathbb{N}_0}.p, \mathcal{I}^{\alpha}_{\mathbb{N}_0}.q\})
\end{array}
$$

sowie $\mathcal{I}^{\alpha}_{\mathbb{N}_0}.\mathsf{T} = 1$, $\mathcal{I}^{\alpha}_{\mathbb{N}_0}.\mathsf{F} = 0$.

Kurz gesagt, $\mathfrak{i} : (\neg, \wedge, \vee, \mathsf{F}, \mathsf{T}) \mapsto (\lambda x.1 - x,\ \min, \max, 0, 1)$ und $\longrightarrow_{\mathfrak{i}}$ wird über $\neg_{\mathfrak{i}}$ und $\vee_{\mathfrak{i}}$ definiert

PRL-Semantik: Halbringsemantik

Def. 10: PRL-Semantik via Halbring $\mathcal{I}^{\alpha}_{\mathfrak{S}}.p$

Man wählt einen idempotenten kommutativen Halbring $\mathfrak{S} = \langle \Omega, \cdot, +, \mathsf{e}, \mathsf{n} \rangle$ mit $\Omega = \{\mathsf{n}, \mathsf{e}\}$ und definiert ein Komplement $^-$ als $x + x^- = \mathsf{e}$ und $x \cdot x^- = \mathsf{n}$.

$$
\begin{array}{llcl}
1. & \mathcal{I}^{\alpha}_{\mathfrak{S}}.p & = & \alpha(p) \text{ für } p \in \mathrm{Prp} \\
2. & \mathcal{I}^{\alpha}_{\mathfrak{S}}.\neg p & = & (\mathcal{I}^{\alpha}_{\mathfrak{S}}.p)^- \\
3. & \mathcal{I}^{\alpha}_{\mathfrak{S}}.(p \wedge q) & = & \mathcal{I}^{\alpha}_{\mathfrak{S}}.p \cdot \mathcal{I}^{\alpha}_{\mathfrak{S}}.q \\
4. & \mathcal{I}^{\alpha}_{\mathfrak{S}}.(p \vee q) & = & \mathcal{I}^{\alpha}_{\mathfrak{S}}.p + \mathcal{I}^{\alpha}_{\mathfrak{S}}.q \\
5. & \mathcal{I}^{\alpha}_{\mathfrak{S}}.(p \longrightarrow q) & = & (\mathcal{I}^{\alpha}_{\mathfrak{S}}.p)^- + \mathcal{I}^{\alpha}_{\mathfrak{S}}.q = \mathcal{I}^{\alpha}_{\mathfrak{S}}.p \backslash \mathcal{I}^{\alpha}_{\mathfrak{S}}.q
\end{array}
$$

sowie $\mathcal{I}^{\alpha}_{\mathfrak{S}}.\mathsf{T} = \mathsf{e}$, $\mathcal{I}^{\alpha}_{\mathfrak{S}}.\mathsf{F} = \mathsf{n}$.
$x = x^{--}$ folgt aus $x + x^- = x^- + x^{--} = \mathsf{e}$.

Der Linguistentrick

Das Linguistenproblem

Um die Bedeutung des Satzes "Karlchen fährt Roller" zu definieren, muß man sie "hinschreiben" können.

Die Linguistenlösung

Def. Die Bedeutung des Satzes *Karlchen fährt Roller* ist *Karlchen fährt Roller*'.

Die Anwendung des Linguistentricks p'

Wann immer $\mathcal{I} = \langle \mathfrak{i}, \alpha \rangle$ und somit auch $\mathfrak{A}$ durch Kontext definiert sind, kann man sie weglassen.

$$\text{Die Semantik von } p \text{ ist } \mathcal{I}_{\mathfrak{A}}^{\alpha}.p =: p'.$$

Tabellen-, $\mathcal{B}$-, $\mathbb{N}_0$- und $\mathfrak{S}$-Semantik sind gleichwertig

Thm. 1: Alle Semantiken sind isomorph (Umbenennung Ω)

$$p' \simeq \mathcal{I}^{\alpha}.p \simeq \mathcal{I}^{\alpha}_{\mathcal{B}}.p \simeq \mathcal{I}^{\alpha}_{\mathbb{N}_0}.p \simeq \mathcal{I}^{\alpha}_{\mathfrak{S}}.p$$

wobei $\mathbf{1} \simeq \top \simeq 1_{\mathbb{N}_0} \simeq$ e und $\mathbf{0} \simeq \bot \simeq 0_{\mathbb{N}_0} \simeq$ n.

Bew.

$\mathsf{T}' = \mathbf{1} \simeq \top = \mathcal{I}_{\mathcal{B}}.\mathsf{T} \simeq \mathcal{I}_{\mathbb{N}_0}.\mathsf{T} = 1 \simeq \mathsf{e} = \mathcal{I}_{\mathfrak{S}}.\mathsf{T}$.

$\mathcal{I}^{\alpha}.p$	$\mathcal{I}^{\alpha}.q$	$\mathcal{I}^{\alpha}_{\mathfrak{A}}.(p \wedge q)$	$\mathcal{I}^{\alpha}_{\mathcal{B}}.(p \wedge q)$	$\mathcal{I}^{\alpha}_{\mathbb{N}_0}.(p \wedge q)$	$\mathcal{I}^{\alpha}_{\mathfrak{S}}.(p \wedge q)$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\bot \sqcap \bot = \bot$	$\min(\{0,0\}) = 0$	$\mathsf{n} \cdot \mathsf{n} = \mathsf{n}$
$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$	$\bot \sqcap \top = \bot$	$\min(\{0,1\}) = 0$	$\mathsf{n} \cdot \mathsf{e} = \mathsf{n}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$	$\top \sqcap \bot = \bot$	$\min(\{1,0\}) = 0$	$\mathsf{e} \cdot \mathsf{n} = \mathsf{n}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\top \sqcap \top = \top$	$\min(\{1,1\}) = 1$	$\mathsf{e} \cdot \mathsf{e} = \mathsf{e}$

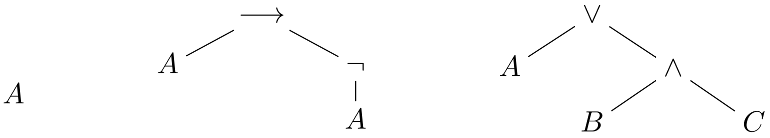
Die Beweise für F', $\neg$, $\vee$ und $\longrightarrow$ folgen dem selben Schema.

Auswertung von Formeln

Formeln als Bäume

1. Jedes Vorkommen jeder Aussagenvariablen ist ein Blatt
2. "Formelbäume" werden durch Einführung einer neuen Wurzel mit den Argumenten als Nachfolgern konstruiert.

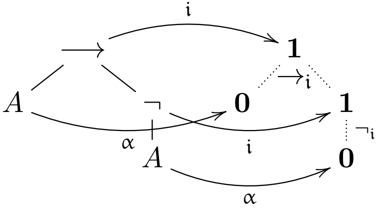
Beispiel: A, $(A \longrightarrow \neg A)$ und $(A \vee (B \wedge C))$

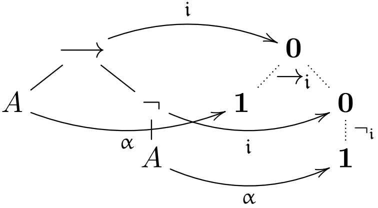


Jeder Knoten ist Wurzel einer Teilformel.
Eine Formel kann bottom-up durch $\mathcal{I} = \langle \mathfrak{i}, \alpha \rangle$ ausgewertet werden.

Auswertung von Formeln

Baumdarstellung von $(A \longrightarrow \neg A)$





Tabellendarstellung von $(A \longrightarrow \neg A)$

A	$p = \neg A$	$(A \longrightarrow p)$
0	**1**	**1**
1	**0**	**0**

2.3.
WAHRHEIT, ERFÜLLBARKEIT, GÜLTIGKEIT UND MODELLE

Wahrheit und Erfüllbarkeit

Wahrheit, Gültigkeit

Wahrheit oder Gültigkeit einer Aussage hängt von $\mathcal{I} = \langle \mathfrak{i}, \alpha \rangle$ ab.
Die *Wahrheit* einer Formel hängt insbesondere ab von

- der tatsächlichen Belegung α

wohingegen die *Gültigkeit* einer Formel unabhängig von konkreten α ist ("für alle α wahr ergeben muß") und somit

- von $\mathfrak{i}$ abhängt.

Daher benennen wir α und $\mathrm{cod}(\mathfrak{i})$ der Deutlichkeit halber explizit.

Def. 11: Eine abstrakte Definition

Eine Formel $p \in$ L ist ω-*wahr bzgl.* Ω *und* α *in* $\mathfrak{A}$ *unter* $\mathcal{I}$ gdw:

$$\mathcal{I}^{\alpha}_{\mathfrak{A}}.p \sqsupseteq \omega$$

wobei Ω durch $\sqsubseteq$ partiell geordnet ist.

Wiederholung: Semantik von PRL, Interpretation

Wähle:

$$\mathfrak{A} = \mathcal{B} = \langle \mathcal{U}, \sqcap, \sqcup, \setminus, ^{-}, \top, \bot \rangle \text{ mit } \sqsubseteq$$
$$\mathcal{U} = \Omega = \{\mathbf{0}, \mathbf{1}\} \simeq \{\bot, \top\}$$
$$\alpha : \mathrm{Prp} \to \Omega$$
$$\mathfrak{i} : \Sigma \to \mathcal{B}$$

Dann ist die Semantik schnell definiert:

$$\begin{aligned} \mathcal{I}^{\alpha}_{\mathcal{B}}.p &:= \alpha(p), \text{ für } p \in \mathrm{Prp} \\ \mathcal{I}^{\alpha}_{\mathcal{B}}.\neg p &:= \neg_{\mathfrak{i}} \mathcal{I}^{\alpha}_{\mathcal{B}}.p = \overline{\mathcal{I}^{\alpha}_{\mathcal{B}}.p} \\ \mathcal{I}^{\alpha}_{\mathcal{B}}.(p \circledast q) &:= \mathcal{I}^{\alpha}_{\mathcal{B}}.p \circledast_{\mathfrak{i}} \mathcal{I}^{\alpha}_{\mathcal{B}}.q \end{aligned}$$

mit $\mathfrak{i} : \{\neg, \wedge, \vee, \longrightarrow, \mathsf{F}, \mathsf{T}\} \mapsto \{^{-}, \sqcap, \sqcup, \setminus, \bot, \top\}$.

Vorschau: $\{\neg, \wedge, \vee, \longrightarrow, \mathsf{F}, \mathsf{T}\}$ ist eine *Signatur* Σ, und $\mathfrak{A}$ eine Σ-*Algbra*.

Wahrheit und Erfüllbarkeit

Def. 12: *Erfüllbarkeit, Modelle* $\models, Sat_{\mathcal{I}}(p)$

1. $\mathcal{I}^{\alpha}_{\mathfrak{A}}$ *erfüllt* $p \in \mathrm{Fml}_{\mathsf{PRL}}$ gdw. $\mathcal{I}^{\alpha}_{\mathfrak{A}}.p = \mathbf{1}$. Man schreibt $\mathcal{I}^{\alpha} \models p$.
2. p *gilt* unter $\mathcal{I}$, gdw. $\mathcal{I}^{\alpha}.p = \mathbf{1}$ *für alle* α. Man schreibt $\mathcal{I} \models p$.
3. p ist *erfüllbar*, wenn es erfüllende $\mathcal{I}^{\alpha}$ für p gibt.
4. $Sat_{\mathcal{I}}(p) := \{\alpha \parallel \alpha \text{ erfüllt } p\}$ heißt die *Erfüllungsmenge* von p.
5. p ist also *gültig*, gdw. $Sat_{\mathcal{I}}(p) = \Omega^{\mathrm{Prp}}$. Man schreibt auch $\models p$.

Da in PRL $\mathfrak{i}$ idR fix ist, ist $\mathcal{I}$ gleichbedeutend mit α.

Bemerkung

Manche nennen $\mathfrak{A}$ bereits ein Modell und schreiben $\mathfrak{A} \models p$. Andere nennen $\mathcal{I}^{\alpha}$ ein Model, schreiben aber $\mathfrak{A} \models_{\alpha} p$. Für uns ist die *Interpretation* $\mathfrak{i}$ die eigentliche *Modellierung*; $\mathfrak{A}$ ist eigentlich die "Theorie" vor deren Hintergrund wir logische Ausdrücke interpretieren.

Semantische Implikation, Folgerung

Subjunktion vs. Implikation

Die *Subjunktion* dient der *Darstellung* einer Aussage "Wenn p, dann q" als $(p \longrightarrow q)$. *Implikation bedeutet*, daß wenn p gilt, auch q gilt.

Def. 13: Implikation und Äquivalenz $\Longrightarrow, \Longleftrightarrow$

p *impliziert* q, gdw. $p \Longrightarrow q$ gdw. $p\boldsymbol{'} \sqsubseteq q\boldsymbol{'}$:

$$\text{Wenn } \mathcal{I}^{\alpha}_{\mathfrak{A}}.p = \mathbf{1} \text{ dann } \mathcal{I}^{\alpha}_{\mathfrak{A}}.q = \mathbf{1}$$

Man schreibt dann $p \Longrightarrow q$. p und q heißen *äquivalent*, $p \Longleftrightarrow q$, gdw. $(p \Longrightarrow q \wedge q \Longrightarrow p)$.

Andere Schreibweisen: $p \equiv q$, $p \mathrel{=\!\!|\!\models} q$, $\mathrel{|\!\approx}$ ...

Kor. $p \Longrightarrow q$ gdw $Sat_{\mathcal{I}}(p) \subseteq Sat_{\mathcal{I}}(q)$.

Formelmengen

Formelmengen $P \subseteq \mathrm{Fml}$, Lifting.

Eine Formelmenge P hat eine Eigenschaft E, wenn *alle* $p \in P$ die Eigenschaft E haben.
Sei $P \subseteq \mathrm{Fml}$.

- P ist *erfüllbar*, gdw. es gibt α, die *alle* $p \in P$ erfüllt. Andernfalls heißt P *unerfüllbar* oder *widersprüchlich*.
- $\mathcal{I}^{\alpha}_{\mathfrak{A}}.P = \mathbf{1}$ gdw. $\mathcal{I}^{\alpha}_{\mathfrak{A}}.p = \mathbf{1}$ für alle $p \in P$.
- $\mathcal{I} \models P$ gdw. $\mathcal{I} \models p$ für alle $p \in P$.
- $Sat_{\mathcal{I}}(P)$ bezeichnet die Erfüllungsmenge von P.

Kor.

$$P \subseteq \mathrm{Fml} \text{ ist erfüllbar gdw. } Sat_{\mathcal{I}}(P) = \bigcap_{p \in P} Sat_{\mathcal{I}}(p) \neq \emptyset.$$

Erfüllbarkeit von Formelmengen

Kor.

$$Sat(P) = Sat(\bigwedge P).$$

Für $P, Q \subseteq \mathrm{Fml}$,

$$\begin{array}{ccc} \text{Wenn } P \subseteq Q & \text{dann} & Sat(Q) \subseteq Sat(P) \\ Sat(P \cup Q) & \subseteq & Sat(P) \cap Sat(Q). \end{array}$$

Hinweis: P, Q sind endlich.

Erfüllbarkeit von Formelmengen

Bew. $Sat(P) = Sat(\bigwedge P)$.

1. Sei α in $Sat(P)$.
2. Dann erfüllt α alle $p_i \in P = \{p_1, \ldots, p_n\}$.
3. Daher, $\mathcal{I}^\alpha.p_1 = \mathbf{1}$ und $\cdots$ und $\mathcal{I}^\alpha.p_n = \mathbf{1}$.
4. Nach Definition der Konjunktion,
   $\mathcal{I}^\alpha.(p_1 \wedge p_2) = \mathbf{1}$ und $\mathcal{I}^\alpha.p_3 = \mathbf{1}$ und $\cdots$ und $\mathcal{I}_\alpha.p_n = \mathbf{1}$.
5. Iterierte Anwendung ergibt $\mathcal{I}^\alpha.(((p_1 \wedge p_2) \wedge \cdots) \wedge p_n) = \mathbf{1}$.
6. Es folgt also $\mathcal{I}^\alpha \models (((p_1 \wedge p_2) \wedge \cdots) \wedge p_n)$;
7. kurz $\mathcal{I}^\alpha \models \bigwedge P$, und somit letztendlich
8. $\alpha \in Sat(\bigwedge P)$.

Jeder Schritt ist auch in umgekehrter Richtung gültig ($\supseteq$) und somit ist die Gleichheit gezeigt.

Erfüllbarkeit von Formelmengen

Bew. Wenn $P \subseteq Q$ dann $Sat(Q) \subseteq Sat(P)$

1. Seien $P \subseteq Q$ und $\alpha \in Sat(Q)$.
2. $\alpha \in Sat(Q)$ bedeutet $\mathcal{I}^{\alpha}.q = \mathbf{1}$ für *alle* $q \in Q$.
3. Da $P \subseteq Q$, gilt für jedes (erfüllte) $q \in Q$ auch $q \in P \subseteq Q$
4. Somit erfüllt jedes Q erfüllende α auch P: $Sat(Q) \subseteq Sat(P)$.

Bew. $Sat(P \cup Q) \subseteq Sat(P) \cap Sat(Q)$

1. Sei $\alpha \in Sat(P \cup Q)$.
2. Dann erfüllt α alle $p \in P$ und α erfüllt alle $q \in Q$.
3. Daher $\alpha \in Sat(P) \cap Sat(Q)$.

2.4.
FOLGERUNGEN

Äquivalenzumformungen

Thm. 2: Ersetzung äquivalenter Teilformeln

Sei $p \in \mathrm{Fml}$ mit einer Teilformel q. Sei r mit $q \Longleftrightarrow r$. Die Ersetzung von Vorkommen von q in p durch r resultiert in einer Formel p' für die gilt: $p \Longleftrightarrow p'$.

“Beweis”

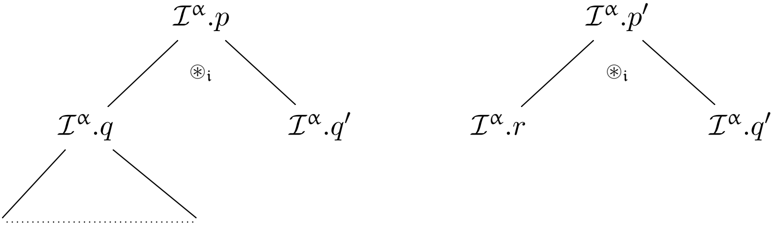
- Die “Baumauswertung” von p' gleicht der Auswertung von p.
- Nur an den Stellen, in denen in p die Formel q steht, steht in p' die Formel r.
- Da $q \Longleftrightarrow r$, ist für alle α-Belegung an der Front des Baumes immer $\mathcal{I}^{\alpha}.q = \mathcal{I}^{\alpha}.r$.
- Damit ändert sich der Wahrheitswert an dieser Stelle nicht und entsprechend auch nicht weiter aufwärts bis zur Wurzel.
- Der Wahrheitswert bleibt also erhalten.

Äquivalenzumformungen

Thm. 3: Ersetzung äquivalenter Teilformeln

Sei $p \in \mathrm{Fml}$ mit einer Teilformel q. Sei r mit $q \Longleftrightarrow r$. Die Ersetzung von Vorkommen von q in p durch r resultiert in einer Formel p' für die gilt: $p \Longleftrightarrow p'$.

"Beweis"

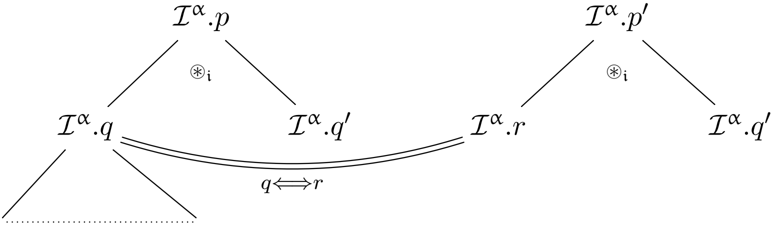


Äquivalenzumformungen

Thm. 4: Ersetzung äquivalenter Teilformeln

Sei $p \in \mathrm{Fml}$ mit einer Teilformel q. Sei r mit $q \iff r$. Die Ersetzung von Vorkommen von q in p durch r resultiert in einer Formel p' für die gilt: $p \iff p'$.

“Beweis”

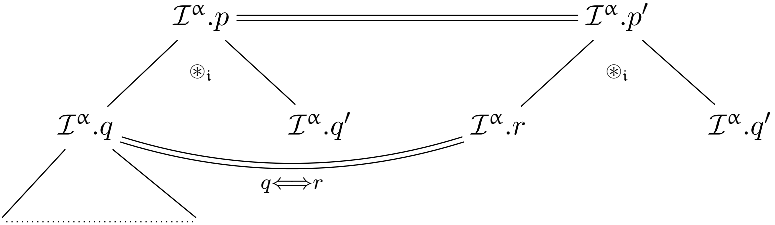


Äquivalenzumformungen

Thm. 5: Ersetzung äquivalenter Teilformeln

Sei $p \in \mathrm{Fml}$ mit einer Teilformel q. Sei r mit $q \iff r$. Die Ersetzung von Vorkommen von q in p durch r resultiert in einer Formel p' für die gilt: $p \iff p'$.

"Beweis"

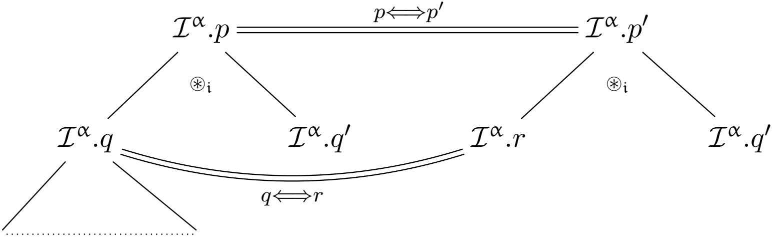


Äquivalenzumformungen

Thm. 6: Ersetzung äquivalenter Teilformeln

Sei $p \in \mathrm{Fml}$ mit einer Teilformel q. Sei r mit $q \Longleftrightarrow r$. Die Ersetzung von Vorkommen von q in p durch r resultiert in einer Formel p' für die gilt: $p \Longleftrightarrow p'$.

“Beweis”



Äquivalenzumformungen

Thm. 7: Ersetzung äquivalenter Teilformeln

Sei $p \in \mathrm{Fml}$ mit einer Teilformel q. Sei r mit $q \Longleftrightarrow r$. Die Ersetzung von Vorkommen von q in p durch r resultiert in einer Formel p' für die gilt: $p \Longleftrightarrow p'$.

Bew.

B Sei $p = q$. Dann $\mathcal{I}^\alpha.p = \mathcal{I}^\alpha.q = \mathcal{I}^\alpha.r = \mathcal{I}^\alpha.p'$.

A Gelte Behauptung für q, q'.

C
1. $p = \neg q$. Dann
   $\mathcal{I}^\alpha.p = \mathcal{I}^\alpha.\neg q = 1 - \mathcal{I}^\alpha.q \stackrel{\mathsf{A}}{=} 1 - \mathcal{I}^\alpha.r = \mathcal{I}^\alpha.\neg r = \mathcal{I}^\alpha.p'$.
2. $p = q \circledast q'$. Dann
   $\mathcal{I}^\alpha.p = \mathcal{I}^\alpha.q \circledast_{\mathrm{i}} \mathcal{I}^\alpha.q' \stackrel{\mathsf{A}}{=} \mathcal{I}^\alpha.r \circledast_{\mathrm{i}} \mathcal{I}^\alpha.r' = \mathcal{I}^\alpha.(r \circledast r') = \mathcal{I}^\alpha.p'$.

Subjunktion und "Kleiner-Gleich"

Lemma. "$\longrightarrow_{\text{i}}=\leq$"

$$\mathcal{I}^\alpha \models (p \longrightarrow q) \text{ gdw. } \mathcal{I}^\alpha.(p \longrightarrow q) = \mathbf{1} \text{ gdw. } \mathcal{I}^\alpha.p \leq \mathcal{I}^\alpha.q.$$

Bew. Über Wahrheitstabelle

Lemma. Konditionale Abschwächung

Wenn q (sowieso) gilt, gilt q auch, falls (außerdem) p gilt.

$$\mathcal{I}^\alpha.q = \mathbf{1} \quad \Longrightarrow \quad \mathcal{I}^\alpha.(p \longrightarrow q) = \mathbf{1}$$

Bew. Über Wahrheitstabelle

p'	q'	$(p \longrightarrow q)'$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$

"Entailment", Schluß, Implikation, Folgerung

Def. 14: Schlussfolgerung, (logisches) "Schliessen" $\mid\!\approx$

p *folgt aus* P gdw. wenn P erfüllt ist, auch p erfüllt ist:

$$P \mid\!\approx p \text{ gdw } \mathcal{I} \models P \Longrightarrow \mathcal{I} \models p$$

d.h. "jedes Modell von P ist auch ein Modell von p".

ACHTUNG: In der Literatur wird oft $\models$ statt $\mid\!\approx$ benutzt.

In einfachen Worten...

$Sat(P)$ ist die Menge aller "Welten", in denen alle p aus P wahr werden. **Wenn** in jeder dieser Welten auch q erfüllt ist, **dann**:

Die Erfüllbarkeit von q schließt die Erfüllbarkeit von P mit ein:

$$Sat(P) \subseteq Sat(q).$$

Wenn also P "gilt", dann folglich auch q.

Allgemeingültigkeit und Tautologien

Def. 15: Allgemeingültigkeit von Tautologien

Eine Tautologie folgt aus dem Nichts:

$$\begin{aligned}
\{\} \mathrel{|}\!\approx p \quad & \text{gdw.} \quad \text{Für alle } \mathcal{I} \text{ gilt: } \mathcal{I} \models \{\} \Longrightarrow \mathcal{I} \models p \\
& \text{gdw.} \quad \text{Für alle } \mathcal{I} \text{ gilt: } \mathcal{I} \models q \text{ für alle } q \in \{\} \Longrightarrow \mathcal{I} \models p \\
& \text{gdw.} \quad \text{Für alle } \mathcal{I} \text{ gilt: } \mathsf{T} \Longrightarrow \mathcal{I} \models p \\
& \text{gdw.} \quad \text{Für alle } \mathcal{I} \text{ gilt: } \mathcal{I} \models p \\
& \text{gdw.} \quad \models p
\end{aligned}$$

Unerfüllbarkeit

Thm. 8: F ist unerfüllbar

F hat kein Modell.

Thm. 9: Ex falso sequitur quodlibet (Explosionsprinzip)

Es gilt für alle $p \in \mathrm{Fml}$ und $P \subseteq \mathrm{Fml}$:

$$\mathsf{F} \in P \Longrightarrow P \mid\!\approx p$$

Bew. Durch Widerspruch: Gelte $\mathsf{F} \in P$ aber $P \not\mid\!\approx p$.

$$\begin{aligned} \mathsf{F} \in P &\Longrightarrow P \text{ unerfüllbar} \\ &\Longrightarrow P \text{ hat kein Modell} \end{aligned}$$

$$\begin{aligned} P \not\mid\!\approx p &\Longrightarrow \text{Es gibt ein Modell } \mathcal{I}^{\alpha} \text{ mit } \mathcal{I}^{\alpha} \models P \text{ aber } \mathcal{I}^{\alpha}.p = \mathbf{0} \\ &\Longrightarrow \text{Es gibt ein Modell } \mathcal{I}^{\alpha} \text{ von } P \end{aligned}$$

Widerspruch.

Meta-X

"Meta"-Aussagen

p kann nun immer als eine konkrete Formel oder aber auch als eine "Metavariable" für alle äquivalenten Formeln benutzt werden.

Man setzt generös $\mathfrak{i}$- und $\mathfrak{A}$-Kompatibilät voraus und schreibt:

"Meta"-Logische Ausdrücke

- $p \Longleftrightarrow q$ ist eine Aussage.
- "$\{p\} \approx q$ und $\{q\} \approx p$" ist eine Aussage.
- "$p \Longleftrightarrow q$ gdw. $\{p\} \approx q$ und $\{q\} \approx p$" formuliert eine Äquivalenz:

$$(p \Longleftrightarrow q) \overset{\text{"gdw"}}{\Longleftrightarrow} (\{p\} \approx q \wedge \{q\} \approx p)$$

Deshalb i.d. Lit. "iff", $\equiv$, $=\!\!|\!\!\models$ statt $\Longleftrightarrow$, ...

Das (semantische) Deduktionstheorem

Thm. 10: Das Deduktionstheorem für PRL(I/II) DT

$$P \cup \{p\} \mathrel{|\!\approx} q \implies P \mathrel{|\!\approx} (p \longrightarrow q)\,.$$

Bew.

1. Gelte $P \cup \{p\} \mathrel{|\!\approx} q$ aber $P \mathrel{|\!\not\approx} (p \longrightarrow q)$.
2. Dann existiert $\mathcal{I}^{\alpha}$ mit $\mathcal{I}^{\alpha} \models P$ aber $\mathcal{I}^{\alpha}.(p \longrightarrow q) = \mathbf{0}$.
3. Wegen $\longrightarrow_{\mathfrak{i}}$ muss dann gelten: $\mathcal{I}^{\alpha} \models p$ aber $\alpha_q.{=}\mathbf{0}$.
4. Da aber $\mathcal{I}^{\alpha} \models P$ und $\mathcal{I}^{\alpha} \models p$ gilt wegen 1: $\mathcal{I}^{\alpha}.q = \mathbf{1}$
5. Widerspruch!

Das (semantische) Deduktionstheorem

Thm. 11: Das Deduktionstheorem für PRL(II/II) DT

$$P \cup \{p\} \mathrel{|\!\approx} q \;\Longleftarrow\; P \mathrel{|\!\approx} (p \longrightarrow q)\,.$$

Bew.

Wir zeigen die Kontraposition $P \cup \{p\} \mathrel{|\!\not\approx} q \;\Longrightarrow\; P \mathrel{|\!\not\approx} (p \longrightarrow q)\,.$

1. Gelte $P \cup \{p\} \mathrel{|\!\not\approx} q$
2. Also existiert α mit $\mathcal{I}^\alpha.(\bigwedge P \wedge p) = \mathbf{1}$ und $\mathcal{I}^\alpha.q = \mathbf{0}$.
3. Gemäß der Semantik von $\wedge$ gilt für diese α, daß $\mathcal{I}^\alpha.\bigwedge P = \mathbf{1}$ und $\mathcal{I}^\alpha.p = \mathbf{1}$ und $\mathcal{I}^\alpha.q = \mathbf{0}$.
4. Insbesondere also $\mathcal{I}^\alpha.p = \mathbf{1}$ und $\mathcal{I}^\alpha.q = \mathbf{0}$.
5. Nach Semantik von $\longrightarrow$ ist dann $\mathcal{I}^\alpha.(p \longrightarrow q) = \mathbf{0}$, also
6. $P \mathrel{|\!\not\approx} (p \longrightarrow q)\,.$

Anwendung des Deduktionstheorems

Das Deduktionstheorem in Anwendung

Um zu zeigen, daß $(p \longrightarrow q)$ aus P folgt,

$$P \approx\!\!\!\!| \; (p \longrightarrow q)$$

reicht es zu zeigen, daß q aus P zusammen mit p folgt:

$$P \cup \{p\} \approx\!\!\!\!| \; q$$

weil

$$\textbf{Wenn } P \cup \{p\} \approx\!\!\!\!| \; q, \textbf{ dann } P \approx\!\!\!\!| \; (p \longrightarrow q)\,.$$

Wie man Subjunktionen beweist

Um die Gültigkeit von $(p \longrightarrow q)$ zu zeigen, *nehme man an* daß p gilt und zeigt dann, daß daraus q *folgt* ("$\Longrightarrow$").

Beispiel

Beispiel zur Anwendung des Deduktionstheorems

Zur zeigen sei, daß $(p \longrightarrow (q \longrightarrow p))$ eine Tautologie ist:

	$\models (p \longrightarrow (q \longrightarrow p))$	$\vert$: Def. Tautologie
gdw.	$\{\} \mathrel{\vert\!\approx} (p \longrightarrow (q \longrightarrow p))$	$\vert$: Deduktionstheorem
gdw.	$\{p\} \mathrel{\vert\!\approx} (q \longrightarrow p)$	$\vert$: Deduktionstheorem
gdw.	$\{p\} \cup \{q\} \mathrel{\vert\!\approx} p$	
gdw.	$\{p, q\} \mathrel{\vert\!\approx} p$	$\vert$: Def. Entailment
gdw.	$(\mathcal{I}^\alpha \models p \wedge \mathcal{I}^\alpha \models q) \Longrightarrow \mathcal{I}^\alpha \models p$	
ist	immer wahr.	

2.5.
TAUTOLOGIEN UND ÄQUIVALENZEN

Belegungsänderung (“Substitutionen”)

Def. 16: Punktweise Funktionsänderung

Sei $f : \mathcal{U} \to \mathcal{V}$ eine Funktion.

$$f \langle y \hookleftarrow a \rangle (x) := \begin{cases} a, & x = y \\ f(x), & \text{sonst.} \end{cases}$$

Lemma (Koinzidenzlemma für PRL**).**

Bezeichne $Var(p)$ die Menge aller Aussagenvariablen in p. Dann

$$\mathcal{I}^{\alpha}.p = \mathcal{I}^{\alpha'}.p$$

für alle $\alpha' \in \{\beta \parallel X \in Var(p) \wedge \alpha(X) = \beta(X)\}$.

Kor. Unwirksame Belegungen sind beliebig veränderbar.

Negation und Dualität

Thm. 12: Negation und Äquivalenz NEG

$$p \iff \neg q \text{ gdw } \neg p \iff q.$$

Bew. $\mathsf{T} \iff p \iff \neg q$ gdw. $q \iff \mathsf{F} \iff \neg p$

$Sat(p) = Sat(\neg q) = \overline{Sat(q)} = \overline{\overline{Sat(p)}} = \overline{Sat(\neg p)}$.

Thm. 13: Dualität DUA

$$(p \wedge q) \iff \neg(\neg p \vee \neg q) \quad \text{und} \quad (p \vee q) \iff \neg(\neg p \wedge \neg q)$$

Bew. Kurz: In $\mathcal{B}$ sind $\sqcap$ und $\sqcup$ dual. — Lange Version:

p'	q'	$(p \wedge q)'$	$\neg p'$	$\neg q'$	$(\neg p \vee \neg q)'$	$\neg(\neg p \vee \neg q)'$
0	**0**	**0**	**1**	**1**	**1**	**0**
0	**1**	**0**	**1**	**0**	**1**	**0**
1	**0**	**0**	**0**	**1**	**1**	**0**
1	**1**	**1**	**0**	**0**	**0**	**1**

Tautologien

Thm. 14: Tautologien

Jede Instanziierung der folgenden Formelschemata ist eine Tautologie:

1. $(p \vee \neg p)$ sowie $\neg\,(p \wedge \neg p)$
2. $(p \longrightarrow (q \longrightarrow p))$
3. $(p \longrightarrow q) \longrightarrow ((p \longrightarrow (q \longrightarrow r)) \longrightarrow (p \longrightarrow r))$
4. $(p \longrightarrow (q \longrightarrow (p \wedge q)))$
5. $((p \wedge q) \longrightarrow p)$ sowie $((p \wedge q) \longrightarrow q)$.
6. $(p \longrightarrow (p \vee q))$ sowie $(q \longrightarrow (p \vee q))$
7. $((\neg(\neg p)) \longrightarrow p)$
8. $((p \longrightarrow r) \longrightarrow ((q \longrightarrow r) \longrightarrow ((p \vee q) \longrightarrow r)))$.
9. $((p \longrightarrow q) \longrightarrow ((p \longrightarrow \neg q) \longrightarrow \neg p))$.

Äquivalenzen

Thm. 15: Äquivalenzen und Umformungsregeln

Negation	:	p	$\Longleftrightarrow$	$\neg\neg p$	NEG
Implication	:	$(p \longrightarrow q)$	$\Longleftrightarrow$	$(\neg p \vee q)$	IMP
Contrapos.	:	$(p \longrightarrow q)$	$\Longleftrightarrow$	$(\neg q \longrightarrow \neg p)$	CTP
Shunting	:	$((p \wedge q) \longrightarrow r)$	$\Longleftrightarrow$	$(p \longrightarrow (\neg q \vee r))$	SHN
deMorgan	:	$\neg (p \wedge q)$	$\Longleftrightarrow$	$(\neg p \vee \neg q)$	DEM
Distributivity $\wedge$	:	$(p \wedge (q \vee r))$	$\Longleftrightarrow$	$((p \wedge q) \vee (p \wedge r))$	DST
Distributivity $\vee$	:	$(p \vee (q \wedge r))$	$\Longleftrightarrow$	$((p \vee q) \wedge (p \vee r))$	DST
Weakening $\wedge$	:	$(p \wedge q)$	$\Longrightarrow$	p	WKN
Weakening $\vee$	:	p	$\Longrightarrow$	$(p \vee q)$	WKN
	:	$\neg p$	$\Longleftrightarrow$	$(p \longrightarrow \mathsf{F})$	PSN
	:	$(\mathsf{F} \longrightarrow p)$	$\Longleftrightarrow$	T	EFQ
	:	$(\neg p \wedge p)$	$\Longleftrightarrow$	F	CTR

DEM basiert auf der Dualität DUA in Boole'scher Algebra.
Deshalb wird manchmal auch DUA statt DEM geschrieben.

Anwendung von Äquivalenzumformungen

Beispiel: “Doppelshunting” (DMLA) DSH

$$
\begin{array}{rl}
 & (p \longrightarrow (q \longrightarrow r)) \\
\overset{\text{IMP}}{\Longleftrightarrow} & (p \longrightarrow (\neg q \vee r)) \\
\overset{\text{SHN}}{\Longleftrightarrow} & ((p \wedge q) \longrightarrow r) \\
\overset{\text{COM}}{\Longleftrightarrow} & ((q \wedge p) \longrightarrow r) \\
\overset{\text{SHN}}{\Longleftrightarrow} & (q \longrightarrow (\neg p \vee r)) \\
\overset{\text{IMP}}{\Longleftrightarrow} & (q \longrightarrow (p \longrightarrow r))
\end{array}
$$

Äquivalenz und Tautologie

Thm. 16: Subjunktion und Implikation

$$p \Longrightarrow q \qquad \text{gdw} \qquad (p \longrightarrow q) \text{ ist eine Tautologie}$$

Bew.

$$\begin{aligned} p \Longrightarrow q \quad & \text{gdw} \quad \text{Wenn } \mathcal{I}^\alpha.p = \mathbf{1} \text{ dann } \mathcal{I}^\alpha.q = \mathbf{1} \text{ für alle } \mathcal{I}^\alpha \\ & \text{gdw} \quad \mathcal{I}^\alpha.(p \longrightarrow q) = \mathbf{1} \text{ für alle } \mathcal{I}^\alpha \\ & \text{gdw} \quad \models (p \longrightarrow q) \end{aligned}$$

Kor.

$$p \Longleftrightarrow q \qquad \text{gdw} \qquad (p \longleftrightarrow q) \text{ ist eine Tautologie}$$

3.
BEWEISE

Beweise

Was ist ein Beweis?

Ein Beweis ist ein formales Argument.
Ein Beweis ist eine endliche Sequenz zulässiger Folgerungen, die jeweils auf allen vorhergenden Folgerungen aufbauen können.
Man nutzt:

1. Direkte Beweise
2. Beweise durch Kontraposition
3. Beweise durch Widerspruch
4. Beweise durch Induktion

3.1.
BEWEISTECHNIKEN

Direkter Beweis mit Warheitstabellen

Beispiel: DUA/DEM

$$(p \wedge q) \Longleftrightarrow \neg(\neg p \vee \neg q) \quad \text{und} \quad (p \vee q) \Longleftrightarrow \neg(\neg p \wedge \neg q)$$

Bew. (direkt, Wahrheitstabelle):

p'	q'	$(p \wedge q)$'	$\neg p$'	$\neg q$'	$(\neg p \vee \neg q)$'	$\neg(\neg p \vee \neg q)$'
0	**0**	**0**	**1**	**1**	**1**	**0**
0	**1**	**0**	**1**	**0**	**1**	**0**
1	**0**	**0**	**0**	**1**	**1**	**0**
1	**1**	**1**	**0**	**0**	**0**	**1**

Die zweite Äquivalenz erhält man durch Vertauschen der Negation und Negation über Äquivalenz oder durch eine ähnliche Wahrheitstabelle.

Direkter Beweis durch Ableitung/Folgerung

Bew. Gültigkeit der Rangierregel SHN

$$
\begin{array}{rll}
 & ((p \wedge q) \longrightarrow r) & |\text{: Auflösen der Subjunktion} \\
\overset{\text{IMP}}{\Longleftrightarrow} & (\neg(p \wedge q) \vee r) & |\text{: Dualität} \\
\overset{\text{DUA}}{\Longleftrightarrow} & ((\neg p \vee \neg q) \vee r) & |\text{: Assoziativität der Disjunktion} \\
\overset{\text{ASC}}{\Longleftrightarrow} & (\neg p \vee (\neg q \vee r)) & |\text{: Einführung der Subjunktion} \\
\overset{\text{IMP}}{\Longleftrightarrow} & (p \longrightarrow (\neg q \vee r)) &
\end{array}
$$

Direkter Beweis zur Reduktion auf Tautologie

Bew. Gültigkeit der Abschwächungsregel: $(p \wedge q) \Longrightarrow q$

$$\begin{array}{lll}
 & ((p \wedge q) \longrightarrow q) & |: \text{ Auflösen der Subjunktion} \\
\overset{\text{IMP}}{\Longleftrightarrow} & (\neg\,(p \wedge q) \vee q) & |: \text{ Dualität} \\
\overset{\text{DUA}}{\Longleftrightarrow} & ((\neg p \vee \neg q) \vee q) & |: \text{ Assoziativität der Disjunktion} \\
\overset{\text{ASC}}{\Longleftrightarrow} & (\neg p \vee (\neg q \vee q)) & |: \text{ Tautologie} \\
\overset{\mathsf{T}}{\Longleftrightarrow} & (\neg p \vee \mathsf{T}) & |: \max(\{(\neg p)', 1\}) = 1 \\
\overset{\mathsf{T},\vee}{\Longleftrightarrow} & \mathsf{T} &
\end{array}$$

Beweis durch Kontraposition

Thm. 17: Kontraposition CTP

$$(p \longrightarrow q) \iff (\neg q \longrightarrow \neg p)$$

Bew. Gültigkeit des Kontrapositionsprinzips

$$
\begin{aligned}
& (p \longrightarrow q) && |\text{: Auflösen der Subjunktion} \\
\overset{\text{IMP}}{\iff} \; & (\neg p \vee q) && |\text{: Kommutativität} \\
\overset{\text{COM}}{\iff} \; & (q \vee \neg p) && |\text{: Doppelte Negation} \\
\overset{\text{NEG}}{\iff} \; & (\neg\neg q \vee \neg p) && |\text{: Einführung der Subjunktion} \\
\overset{\text{IMP}}{\iff} \; & (\neg q \longrightarrow \neg p)
\end{aligned}
$$

Zwei weitere Beweiswerkzeuge

Wechselseitige Inklusion

Anstatt $p \iff q$ zu beweisen, wird $p \implies q$ und $q \implies p$ bewiesen.

Die mit Abstand wichtigste Schlußregel und das mächtigste Beweiswerkzeug ist:

Modus Ponens MP

WENN...	p gilt und $(p \longrightarrow q)$ gilt,
DANN...	gilt auch q.

$\{p, (p \longrightarrow q)\} \mathrel{|}\!\approx q$ erlaubt es, einen Beweis für q zu zerlegen: Wenn $\mathcal{I}^\alpha \models p$ und wenn $\mathcal{I}^\alpha(p \longrightarrow q)$, dann folgt $\mathcal{I}^\alpha \models q$ durch Anwendung von MP.

Thm. 18: Kompaktheitstheorem

Sei $P \subseteq \mathrm{Fml}$ höchstens abzählbar unendlich.

P erfüllbar gdw. alle *endlichen* $Q \subseteq P$ sind erfüllbar.

Kor.

Eine Formelmenge ist *un*erfüllbar, gdw sie eine (endliche) unerfüllbare Teilmenge von Formeln hat.

Bew.

Sei P unerfüllbar. Genau dann existiert eine endliche Herleitung eines Widerspruchs, d.h. eine unerfüllbare endliche Teilmenge von Formeln. — Seien alle $Q \in \wp(P)$ erfüllbar (und insbesondere auch deren Abschlüsse unter $\neg, \wedge, \vee$). Dann existiert kein endlicher Widerspruch, somit folgt Erfüllbarkeit.

3.2.
NORMALFORMEN

Operatorbasis

Def. 17: Operatorbasis

Eine Menge von Operatoren heißt Operatorbasis, wenn sie vollständig bzgl. Boolescher Funktionen ist.

Thm. 19: $\{\uparrow\}$ ist eine minimale Operatorbasis

Bew.

$$
\begin{array}{lcl}
\mathsf{T} & \Longleftrightarrow & (p \uparrow (p \uparrow p)) \\
\neg p & \Longleftrightarrow & (p \uparrow p) \\
(p \vee q) & \overset{\text{DEM}}{\Longleftrightarrow} & \neg(\neg p \wedge \neg q) \\
 & \overset{\uparrow}{\Longleftrightarrow} & (\neg p \uparrow \neg q) \\
 & \overset{\neg}{\Longleftrightarrow} & ((p \uparrow p) \uparrow (q \uparrow q)) \\
(p \wedge q) & \overset{\text{NEG}}{\Longleftrightarrow} & \neg\neg(p \wedge q) \\
 & \overset{\uparrow}{\Longleftrightarrow} & \neg(p \uparrow q) \overset{\neg}{\Longleftrightarrow} ((p \uparrow q) \uparrow (p \uparrow q)) \\
(p \longrightarrow q) & \overset{\text{IMP}}{\Longleftrightarrow} & (\neg p \vee q) \overset{\neg,\vee}{\Longleftrightarrow} (((p \uparrow p) \uparrow (p \uparrow p)) \uparrow (q \uparrow q))
\end{array}
$$

Beispiele für Operatorbasen

$\{\neg, \wedge\}$

$(p \vee q) :\overset{\text{DEM}}{\Longleftrightarrow} \neg(\neg p \wedge \neg q)$ und $(p \longrightarrow q) :\overset{\text{IMP}}{\Longleftrightarrow} (\neg p \vee q)$.

$\{\longrightarrow, \mathsf{F}\}$

$\neg p :\overset{\text{PSN}}{\Longleftrightarrow} (p \longrightarrow \mathsf{F})$, $(p \vee q) \overset{\text{IMP}}{\Longleftrightarrow} (\neg p \longrightarrow q)$ und $\wedge$ über DEM

Beispiel

$$
\begin{aligned}
(p \wedge (q \vee \neg p)) &\overset{\text{PSN}}{\Longleftrightarrow} (p \wedge (q \vee (p \longrightarrow \mathsf{F}))) \\
&\overset{\text{IMP}}{\Longleftrightarrow} (p \wedge (\neg q \longrightarrow (p \longrightarrow \mathsf{F}))) \\
&\overset{\text{PSN}}{\Longleftrightarrow} (p \wedge ((q \longrightarrow \mathsf{F}) \longrightarrow (p \longrightarrow \mathsf{F}))) \\
&\overset{\text{DEM}}{\Longleftrightarrow} \neg(\neg p \vee \neg((q \longrightarrow \mathsf{F}) \longrightarrow (p \longrightarrow \mathsf{F}))) \\
&\overset{\text{IMP}}{\Longleftrightarrow} \neg(\neg\neg p \longrightarrow \neg((q \longrightarrow \mathsf{F}) \longrightarrow (p \longrightarrow \mathsf{F}))) \\
&\overset{\text{NEG}}{\Longleftrightarrow} \neg(p \longrightarrow \neg((q \longrightarrow \mathsf{F}) \longrightarrow (p \longrightarrow \mathsf{F}))) \\
&\overset{\text{PSN,PSN}}{\Longleftrightarrow} ((p \longrightarrow (((q \longrightarrow \mathsf{F}) \longrightarrow (p \longrightarrow \mathsf{F})) \longrightarrow \mathsf{F})) \longrightarrow \mathsf{F})
\end{aligned}
$$

n-stellige Operatoren auf o Wahrheitswerten

Logische Junktoren

Die Semantik logischer Junktoren sind durch *boole'sche Funktionen* definiert (Wahrheitstabellen). Somit ergeben sich

$$o^{o^n}$$

Definitionen n-stelliger Operatoren auf $o = \mathcal{C}(\Omega)$ Wahrheitswerten.
T und F sind eigentlich Abkürzungen für $(p \vee \neg p)$ und $(p \wedge \neg p)$.

Weitere Operatoren

NAND ($\uparrow$), NOR ($\downarrow$) und XOR ($\dot\vee$), konverse Subjunktion $\longleftarrow$, sowie $>$ und $<$ als Komplemente von $\longrightarrow$ und $\longleftarrow$:

$\uparrow$	**0**	**1**
0	**1**	**1**
1	**1**	**0**

$\downarrow$	**0**	**1**
0	**1**	**0**
1	**0**	**0**

$\dot\vee$	**0**	**1**
0	**0**	**1**
1	**1**	**0**

$\leftarrow$	**0**	**1**
0	**1**	**0**
1	**1**	**1**

$>$	**0**	**1**
0	**0**	**0**
1	**1**	**0**

$<$	**0**	**1**
0	**0**	**1**
1	**0**	**0**

Konjunktive/Disjunktive Normalform

Def. 18: Konjunktive/Disjunktive Normalform (KNF/DNF)

Formeln p, q liegen in KNF/DNF vor, gdw.

$$p = \bigwedge_i (\bigvee_j l_{i,j}) \text{ bzw. } q = \bigvee_i (\bigwedge_j l_{i,j})$$

wobei $l_{i,j}$ *Literale* ($\mathrm{Lit} = \mathrm{Prp} \cup \{\neg p \parallel p \in \mathrm{Prp}\}$) sind. Ein Literal $l \in \mathrm{Prp}$ heißt *positives* Literal; negierte Literale werden mit $\sim l$ bezeichnet und *negative* Literale genannt. Es gilt $\sim\neg l = l$.

Der Syntaxbaum von Normalformen

Sei p in KNF. Dann:

- Blätter sind aus Prp.
- Ein $\neg$-Knoten hat immer ein Prp-Blatt als Nachfolger.
- Ein Teilbaum mit $\vee$-Wurzel hat keine inneren $\wedge$-Knoten.

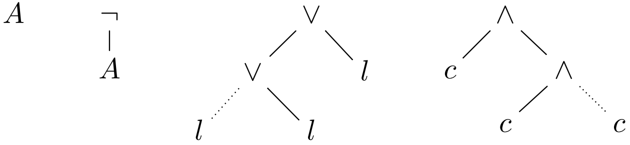
Normalformbäume

Def. 19: Klausel

Eine Disjunktion von Literalen heißt *Klausel*. Sie werden oft einfach als Mengen von Literalen dargestellt. Die leere Klausel wird mit $\oslash$ bezeichnet.

KNF Bäume

$A \in \mathrm{Prp}$, $l \in \mathrm{Lit}$, c Klausel.



Sobald ein l zu $\mathbf{1}$ ausgewertet wird, kann die $\vee$-Wurzel mit $\mathbf{1}$ gelabelt werden. Sobald ein c zu $\mathbf{0}$ ausgewertet wird, kann die $\wedge$-Wurzel mit $\mathbf{0}$ gelabelt werden.

Existenz äquivalenter Normalformen

Thm. 20: Existenz von Normalformen

Zu jeder Formel $p \in \mathrm{Fml}$ existiert eine Formel $p' \in \mathrm{Fml}$ in KNF/DNF mit $p \Longleftrightarrow p'$.

Bew. KNF (DNF analog)

1. In jedem Schritt, eliminiere doppelte Negation ($\sim$ statt $\neg$.).
2. Auflösung der Subjunktion: $(q \longrightarrow r) \Longleftrightarrow (\neg q' \vee r')$
3. Herausziehen der Konjunktion:
   Ersetze $((q \wedge r) \vee s)$ mit DST durch $\big((q' \vee s')' \wedge (r' \vee s')'\big)$
4. Einschachteln der Negation:
   Ersetze $\neg\,(q \wedge r)$ mit DEM durch $(\neg q' \vee \neg r')'$ (desgl. $\vee$)

DST (3.) zieht Konjunktionen von links unten nach rechts oben und DEM (4.) drückt die Negation vor die Blätter.

KNF/DNF aus Wahrheitstabellen

Seien $V = \mathrm{var}(p)$ die Menge der Aussagenvariablen in p .

DNF aus W'tabelle - Alternative Wahl erfüllender α

$$p' = \bigvee_{\alpha \in Sat(p)} \bigwedge_{X \in V} X'$$

mit $X' = X$ für $\alpha(X) = \mathbf{1}$ und $X' = \neg X$ für $\alpha(X) = \mathbf{0}$.

KNF aus W'tabelle - Ausschluß aller nicht erfüllender α

$$p' = \bigwedge_{\alpha \notin Sat(p)} \bigvee_{X \in V} X'$$

mit $X' = X$ für $\alpha(X) = \mathbf{0}$ und $X' = \neg X$ für $\alpha(X) = \mathbf{1}$.

KNF/DNF aus Wahrheitstabellen

Beispiel: $((A \vee \neg B) \longrightarrow (A \wedge B))$

$$
\begin{array}{cl}
 & ((A \vee \neg B) \longrightarrow (A \wedge B)) \\
\overset{\text{IMP}}{\Longleftrightarrow} & (\neg (A \vee \neg B) \vee (A \wedge B)) \\
\overset{\text{DEM}}{\Longleftrightarrow} & ((\neg A \wedge B) \vee (A \wedge B)) \\
\overset{\text{genDST}}{\Longleftrightarrow} & ((\neg A \vee A) \wedge (\neg A \vee B) \wedge (B \vee A) \wedge (B \vee B)) \\
\overset{\text{T,IDM}}{\Longleftrightarrow} & ((\neg A \vee B) \wedge (B \vee A) \wedge B) \\
\overset{\text{ABS}}{\Longleftrightarrow} & B
\end{array}
$$

KNF/DNF aus Wahrheitstabellen

Beispiel: $((A \vee \neg B) \longrightarrow (A \wedge B))$

Man kann DST auch verkürzend verwenden:

$$
\begin{aligned}
& ((A \vee \neg B) \longrightarrow (A \wedge B)) \\
\overset{\text{IMP}}{\Longleftrightarrow}\quad & (\neg\,(A \vee \neg B) \vee (A \wedge B)) \\
\overset{\text{DEM}}{\Longleftrightarrow}\quad & ((\neg A \wedge B) \vee (A \wedge B)) \\
\overset{\text{DST}}{\Longleftrightarrow}\quad & ((\neg A \vee A) \wedge B) \\
\overset{\text{Taut.}}{\Longleftrightarrow}\quad & (\mathsf{T} \wedge B) \\
\overset{\text{ntr}}{\Longleftrightarrow}\quad & B
\end{aligned}
$$

KNF/DNF aus Wahrheitstabellen

Beispiel: $((A \vee \neg B) \longrightarrow (A \wedge B))$

A'	B'	$q' = \neg B'$	$r' = (A \vee q)'$	$s' = (A \wedge B)'$	$(r \longrightarrow s)'$
0	**0**	**1**	**1**	**0**	**0**
0	**1**	**0**	**0**	**0**	**1**
1	**0**	**1**	**1**	**0**	**0**
1	**1**	**0**	**1**	**1**	**1**

$$\begin{aligned} dnf(p) &= ((\neg A \wedge B) \vee (A \wedge B)) \Longleftrightarrow B \\ knf(p) &= ((A \vee B) \wedge (\neg A \vee B)) \Longleftrightarrow B \end{aligned}$$

Erfüllbarkeit und Gültigkeit in KNF/DNF

Kor.

- Jede Formel p mit $p \Longleftrightarrow \bigvee L$
  - ist immer erfüllbar (wähle $\mathcal{I}^\alpha.l = \mathbf{1}$ für ein $l \in L$)
  - ist **gültig**, wenn es $l, \sim l \in L$ gibt (*komplementäres* Paar)
- Jede Formel p mit $p \Longleftrightarrow \bigwedge L$
  - ist **erfüllbar**, wenn sie *kein* komplementäres Paar enthält.
  - ist nie gültig (wähle α so daß $\mathcal{I}^\alpha.l = \mathbf{0}$, für ein $l \in L$).

Thm. 21: Hinweis auf Resolution

$$\begin{aligned}
\{(p \wedge (p \longrightarrow q))\} \mathrel{|\!\!\approx} q \quad &\overset{\text{PSN}}{\Longleftrightarrow} \quad \{(p \wedge (p \longrightarrow q))\} \mathrel{|\!\!\approx} (\neg q \longrightarrow \mathsf{F}) \\
&\overset{\text{DT}}{\Longleftrightarrow} \quad \{(p \wedge (p \longrightarrow q)), \neg q\} \mathrel{|\!\!\approx} \mathsf{F} \\
&\overset{\text{CNF}}{\Longleftrightarrow} \quad \{\{p\}, \{\sim p, q\}, \{\sim q\}\} \mathrel{|\!\!\approx} \emptyset \\
&\Longleftrightarrow \quad \{\{p\}, \{\sim p, q\}, \{\sim q\}\} \text{ ist unerfüllbar}
\end{aligned}$$

4.
AXIOMATISCHE SEMANTIK DER AUSSAGENLOGIK

Axiomatische Semantik der Aussagenlogik

Def. 20: Ein vollst./korr. Kalkül für gültige Aussagen

Seien $p, q, r \in \mathrm{Fml}$. Alle durch folgende Regeln ableitbaren Formeln sind Tautologien.

$$\frac{}{(p \longrightarrow (q \longrightarrow p))} \qquad (\textsc{h}1)$$

$$\frac{}{((p \longrightarrow (q \longrightarrow r)) \longrightarrow ((p \longrightarrow q) \longrightarrow (p \longrightarrow r)))} \qquad (\textsc{h}2)$$

$$\frac{}{((\neg p \longrightarrow \neg q) \longrightarrow (q \longrightarrow p))} \qquad (\textsc{h}3)$$

Weiterhin gilt natürlich MP:

$$\frac{p, \qquad (p \longrightarrow q)}{q} \qquad (\textsc{mp})$$

Weiterführendes zu **HK**

Axiomatische Semantik und **HK** sind Gegenstand
einer weiterführenden Vorlesung zur Logik.

NB.:
Mit der minimalen Operatorbasis und kompakten Axiomatisierung ist **HK** v.a. für theoretische Untersuchungen nützlich; ist aber ebenso auch als Beweiskalkül verwendbar (wenn auch unpraktisch).

Trotzdem: Ein kleines Beispiel

Zu beweisen sei: $p \Longrightarrow p$

Nach DT ist also zu zeigen, daß $(p \longrightarrow p)$ allgemeingültig ist.
Wir wollen also $(p \longrightarrow p)$ aus $\textsc{h}1$-$\textsc{h}3$ und $\textsc{mp}$ ableiten.

1	
2	
3	
4	
5	$(p \longrightarrow p)$

Trotzdem: Ein kleines Beispiel

Zu beweisen sei: $p \Longrightarrow p$

Nach DT ist also zu zeigen, daß $(p \longrightarrow p)$ allgemeingültig ist.
Wir wollen also $(p \longrightarrow p)$ aus $\textsc{h}1$-$\textsc{h}3$ und $\textsc{mp}$ ableiten.

1		
2		
3		
4		
5	$(p \longrightarrow p)$	$\textsc{mp}(3,4)$

Trotzdem: Ein kleines Beispiel

Zu beweisen sei: $p \Longrightarrow p$

Nach DT ist also zu zeigen, daß $(p \longrightarrow p)$ allgemeingültig ist.
Wir wollen also $(p \longrightarrow p)$ aus $\textsc{h}1$-$\textsc{h}3$ und $\textsc{mp}$ ableiten.

1		
2		
3		
4	$((p \longrightarrow (p \longrightarrow p)) \longrightarrow (p \longrightarrow p))$	
5	$(p \longrightarrow p)$	$\textsc{mp}(3,4)$

Trotzdem: Ein kleines Beispiel

Zu beweisen sei: $p \Longrightarrow p$

Nach DT ist also zu zeigen, daß $(p \longrightarrow p)$ allgemeingültig ist.
Wir wollen also $(p \longrightarrow p)$ aus $\textsc{h}1$-$\textsc{h}3$ und $\textsc{mp}$ ableiten.

1		
2		
3	$(p \longrightarrow (p \longrightarrow p))$	$\textsc{h}1$
4	$((p \longrightarrow (p \longrightarrow p)) \longrightarrow (p \longrightarrow p))$	
5	$(p \longrightarrow p)$	$\textsc{mp}(3,4)$

$(3)\ q := p$

Trotzdem: Ein kleines Beispiel

Zu beweisen sei: $p \Longrightarrow p$

Nach DT ist also zu zeigen, daß $(p \longrightarrow p)$ allgemeingültig ist.
Wir wollen also $(p \longrightarrow p)$ aus $\textsc{h}1$-$\textsc{h}3$ und $\textsc{mp}$ ableiten.

1		
2		
3	$(p \longrightarrow (p \longrightarrow p))$	$\textsc{h}1$
4	$((p \longrightarrow (p \longrightarrow p)) \longrightarrow (p \longrightarrow p))$	$\textsc{mp}(1,2)$
5	$(p \longrightarrow p)$	$\textsc{mp}(3,4)$

$(3)\ q := p$

Trotzdem: Ein kleines Beispiel

Zu beweisen sei: $p \Longrightarrow p$

Nach DT ist also zu zeigen, daß $(p \longrightarrow p)$ allgemeingültig ist.
Wir wollen also $(p \longrightarrow p)$ aus $\textsc{h}1$-$\textsc{h}3$ und $\textsc{mp}$ ableiten.

1	$(p \longrightarrow ((p \longrightarrow p) \longrightarrow p))$	$\textsc{h}1$
2		
3	$(p \longrightarrow (p \longrightarrow p))$	$\textsc{h}1$
4	$((p \longrightarrow (p \longrightarrow p)) \longrightarrow (p \longrightarrow p))$	$\textsc{mp}(1,2)$
5	$(p \longrightarrow p)$	$\textsc{mp}(3,4)$

(3) $q := p$

(1) $q := (p \longrightarrow p)$

Trotzdem: Ein kleines Beispiel

Zu beweisen sei: $p \Longrightarrow p$

Nach DT ist also zu zeigen, daß $(p \longrightarrow p)$ allgemeingültig ist.
Wir wollen also $(p \longrightarrow p)$ aus $\text{H}1$-$\text{H}3$ und MP ableiten.

1	$(p \longrightarrow ((p \longrightarrow p) \longrightarrow p))$	H1
2	$((p \longrightarrow ((p \longrightarrow p) \longrightarrow p)) \longrightarrow ((p \longrightarrow (p \longrightarrow p)) \longrightarrow (p \longrightarrow p)))$	H2
3	$(p \longrightarrow (p \longrightarrow p))$	H1
4	$((p \longrightarrow (p \longrightarrow p)) \longrightarrow (p \longrightarrow p))$	$\text{MP}(1, 2)$
5	$(p \longrightarrow p)$	$\text{MP}(3, 4)$

$(3)\ q := p$

$(1)\ q := (p \longrightarrow p)$

$(2)\ p := p, q := (p \longrightarrow p), r := p$

5.
NATÜRLICHE DEDUKTION

Wie funktioniert ein Beweis?

Der Mathelehrer sagt:

Wenn x nicht gerade ist, dann ist x keine Primzahl und ungerade.

... und beweist:

Angenommen, x sei nicht gerade. Sei x sowohl prim als auch gerade. Wenn x aber sowohl prim und gerade ist (also z.B. $x = 2$), ist x natürlich insbesondere auch einfach nur gerade. Das aber widerspricht der allerersten Annahme, daß x nicht gerade sei. Somit muß die Annahme, daß x prim und gerade sei, falsch gewesen sein.

Wie funktioniert ein Beweis?

Behauptung

Wenn x nicht gerade ist, dann ist x keine Primzahl und ungerade.

Beweis

0. Sei x nicht gerade.
   Zu beweisen: x ist nicht prim und ungerade.
1. Annahme: x *sei sowohl* prim als auch gerade (nicht ungerade).
2. Wenn x prim und gerade ist, ist x natürlich prim.
3. Genauso ist x natürlich gerade.
4. Die Schlußfolgerung 3 widerspricht aber der Fundamentalannahme 0!
   Deshalb muss Annahme 1 falsch gewesen sein.
5. Also kann x nicht zugleich prim und gerade sein.

Wie funktioniert ein Beweis?

Behauptung

Wenn x nicht gerade ist, dann ist x keine Primzahl und ungerade.

Beweis

0.	Sei x nicht gerade.	
1.	Sei x *sowohl* prim und gerade	(Annahme)
2.	x ist prim	(wegen 1.)
3.	x ist gerade	(auch wegen 1.)
4.	Widerspruch!	(3. widerspricht 0.)
5.	x ist **nicht** *sowohl* prim und gerade	(Negation Annahme 1.).

Natürliche Deduktion

"Intuitives logisches Schliessen"

Der Kalkül **ND** der *natürlichen Deduktion* überführt das "intuitive logische Schliessen" in einfach nachvollziehbare Ableitungsregeln die eine formal genaue Beweisführung ermöglichen.

Def. 21: ND 1/3: Strukturelle Regeln

$$\frac{p}{\neg\neg p}\,\text{NNI} \qquad \frac{\neg\neg p}{p}\,\text{NNE}$$

$$\frac{p, \quad q}{(p \land q)}\,\text{CI} \qquad \frac{(p \land q)}{p}\,\text{CE} \qquad \frac{(p \land q)}{q}\,\text{CE}$$

$$\frac{p}{(p \lor q)}\,\text{DI} \qquad \frac{p}{(q \lor p)}\,\text{DI}$$

$$\frac{p, \quad (p \longrightarrow q)}{q}\,\text{MP} \qquad \frac{(p \longrightarrow q), \quad \neg q}{\neg p}\,\text{MT}.$$

Ein formaler Beweis in ND

Darstellung eines **ND**-Beweises für $P \approx p$

Beweise lassen sich wie folgt strukturiert darstellen:

1	p_1	Prämisse 1
$\vdots$	$\vdots$	$\vdots$
n	p_n	Prämisse n
1	q_1	Anwendung einer **ND**-Regel auf $p_1, \ldots, p_n$
$\vdots$	$\vdots$	$\vdots$
k	q_k	Anwendung einer **ND**-Regel auf $p_1, \ldots, p_n, q_1, \ldots q_{k-1}$

mit den Prämissen $P = \{p_1, \ldots, p_n\}$ und den Beweisschritten bis hin zum zu beweisenden Theorem $q_k = p$.

Beispiel: $P = \{((p \wedge q) \wedge r), (s \wedge t)\} \vdash^*_{\textbf{ND}} (q \wedge s)$

Die Prämissen sind:

a	$((p \wedge q) \wedge r)$	Prämisse 1
b	$(s \wedge t)$	Prämisse 2

Mit der Anwendung der Regeln ...

1	$(p \wedge q)$	$\text{CE}(a)$
2	r	$\text{CE}(a)$
3	p	$\text{CE}(1)$
4	q	$\text{CE}(1)$
5	s	$\text{CE}(b)$
6	t	$\text{CE}(b)$
7	$(q \wedge s)$	$\text{CI}(4, 5)$

wird das gewünschte Ergebnis hergeleitet.

Korrektheit von **ND** 1/3

Thm. 22: ND ist korrekt bzgl. PRL

$$P \vdash^*_{\textbf{ND}} p \Longrightarrow P \approx p.$$

Bew. Korrektheit von **ND** 1a/2

NNI Gelte p, d.h. $\mathcal{I}^\alpha.p = 1$ für ein beliebiges α. Dann ist $\mathcal{I}^\alpha.\neg\neg p = 1 - (1 - 1) = 1$. Somit gilt also auch $\neg\neg p$, d.h. NNI ist korrekt.

CI Sei $\mathcal{I}^\alpha.p = 1 = \mathcal{I}^\alpha.q$. Es gilt $\mathbf{1} \sqcap \mathbf{1} = \mathbf{1}$, also gilt auch $(p \wedge q)$ und CI ist korrekt.

CE Es ist $\mathcal{I}^\alpha.(p \wedge q) = 1 = \min(\{1\})$. Also muß $\mathcal{I}^\alpha.p = \mathcal{I}^\alpha.q = 1$; es gelten auch p und q und CE ist korrekt.

Korrektheit von **ND** 1/3

Bew. Korrektheit von **ND** 1b/3

MP
1. Gelte p und $(p \longrightarrow q)$. (Prämisse der MP -Regel).
2. Also $\mathcal{I}^{\alpha}.p = 1$.
3. $\mathcal{I}^{\alpha}.(p \longrightarrow q) = \max(\{1 - \mathcal{I}^{\alpha}.p, \mathcal{I}^{\alpha}.q\})$.
4. Da $\mathcal{I}^{\alpha}.p = 1$ ist, $\mathcal{I}^{\alpha}.(p \longrightarrow q) = \max(\{0, \mathcal{I}^{\alpha}.q\}) = \mathcal{I}^{\alpha}.q$.
   4.1 Fall 1: $\mathcal{I}^{\alpha}.q = \mathbf{0}$. Dann ist wegen 2. bereits $\mathcal{I}^{\alpha}.(p \longrightarrow q) = \mathbf{0}$ und MP nicht anwendbar (Widerspruch zu 1.).
   4.2 Fall 2: $\mathcal{I}^{\alpha}.q = \mathbf{1}$. Dann ist wegen 2., 3. $\mathcal{I}^{\alpha}.(p \longrightarrow q) = \mathbf{1}$ und der Schluss auf $\mathcal{I}^{\alpha}.q = \mathbf{1}$ ist in diesem Fall korrekt.

Somit ist auch MP korrekt.

Die Korrektheit der anderen Regeln wird analog bewiesen.

Fundamentale klassische Prinzipien

Def. 22: ND 2/3: Logische Prinzipien

$$\frac{}{(p \vee \neg p)}\ \textsc{tnd} \qquad \frac{\mathsf{F}}{p}\ \textsc{vac}$$

$$\frac{(p \wedge \neg p)}{q}\ \textsc{ecq} \qquad \frac{p, \qquad \neg p}{q}\ \textsc{efq} \qquad \frac{p, \qquad \neg p}{\mathsf{F}}\ \textsc{ctr}$$

Bew. Korrektheit von **ND** 2/3

TND. $\max\{p', 1 - p'\} = 1$ für alle $p' \in \{0, 1\}$.

VAC. $\mathsf{F}' = 0 \leq p'$ für $p' \in \{0, 1\}$.

ECQ. Beachte $(p \wedge \neg p) \Longleftrightarrow \mathsf{F}$. Damit ergibt sich VAC.

EFQ. Bedenke $\mathcal{I}^\alpha \models \{p, \neg p\}$ gdw. $\mathcal{I}^\alpha \models (p \wedge \neg p)$. Dann ECQ.

CTR. Weil q in EFQ beliebig, auch für $q = \mathsf{F}$.

Natürliche Deduktion

Def. 23: ND 3a/3: Schlußregeln

Negation:

$$\frac{\begin{array}{c}\underline{p}\\ \vdots\\ \overline{\mathsf{F}}\end{array}}{\neg p}\ \text{NI} \qquad \frac{\begin{array}{c}\underline{\neg p}\\ \vdots\\ \overline{\mathsf{F}}\end{array}}{p}\ \text{NE}$$

Disjunktionselimination:

$$\frac{(p \vee q), \quad \begin{array}{c}\underline{p}\\ \vdots\\ \overline{r}\end{array}, \quad \begin{array}{c}\underline{q}\\ \vdots\\ \overline{r}\end{array}}{r}\ \text{DE}$$

Natürliche Deduktion

Def. 24: ND 3b/3: Implikationseinführung ("Annahme")

$$\dfrac{\dfrac{\dfrac{p}{\vdots}}{q}}{(p \longrightarrow q)}\ \text{II}$$

Wozu Implikationseinführung?

- Ich will q "direkt" beweisen, es klappt aber nicht.
- Ich mache eine Hilfsannahme p.
- Mit deren Hilfe wird q herleitbar.
- Also habe ich $(p \longrightarrow q)$ bewiesen.
- **Wenn** ich jetzt noch p beweise,
- **dann** folgt mit MP die Gültigkeit von q.

Korrektheit von **ND**

Def. 25: Korrektheit von **ND** 3/3

NI Sei P erfüllt. Gelänge ohne Anwendung von NI $P \cup \{p\} \vdash^*_{\mathbf{ND}}$ F so gälte wegen Korrektheit von **ND** $P \cup \{p\} \models\!\!\approx$ F. Dann aber wäre $P \cup \{p\}$ unerfüllbar und wegen TND folgt also $P \models\!\!\approx \neg p$.

NE Analog.

II Deduktionstheorem.

Anmerkung zu **ND**

Verschiedene Arten der Kalkülregeln

Natürliche, “intuitive” Beweisführung vermischt Wissen über Formeln und Wissen über die Herleitung von Formeln:

S A ist wahr vs. eine Herleitung von A.

- Die Regeln aus Definition **ND** 1/3 haben die Struktur

$$\frac{P}{p}$$

- Die Regeln aus Definition **ND** 2/3 haben die Struktur

$$\frac{p_1 \vdash \cdots \vdash p_n}{q}$$

5.
BEWEISEN MIT NATÜRLICHER DEDUKTION

Komplexere Beweise in **ND**

Nutzung von II

1	p_1	$\vdash$ Anwendung
$\vdots$	$\vdots$	$\vdots$
i	$\lceil q$	Annahme
$\vdots$	$\vdots$	$\vdash$ Anwendungen
j	$\lfloor r$	$\vdash$ Anwendung
$\vdots$	$(q \longrightarrow r)$	$\mathrm{II}(i, j)$
$\vdots$	$\vdots$	$\vdots$
k	q	$\vdash$ Anwendung
$k+1$	r	$\mathrm{MP}(k, j+1)$

Beispiel für einen **ND**-Beweis

Ein **ND**-Beweis für $\textsc{h}1$

		Leere Prämisse
1	$\lceil p$	Annahme 1
2	$\quad\lceil q$	Annahme 2
3	$\quad\lfloor p$	wie angenommen in 1
4	$\lfloor (q \longrightarrow p)$	$\textsc{ii}(2,3)$
5	$(p \longrightarrow (q \longrightarrow p))$	$\textsc{ii}(1,4)$

Warum **ND** "natürlich" ist

Behauptung

Wenn x nicht gerade ist, dann ist x keine Primzahl und ungerade.

Beweis

0.	Sei x nicht gerade.	
1.	Sei x *sowohl* prim und gerade	(Annahme)
2.	x ist prim	(wegen 1.)
3.	x ist gerade	(auch wegen 1.)
4.	Widerspruch!	(3. widerspricht 0.)
5.	x ist **nicht** *sowohl* prim und gerade	(Negation Annahme 1.).

Warum **ND** "natürlich" ist

Behauptung

Wenn x nicht gerade ist, dann ist x keine Primzahl und ungerade.

Beweis

Die Behauptung lautet: $\neg p \Longrightarrow \neg(p \wedge q)$.

a	$\neg p$	Prämisse
1	$\lceil (p \wedge q)$	Annahme
2	q	$\textsc{ce}(1)$
3	p	$\textsc{ce}(1)$
4	$\lfloor \mathsf{F}$	$\textsc{ctr}(1,3)$
5	$\neg(p \wedge q)$	$\textsc{ni}(1)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \mathrel{|}\!\approx p \longrightarrow (\neg q \vee r)$

a		
	$((p \wedge q) \longrightarrow r)$	Prämisse
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20	$(p \longrightarrow (\neg q \vee r))$	$\textsc{ii}(1, 19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \approx p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19	$\lfloor (\neg q \vee r)$	
20	$(p \longrightarrow (\neg q \vee r))$	$\text{II}(1, 19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \approx p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2		
3		
4		
5		
6		
7	$(p \longrightarrow (q \longrightarrow r))$	
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19	$\lfloor (\neg q \vee r)$	
20	$(p \longrightarrow (\neg q \vee r))$	$\text{II}(1, 19)$

Beispiel $\{(p \land q) \longrightarrow r\} \approx p \longrightarrow (\neg q \lor r)$

a	$((p \land q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad \lceil p$	Annahme
3		
4		
5		
6	$\quad \lfloor (q \longrightarrow r)$	
7	$\quad (p \longrightarrow (q \longrightarrow r))$	$\textsc{ii}(2, 6)$
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19	$\lfloor (\neg q \lor r)$	
20	$(p \longrightarrow (\neg q \lor r))$	$\textsc{ii}(1, 19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \approx p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\lceil p$	Annahme
3	$\lceil q$	Annahme
4		
5	$\lfloor r$	
6	$\lfloor (q \longrightarrow r)$	II$(3,5)$
7	$(p \longrightarrow (q \longrightarrow r))$	II$(2,6)$
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19	$\lfloor (\neg q \vee r)$	
20	$(p \longrightarrow (\neg q \vee r))$	II$(1,19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \mid\!\approx p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad \lceil p$	Annahme
3	$\quad\quad \lceil q$	Annahme
4	$\quad\quad\quad (p \wedge q)$	$\textsc{ci}(2,3)$
5	$\quad\quad \lfloor r$	$\textsc{mp}(4,a)$
6	$\quad \lfloor (q \longrightarrow r)$	$\textsc{ii}(3,5)$
7	$\quad (p \longrightarrow (q \longrightarrow r))$	$\textsc{ii}(2,6)$
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19	$\lfloor (\neg q \vee r)$	
20	$(p \longrightarrow (\neg q \vee r))$	$\textsc{ii}(1,19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \approx p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad \lceil p$	Annahme
3	$\quad\quad \lceil q$	Annahme
4	$\quad\quad\quad (p \wedge q)$	$\text{CI}(2,3)$
5	$\quad\quad \lfloor r$	$\text{MP}(4,a)$
6	$\quad \lfloor (q \longrightarrow r)$	$\text{II}(3,5)$
7	$\quad (p \longrightarrow (q \longrightarrow r))$	$\text{II}(2,6)$
8	$\quad (q \longrightarrow r)$	$\text{MP}(1,7)$
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19	$\lfloor (\neg q \vee r)$	
20	$(p \longrightarrow (\neg q \vee r))$	$\text{II}(1,19)$

Beispiel $\{(p \land q) \longrightarrow r\} \mathrel{|}\!\!\approx p \longrightarrow (\neg q \lor r)$

a	$((p \land q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad \lceil p$	Annahme
3	$\quad\quad \lceil q$	Annahme
4	$\quad\quad\quad (p \land q)$	$\textsc{ci}(2,3)$
5	$\quad\quad \lfloor r$	$\textsc{mp}(4,a)$
6	$\quad \lfloor (q \longrightarrow r)$	$\textsc{ii}(3,5)$
7	$\quad (p \longrightarrow (q \longrightarrow r))$	$\textsc{ii}(2,6)$
8	$\quad (q \longrightarrow r)$	$\textsc{mp}(1,7)$
9	$\quad \lceil \neg(\neg q \lor r)$	Annahme f. Widerspr.
10		
11		
12		
13		
14		
15		
16		
17	$\quad \lfloor \mathsf{F}$	$\textsc{ctr}()$
18		
19	$\lfloor (\neg q \lor r)$	
20	$(p \longrightarrow (\neg q \lor r))$	$\textsc{ii}(1,19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \approx\!\!\!\!| \; p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad \lceil p$	Annahme
3	$\quad\quad \lceil q$	Annahme
4	$\quad\quad\quad (p \wedge q)$	$\text{CI}(2,3)$
5	$\quad\quad \lfloor r$	$\text{MP}(4,a)$
6	$\quad \lfloor (q \longrightarrow r)$	$\text{II}(3,5)$
7	$\quad (p \longrightarrow (q \longrightarrow r))$	$\text{II}(2,6)$
8	$\quad (q \longrightarrow r)$	$\text{MP}(1,7)$
9	$\quad \lceil \neg(\neg q \vee r)$	Annahme f. Widerspr.
10		
11		
12		
13		
14	$\quad\quad q$	
15	$\quad\quad r$	
16		
17	$\quad \lfloor \mathsf{F}$	$\text{CTR}()$
18		
19	$\lfloor (\neg q \vee r)$	
20	$(p \longrightarrow (\neg q \vee r))$	$\text{II}(1,19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \mathrel{|}\!\!\approx p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad \lceil p$	Annahme
3	$\quad\quad \lceil q$	Annahme
4	$\quad\quad\quad (p \wedge q)$	$\textsc{ci}(2,3)$
5	$\quad\quad \lfloor r$	$\textsc{mp}(4,a)$
6	$\quad \lfloor (q \longrightarrow r)$	$\textsc{ii}(3,5)$
7	$\quad (p \longrightarrow (q \longrightarrow r))$	$\textsc{ii}(2,6)$
8	$\quad (q \longrightarrow r)$	$\textsc{mp}(1,7)$
9	$\quad \lceil \neg(\neg q \vee r)$	Annahme f. Widerspr.
10	$\quad\quad \lceil \neg q$	Annahme f. Widerspr.
11		
12	$\quad\quad \lfloor \mathsf{F}$	$\textsc{ctr}()$
13		
14	$\quad\quad q$	
15	$\quad\quad r$	
16		
17	$\quad \lfloor \mathsf{F}$	$\textsc{ctr}()$
18		
19	$\lfloor (\neg q \vee r)$	
20	$(p \longrightarrow (\neg q \vee r))$	$\textsc{ii}(1,19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \mid\!\approx p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad \lceil p$	Annahme
3	$\qquad \lceil q$	Annahme
4	$\qquad\quad (p \wedge q)$	$\textsc{ci}(2,3)$
5	$\qquad \lfloor r$	$\textsc{mp}(4,a)$
6	$\quad \lfloor (q \longrightarrow r)$	$\textsc{ii}(3,5)$
7	$\quad (p \longrightarrow (q \longrightarrow r))$	$\textsc{ii}(2,6)$
8	$\quad (q \longrightarrow r)$	$\textsc{mp}(1,7)$
9	$\quad \lceil \neg(\neg q \vee r)$	Annahme f. Widerspr.
10	$\qquad \lceil \neg q$	Annahme f. Widerspr.
11	$\qquad\quad (\neg q \vee r)$	$\textsc{di}(10)$
12	$\qquad \lfloor \mathsf{F}$	$\textsc{ctr}(9,11)$
13		
14	$\qquad q$	
15	$\qquad r$	
16		
17	$\quad \lfloor \mathsf{F}$	$\textsc{ctr}()$
18		
19	$\lfloor (\neg q \vee r)$	
20	$(p \longrightarrow (\neg q \vee r))$	$\textsc{ii}(1,19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \mathrel{|\!\!\approx} p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad \lceil p$	Annahme
3	$\quad\quad \lceil q$	Annahme
4	$\quad\quad\quad (p \wedge q)$	$\textsc{ci}(2,3)$
5	$\quad\quad \lfloor r$	$\textsc{mp}(4,a)$
6	$\quad \lfloor (q \longrightarrow r)$	$\textsc{ii}(3,5)$
7	$\quad (p \longrightarrow (q \longrightarrow r))$	$\textsc{ii}(2,6)$
8	$\quad (q \longrightarrow r)$	$\textsc{mp}(1,7)$
9	$\quad \lceil \neg(\neg q \vee r)$	Annahme f. Widerspr.
10	$\quad\quad \lceil \neg q$	Annahme f. Widerspr.
11	$\quad\quad\quad (\neg q \vee r)$	$\textsc{di}(10)$
12	$\quad\quad \lfloor \mathsf{F}$	$\textsc{ctr}(9,11)$
13	$\quad\quad \neg\neg q$	$\textsc{ni}(10,12)$
14	$\quad\quad q$	$\textsc{dne}(13)$
15	$\quad\quad r$	
16		
17	$\quad \lfloor \mathsf{F}$	$\textsc{ctr}()$
18		
19	$\lfloor (\neg q \vee r)$	
20	$(p \longrightarrow (\neg q \vee r))$	$\textsc{ii}(1,19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \mathrel{|}\!\approx p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad \lceil p$	Annahme
3	$\quad\quad \lceil q$	Annahme
4	$\quad\quad\quad (p \wedge q)$	$\textsc{ci}(2,3)$
5	$\quad\quad \lfloor r$	$\textsc{mp}(4,a)$
6	$\quad \lfloor (q \longrightarrow r)$	$\textsc{ii}(3,5)$
7	$\quad (p \longrightarrow (q \longrightarrow r))$	$\textsc{ii}(2,6)$
8	$\quad (q \longrightarrow r)$	$\textsc{mp}(1,7)$
9	$\quad \lceil \neg(\neg q \vee r)$	Annahme f. Widerspr.
10	$\quad\quad \lceil \neg q$	Annahme f. Widerspr.
11	$\quad\quad\quad (\neg q \vee r)$	$\textsc{di}(10)$
12	$\quad\quad \lfloor \mathsf{F}$	$\textsc{ctr}(9,11)$
13	$\quad\quad \neg\neg q$	$\textsc{ni}(10,12)$
14	$\quad\quad q$	$\textsc{dne}(13)$
15	$\quad\quad r$	$\textsc{mp}(8,14)$
16		
17	$\quad \lfloor \mathsf{F}$	$\textsc{ctr}()$
18		
19	$\lfloor (\neg q \vee r)$	
20	$(p \longrightarrow (\neg q \vee r))$	$\textsc{ii}(1,19)$

Beispiel $\{(p \land q) \longrightarrow r\} \mid\!\approx p \longrightarrow (\neg q \lor r)$

a	$((p \land q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad\lceil p$	Annahme
3	$\quad\quad\lceil q$	Annahme
4	$\quad\quad\quad(p \land q)$	$\textsc{ci}(2,3)$
5	$\quad\quad\lfloor r$	$\textsc{mp}(4,a)$
6	$\quad\lfloor (q \longrightarrow r)$	$\textsc{ii}(3,5)$
7	$\quad(p \longrightarrow (q \longrightarrow r))$	$\textsc{ii}(2,6)$
8	$\quad(q \longrightarrow r)$	$\textsc{mp}(1,7)$
9	$\quad\lceil \neg(\neg q \lor r)$	Annahme f. Widerspr.
10	$\quad\quad\lceil \neg q$	Annahme f. Widerspr.
11	$\quad\quad\quad(\neg q \lor r)$	$\textsc{di}(10)$
12	$\quad\quad\lfloor \mathsf{F}$	$\textsc{ctr}(9,11)$
13	$\quad\quad\neg\neg q$	$\textsc{ni}(10,12)$
14	$\quad\quad q$	$\textsc{dne}(13)$
15	$\quad\quad r$	$\textsc{mp}(8,14)$
16	$\quad\quad(\neg q \lor r)$	$\textsc{di}(15)$
17	$\quad\lfloor \mathsf{F}$	$\textsc{ctr}(9,16)$
18		
19	$\lfloor (\neg q \lor r)$	
20	$(p \longrightarrow (\neg q \lor r))$	$\textsc{ii}(1,19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \approx p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad \lceil p$	Annahme
3	$\quad\quad \lceil q$	Annahme
4	$\quad\quad\quad (p \wedge q)$	$\textsc{ci}(2,3)$
5	$\quad\quad \lfloor r$	$\textsc{mp}(4,a)$
6	$\quad \lfloor (q \longrightarrow r)$	$\textsc{ii}(3,5)$
7	$\quad (p \longrightarrow (q \longrightarrow r))$	$\textsc{ii}(2,6)$
8	$\quad (q \longrightarrow r)$	$\textsc{mp}(1,7)$
9	$\quad \lceil \neg(\neg q \vee r)$	Annahme f. Widerspr.
10	$\quad\quad \lceil \neg q$	Annahme f. Widerspr.
11	$\quad\quad\quad (\neg q \vee r)$	$\textsc{di}(10)$
12	$\quad\quad \lfloor \mathsf{F}$	$\textsc{ctr}(9,11)$
13	$\quad\quad \neg\neg q$	$\textsc{ni}(10,12)$
14	$\quad\quad q$	$\textsc{dne}(13)$
15	$\quad\quad r$	$\textsc{mp}(8,14)$
16	$\quad\quad (\neg q \vee r)$	$\textsc{di}(15)$
17	$\quad \lfloor \mathsf{F}$	$\textsc{ctr}(9,16)$
18	$\quad \neg\neg(\neg q \vee r)$	$\textsc{ni}(9,17)$
19	$\lfloor (\neg q \vee r)$	
20	$(p \longrightarrow (\neg q \vee r))$	$\textsc{ii}(1,19)$

Beispiel $\{(p \wedge q) \longrightarrow r\} \mathrel{|\!\approx} p \longrightarrow (\neg q \vee r)$

a	$((p \wedge q) \longrightarrow r)$	Prämisse
1	$\lceil p$	Annahme
2	$\quad\lceil p$	Annahme
3	$\qquad\lceil q$	Annahme
4	$\qquad\quad(p \wedge q)$	$\textsc{ci}(2,3)$
5	$\qquad\lfloor r$	$\textsc{mp}(4,a)$
6	$\quad\lfloor (q \longrightarrow r)$	$\textsc{ii}(3,5)$
7	$\quad(p \longrightarrow (q \longrightarrow r))$	$\textsc{ii}(2,6)$
8	$\quad(q \longrightarrow r)$	$\textsc{mp}(1,7)$
9	$\quad\lceil \neg(\neg q \vee r)$	Annahme f. Widerspr.
10	$\qquad\lceil \neg q$	Annahme f. Widerspr.
11	$\qquad\quad(\neg q \vee r)$	$\textsc{di}(10)$
12	$\qquad\lfloor \mathsf{F}$	$\textsc{ctr}(9,11)$
13	$\qquad\neg\neg q$	$\textsc{ni}(10,12)$
14	$\qquad q$	$\textsc{dne}(13)$
15	$\qquad r$	$\textsc{mp}(8,14)$
16	$\qquad(\neg q \vee r)$	$\textsc{di}(15)$
17	$\quad\lfloor \mathsf{F}$	$\textsc{ctr}(9,16)$
18	$\quad\neg\neg(\neg q \vee r)$	$\textsc{ni}(9,17)$
19	$\lfloor (\neg q \vee r)$	$\textsc{dne}(18)$
20	$(p \longrightarrow (\neg q \vee r))$	$\textsc{ii}(1,19)$

Zusammenfassung

Natürliche Deduktion

- **ND** ist eine formale Darstellung des "üblichen" Beweisens.
- Er erlaubt eine *exakte* und unmißverständliche Darstellung.
- **ND** ist korrekt (gezeigt) und vollständig (weitere Vorlesung).
- Damit ist **ND** ein sicheres und genügend mächtiges Werkzeug:
  - Zu jeder gültigen Formel gibt es eine syntaktisch korrekte **ND**-Ableitung
  - Jede syntaktisch korrekte **ND**-Ableitung ist ein korrekter Beweis
- Achtung: *inkorrekte* **ND**-Ableitungen können wahre oder falsche Aussagen suggerieren; beide wiederum können falsch sein.
- Also: **ND** ist ein sinnvolles Werzeug, um eine formal korrekte und genaue Beweisführung zu erlernen!

Natürliche Deduktion - Quellen & Theorembeweiser

Literatur

- Bücher, Skripte, etc.
  1. Huth/Ryan, *Logic in Computer Science*, CUP, 2004.
  2. Ben-Ari, *Mathematical Logic for Computer Science* (3 ed.), Springer, 2012 (Prentice-Hall, 1993).

  Ursprünglich als **NJ** von Gentzen in *Untersuchungen über das logische Schließen*, Math. Zeitschrift (39), 1934.
- Online Tutorials

Online Theorembeweiser

`https://proofs.openlogicproject.org/`

SEQUENZENKALKÜL

Sequenzenkalkül

Sequenzen ...

sind Ab*folgen* von Paaren von Formellisten, die jeweils die Prämisse und die Konklusion einer gültigen Implikation darstellen.
Sequenzen “umkapseln” sauber sowohl Formel- wie auch Ableitungs*sequenz*regeln.

Def. 26: Sequenz

$$\mathrm{Fml}_{\mathbf{LK}} := \{P \Vdash Q \parallel P, Q \text{ endlich und } P, Q \subseteq \mathrm{Fml}\}$$

Def. 27: Gültigkeit von Sequenzen

$$\mathcal{J} \models P \Vdash Q \;\text{ gdw. }\; \mathcal{I} \models \bigwedge P \implies \mathcal{I} \models \bigvee Q$$

Weiterführendes zu **LK**

LK als Beweiskalkül

Man benutzt **LK**-Regeln und zeigt $P \approx\!\!\!\!| \; p$ durch Konstruktion einer Sequenz

$$P \Vdash p \text{ aus } \textsc{Axm} \text{ und Regelanwendungen}$$

Damit ist (Korrektheit vorausgesetzt) bewiesen:

$$\begin{aligned}
\mathbf{G} \vdash^*_{\mathsf{LK}} P \Vdash p &\implies \mathcal{G} \models P \Vdash p \\
&\implies (\mathcal{I}^\alpha \models P \Longrightarrow \mathcal{I}^\alpha \models p) \\
&\implies P \approx\!\!\!\!| \; p.
\end{aligned}$$

Sequenzenkalküle und insbesondere **LK** sind
Gegenstand einer weiterführenden Vorlesung zur Logik.

NB.:

LK spielt in der Anwendung eine wichtigere Rolle als **HK** oder **ND**!

6.
RESOLUTION

Propositionale Resolution, **RES**$_{\mathsf{PRL}}$ *

Der Begriff "Resolution"

1. **re**-. wiederholt (es)
2. **solvere** (solu-). Entbinden, (auf-) lösen.

Bei der Resolution werden wiederholt nicht zu den Wahrheitsbedingungen beitragende Literal(-paare) aufgelöst.

Das Prinzip des Resolutionskalküls **RES**$_{\mathsf{PRL}}$

RES$_{\mathsf{PRL}}$ operiert auf *Klauselmengen* $\mathbf{K}$. Enthält $\mathbf{K}$ oder eine zu $\mathbf{K}$ äquivalente Klauselmenge $\mathbf{K}'$ die leere Klausel, so ist $\mathbf{K}$ und jede zu $\mathbf{K}$ (erfüllungs-) äquivalente Formelmenge P unerfüllbar.

Beispiele:
$\mathbf{K} = \{K_1, K_2\} = \{\{A, \sim B\}, \emptyset\}$ ist unerfüllbar.
$\mathbf{K} = \{K_1, K_2\} = \{\{A, \sim B\}, \{\sim A, \sim B\}\}$ ist erfüllbar.

6.1
RESOLUTIONSKALKÜL

Vom Ursprung der Resolutionsidee*

CNF — kanonisch

Sie haben aus einer gegebenen Formel folgende CNF erhalten:

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

Durch Äquivalenzumformungen ergab sich als CNF *und* DNF: q

Schlussfolgerung

In diesem Fall galt also:

$$((p \vee q) \wedge (\neg p \vee q))' == \left\langle \begin{array}{lccc} \text{falls } p' = \mathbf{0}: & q' & \sqcap & \mathbf{1} \\ \text{falls } p' = \mathbf{1}: & \mathbf{1} & \sqcap & q' \end{array} \right\rangle == q'$$

Allgemein wäre als Schlußregel zu vermuten:

$$\frac{(A \vee B), \qquad (\neg A \vee C)}{(B \vee C)}$$

Der propositionale Resolutionskalkül **RES**$_{\text{PRL}}$

Def. 28: **RES**$_{\text{PRL}}$

RES$_{\text{PRL}}$ besteht aus nur einer einzigen Regel:

$$\frac{\left\{l_1, \ldots, l_{i-1}, l, l_{i+1}, \ldots, l_m\right\}, \quad \left\{l'_1, \ldots, l'_{j-1}, {\sim}l, l'_{j+1}, \ldots, l'_n\right\}}{\left\{l_1, \ldots, l_{i-1}, l_{i+1}, \ldots, l_m, l'_1, \ldots, l'_{j-1}, l'_{j+1}, \ldots, l'_n\right\}}\ \mathrm{RES}$$

Darstellung

Zwei *Elternklauseln* K_1 und K_2 *resolvieren* zur *Resolvente* R unter Streichung eines *komplementären Paares*:

$$\begin{array}{ccc} K_1 & & K_2 \\ & R & \end{array}$$

$\oslash$ wird in der Literatur oft mit $\square$ bezeichnet.

Thm. 23: Resolutionslemma

Sei $p \in \mathrm{Fml}$ und $P \iff p$ in KNF. Sei R eine Resolvente aus K_1 und K_2 aus P:

$$\frac{K_1 = \{l_1, \ldots, l, \ldots, l_m\}, \quad \{l'_1, \ldots, {\sim}l, \ldots, l'_n\} = K_2}{\{l_1, \ldots, l_m, l'_1, \ldots, l'_n\} = R}\ \mathrm{RES}$$

Dann gilt $p \iff (p \wedge R)$ bzw. $P \iff P \cup \{R\}$.

Resolutionslemma

$\{K_1, K_2\} \subseteq P$ und $K_1, K_2 \vdash R$ impliziert $P \Longleftrightarrow P \cup \{R\}$.

Bew. Resolutionslemma

$\Longleftarrow$: Wenn $\alpha \in Sat(P \cup \{R\})$ dann auch $\alpha \in Sat(P)$.

$\Longrightarrow$: Gelte $\mathcal{I}^\alpha \models P$.

1. Dann gilt natürlich $\mathcal{I}^\alpha \models K_1$ und $\mathcal{I}^\alpha \models K_2$.
2. Fall 1.: Sei $\mathcal{I}^\alpha \models l \in K_1$.
   - 2.1 Es folgt $\mathcal{I}^\alpha \not\models \sim l \in K_2$.
   - 2.2 Da aber $\mathcal{I}^\alpha \models K_2$, ex. $l'_i \neq \sim l$ mit $\mathcal{I}^\alpha \models l'_i \in K_2$.
   - 2.3 Somit $\mathcal{I}^\alpha \models K_2 - \{\sim l\}$.
   - 2.4 Weil $K_2 - \{\sim l\} \subseteq R$, gilt auch $\mathcal{I}^\alpha \models R$.
   - 2.5 Schliesslich also auch $\mathcal{I}^\alpha \models P \cup \{R\}$.
3. Fall 2.: $\mathcal{I}^\alpha \not\models l \in K_1$: — Beweis analog.

Resolutionsoperator

Def. 29: Resolutionsoperation

$\mathrm{Res} : \wp(\mathrm{Fml}) \to \wp(\mathrm{Fml})$ ist definiert als

$$\mathrm{Res}(P) := P \cup \{R \,\|\, \exists K_i, K_j \colon (K_i, K_j \in P \wedge K_i, K_j \vdash R)\}$$

Es gilt die übliche Exponentation für iterierte Anwendung sowie die Definition des reflexiv transitiven Abschlusses:

$$\mathrm{Res}^*(P) = \bigcup_{i \in \mathbb{N}_0} \mathrm{Res}^i(P).$$

"Brute-Force"-Berechnung der deduktiven Hülle

Durch iterierte Expansion der quadratischen Matrizen aller Klauseln. Abbruch bei $\oslash$ oder bei Erreichen des Fixpunkts.

Beweisen mit $\textbf{RES}_{\text{PRL}}$

Deduktiver "Vorwärts-" Ableitungsbeweis in $\textbf{RES}_{\text{PRL}}$

- $\{K_1, K_2\} \subseteq P$ und $K_1, K_2 \vdash R$ impliziert $P \iff P \cup \{R\}$
- $p \in \mathrm{Res}^*(P)$ impliziert $P \iff P \cup \{p\}$

Thm. 24: Widerlegungsbeweise in $\textbf{RES}_{\text{PRL}}$ mit Res^*

$p \in \mathrm{Fml}$ ist unerfüllbar gdw. $\oslash \in \mathrm{Res}^*(P)$.

Kor.

$p \in \mathrm{Fml}$ ist erfüllbar gdw. $\oslash \notin \mathrm{Res}^*(P)$.

Warum hat $\oslash$ kein Modell?

$\{K_1, K_2\} \vdash R$ bedeutet: $\{K_1, K_2\} \models\!\!\!\!\approx R$. Die einzige Möglichkeit, $\oslash$ herzuleiten ist $\{l\}, \{\sim l\} \vdash \oslash$. Wenn also $\oslash$ ein Modell *hätte*, müsste auch $(l \wedge \neg l)$ ein Modell haben. Widerspruch.

$\mathbf{RES}_{\mathsf{PRL}}$ als Widerlegungskalkül*

Anmerkung: Unvollständigkeit als Deduktionskalkül

Offensichtlich gilt $\emptyset \not\vdash (p \longrightarrow (q \longrightarrow p)) = \mathrm{H}1 \Longleftrightarrow \mathsf{T}$.

Idee zum konstruktiven Widerlegungsbeweis 1:

Sei P erfüllbar. Zu zeigen sei, daß $P \cup \{p\}$ erfüllbar ist.
Wenn also $P \cup \{\neg p\}$ *un*erfüllbar ist, dann ist $P \cup \{p\}$ erfüllbar.

Idee zum konstruktiven Widerlegungsbeweis 2:

$$
\begin{array}{rcl}
P \mathrel{|}\!\!\approx p & \overset{\mathsf{NEG}}{\Longleftrightarrow} & P \mathrel{|}\!\!\approx \neg\neg p \\
 & \overset{\mathsf{PSN}}{\Longleftrightarrow} & P \mathrel{|}\!\!\approx (\neg p \longrightarrow \mathsf{F}) \\
 & \overset{\mathsf{DT}}{\Longleftrightarrow} & P \cup \{\neg p\} \mathrel{|}\!\!\approx \mathsf{F} \\
 & \overset{|\!\approx, Sat(\mathsf{F})}{\Longleftrightarrow} & P \cup \{\neg p\} \text{ ist unerfüllbar.}
\end{array}
$$

$\mathbf{RES}_{\mathsf{PRL}}$ als Widerlegungskalkül

Thm. 25: $\mathbf{RES}_{\mathsf{PRL}}$ als Widerlegungskalkül

$\mathbf{RES}_{\mathsf{PRL}}$ ist korrekt und widerlegungsvollständig.

Bew.

Der Beweis zerfällt in zwei Teile:

1. Korrektheit: $\oslash \in \mathrm{Res}^*(P) \Longrightarrow P$ ist unerfüllbar
2. Vollständigkeit: P ist unerfüllbar $\Longrightarrow \oslash \in \mathrm{Res}^*(P)$

$\mathbf{RES}_{\mathsf{PRL}}$ als Widerlegungskalkül

Bew. Korrektheit.

1. Sei $\oslash \in \mathrm{Res}^*(P)$.
2. $\oslash = \emptyset$ kann nach RES allein durch Resolution zweier unärer Klauseln mit einem komplementären Paar entstanden sein:

$$
\begin{array}{ccc}
K_1 = \{l\} & & \{\sim l\} = K_2 \\
& \oslash = \emptyset &
\end{array}
$$

3. Nach Def. Res^* und Resolutionslemma gilt also: P erfüllbar gdw. $\mathrm{Res}^*(P)$ erfüllbar; dann $P \cup \{K_1, K_2\}$ erfüllbar.
4. Da $\{K_1, K_2\} = \{\{l\}, \{\sim l\}\}$ **un**erfüllbar:
   4.1 $P \cup \{K_1, K_2\}$ ist **un**erfüllbar
   4.2 daher ist auch P **un**erfüllbar.

$\mathbf{RES}_{\mathrm{PRL}}$ als Widerlegungskalkül

Bew. Vollständigkeit.

Der Vollständigkeitsbeweis wird in einer Folgevorlesung behandelt.

Nutzung von $\mathbf{RES}_{\mathsf{PRL}}$

Widerlegungskalkül

1. Bilde $\mathrm{Res}^*(P)$ und überprüfe $\oslash \in \mathrm{Res}^*(P)$. Problem: P unendlich.
2. Kompaktheitstheorem und Vollständigkeit von $\mathbf{RES}_{\mathsf{PRL}}$ als Widerlegungskalkül: Erzeuge eine endliche Ableitung von $\oslash$ aus P.

Variante 1

```
R={};
while R != P do
  R := P;
  P := Res(R);
done;
if ({} in R) then
  ret(0) else ret(1);
```

Variante 2.

```
while ({} !in P) do
  if (choose K1, K2) then
    P := P + Res(K1, K2);
  else
    ret(1)
done;
ret(0)
```

Beispiel (Un-) Erfüllbarkeit*

Beispiel 1. $p = ((l_1 \wedge l_2) \wedge \neg(l_1 \longrightarrow l_2))$ ist unerfüllbar.

$p \overset{\text{CNF}}{\iff} \{\{l_1\}_1, \{l_2\}_2, \{l_1\}_1, \{\sim l_2\}_3\}$ und $c_2, c_3 \vdash \oslash$.

Beispiel 2. $p = (l_1 \wedge ((l_1 \longrightarrow l_2) \wedge \neg l_2))$ ist unerfüllbar.

$p \overset{\text{CNF}}{\iff} \{\{l_1\}_1, \{\sim l_1, l_2\}_2, \{\sim l_2\}_3\} =: P$. Dann:

Deduktive Hüllenbildung

$$
\begin{aligned}
\mathrm{Res}^0(P) &= P = \{\{l_1\}_1, \{\sim l_1, l_2\}_2, \{\sim l_2\}_3\} \\
\mathrm{Res}^1(P) &= \mathrm{Res}^0(P) \cup \left\{\{l_2\}_4^{(1,2)}, \{\sim l_1\}_5^{(2,3)}\right\} \\
\mathrm{Res}^2(P) &= \mathrm{Res}^1(P) \cup \left\{\{\}_6^{(3,4)}, \{\}_6^{(1,5)}\right\} \\
\mathrm{Res}^3(P) &= \mathrm{Res}^2(P) \cup \emptyset = \mathrm{Res}^2(P) = \mathrm{Res}^*(P).
\end{aligned}
$$

Beispiel (Un-) Erfüllbarkeit*

Beispiel 1. $p = ((l_1 \wedge l_2) \wedge \neg(l_1 \longrightarrow l_2))$ ist unerfüllbar.

$p \overset{\text{CNF}}{\Longleftrightarrow} \{\{l_1\}_1, \{l_2\}_2, \{l_1\}_1, \{\sim l_2\}_3\}$ und $c_2, c_3 \vdash \oslash$.

Beispiel 2. $p = (l_1 \wedge ((l_1 \longrightarrow l_2) \wedge \neg l_2))$ ist unerfüllbar.

$p \overset{\text{CNF}}{\Longleftrightarrow} \{\{l_1\}_1, \{\sim l_1, l_2\}_2, \{\sim l_2\}_3\} =: P$. Dann:

Konstruktive Ableitung

$$
\begin{tikzcd}
\{l_1\}_{1} \arrow[dr, dash] & & \{\sim l_1, l_2\}_{2} \arrow[dl, dash] & & \{\sim l_2\}_{3} \arrow[ddl, dash] & = \mathrm{Res}^0(P) \\
& \{l_2\}_{4} \arrow[drr, dash] & & & & \subseteq \mathrm{Res}^1(P) \\
& & & \{\}_{6}^{(3,4)} & & \subseteq \mathrm{Res}^2(P)
\end{tikzcd}
$$

Beispiel (Un-) Erfüllbarkeit

Beispiel 3. $p = ((l_1 \wedge l_2) \wedge (l_1 \vee \neg l_3))$ ist erfüllbar.

$$p \overset{\mathsf{CNF}}{\Longleftrightarrow} \{\{l_1\}, \{l_2\}, \{l_1, \sim l_3\}\} = P$$

Kein komplementäres Paar vorhanden, keine Resolution möglich:

$$\oslash \notin P = \mathrm{Res}^0(P) = \mathrm{Res}^0(P) \cup \{\} = \mathrm{Res}^1(P) = \mathrm{Res}^*(P)$$

Beispiel 4. $p = ((\neg l_1 \wedge l_2) \wedge (l_1 \longrightarrow l_2))$ ist erfüllbar.

$$p \overset{\mathsf{CNF}}{\Longleftrightarrow} \{\{\sim l_1\}, \{l_2\}, \{\sim l_1, l_2\}\} = P$$

Kein komplementäres Paar vorhanden, $\oslash \notin P$.

Beispiel (Un-) Erfüllbarkeit

Beispiel 5. $p = ((l_3 \longrightarrow l_1) \wedge (l_2 \wedge \neg((l_2 \vee l_3) \longrightarrow l_1)))$.

$$
\begin{array}{cl}
 & p \\
\Longleftrightarrow & ((\neg l_3 \vee l_1) \wedge (l_2 \wedge \neg(\neg(l_2 \vee l_3) \vee l_1))) \\
\overset{\text{DEM}}{\Longleftrightarrow} & ((\neg l_3 \vee l_1) \wedge (l_2 \wedge \neg((\neg l_2 \wedge \neg l_3) \vee l_1))) \\
\overset{\text{DEM}}{\Longleftrightarrow} & ((\neg l_3 \vee l_1) \wedge (l_2 \wedge (\neg(\neg l_2 \wedge \neg l_3) \wedge \neg l_1))) \\
\overset{\text{DEM,COM}}{\Longleftrightarrow} & ((l_2 \wedge ((l_2 \vee l_3) \wedge \neg l_1)) \wedge (\neg l_3 \vee l_1)) \\
\overset{\text{COM,ASC}}{\Longleftrightarrow} & (((\neg l_1 \wedge (l_2 \vee l_3)) \wedge l_2) \wedge (\neg l_3 \vee l_1)) \\
\overset{\text{DST}}{\Longleftrightarrow} & (((\neg l_1 \wedge l_2) \wedge (l_2 \vee l_3)) \wedge (\neg l_3 \vee l_1)) \\
\overset{\text{CNF}}{\Longleftrightarrow} & \{\{\sim l_1\}_1, \{l_2\}_2, \{l_2, l_3\}_3, \{\sim l_3, l_1\}_4\} \\
\overset{\text{Thm.17}}{\Longleftrightarrow} & \left\{\{\sim l_1\}_1, \{l_2\}_2, \{l_2, l_3\}_3, \{\sim l_3, l_1\}_4, \{\sim l_3\}_5^{(1,4)}, \{l_1, l_2\}_6^{(3,4)}\right\} \\
 & \not\ni \emptyset
\end{array}
$$

Beispiel (Un-) Erfüllbarkeit

Beispiel 5. $\{p_1, p_2, p_3\} = \{(l_1 \longrightarrow l_2), \neg l_2, l_1\}$.

Beachte: $Sat(\{p_1, p_2, p_3\}) = Sat((p_1 \wedge (p_2 \wedge p_3)))$.

$$
\begin{array}{ll}
 & (p_1 \wedge (p_2 \wedge p_3)) \\
\iff & ((l_1 \longrightarrow l_2) \wedge (\neg l_2 \wedge l_1)) \\
\iff & \{\{\sim l_1, l_2\}_1, \{\sim l_2\}_2, \{l_1\}_3\} \\
\iff & \left\{\{\sim l_1, l_2\}_1, \{\sim l_2\}_2, \{l_1\}_3, \{\sim l_1\}_4^{(1,2)}, \{l_2\}_5^{(1,3)}\right\} \\
\iff & \left\{\{\sim l_1, l_2\}_1, \{\sim l_2\}_2, \{l_1\}_3, \{\sim l_1\}_4^{(1,2)}, \{l_2\}_5^{(1,3)}, \{\}_6^{(3,4)}, \{\}_6^{(2,5)}\right\} \\
 & \ni \emptyset
\end{array}
$$

6.2
ANWENDUNG DES RESOLUTIONSKALKÜLS

Anwendung der Resolution zur Deduktion

"Modus Ponens"

MP ist *keine* $\mathbf{RES}_{\mathsf{PRL}}$ -Regel. Ebenso enthält $\mathbf{RES}_{\mathsf{PRL}}$ nichts einer II-Regel entsprechendes. Wie beweist man dann

$$\{p, (p \longrightarrow q)\} \approx q \text{ ?}$$

Deduktion durch Widerspruch

$$\begin{array}{rcccl} & \mathcal{I}^{\alpha}.\{p, (p \longrightarrow q)\} = \mathbf{1} & \Longrightarrow & \mathcal{I}^{\alpha}.q = \mathbf{1} & \\ \text{gdw.} & \mathcal{I}^{\alpha}.\{p, (p \longrightarrow q)\} = \mathbf{1} & \wedge & \mathcal{I}^{\alpha}.q = \mathbf{0} & \Longleftrightarrow \mathsf{F} \end{array}$$

Mit $\mathsf{F}' = \oslash'$ bzw. $Sat(\mathsf{F}) = Sat(\oslash) = \emptyset$ und Resolutionslemma:[1]

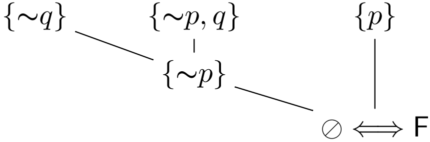
$$\{p, (p \longrightarrow q)\} \approx q \text{ gdw. } \{p, \{\sim p, q\}\} \cup \{\{\sim q\}\} \vdash^{*}_{\mathbf{RES}_{\mathsf{PRL}}} \oslash$$

[1] Wir nehmen implizite Umformungen und Umbennungen in CNF an.

Anwendung der Resolution zur Deduktion

Zu zeigen sei $\{p, (p \longrightarrow q)\} \mathrel{|}\!\!\approx q$ ("Semantisch")

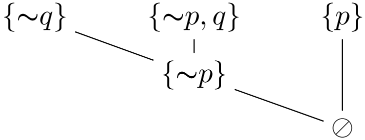
1. Umformung von q ergibt: $q \iff \neg\neg q \iff (\neg q \longrightarrow \mathsf{F})$.
2. Anwendung von DT also: $\{p, (p \longrightarrow q), \neg q\} \mathrel{|}\!\!\approx \mathsf{F}$.
3. Resolution ergibt:



Anwendung der Resolution zur Deduktion

Zu zeigen sei $\{p, (p \longrightarrow q)\} \mathrel{|\!\!\approx} q$ ("Syntaktisch a.")

1. Umformung in CNF ergibt $\{\{p\}, \{\sim p, q\}\}$ und $\{\{q\}\}$
2. Negation der These und Vereinigung ergibt $\{\{p\}, \{\sim p, q\}, \{\sim q\}\}$
3. Resolution ergibt:



Anwendung der Resolution zur Deduktion

Zu zeigen sei $\{p, (p \longrightarrow q)\} \mathrel{|\!\!\approx} q$ ("Syntaktisch b.")

1. Umformung in CNF ergibt $\{\{p\}, \{\sim p, q\}\}$ und $\{\{q\}\}$
2. Negation der These und Vereinigung ergibt $\{\{p\}, \{\sim p, q\}, \{\sim q\}\}$
3. Resolution ergibt:

1	$\{p\}$	
2	$\{\sim p, q\}$	
3	$\{\sim q\}$	
4	$\{q\}$	$(1, 2)$
5	$\{\}$	$(3, 4)$

Beweis der Korrektheit von SHN

Bew. $((p \wedge q) \longrightarrow r) \Longleftrightarrow (p \longrightarrow (\neg q \vee r))$

Wir zeigen nur "$\Longrightarrow$":

$$\begin{aligned}
& \{((p \wedge q) \longrightarrow r)\} \approx (\neg (p \longrightarrow (\neg q \vee r)) \longrightarrow \mathsf{F}) \\
\overset{\mathsf{DT}}{\Longleftrightarrow}\quad & \{((p \wedge q) \longrightarrow r), \neg (p \longrightarrow (\neg q \vee r))\} \approx \mathsf{F} \\
\overset{\mathrm{CNF}}{\Longleftrightarrow}\quad & \{\{\sim p, \sim q, r\}, \{p\}, \{q\}, \{\sim r\}\} \vdash^* \oslash \\
\overset{\mathrm{Res}^*}{\Longleftrightarrow}\quad & \{\sim p, \sim q, r\}, \{p\} \vdash \{\sim q, r\} \\
& \{\sim q, r\}, \{q\} \vdash \{r\} \\
& \{r\}, \{\sim r\} \vdash \oslash
\end{aligned}$$

Hinweis zur Nutzung

Praktikabilität

RES ist praktisch, da es nur eine Regel (vgl. **ND**) gibt.

Anwendung

1. Bei einer Nutzung von Res^* bietet sich eine Matrixdarstellung an. Alle n Ausgangsklauseln werden als Spalten- und Zeilenlabel einer $n \times n$-Matrix verwendet; die Zellen enthalten die Resolventen. Neue Resolventen erweitern die Matrixspalten und -zeilen bis die Matrix maximal ist oder $\oslash$ erzeugt wurde.
2. Bei einer Nutzung von RES kann man eine lineare Darstellung wie für **ND**-Beweise verwenden.
3. Alternativ kann eine Baumdarstellung genutzt werden; diese macht zwar die Sequenz der Resolutionsschritte schön sichtbar, wird aber bei großen Beweisen unübersichtlich.

7.
PRÄDIKATENLOGIK ERSTER STUFE

Prädikatenlogik (erster Stufe)

erweitert das klassische Konzept einer zweiwertigen Boole'schen Logik um:

1. *Prädikative* Aussagen über
2. *Terme* und *Variablen*
3. die *quantifiziert* sein können.

Zum Beispiel:

- $\forall x\colon (x \in \mathbb{N}_0 \longrightarrow \exists y\colon (y \in \mathbb{N}_0 \wedge x < y + 1))$
- $\exists x\colon (x \in \mathbb{N}_0 \wedge \forall y\colon (x \in \mathbb{N} \longrightarrow x \cdot y = x))$

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x + k) = y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x + k) = y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x + k) = y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik
2. Aussagen über Objekte x, y, k aus der Domäne $\mathbb{N}_0$

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x + k) = y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik
2. Aussagen über Objekte x, y, k aus der Domäne $\mathbb{N}_0$
3. Beziehungen, Eigenschaften, Prädikate auf der Domäne $\mathbb{N}_0$

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x+k)=y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik
2. Aussagen über Objekte x, y, k aus der Domäne $\mathbb{N}_0$
3. Beziehungen, Eigenschaften, Prädikate auf der Domäne $\mathbb{N}_0$
4. Funktionen, Terme: $+ \in \mathrm{Fnc}$ in der Domäne $\mathbb{N}_0$

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x+k) = y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik
2. Aussagen über Objekte x, y, k aus der Domäne $\mathbb{N}_0$
3. Beziehungen, Eigenschaften, Prädikate auf der Domäne $\mathbb{N}_0$
4. Funktionen, Terme: $+ \in \mathrm{Fnc}$ in der Domäne $\mathbb{N}_0$
5. Logische Junktoren

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x{:}\forall y{:}(x \leq y \longleftrightarrow \exists k{:}(x+k)=y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik
2. Aussagen über Objekte x, y, k aus der Domäne $\mathbb{N}_0$
3. Beziehungen, Eigenschaften, Prädikate auf der Domäne $\mathbb{N}_0$
4. Funktionen, Terme: $+ \in \mathrm{Fnc}$ in der Domäne $\mathbb{N}_0$
5. Logische Junktoren
6. Quantifikation

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw.M_2 die Vereinigung von einer Menge N mit M_1 ist.

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die “betrachtete Welt” ist Mengentheorie.

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die "betrachtete Welt" ist Mengentheorie.
2. Aussagen über Objekte M_1, M_2, N aus der Klasse der Mengen

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die "betrachtete Welt" ist Mengentheorie.
2. Aussagen über Objekte M_1, M_2, N aus der Klasse der Mengen
3. Beziehungen, Eigenschaften, Prädikate zwischen Mengen

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die "betrachtete Welt" ist Mengentheorie.
2. Aussagen über Objekte M_1, M_2, N aus der Klasse der Mengen
3. Beziehungen, Eigenschaften, Prädikate zwischen Mengen
4. Funktionen, Terme: $\cup \in \mathrm{Fnc}$ auf Mengen

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw.M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die "betrachtete Welt" ist Mengentheorie.
2. Aussagen über Objekte M_1, M_2, N aus der Klasse der Mengen
3. Beziehungen, Eigenschaften, Prädikate zwischen Mengen
4. Funktionen, Terme: $\cup \in \mathrm{Fnc}$ auf Mengen
5. Logische Junktoren

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die "betrachtete Welt" ist Mengentheorie.
2. Aussagen über Objekte M_1, M_2, N aus der Klasse der Mengen
3. Beziehungen, Eigenschaften, Prädikate zwischen Mengen
4. Funktionen, Terme: $\cup \in \mathrm{Fnc}$ auf Mengen
5. Logische Junktoren
6. Quantifikation

7.1
SYNTAX DER PRÄDIKATENLOGIK

Def. 30: Signatur Σ

Eine Signatur Σ besteht aus drei Teilen:

1. $\mathrm{Srt}_\Sigma = \{\mathtt{s}_i \parallel i \in \mathbf{k}\}$
   ist eine endl. Fam. von *Domänen* $\mathcal{U}_i$ (*Sorten* oder *Typen*)
2. $\mathrm{Prd}_\Sigma = \left\{\mathtt{p}_i^{n_i} : \mathtt{s}_{i_1}, \ldots, \mathtt{s}_{i_{n_i}} \parallel n_i \in \mathbb{N}_0, i \in \mathbf{m}\right\}$
   ist eine endl. Menge von *Prädikatssymbolen*
3. $\mathrm{Fnc}_\Sigma = \left\{\mathtt{f}_j^{n_j} : \mathtt{s}_{j_1}, \ldots, \mathtt{s}_{j_{n_j}} \rightarrow \mathtt{s}_j \parallel n_j \in \mathbb{N}_0, j \in \mathbf{n}\right\}$
   ist endl. Menge der *Funktionssymbole (Termkonstruktoren)*
   $\mathtt{c}^0 :\rightarrow \mathtt{s} \in \mathrm{Fnc}_\Sigma$ nennt man *Konstanten*, $\mathrm{Con}_\Sigma^{\mathtt{s}}$.

Die *Stelligkeiten* n_i bzw. n_j werden meist nicht explizit erwähnt.

Meist kann auf eine explizite Nennung von Σ verzichtet werden.

Zwischenbemerkung

Eine Signatur bestimmt die strukturellen Eigenschaften einer Sprache. Ter ist die Menge der aus der zugrunde liegenden Signatur erzeugten Terme (Formeln, Wörter).

Ein einfaches Beispiel - das nebenbei $\mathfrak{i}$ aus $\mathcal{I}^\alpha$ erklärt:

Folgende Signatur Σ_{PRL} legt die Formelstruktur von PRL fest:

- F :→ $\mathtt{omega}$
- T :→ $\mathtt{omega}$
- $\neg$: $\mathtt{omega}$ → $\mathtt{omega}$
- $\wedge$: $\mathtt{omega}, \mathtt{omega}$ → $\mathtt{omega}$
- $\vee$: $\mathtt{omega}, \mathtt{omega}$ → $\mathtt{omega}$
- $\longrightarrow$: $\mathtt{omega}, \mathtt{omega}$ → $\mathtt{omega}$

Syntax der FOL: Terme

Def. 31: Σ-Grundterme $\quad \mathrm{Gnd}_\Sigma$

$\mathrm{Gnd}^{\mathtt{s}}_\Sigma$ ist die kleinste Menge für die gilt:

1. $\mathtt{c} :\rightarrow \mathtt{s} \in \mathrm{Con} \Longrightarrow \mathtt{c} \in \mathrm{Gnd}^{\mathtt{s}}_\Sigma$ und
2. $\left(\mathtt{f} : \mathtt{s}_1, \ldots \mathtt{s}_n \rightarrow \mathtt{s} \in \mathrm{Fnc} \wedge t_i \in \mathrm{Gnd}^{\mathtt{s}_i}_\Sigma\right) \Longrightarrow \mathtt{f}(t_1, \ldots, t_n) \in \mathrm{Gnd}^{\mathtt{s}}_\Sigma$.

Meist kann auf eine explizite Nennung von Σ und $\mathtt{s}$ verzichtet werden.

Zwischenbemerkung

$\mathscr{B} = \langle \Omega, \sqcap, \sqcup, \setminus, ^{-}, \top, \bot \rangle$ ist eine Σ_{PRL}-Algebra. Die Zuordnung der durch Σ_{PRL} generierten Terme (also jungierten Atome) erfolgt durch

- α für die Atome und
- $\mathfrak{i}$ für die Junktoren.

Zusammen ergeben diese $\mathcal{I}$.

Syntax der FOL: Terme

Variablen

Wir erweitern den Begriff der Signatur um *Variablendeklarationen*: $\mathrm{Var}_{\Sigma}^{(\mathtt{s})}$ sei also die Menge der Variablensymbole (vom Typ $\mathtt{s}$) deklariert als

$$\mathtt{s}\ x, y, z, \ldots$$

Def. 32: Σ-Terme $\qquad \mathrm{Ter}_{\Sigma}$

Die Menge Ter_{Σ} ist die kleinste Menge, für die gilt:

1. $t \in \mathrm{Gnd}_{\Sigma} \Longrightarrow t \in \mathrm{Ter}_{\Sigma}$
2. $x \in \mathrm{Var}_{\Sigma} \Longrightarrow x \in \mathrm{Ter}_{\Sigma}$
3. $(\mathtt{f} : \mathtt{s}_1, \ldots \mathtt{s}_n \rightarrow \mathtt{s} \in \mathrm{Fnc}_{\Sigma} \wedge t_i \in \mathrm{Ter}_{\Sigma}) \Longrightarrow \mathtt{f}(t_1, \ldots, t_n) \in \mathrm{Ter}_{\Sigma}$.

Meist kann auf eine explizite Nennung von Σ verzichtet werden.

Syntax der Prädikatenlogik

Def. 33: (Σ-) Prädikate

Die Menge der *Prädikate* ist die kleinste Menge für die gilt:

1. $\mathtt{p} :\in \mathrm{Prd}_\Sigma$
2. $\big(\mathtt{p} : \mathtt{s}_1, \dots \mathtt{s}_n \in \mathrm{Prd}_\Sigma \wedge t_i \in \mathrm{Ter}_\Sigma^{\mathtt{s}_i}\big) \Longrightarrow \mathtt{p}(t_1, \dots, t_n) \in \mathrm{Prd}_\Sigma.$

Man beachte, daß Prädikate keine explizit angegebene Sorte haben.

Prädikate dienen der Darstellung von Aussagen

Daß (und wie) Prädikate Aussagen darstellen, wird in der Semantik von FOL erläutert.

Syntax der Prädikatenlogik

Def. 34: Die Sprache der Prädikatenlogik, Fml_Σ

Fml_Σ ist die kleinste Menge der

1. *atomaren* Formeln der Form $\mathtt{p}(t_1, \ldots, t_n)$ mit $\mathtt{p} \in \mathrm{Prd}_\Sigma$ und $t_i \in \mathrm{Ter}_\Sigma$ sowie
2. der *komplexen* Formeln $\neg p, (p \wedge q), (p \vee q), (p \longrightarrow q)$ für $p, q \in \mathrm{Fml}_\Sigma$
3. und der *quantifizierten* Formeln $\forall x : p$ und $\exists x : p$ für $p \in \mathrm{Fml}_\Sigma$.

Bezeichnungen

In $p = \mathsf{Q}x : q$ nennt man q den *Skopus* des Quantors $\mathsf{Q}x$. Alle Vorkommen von x im Skopus eines Quantors nennt man (durch Q) *gebunden*.

Der Skopus ergibt sich immer exklusiv aus dem direkt folgenden Klammerausdruck (außer für atomare und quantifizierte Formeln).

Signaturen und "sinnvolle" Aussagen*

$$p = \forall x\colon \forall y\colon (x \leq y \longleftrightarrow \exists z\colon (x{+}z) = y)$$

- $\{\mathtt{s}\ x, y, z\} \subseteq \mathrm{Var}.$
- $\{+ : \mathtt{s}, \mathtt{s} \to \mathtt{s}\} \subseteq \mathrm{Fnc}$
- $\{\leq : \mathtt{s}, \mathtt{s}, = : \mathtt{s}, \mathtt{s}\} \subseteq \mathrm{Prd}$

Daher

- $\mathrm{Ter}(p) = \{x, y, z, x{+}z\}$
- $\mathrm{Fml}(p) = \{x{+}z = y,\ x \leq y,\ \exists z\colon x{+}z = y,\ \ldots\}$

Formeln werden als Aussagen betrachtet, Terme als Bezeichner für Objekte.

Signaturen helfen "Unsinn" zu vermeiden

$$\forall x\colon \forall y\colon (x{+}y \longleftrightarrow \exists z\colon (x \leq z) = y)$$

Variablen in FOL

Def. 35: Vorkommen von Variablen

- In p nicht gebundene Variablen heißen *frei in* p. Sie können als *Parameter* verstanden werden.
- $\mathrm{var}(p)$ ist die Menge aller in der Formel p vorkommenden Variablen. $\mathrm{var}(t)$ ist die Menge aller in dem Term t vorkommenden Variablen.
- $\mathrm{fvr}(p)$ und $\mathrm{bvr}(p)$ sind die Teilmengen der frei/gebunden vorkommenden Variablen.
- p heißt *geschlossen*, wenn $\mathrm{fvr}(p) = \emptyset$.
- p heißt *bereinigt*, wenn $\mathrm{bvr}(p) \cap \mathrm{fvr}(p) = \emptyset$.
- Ein Term (Formel) t (p) heißt *Grundterm* (*Grundformel*), wenn er (sie) *keine* Variablen beinhaltet $\mathrm{var}(t) = \emptyset$ (bzw. $\mathrm{var}(p) = \emptyset$).

Operationen auf Sprachelementen von FOL

Substitution: Syntaktische Ersetzung von Teilzeichenketten

Def. 36: Σ-Substitution

Eine *Substitution* ist eine Ersetzung von *Variablen* durch *Terme*:

$$\sigma = [x_1/t_1, \ldots, x_n/t_n] \text{ mit } x_i \in \mathrm{Var}_{\mathsf{FOL}}, t_i \in \mathrm{Ter}_\Sigma$$

$t\sigma = s$ entsteht durch *gleichzeitiges* Ersetzen *aller* Vorkommen *aller* x_i durch t_i. $p\sigma = q$ entsteht durch *gleichzeitiges* Ersetzen *aller freien* Vorkommen *aller* x_i durch t_i.

Beispiel: $\sigma = [x/\mathtt{g}(z), y/\mathtt{f}(\mathtt{g}(y)), z/x]$

$((\mathtt{p}(x) \lor \exists y\colon \mathtt{r}(y,z)) \longrightarrow (\mathtt{q}(\mathtt{f}(x), y) \land \mathtt{r}(y, \mathtt{f}(\mathtt{g}(z)))))\,\sigma =$
$((\mathtt{p}(\mathtt{g}(z)) \lor \exists y\colon \mathtt{r}(y,x)) \longrightarrow (\mathtt{q}(\mathtt{f}(\mathtt{g}(z)), \mathtt{f}(\mathtt{g}(y))) \land \mathtt{r}(\mathtt{f}(\mathtt{g}(y)), \mathtt{f}(\mathtt{g}(x)))))$

Substitutionen

Def. 37: Zulässigkeit von Substitutionen

Sei $\sigma = [x_1/t_1, \ldots, x_n/t_n]$ eine Substitution. σ ist *zulässig für* p, gdw. keine Variable in t_i nach der Substitution gebunden ist: $\sigma = [y/t]$ ist unzulässig für $\mathsf{Q}x : p$, wenn $y \neq x \in \mathrm{var}(t)$.

$\sigma = [y/x]$ unzulässig für $p = \forall x : \mathtt{p}(x, y)$ weil $p\sigma = \forall x : \mathtt{p}(x, x)$.
$\sigma = [y/x + 1]$ unzulässig für $q = \exists x : y|x$ weil $p\sigma = \exists x : x + 1|x$.

Def. 38: Komposition von Substitutionen

Seien $\sigma = [x/t]$ und $\theta = [y/s]$. Dann

$$\sigma\theta := [x/t\theta] \cup [y/s \| y \neq x] \,,$$

Thm. 26: Rechnen mit Substitutionen

(1) $t(\sigma\theta) = (t\sigma)\theta$. (2) Wenn $p\sigma$ und $p\sigma\theta$ zulässig, dann auch $p(\sigma\theta) = (p\sigma)\theta$. (3) Komposition von Substitutionen ist assoziativ.

Varianten

Def. 39: Varianten von Substitutionen

ϑ heißt *Variante* von σ, wenn es Subsitutionen τ_1 und τ_2 gibt, so daß $\sigma = \vartheta\tau_1$ und $\vartheta = \sigma\tau_2$

Def. 40: Umbenennung

Eine Substitution ρ heißt *Umbenennung (in t)*, gdw.

$$\rho = [x_i/y_i]_I\,, \quad x_i, y_i \in \mathrm{Var}, i \in I$$

$\{x_i\}_I \subseteq \mathrm{var}(t)$, $y_i \neq y_j$ für alle $i \neq j$, $y_i \notin \mathrm{var}(t)$ oder $y_i \in \{x_i\}_I$.

Def. 41: Varianten von $\mathbf{w} \in \{t, p, P\}$

Seien $t, t' \in \mathrm{Ter}$, $p, p' \in \mathrm{Fml}$, $P, P' \subseteq \mathrm{Fml}$. $\mathbf{w}'$ heißt *Variante* von $\mathbf{w}$, gdw. es existieren Substitutionen σ und ϑ, so daß

$$\mathbf{w}\sigma = \mathbf{w}' \text{ und } \mathbf{w} = \mathbf{w}'\vartheta$$

Unifikation

Def. 42: Unifikator

Eine Substitution σ heißt *Unifikator für* eine Menge W von Termen oder Formeln $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$, gdw. $\{\mathbf{w}_1\sigma, \ldots, \mathbf{w}_n\sigma\}$ nur ein Element enthält.

Wirkung von Unifikatoren

D.h. ein Unifikator σ macht Terme/Formeln gleich: $p\sigma = q\sigma$.

Def. 43: Allgemeinste Unifikatoren

Ein Unifikator μ heißt *allgemeinster Unifikator*, wenn alle andere Unifikatoren σ durch Anwendung einer nachfolgenden Substitution dargestellt werden können:

$$\sigma = \mu\theta$$

WICHTIGE BEMERKUNG ZUR NOTATION

Zur Nomenklatur

- In Signaturen haben wir Buchstaben $\mathtt{c}$, $\mathtt{f}$, $\mathtt{p}$ für Konstanten, Funktions- und Prädikats*symbole* benutzt.
- Wir benutzen $p, q, r \in \mathrm{Fml}$, $t, s, u \in \mathrm{Ter}$ als Bezeichner für Formeln und Terme, also $p = (\mathtt{p}(x) \longrightarrow \mathtt{q}(\mathtt{f}(z), \mathtt{a}))$ mit einem Term $t = \mathtt{f}(z)$.

Vereinfachung

Da Σ aus dem Kontext klar ist, ist auch klar, ob wir von einer Formel $p = \mathtt{p}(x)$ oder einem Prädikat $p(x)$ reden. Daher werden die verschiedenen Schriftarten oft nicht genutzt. Das ist in einem bestimmten Fall auch absolut unproblematisch - kann sonst aber oft zu Verwirrung führen, ohne das man es merkt.

7.2
SEMANTIK DER PRÄDIKATENLOGIK

Semantik der Prädikatenlogik

Bedeutung der Sprachelemente

- Verschiedene Konstanten *bezeichnen* verschiedene *Objekte*.
- Terme stehen für das *Ergebnis*, zu dem sie *ausgewertet* werden
- Prädikate bezeichnen *Relationen* zwischen Objekten
- Formeln sind *Aussagen*, die wahr/falsch sein können

FOL wurde für eine mächtigere Modellklasse als nur $\mathscr{B}$ entworfen.

Modelle

$$\mathcal{I} : \mathrm{Fml}_\Sigma \to {}^?_?\mathfrak{A}^?_?$$

Semantik FOL

Modelle

(Rechen-) Strukturen, die gegebenen Signaturen entsprechen.

1. Problem $\rightsquigarrow$ Formalisierung:
   $\mathfrak{A}$ "bekannt", Σ "passend" deklariert (s.a. "Theorie")
2. Formalisierung $\rightsquigarrow$ Modell:
   "Theorie" gegeben, Ausdrucksfähigkeit analysieren.

Zur Wichtigkeit der Prädikatenlogik

1. Formales Beweisen in komplexeren Zusammenhängen:
   Folgt aus einer Menge von Fakten/Regeln eine Aussage?

$$P \mid\!\approx p$$

2. Kann eine *Theorie* $\mathfrak{A}$ *definiert* werden? Kann $P \mid\!\approx p$ immer entschieden werden? Was muß in einer Theorie gelten/angenommen werden, damit bestimmte Schlussformen möglich sind?

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x + k) = y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x + k) = y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x + k) = y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik
2. Aussagen über $x, y, k \in \mathrm{Var}$ vom Typ $\mathtt{s}$, der für $\mathbb{N}_0$ stehen soll

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x + k) = y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik
2. Aussagen über $x, y, k \in \mathrm{Var}$ vom Typ $\mathfrak{s}$, der für $\mathbb{N}_0$ stehen soll
3. Beziehungen, Eigenschaften, Prädikate in $\mathbb{N}_0$: $\leq, = \in \mathrm{Prd}$

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x+k)=y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik
2. Aussagen über $x, y, k \in \mathrm{Var}$ vom Typ $\mathfrak{s}$, der für $\mathbb{N}_0$ stehen soll
3. Beziehungen, Eigenschaften, Prädikate in $\mathbb{N}_0$: $\leq, = \in \mathrm{Prd}$
4. Funktionen, Terme in $\mathbb{N}_0$: $+ \in \mathrm{Fnc}$

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x : \forall y : (x \leq y \longleftrightarrow \exists k : (x+k) = y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik
2. Aussagen über $x, y, k \in \mathrm{Var}$ vom Typ $\mathfrak{s}$, der für $\mathbb{N}_0$ stehen soll
3. Beziehungen, Eigenschaften, Prädikate in $\mathbb{N}_0$: $\leq, = \in \mathrm{Prd}$
4. Funktionen, Terme in $\mathbb{N}_0$: $+ \in \mathrm{Fnc}$
5. Logische Junktoren

Ein **Beispiel** zu Beginn I

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall x{:}\forall y{:}(x \leq y \longleftrightarrow \exists k{:}(x+k)=y)$$

x ist kleiner gleich y, gdw. sich y aus der Addition einer Zahl k zu x ergibt.

1. Die "betrachtete Welt" ist $\mathbb{N}_0$-Arithmetik
2. Aussagen über $x, y, k \in \mathrm{Var}$ vom Typ $\mathfrak{s}$, der für $\mathbb{N}_0$ stehen soll
3. Beziehungen, Eigenschaften, Prädikate in $\mathbb{N}_0$: $\leq, = \in \mathrm{Prd}$
4. Funktionen, Terme in $\mathbb{N}_0$: $+ \in \mathrm{Fnc}$
5. Logische Junktoren
6. Quantifikation

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die "betrachtete Welt" ist Mengentheorie $\mathbf{Set}$.

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die "betrachtete Welt" ist Mengentheorie $\mathbf{Set}$.
2. Aussagen über $M_1, M_2, N \in \mathrm{Var}$ vom Typ s (Klasse der Mengen)

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die "betrachtete Welt" ist Mengentheorie $\mathbf{Set}$.
2. Aussagen über $M_1, M_2, N \in \mathrm{Var}$ vom Typ s (Klasse der Mengen)
3. Beziehungen, Eigenschaften, Prädikate in $\mathbf{Set}$: $\subseteq, = \in \mathrm{Prd}$

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die “betrachtete Welt” ist Mengentheorie $\mathbf{Set}$.
2. Aussagen über $M_1, M_2, N \in \mathrm{Var}$ vom Typ s (Klasse der Mengen)
3. Beziehungen, Eigenschaften, Prädikate in $\mathbf{Set}$: $\subseteq, = \in \mathrm{Prd}$
4. Funktionen, Terme in $\mathbf{Set}$: $\cup \in \mathrm{Fnc}$

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die "betrachtete Welt" ist Mengentheorie $\mathbf{Set}$.
2. Aussagen über $M_1, M_2, N \in \mathrm{Var}$ vom Typ s (Klasse der Mengen)
3. Beziehungen, Eigenschaften, Prädikate in $\mathbf{Set}$: $\subseteq, = \in \mathrm{Prd}$
4. Funktionen, Terme in $\mathbf{Set}$: $\cup \in \mathrm{Fnc}$
5. Logische Junktoren

Ein **Beispiel** zu Beginn II

Folgende FOL-Formel dürfte Ihnen bekannt vorkommen:

$$\forall M_1 : \forall M_2 : (M_1 \subseteq M_2 \longleftrightarrow \exists N : (M_1 \cup N) = M_2)$$

M_1 ist Teilmenge von M_2, gdw. M_2 die Vereinigung von einer Menge N mit M_1 ist.

1. Die "betrachtete Welt" ist Mengentheorie $\mathbf{Set}$.
2. Aussagen über $M_1, M_2, N \in \mathrm{Var}$ vom Typ s (Klasse der Mengen)
3. Beziehungen, Eigenschaften, Prädikate in $\mathbf{Set}$: $\subseteq, = \in \mathrm{Prd}$
4. Funktionen, Terme in $\mathbf{Set}$: $\cup \in \mathrm{Fnc}$
5. Logische Junktoren
6. Quantifikation

Ein **Beispiel** III*

Das Wort abb ist kürzer als das Wort jjgwa, weil man an abb noch xy hängen kann und dann abbxy genauso lang ist wie jjgwa. Folgende Aussage dürfte Ihre Zustimmung finden:

Ein Wort u ist kürzer/gleich lang als v, gdw. man an u noch ein Wort w hängen kann, so daß uw so lang ist wie v.

Die genaue Semantik von <= und == und die tatsächliche Gültigkeit ist für dieses Beispiel nicht so wichtig!

Ein **Beispiel** III*

Das Wort abb ist kürzer als das Wort jjgwa, weil man an abb noch xy hängen kann und dann abbxy genauso lang ist wie jjgwa. Folgende Aussage dürfte Ihre Zustimmung finden:

Ein Wort u ist kürzer/gleich lang als v, gdw. man an u noch ein Wort w hängen kann, so daß uw so lang ist wie v.

$$\forall u{:}\forall v{:}(u\texttt{<=}v \longleftrightarrow \exists w{:}\texttt{strconc}(u,w)\texttt{==}v)$$

1. Die "betrachtete Welt" sind Wörter über $\mathcal{A} = \{\mathrm{a}, \ldots, \mathrm{z}\}$
2. Aussagen über Wörter $u, v, w \in \mathrm{Var}$
3. Vergleichsoperatoren auf Wörtern: $\texttt{<=},\texttt{==} \in \mathrm{Prd}$.
4. Funktionen: $\texttt{strconc} \in \mathrm{Fnc}$
5. Logische Junktoren
6. Quantifikation

Die genaue Semantik von <= und == und die tatsächliche Gültigkeit ist für dieses Beispiel nicht so wichtig!

Ein **Beispiel** zu Beginn IV

Gegeben sei eine Signatur mit:

$\mathtt{s}, \mathtt{s}\ x, y, z, \mathtt{f} : \mathtt{s}, \mathtt{s} \rightarrow \mathtt{s}, \mathtt{p} : \mathtt{s}, \mathtt{s}, \mathtt{q} : \mathtt{s}, \mathtt{s}.$

Über dieser Signatur kann man folgende Formel aufbauen:

$$\forall x : \forall y : (\mathtt{p}(x, y) \longleftrightarrow \exists z : \mathtt{q}(\mathtt{f}(x, z), y))$$

Ist diese Formel wahr? Was bedeutet sie?

Ein **Beispiel** zu Beginn IV

Gegeben sei eine Signatur mit:

$\mathtt{s}, \mathtt{s}\ x, y, z, \mathtt{f} : \mathtt{s}, \mathtt{s} \to \mathtt{s}, \mathtt{p} : \mathtt{s}, \mathtt{s}, \mathtt{q} : \mathtt{s}, \mathtt{s}.$

Über dieser Signatur kann man folgende Formel aufbauen:

$$\forall x \colon \forall y \colon (\mathtt{p}(x, y) \longleftrightarrow \exists z \colon \mathtt{q}(\mathtt{f}(x, z), y))$$

Ist diese Formel wahr? Was bedeutet sie?

1. Sie ist z.B. wahr in der $\mathbb{N}_0$-Arithmetik, wenn $\mathtt{s}$ die Menge $\mathbb{N}_0$ ist, und wenn $\mathtt{p}, \mathtt{q}, \mathtt{f}$ die Bedeutung von $\leq, =$ und $+$ haben!

Ein **Beispiel** zu Beginn IV

Gegeben sei eine Signatur mit:

$\mathtt{s}, \mathtt{s}\ x, y, z, \mathtt{f} : \mathtt{s}, \mathtt{s} \to \mathtt{s}, \mathtt{p} : \mathtt{s}, \mathtt{s}, \mathtt{q} : \mathtt{s}, \mathtt{s}.$

Über dieser Signatur kann man folgende Formel aufbauen:

$$\forall x : \forall y : (\mathtt{p}(x, y) \longleftrightarrow \exists z : \mathtt{q}(\mathtt{f}(x, z), y))$$

Ist diese Formel wahr? Was bedeutet sie?

1. Sie ist z.B. wahr in der $\mathbb{N}_0$-Arithmetik, wenn $\mathtt{s}$ die Menge $\mathbb{N}_0$ ist, und wenn $\mathtt{p}, \mathtt{q}, \mathtt{f}$ die Bedeutung von $\leq, =$ und $+$ haben!
2. Sie ist z.B. wahr in der Mengentheorie, wenn $\mathtt{s}$ die Menge $\wp(\mathcal{U})$ ist, und wenn $\mathtt{p}, \mathtt{q}, \mathtt{f}$ die Bedeutung von $\subseteq, =$ und $\cup$ haben!

Ein **Beispiel** zu Beginn IV

Gegeben sei eine Signatur mit:
$\mathtt{s}, \mathtt{s}\ x, y, z, \mathtt{f} : \mathtt{s}, \mathtt{s} \rightarrow \mathtt{s}, \mathtt{p} : \mathtt{s}, \mathtt{s}, \mathtt{q} : \mathtt{s}, \mathtt{s}.$
Über dieser Signatur kann man folgende Formel aufbauen:

$$\forall x \colon \forall y \colon (\mathtt{p}(x, y) \longleftrightarrow \exists z \colon \mathtt{q}(\mathtt{f}(x, z), y))$$

Ist diese Formel wahr? Was bedeutet sie?

1. Sie ist z.B. wahr in der $\mathbb{N}_0$-Arithmetik, wenn $\mathtt{s}$ die Menge $\mathbb{N}_0$ ist, und wenn $\mathtt{p}, \mathtt{q}, \mathtt{f}$ die Bedeutung von $\leq, =$ und $+$ haben!
2. Sie ist z.B. wahr in der Mengentheorie, wenn $\mathtt{s}$ die Menge $\wp(\mathcal{U})$ ist, und wenn $\mathtt{p}, \mathtt{q}, \mathtt{f}$ die Bedeutung von $\subseteq, =$ und $\cup$ haben!
3. Sie falsch, wenn wir die Formel interpretieren als:

$$\forall x \colon \forall y \colon (\mathtt{pfx}(x, y) \longleftrightarrow \exists z \colon |x \circ z| < |y|)$$

Für $x = y$ existiert kein z so daß $|xz| = |y| = |x|$.

Ein **Beispiel** zu Beginn V

Wir werden sehen:

$$\begin{array}{ll} & \forall x\colon \forall y\colon (\mathtt{p}(x,y) \longleftrightarrow \exists z\colon \mathtt{q}(\mathtt{f}(x,z),y)) \\ \models\!\!\!\approx & \forall x\colon \qquad (\mathtt{p}(x,x) \longleftrightarrow \exists z\colon \mathtt{q}(\mathtt{f}(x,z),x)) \end{array}$$

Und zwar **unabhängig** von $\jmath$ bzw. der Σ-Algebra $\mathfrak{A}$!

Ein **Beispiel** zu Beginn V

Wir werden sehen:

$$\begin{array}{rll} & \forall x\colon \forall y\colon & (\mathtt{p}(x,y) \longleftrightarrow \exists z\colon \mathtt{q}(\mathtt{f}(x,z),y)) \\ \models\!\!\approx & \forall x\colon & (\mathtt{p}(x,x) \longleftrightarrow \exists z\colon \mathtt{q}(\mathtt{f}(x,z),x)) \end{array}$$

Und zwar **unabhängig** von $\mathfrak{j}$ bzw. der Σ-Algebra $\mathfrak{A}$!
Und in der Tat:

1. $x \leq x$ ist immer wahr, und auch $x + 0 = x$, also ist auch deren Biimplikation wahr!
2. $M_1 \subseteq M_1$ ist immer wahr, und auch $M_1 \cup \emptyset = M_1$, also ist auch deren Biimplikation wahr!
3. Da die formalen Sprachen *kein* Modell für diese Formel waren, gilt das Entailment trivialerweise.

Semantik FOL: Σ-Algebren

Def. 44: Σ-Algebra

Sei Σ eine Signatur. $\mathfrak{A} = \langle \mathfrak{U}, \mathfrak{F} \rangle$ ist eine Σ-Algebra, gdw.

1. $\mathfrak{U}$ ist eine Familie von Domänen $\mathcal{U}_i = (\mathtt{s}_i)_\mathrm{j}$ für alle $\mathtt{s}_i \in \mathrm{Srt}_\Sigma$.
2. Für alle $\mathtt{f} : \mathtt{s}_1, \ldots, \mathtt{s}_{n-1} \twoheadrightarrow \mathtt{s}_n \in \mathrm{Fnc}_\Sigma$ existiert $f = \mathtt{f}_\mathrm{j}$ mit $f : \mathcal{U}_1 \times \cdots \times \mathcal{U}_{n-1} \to \mathcal{U}_n$ in $\mathfrak{F}$.
3. Für alle $\mathtt{p} : \mathtt{s}_1, \ldots, \mathtt{s}_n \in \mathrm{Prd}_\Sigma$ existiert $P = \mathtt{p}_\mathrm{j}$ mit $P \subseteq \mathcal{U}_1 \times \cdots \times \mathcal{U}_n$.

Vereinfachung der Mehrsortigkeit

Wir vereinfachen zu $\mathrm{Srt}_\Sigma = \{\mathtt{s}\}$, d.h. $\mathfrak{U} = (\mathcal{U}_i)_1 \simeq \mathcal{U}$. Also wird $\mathtt{s}$ vernachlässigt, und man spricht von der *Domäne* $\mathcal{U}$ (oder *Grundmenge/-bereich*) von $\mathfrak{A}$. Damit kann man den Index Σ von Var weglassen.

Natürlich gibt es auch echte mehrsortige Prädikatenlogik.

Variablen

Variablen

Variablen stehen für Wertemengen. Ihr *konkreter* Wert aus $\mathcal{U}$ wird explizit (dynamisch) *festgelegt*.

Def. 45: (Variablen-) Belegung in FOL α

Eine (Variablen-) Belegung ist eine Funktion

$$\alpha : \mathrm{Var} \to \mathcal{U}$$

Für $\alpha\langle\cdots\rangle$ gilt dieselbe Definition wie in PRL.

Termauswertung

Def. 46: Auswertung von Σ-Termen $\mathcal{E}^{\alpha}_{\mathfrak{A}}$

Die Termauswertung ist eine Funktion $\mathcal{E}_{\mathfrak{A}} : \mathcal{U}^{\mathrm{Var}} \times \mathrm{Ter} \to \mathcal{U}$ mit:

$$\begin{array}{rcll} \mathcal{E}^{\alpha}_{\mathfrak{A}}.\mathsf{c} & = & \mathsf{c}_{\mathsf{j}} \in \mathcal{U} & \text{für } \mathsf{c} \in \mathrm{Con} \subseteq \mathrm{Ter} \\ \mathcal{E}^{\alpha}_{\mathfrak{A}}.x & = & \alpha(x), & \text{für } x \in \mathrm{Var} \subseteq \mathrm{Ter} \\ \mathcal{E}^{\alpha}_{\mathfrak{A}}.\mathtt{f}(t_1, \ldots, t_n) & = & f(\mathcal{E}^{\alpha}.t_1, \ldots, \mathcal{E}^{\alpha}.t_n) & \text{sonst.} \end{array}$$

Bemerkung: $\mathcal{E}^{\alpha}.\mathtt{f}(t_1, \ldots, t_n) = \mathtt{f}_{\mathrm{j}}((t_1)_{\mathrm{j}}, \ldots (t_n)_{\mathrm{j}}) = f(\mathcal{E}^{\alpha}.t_1, \ldots, \mathcal{E}^{\alpha}.t_n)$

Thm. 27: Substitutionslemma für Terme Ter_{Σ} in FOL

Wenn $\mathcal{E}^{\alpha}.t = a$ dann $\mathcal{E}^{\alpha}.t'\,[x/t] = \mathcal{E}^{\alpha\langle x \leftarrow a\rangle}.t'$

Thm. 28: Koinzidenzlemma für Ter_{Σ} in FOL

Wenn $\alpha(x) = \beta(x)$ für alle $x \in \mathrm{var}(t)$, dann $\mathcal{E}^{\alpha}.t = \mathcal{E}^{\beta}.t$.

Vorbemerkung zur Def. der Semantik von FOL

Benennungen

1. Symbole aus Σ werden durch $\mathfrak{j}$ in $\mathfrak{A}$ *interpretiert.*
2. Terme werden durch $\mathcal{E}$ auf $\mathcal{U}$ *ausgewertet.*
3. Variablen sind durch α *belegt*.

Wir sprechen also wieder von einer Interpretation, $\mathcal{J}$, denn:

- $\mathcal{J}$ beinhaltet $\mathcal{E}$
- $\mathcal{E}$ beinhaltet α
- α bestimmt die Domäne $\mathcal{U}$ von $\mathfrak{A}$.

Zusammenspiel PRL und FOL

Prädikatenlogische Formeln werden durch $\mathcal{J}$ bis hinunter auf $\mathbf{0}, \mathbf{1} \in \Omega \subseteq \mathcal{U}$ interpretiert.
Die logischen Junktoren werden dann durch die aus PRL bekannte Semantik interpretiert.

Def. 47: Semantik von FOL- Formeln $\mathcal{J}^{\alpha}_{\mathfrak{A}}.p, \mathcal{J} \models p$

Σ Signatur, $\mathfrak{A}$ eine Σ-Algebra. Dann $\mathcal{J}^{\alpha}_{\mathfrak{A}} : \mathrm{Fml}_{\mathsf{FOL}} \to \Omega$ mit:

1. Prädikate, atomare Formeln:

$$\begin{aligned}\mathcal{J}^{\alpha}_{\mathfrak{A}} \models \mathtt{p}(t_1, \ldots, t_n) \quad &:\Longleftrightarrow \quad \mathcal{J}^{\alpha}_{\mathfrak{A}}.\mathtt{p}(t_1, \ldots, t_n) = \mathbf{1} \\ &:\Longleftrightarrow \quad \langle \mathcal{E}^{\alpha}_{\mathfrak{A}}.(t_1), \ldots, \mathcal{E}^{\alpha}_{\mathfrak{A}}.(t_n) \rangle \in P = \mathtt{p}_{\mathsf{j}}\end{aligned}$$

2. (komplexe) Formeln:

$$\begin{aligned}\mathcal{J}^{\alpha}_{\mathfrak{A}} \models \circledast(p \circledast q) \quad &:\Longleftrightarrow \quad \mathcal{J}^{\alpha}_{\mathfrak{A}}.\circledast(p \circledast q) = \mathbf{1} \\ &:\Longleftrightarrow \quad \mathcal{I}^{\alpha}_{\circledast(\mathcal{J}^{\alpha}_{\mathfrak{A}}.p \circledast \mathcal{J}^{\alpha}_{\mathfrak{A}}.q)}. = \mathbf{1} \\ &:\Longleftrightarrow \quad \circledast_{\mathsf{i}}(\mathcal{J}^{\alpha}_{\mathfrak{A}}.p \circledast_{\mathsf{i}} \mathcal{J}^{\alpha}_{\mathfrak{A}}.q) = \mathbf{1}\end{aligned}$$

Schreibweisen: $\mathcal{J}^{\alpha}_{\mathfrak{A}} = \mathcal{J}^{\alpha}_{\mathsf{j}} = \langle \mathsf{j}, \alpha \rangle$. Wenn $\mathsf{j}, \mathfrak{A}$ aus dem Kontext ersichtlich, dann abkürzend $\mathcal{J}^{\alpha}$.

Semantik der Prädikatenlogik

Def. (ctd): Semantik von FOL- Formeln $\mathcal{J}^{\alpha}_{\mathfrak{A}}.p, \mathcal{J} \models p$

3. Universell quantifizierte Formeln:

$$\begin{aligned}
\mathcal{J}^{\alpha}_{\mathfrak{A}} \models \forall x : p \quad &:\Longleftrightarrow \quad \mathcal{J}^{\alpha}_{\mathfrak{A}}.\forall x : p = \mathbf{1} \\
&:\Longleftrightarrow \quad \mathcal{J}^{\alpha\langle x \leftarrow\!\dashv a\rangle}_{\mathfrak{A}}.p = \mathbf{1} \text{ für } \underline{\textit{alle}}\ a \in \mathcal{U}
\end{aligned}$$

4. Existentiell quantifizierte Formeln:

$$\begin{aligned}
\mathcal{J}^{\alpha}_{\mathfrak{A}} \models \exists x : p \quad &:\Longleftrightarrow \quad \mathcal{J}^{\alpha}_{\mathfrak{A}}.\exists x : p = \mathbf{1} \\
&:\Longleftrightarrow \quad \mathcal{J}^{\alpha\langle x \leftarrow\!\dashv a\rangle}_{\mathfrak{A}}.p = \mathbf{1} \text{ für } \underline{\textit{ein}}\ a \in \mathcal{U}
\end{aligned}$$

Semantik

Der Wahrheitswert einer Formel ergibt sich daraus, ob die Aussage, als die sie interpretiert wird, in der jeweiligen "Theorie" zutrifft oder nicht (siehe ’ auf Folie 160).

Koinzidenzlemma

Thm. 29: Koinzidenzlemma FOL

Wenn für alle $x \in \mathrm{fvr}(p)$ gilt $\alpha(x) = \beta(x),$ dann $\mathcal{I}^{\alpha} \models p \Longleftrightarrow \mathcal{I}^{\beta} \models p$

Bew. Strukturelle Induktion

B Sei p atomar. $\mathcal{I}^{\alpha}.p$ ergibt sich aus Interpretation des Prädikatssymbols und $\mathcal{E}^{\alpha}$ auf den Argumenten: Koinzidenzlemma für Terme.

A Gelte die Aussage für $p \in \mathrm{Fml}_{\Sigma}$.

C Induktion für logische Junktoren trivial. Wir betrachten $\forall$ ($\exists$ analog):

$$
\begin{aligned}
\mathcal{I}^{\alpha} \models \forall x \colon p \quad & \stackrel{\forall}{\Longleftrightarrow} \quad \mathcal{I}^{\alpha\langle x \leftarrow a\rangle} \models p, \text{für alle } a \\
& \qquad\quad |\colon \text{ Ind. Annahme mit } \beta(x) = \alpha(x) \text{ für } x \in \mathrm{fvr}(p) \\
& \Longleftrightarrow \quad \mathcal{I}^{\beta\langle x \leftarrow a\rangle} \models p, \text{für alle } a \\
& \stackrel{\forall}{\Longleftrightarrow} \quad \mathcal{I}^{\beta} \models \forall x \colon p
\end{aligned}
$$

Gleichheit

Alle Gleichheiten sind gleich, nur manche sind gleicher

- Man kann *ohne* Gleichheit auskommen.
  Das bedeutet aber, dass man zB für strings $u = v$ und die Länge von Strings $\ell(u) = \ell(v)$ jeweils Gleichheiten *definieren muß*.
- Oder, weil ja in Strukturen $\mathfrak{A}$ klar ist, was $x = y$ bedeutet, nimmt man ein Standardprädikat an ($\equiv$, meist nur $=$), und man sagt:
  $$\mathcal{I}^{\alpha}_{\mathfrak{A}}.(t \equiv t') = (\mathcal{E}^{\alpha}_{\mathfrak{A}}.t = \mathcal{E}^{\alpha}_{\mathfrak{A}}.t')'$$

$\equiv$ und $=$ werden genutzt, weil Terme “bedeutungsäquivalent” sind, gdw. sie zum selben Ergebnis ausgewertet werden.
Dies reißt den Unterschied zwischen “Prädikatenlogik” und “Prädikatenlogik mit Gleichheit” nur an; da aber beide gleich ausdrucksstark sind, soll uns das nicht weiter stören.

Def. 48: Wahrheit, Erfüllbarkeit, Gültigkeit und Modelle

Alle wichtigen Begriffe (auch in ihrer abstrakten Form) sind wie in PRL definiert bzw. erben ihre Definition von dort:

1. p ist *wahr* oder *gilt unter* $\mathcal{J}_{\mathfrak{A}}^{\alpha}$ gdw. $\mathcal{J}_{\mathfrak{A}}^{\alpha}.p = \mathbf{1}$ gdw. $\mathcal{J}_{\mathfrak{A}}^{\alpha} \models p$.
2. p heißt *erfüllbar*, wenn es $\mathcal{J}_{\mathfrak{A}}^{\alpha}$ gibt, so daß $\mathcal{J}_{\mathfrak{A}}^{\alpha} \models p$.
3. p *hat ein Modell* $\mathcal{J}$ bzw. $\mathcal{J}$ *ist ein Modell* von p gdw. $\mathcal{J}_{\mathfrak{A}}^{\alpha} \models p$ unter jeder α. Man darf dann auch $\mathcal{J} \models p$ schreiben und sagt, p *gilt in* $\mathcal{J}$ (bzw. in $\mathfrak{A}$).
4. p heißt *(allgemein-) gültig*, $\models p$, gdw. jede Σ-Algebra ein Modell von p ist; also $\mathcal{J} \models p$ für alle Interpretationen.

Beispiele — FOL ohne Quantoren I/II *

$\mathfrak{A} = \mathbb{N}_0,\ \mathsf{3}_\mathsf{j} = 3,\ \mathsf{p}_\mathsf{j} = \leq,\ \mathtt{f}_\mathsf{j} = {}^{\blacktriangleright},\ \alpha(x) = 3.$

Betrachte $p = (\mathsf{p}(\mathsf{3}, x) \wedge \mathsf{p}(\mathsf{3}, \mathtt{f}(x)))$

$$
\begin{aligned}
\mathcal{J}^{\alpha}_{\mathfrak{A}}.p \quad &= \quad \mathcal{J}^{\alpha}_{\mathbb{N}_0}.(\mathsf{p}(\mathsf{3}, x) \wedge \mathsf{p}(\mathsf{3}, \mathtt{f}(x))) \\
&\overset{\wedge_\mathsf{j} = \wedge_\mathsf{i}}{=} \quad \mathcal{I}^{\alpha}_{\mathcal{B}}.\big(\mathcal{J}^{\alpha}_{\mathbb{N}_0}.\mathsf{p}(\mathsf{3}, x) \wedge \mathcal{J}^{\alpha}_{\mathbb{N}_0}.\mathsf{p}(\mathsf{3}, \mathtt{f}(x))\big) \\
&\overset{\wedge_\mathsf{i}}{=} \quad \mathcal{J}^{\alpha}_{\mathbb{N}_0}.\mathsf{p}(\mathsf{3}, x) \sqcap \mathcal{J}^{\alpha}_{\mathbb{N}_0}.\mathsf{p}(\mathsf{3}, \mathtt{f}(x)) \\
&\overset{\mathsf{j}, \mathcal{E}.., \alpha}{=} \quad (\langle \mathsf{3}_\mathsf{j}, \alpha(x) \rangle \in \mathsf{p}_\mathsf{j})' \sqcap \big(\big\langle \mathsf{3}_\mathsf{j}, \mathcal{E}^{\alpha}_{\mathbb{N}_0}.\mathtt{f}(x) \big\rangle \in \mathsf{p}_\mathsf{j}\big)' \\
&= \quad (3 \leq 3)' \sqcap (3 \leq 3^{\blacktriangleright})' = \mathbf{1} \sqcap (3 \leq 4)' = \mathbf{1} \sqcap \mathbf{1} = \mathbf{1}
\end{aligned}
$$

$'$ bezeichnet die Interpretation der resultierenden Aussage in $\mathbb{N}_0$.

Linguistentrick und vereinfachte Darstellung

$(3 \leq 3 \wedge 3 \leq (3 + 1))$ ist wahr, weil: $(\mathsf{p}(\mathsf{3}, x) \wedge \mathsf{p}(\mathsf{3}, \mathtt{f}(x)))' = \mathbf{1}$

Beispiele — FOL ohne Quantoren II/II

Normalerweise macht man sich nicht soviel Schreibarbeit:

$\mathfrak{A} = \mathbb{N}_0$, $\mathtt{3}_{\mathsf{j}} = 3$, $\mathtt{p}_{\mathsf{j}} = \leq$, $\mathtt{f}_{\mathsf{j}} = \blacktriangleright$, $\beta = \alpha \langle x \leftarrow\!\!\mid 2 \rangle$

Betrachte $p = (\mathtt{p}(\mathtt{3}, x) \wedge \mathtt{p}(\mathtt{3}, \mathtt{f}(x)))$

$$\begin{aligned} \mathcal{J}^{\beta}_{\mathbb{N}_0}.p &= (p(3, x) \wedge p(3, f(x)))' \\ &= (3 \leq 2 \wedge 3 \leq (2 + 1) = 3)' \\ &= \mathbf{0} \end{aligned}$$

Im Gegensatz dazu ist

$$q = (\mathtt{p}(x, y) \longrightarrow \mathtt{p}(x, \mathtt{f}(y)))$$

in $\mathbb{N}_0$ eine gültige Formel, weil

$$(x \leq y \longrightarrow x \leq y + 1) .$$

Freie Variablen und unbeschränkte α^*

Achtung

1. $\mathcal{J}_{\mathfrak{A}}^{\alpha} \models (p \vee q)$ gdw $(\mathcal{J}_{\mathfrak{A}}^{\alpha} \models p \vee \mathcal{J}_{\mathfrak{A}}^{\alpha} \models q)$ gdw $\mathcal{J}_{\mathfrak{A}}^{\alpha}.p \sqcup \mathcal{J}_{\mathfrak{A}}^{\alpha}.q = \mathbf{1}$.
2. **Aber:** $\mathcal{J} \models (p \vee q)$ ~~gdw~~. $\mathcal{J} \models p$ oder $\mathcal{J} \models q$!
   - Wähle $\mathfrak{A} = \mathbb{N}_0$, $p = 2|x, q = \neg p$.
   - $\mathcal{J} \models (2|x \vee 2 \not| x)$, denn für alle α: $\mathcal{J}_{\mathbb{N}_0}^{\alpha} \models 2|x$ oder $\mathcal{J}_{\mathbb{N}_0}^{\alpha} \models 2 \not| x$.
   - Es gilt aber weder $\mathcal{J} \models p$ noch $\mathcal{J} \models q$:
     - $\mathcal{J} \not\models 2|x$, z.B. für $\alpha(x) = 3$
     - $\mathcal{J} \not\models \neg 2|x$, z.B. für $\alpha(x) = 4$
3. $\mathcal{J}_{\mathfrak{A}}^{\alpha} \models \neg p$ gdw. $\mathcal{J}_{\mathfrak{A}}^{\alpha} \not\models p$.
4. **Aber:** $\mathcal{J} \models \neg p$ ~~gdw.~~ $\mathcal{J} \not\models p$.
   - Nicht alle Zahlen sind gerade, also: $\mathcal{J} \not\models 2|x$,
   - aber nicht alle Zahlen sind ungerade: $\mathcal{J} \models \neg 2|x$ ist falsch.

Beispiele — FOL mit Quantoren I/III

$p = \exists x\colon (\mathsf{p}(x,y) \land \mathsf{q}(z,x))$ ist erfüllbar

Für $\mathfrak{A} = \mathbb{N}_0$, $\mathsf{p_j} = <$, $\mathsf{q_j} = |$ ist p erfüllbar. Sei $\alpha(y) = 3, \alpha(z) = 2$.

$$
\begin{aligned}
\mathcal{J}^{\alpha}_{\mathbb{N}_0}.p \quad &\overset{\exists}{=\!=} \quad \mathcal{J}^{\alpha\langle x \leftarrow\!\dashv a\rangle}_{\mathbb{N}_0}.(\mathsf{p}(x,y) \land \mathsf{q}(z,x)) \text{ für ein } a \\
&\overset{\land}{=\!=} \quad \mathcal{I}_{\mathcal{B}}.\Big(\mathcal{J}^{\alpha\langle x \leftarrow\!\dashv a\rangle}_{\mathbb{N}_0}.\mathsf{p}(x,y) \land \mathcal{J}^{\alpha\langle x \leftarrow\!\dashv a\rangle}_{\mathbb{N}_0}.\mathsf{q}(z,x)\Big) \text{ für ein } a \\
&\overset{\sqcap}{=\!=} \quad \mathcal{J}^{\alpha\langle x \leftarrow\!\dashv a\rangle}_{\mathbb{N}_0}.\mathsf{p}(x,y) \sqcap \mathcal{J}^{\alpha\langle x \leftarrow\!\dashv a\rangle}_{\mathbb{N}_0}.\mathsf{q}(z,x) \text{ für ein } a \\
&\overset{\mathrm{j}}{=\!=} \quad (\mathcal{E}^{\alpha\langle x \leftarrow\!\dashv a\rangle}.x < \mathcal{E}^{\alpha\langle x \leftarrow\!\dashv a\rangle}.y)' \\
&\qquad\qquad \sqcap(\mathcal{E}^{\alpha\langle x \leftarrow\!\dashv a\rangle}.z | \mathcal{E}^{\alpha\langle x \leftarrow\!\dashv a\rangle}.x)' \text{ für ein } a \\
&\overset{\mathcal{E}}{=\!=} \quad (\alpha\langle x \leftarrow\!\dashv a\rangle(x) < \alpha\langle x \leftarrow\!\dashv a\rangle(y))' \\
&\qquad\qquad \sqcap(\alpha\langle x \leftarrow\!\dashv a\rangle(z) | \alpha\langle x \leftarrow\!\dashv a\rangle(x))' \text{ für ein } a \\
&\overset{\alpha\langle x \leftarrow\!\dashv a\rangle}{=\!=} \quad (a < 3)' \sqcap (2|a)' \text{ für ein } a.\text{ Wir wählen z.B. } a = 2: \\
&\overset{a=2}{=\!=} \quad (2 < 3)' \sqcap (2|2)' \overset{\mathbb{N}_0}{=\!=} \mathbf{1} \sqcap \mathbf{1} \overset{\mathcal{B}}{=\!=} \mathbf{1}
\end{aligned}
$$

Beispiele — FOL mit Quantoren II/III

$p = \forall y\colon \exists x\colon (\mathsf{p}(x, y) \wedge \mathsf{q}(2, x))$ hat ein Modell

$$\forall y\colon \exists x\colon (x < y \wedge 2|x)$$

$\mathbb{N}_0$ Offensichtlich gibt es keine Zahl $a < 0$, also kann es auch keine Belegung α geben, so dass bei $\alpha(y) = 0$ gilt $\mathcal{J}^{\alpha}_{\mathbb{N}_0}.x < y = \mathbf{1}$.

$\mathbb{Z}$ Hier gilt die Formel, denn zu jeder ganzen Zahl y gibt es kleinere Zahlen $y - 1$ und $y - 2$ und eine davon ist auf jeden Fall durch 2 teilbar.

Beispiele — FOL mit Quantoren III/III

$$\forall x\colon ((\mathtt{p}(x) \wedge \mathtt{q}(\mathtt{a}, \mathtt{f}(x))) \longrightarrow ((\mathtt{r}(\mathtt{f}(\mathtt{a})) \longleftrightarrow \mathtt{q}(x, x)) \longrightarrow (\mathtt{p}(x) \wedge \mathtt{q}(\mathtt{a}, \mathtt{f}(x)))))$$

Man schaut genau hin und erkennt:

- $\mathrm{var}(p) = \mathrm{bvr}(p) = \{x\}$, d.h. p ist geschlossen.
- Man vereinfacht mit:
  1. $q(x) :\Longleftrightarrow (\mathtt{p}(x) \wedge \mathtt{q}(\mathtt{a}, \mathtt{f}(x)))$
  2. $r(x) :\Longleftrightarrow (\mathtt{r}(\mathtt{f}(\mathtt{a})) \longleftrightarrow \mathtt{q}(x, x))$

  und erhält: $p \Longleftrightarrow \forall x\colon (q(x) \longrightarrow (r(x) \longrightarrow q(x)))$

Diese Formel ist geschlossen und eine Instanz von $\mathrm{H1}$. Also:

$$\models \forall x\colon ((\mathtt{p}(x) \wedge \mathtt{q}(\mathtt{a}, \mathtt{f}(x))) \longrightarrow ((\mathtt{r}(\mathtt{f}(\mathtt{a})) \longleftrightarrow \mathtt{q}(x, x)) \longrightarrow (\mathtt{p}(x) \wedge \mathtt{q}(\mathtt{a}, \mathtt{f}(x)))))$$

Somit ist diese Formel *gültig*, gilt also für alle $\mathcal{J}$ auf allen Σ-Strukturen!

Implikation/Konsequenz

Def. 49: Implikation, Äquivalenz, Entailment*

Seien $p, q \in \mathrm{Fml}_{\mathsf{FOL}}$ mit $\mathrm{fvr}(p) = \mathrm{fvr}(q) = \emptyset$ und $P \subseteq \mathrm{Fml}_{\mathsf{FOL}}$ eine Menge geschlossener Formeln.

$$
\begin{array}{rll}
p \Longrightarrow q & \text{gdw.} & \text{für alle } \alpha: \text{ Wenn } \mathcal{J}_{\mathfrak{A}}^{\alpha} \models p \text{ dann auch } \mathcal{J}_{\mathfrak{A}}^{\alpha} \models q \\
p \Longleftrightarrow q & \text{gdw.} & p \Longrightarrow q \text{ und } q \Longrightarrow p \\
\mathcal{J}_{\mathfrak{A}}^{\alpha} \models P & \text{gdw.} & \mathcal{J}_{\mathfrak{A}}^{\alpha} \models p \text{ für alle } p \in P \subseteq \mathrm{Fml} \\
P \mid\!\approx p & \text{gdw.} & \text{Wenn } \mathcal{J}_{\mathfrak{A}}^{\alpha} \models P \text{ dann auch } \mathcal{J}_{\mathfrak{A}}^{\alpha} \models p
\end{array}
$$

Thm. 30: Tautologien

$$
\begin{array}{rll}
p \Longleftrightarrow q & \text{gdw} & \models (p \longleftrightarrow q) \\
P \mid\!\approx p & \text{gdw} & \models \left(\left(\bigwedge P\right) \longrightarrow p\right)
\end{array}
$$

mit p, q, P geschlossen. Inbesondere gilt wieder $\emptyset \mid\!\approx p$ gdw $\models p$.

p_1	Sokrates ist ein Mensch	$\mathtt{human}(\mathtt{sokrates})$
p_2	Jeder Mensch ist sterblich	$\forall x \colon (\mathtt{human}(x) \longrightarrow \mathtt{mortal}(x))$
q	Sokrates ist sterblich	$\mathtt{mortal}(\mathtt{sokrates})$

Gelte $\mathcal{J}^\alpha \models \{p_1, p_2\}$.

$\overset{p_1}{\Longrightarrow}\ \mathcal{J}^\alpha \models \mathtt{human}(\mathtt{sokrates}) \iff \mathtt{sokrates}_{\mathfrak{j}} \in \mathtt{human}_{\mathfrak{j}}$

$\overset{p_2}{\Longrightarrow}\ \mathcal{J}^\alpha \models \forall x \colon (\mathtt{human}(x) \longrightarrow \mathtt{mortal}(x))$

$\overset{\forall}{\iff}$ Für alle a, $\mathcal{J}^{\alpha\langle x \leftarrow a\rangle} \models (\mathtt{human}(x) \longrightarrow \mathtt{mortal}(x))$

$\overset{\longrightarrow}{\iff}$ Für alle a, wenn $\mathcal{J}^{\alpha\langle x \leftarrow a\rangle} \models \mathtt{human}(x)$ dann $\mathcal{J}^{\alpha\langle x \leftarrow a\rangle} \models \mathtt{mortal}(x)$

$\iff$ Für alle a, wenn $a \in \mathtt{human}_{\mathfrak{j}}$ dann $a \in \mathtt{mortal}_{\mathfrak{j}}$

|: Alle Menschen a sind sterblich

|: Wähle $a = \mathtt{sokrates}_{\mathfrak{j}} =$ Sokrates:

$\Longrightarrow$ Wenn $\mathtt{sokrates}_{\mathfrak{j}} \in \mathtt{human}_{\mathfrak{j}}$ dann $\mathtt{sokrates}_{\mathfrak{j}} \in \mathtt{mortal}_{\mathfrak{j}}$

|: Wenn Sokrates ein Mensch ist, dann ist Sokrates sterblich

$\overset{p_1}{\Longrightarrow}$ Wenn T dann $\mathtt{sokrates}_{\mathfrak{j}} \in \mathtt{mortal}_{\mathfrak{j}}$

$\overset{\mathsf{T}}{\Longrightarrow}$ $\mathtt{sokrates}_{\mathfrak{j}} \in \mathtt{mortal}_{\mathfrak{j}}$ |: Sokrates ist sterblich.

$\Longrightarrow$ $\mathcal{J}^\alpha \models \mathtt{mortal}(\mathtt{sokrates}) = q$

Also $\{p_1, p_2\} \mathrel{|}\!\!\approx q$.

Beispiel: Entailment IIa

p_1	32 ist 2er-Potenz	$\mathtt{pow2}(32)$
p_2	2er-Potenzen sind Vielf.v. 2	$\forall x\colon (\mathtt{pow2}(x) \longrightarrow \mathtt{mltp2}(x))$
q	32 ist Vielf. v. 2	$\mathtt{mltp2}(32)$

Gelte $\mathcal{J}^\alpha \models \{p_1, p_2\}$.

$\xRightarrow{p_1}$ $\mathcal{J}^\alpha \models \mathtt{pow2}(32) \iff 32 = 32_\mathsf{j} \in \mathtt{pow2}_\mathsf{j}$

$\xRightarrow{p_2}$ $\mathcal{J}^\alpha \models \forall x\colon (\mathtt{pow2}(x) \longrightarrow \mathtt{mltp2}(x))$

$\overset{\forall}{\iff}$ Für alle a, $\mathcal{J}^{\alpha\langle x \leftarrow\!\dashv a\rangle} \models (\mathtt{pow2}(x) \longrightarrow \mathtt{mltp2}(x))$

$\overset{\longrightarrow}{\iff}$ Für alle a, wenn $\mathcal{J}^{\alpha\langle x \leftarrow\!\dashv a\rangle} \models \mathtt{pow2}(x)$ dann $\mathcal{J}^{\alpha\langle x \leftarrow\!\dashv a\rangle} \models \mathtt{mltp2}(x)$

$\iff$ Für alle a, wenn $a \in \mathtt{pow2}_\mathsf{j}$ dann $a \in \mathtt{mltp2}_\mathsf{j}$

Wähle $a = 32 = 32_\mathsf{j}$:

$\Longrightarrow$ Wenn $32_\mathsf{j} \in \mathtt{pow2}_\mathsf{j}$ dann $32_\mathsf{j} \in \mathtt{mltp2}_\mathsf{j}$

$\xRightarrow{p_1}$ Wenn T dann $32_\mathsf{j} \in \mathtt{mltp2}_\mathsf{j}$

$\xRightarrow{\mathsf{T}}$ $32_\mathsf{j} \in \mathtt{mltp2}_\mathsf{j}$

$\Longrightarrow$ $\mathcal{J}^\alpha \models \mathtt{mltp2}(32) = q$

Also $\{p_1, p_2\} \models\!\!\approx q$: Angenommen, 32 ist eine 2er-Potenz, dann ist 32 ist ein Vielfaches von 2, weil jede 2er-Potenz ein Vielfaches von 2 ist. *Wenn Sie nicht einverstanden sind, warten Sie die Folie* “Entailment IIb” *ab!*

Beispiel: Entailment III

$$\begin{array}{cl} p_1 & \mathtt{p}(\mathsf{c}) \\ p_2 & \forall x\colon (\mathtt{p}(x) \longrightarrow \mathtt{q}(x)) \\ \hline q & \mathtt{q}(\mathsf{c}) \end{array}$$

Gelte $\mathcal{J}^{\alpha} \models \{p_1, p_2\}$.

$\stackrel{p_1}{\Longrightarrow}$ $\mathcal{J}^{\alpha} \models \mathtt{p}(\mathsf{c}) \iff \mathsf{c_j} \in \mathtt{p_j}$

$\stackrel{p_2}{\Longrightarrow}$ $\mathcal{J}^{\alpha} \models \forall x\colon (\mathtt{p}(x) \longrightarrow \mathtt{q}(x))$

$$\begin{array}{rl}
\stackrel{\forall}{\iff} & \text{Für alle } a, \mathcal{J}^{\alpha\langle x \leftarrow\!\!\dashv a\rangle} \models (\mathtt{p}(x) \longrightarrow \mathtt{q}(x)) \\
\stackrel{\longrightarrow}{\iff} & \text{Für alle } a, \text{wenn } \mathcal{J}^{\alpha\langle x \leftarrow\!\!\dashv a\rangle} \models \mathtt{p}(x) \text{ dann } \mathcal{J}^{\alpha\langle x \leftarrow\!\!\dashv a\rangle} \models \mathtt{q}(x) \\
\iff & \text{Für alle } a, \text{wenn } a \in \mathtt{p_j} \text{ dann } a \in \mathtt{q_j} \\
 & \text{Wähle } a = \mathsf{c_j}\text{:} \\
\Longrightarrow & \text{Wenn } \mathsf{c_j} \in \mathtt{p_j} \text{ dann } \mathsf{c_j} \in \mathtt{q_j} \\
\stackrel{p_1}{\Longrightarrow} & \text{Wenn T dann } \mathsf{c_j} \in \mathtt{q_j} \\
\stackrel{\mathsf{T}}{\Longrightarrow} & \mathsf{c_j} \in \mathtt{q_j} \\
\Longrightarrow & \mathcal{J}^{\alpha} \models \mathtt{q}(\mathsf{c}) = q
\end{array}$$

Also $\{p_1, p_2\} \approx q$.

Beispiel: Entailment IIb

$$\begin{array}{lll} p_1 & 1 = 2^0 \text{ ist eine 2er-Potenz} & \texttt{pow2}(\texttt{1}) \\ p_2 & & \forall x\colon (\texttt{pow2}(x) \longrightarrow \texttt{mltp2}(x)) \\ \hline q & \text{1 ist ein Vielfaches von 2} & \texttt{mltp2}(\texttt{1}) \end{array}$$

Gelte $\mathcal{J}^\alpha \models \{p_1, p_2\}$.

$$\overset{p_1}{\Longrightarrow}\ \mathcal{J}^\alpha \models \texttt{pow2}(\texttt{1}) \Longleftrightarrow 1 = \texttt{1}_\mathfrak{j} \in \texttt{pow2}_\mathfrak{j}$$

$$\overset{p_2}{\Longrightarrow}\ \mathcal{J}^\alpha \models \forall x\colon (\texttt{pow2}(x) \longrightarrow \texttt{mltp2}(x))$$

$$\overset{\forall}{\Longleftrightarrow}\ \text{Für alle } a, \mathcal{J}^{\alpha\langle x \leftarrow\!\dashv a\rangle} \models (\texttt{pow2}(x) \longrightarrow \texttt{mltp2}(x))$$

$$\vdots$$

$$\Longrightarrow\ \mathcal{J}^\alpha \models \texttt{mltp2}(\texttt{1}) = q$$

Haben wir etwas falsch gemacht? — **Nein!** Nur:
Die Formel p_2 gilt nicht in unserer "Theorie" der Arithmetik! In der Tat ist die von P gebildete Theorie eine Welt, in der auch 1 ein Vielfaches von 2 ist. Es ist eben nur eine *andere* Theorie.
Aber die Schlussfolgerung ist auf Basis unserer ("falschen") Axiome voll und ganz korrekt!

Widerspruchslemma

$$
\begin{array}{lll}
P \mid\!\approx p & \text{gdw.} & \text{Für alle } \alpha : \mathcal{J}_{\mathfrak{A}}^{\alpha} \models P \Longrightarrow \mathcal{J}_{\mathfrak{A}}^{\alpha} \models p \\
& \text{gdw.} & \text{Es gibt kein } \mathcal{J}_{\mathfrak{A}}^{\alpha} \text{ mit } (\mathcal{J}_{\mathfrak{A}}^{\alpha} \models P \wedge \mathcal{J}_{\mathfrak{A}}^{\alpha} \not\models p) \\
& \text{gdw.} & \text{Es gibt kein } \mathcal{J}_{\mathfrak{A}}^{\alpha} \text{ mit } (\mathcal{J}_{\mathfrak{A}}^{\alpha} \models P \wedge \mathcal{J}_{\mathfrak{A}}^{\alpha} \models \neg p) \\
& \text{gdw.} & \text{Es gibt kein } \mathcal{J}_{\mathfrak{A}}^{\alpha} \text{ mit } \mathcal{J}_{\mathfrak{A}}^{\alpha} \models P \cup \{\neg p\} \\
& \text{gdw.} & P \cup \{\neg p\} \text{ ist unerfüllbar}
\end{array}
$$

Semantik der Prädikatenlogik

Zusammenfassung

1. FOL wird in Σ-Algebren $\mathfrak{A}$ interpretiert.
2. atomare Formeln werden zu $\mathbf{0}$ oder $\mathbf{1}$ aus Ω ausgewertet.
3. komplexe Formeln werden wie in PRL interpretiert, nachdem ihre Konstituenten in FOL interpretiert wurden.
4. quantifizierte Formeln werden abhängig von $\mathcal{U}^{\mathrm{Var}}$ wie komplexe Formeln interpretiert.

Das bedeutet:

- Alle logischen Junktoren erben die Bedeutung aus PRL durch $\mathfrak{i}$
- hinzu kommen durch $\mathcal{E}$ ausgewertete Terme und
- (freie) Variablen in **Abhängigkeit** von α (“Parameter”)
- $\mathfrak{j}$ interpretiert Termkonstruktoren und Prädikatssymbole

7.3
DER MODELLBEGRIFF, BESONDERE MODELLE

Der “Modellbegriff”

Def. 50: Modellklassen, Theorien, Axiomensysteme

- Sei P eine Σ-Formelmenge. Die Menge aller Σ-Algebren $\mathfrak{A}$ mit $\mathcal{J} \models P$ heißt *Modellklasse* $\mathrm{Mod}(P)$ von P.
- Sei P eine Formelmenge, $\mathcal{J}$ gegeben. Dann heißt $\mathrm{Thr}(P) = \{p \parallel P \mid\!\approx p\}$ die *Theorie* von P.
- Sei T eine Theorie. Eine Menge P von Formeln heißt *Axiomensystem für* T, gdw. $T = \mathrm{Thr}(P)$. Eine T heißt *(endlich) axiomatisierbar*, wenn es für T ein (endliches) P gibt.

Beispiel: Die Theorie unseres Axiomensystems P auf Folie 167 besagt, dass Sokrates sterblich ist. Alle Modelle, in denen das Modus Ponens gilt bilden die Modellklasse dieser Theorie.

Minimale Axiomensysteme oder Theorien zu finden ist ein eleganter und beliebter Ausgleichssport.

"Einfache" Modelle*

Dieses Beispiel ist mit "Gewalt" konstruiert — soll Ihnen aber einen *anschaulichen* Fall illustrieren.

Aus einer Übung

Seien $\mathtt{s}, \mathtt{t}$ Sorten$^{*)}$, $\mathtt{s}x$, und $\mathtt{c} :\to \mathtt{s}, \mathtt{f} : \mathtt{s} \to \mathtt{t}$.
Die Menge der erzeugbaren Terme ist $\{\mathsf{c}, \mathtt{f}(\mathsf{c})\} = \mathrm{Gnd}_\Sigma$,

$^{*)}$ Eigentlich hatten wir uns ja auf eine Sorte beschränkt, aber es geht nur um ein Beispiel!

Interpretation

Sei $\mathrm{Gnd}_\Sigma.\mathcal{E}_\mathsf{j} = \{0, 1\} \subset \mathbb{N}_0$ und $\mathtt{p}^2 \in \mathrm{Prd}_\Sigma$ mit $\mathsf{p}_\mathsf{j} =\leq$ p.O.
Für die Formel $\forall x : \mathtt{p}(\mathsf{c}, x)$:

- $\mathcal{J}^{\alpha}_{\mathbb{N}_0} \models \mathtt{p}(\mathsf{c}, x)$, gdw. $0 \leq a$, für <u>alle</u> $a \in \mathbb{N}_0$
- $\mathcal{J}^{\alpha}_{\mathrm{Gnd}_\Sigma} \models \mathtt{p}(\mathsf{c}, x)$, gdw. $0 \leq 0$ und $0 \leq 1$.

Herbrand-Algebren

Problem

- Als Strukturen $\mathfrak{A}$ kommen *beliebige* Σ-Algebren und Interpretationen $\mathcal{I}$ in Betracht.
- $\mathcal{I}_{\mathfrak{A}}^{\alpha}.p$ wird beliebig kompliziert.
- **Ziel:** *Gegeben* Σ, finde:
  1. Kanonische Σ-Modellklasse $\mathbf{H}_{\Sigma} = \{\mathfrak{H}_{\Sigma}, \mathfrak{H}'_{\Sigma}, \mathfrak{H}''_{\Sigma} \ldots\}$ mit
  2. festgelegter (einfacher) $\mathcal{I}_{\mathfrak{H}_{\Sigma}} = \mathcal{H}$ für alle $\mathfrak{H} \in \mathbf{H}_{\Sigma}$,
  3. so daß p erfüllbar, gdw. $\mathcal{H} \models p$ für ein $\mathfrak{H} \in \mathbf{H}_{\Sigma}$

Proposition.

Wenn p ein bel. Σ-Modell $\mathfrak{A}$ hat, dann hat p auch ein $\mathfrak{H} \in \mathbf{H}_{\Sigma}$.

Wenn wahr, dann ist *Unerfüllbarkeit* **kanonisch** durch Nachweis der *Nichtexistenz* eines $\mathbf{H} \in \mathbf{H}_{\Sigma}$-Modells gezeigt ($\approx$ Widerspruchslemma).

Ein "einfaches" Modell"

- Warum nicht die syntaktischen Strukturen als (Term-) Algebra begreifen?
- Wir reden i.A. *immer* über Eigenschaften *konkreter Objekte*.
- Auch mit Variablen/quantifizierten Ausdrücken reden wir immer über Mengen *konkreter Objekte*:
  $\forall x\colon \forall y\colon (\mathtt{p}(x,y) \longrightarrow \mathtt{p}(x,\mathtt{f}(y)))$ heißt ja (je nach $\mathcal{J}$) z.B.

  $(0 \leq 0 \longrightarrow 0 \leq (0+1))\,, ((0+7) \leq (0+3) \longrightarrow (0+7) \leq (0+3)+1)\,,$ usw
- Warum belassen wir es nicht bei $\mathtt{f}(x)$ und definieren $\mathtt{p}_\mathsf{j}$ eben auf den Termen statt auf aufwendigen Interpretationen/Auswertungen, also $(\mathtt{0} \leq \mathtt{0} \longrightarrow \mathtt{0} \leq \mathtt{f}(\mathtt{0}))$.
- Dann ist alles an der Interpretation "klar" — man muß sich nur noch um die Prädikate kümmern.

Herbrand-Algebren

Def. 51: Herbrand Algebren $\mathfrak{H}_\Sigma \in \mathbf{H}_\Sigma$.

Sei Σ mit $\mathrm{Con}_\Sigma \neq \emptyset$ und $\mathfrak{H}$ eine Σ-Algebra.
$\mathfrak{H}$ heißt eine *Herbrand-Algebra*, gdw.

1. $\mathrm{dom}(\mathfrak{H}) = \mathcal{U} = \mathrm{Gnd}_\Sigma$ ("Herbrand-Universum") und
2. für alle $t_1, \ldots, t_n \in \mathrm{Gnd}_\Sigma = \mathcal{U}$ und $\mathtt{f}^n \in \mathrm{Fnc}_\Sigma$:

   $\mathcal{H}.\mathtt{f}(t_1, \ldots, t_n) = \mathtt{f}(t_1, \ldots, t_n)$ wobei $\mathcal{H} = \mathcal{J}_\mathfrak{H}$ "kanonisch"

$\mathfrak{H}$ ist ein *Herbrand-Modell* von $P \in \mathrm{Fml}_\Sigma$, gdw. $\mathcal{H} \models P$.

Idee: $\mathcal{E} = \mathit{1}$, d.h. $f = \mathtt{f}_\mathrm{j} = \mathtt{f}$

- Die Domäne $\mathcal{U}$ von $\mathfrak{H}$ *ist* die Menge der Σ-Grundterme Gnd_Σ
- Ein Term wird mit $\mathcal{J}$ interpretiert, also mit $\mathcal{E}$ ausgewertet:

$$\mathcal{H}^\alpha_\mathfrak{H}.\mathtt{f}(t_1, \ldots, t_n) = \mathcal{E}^\alpha_\mathfrak{H}.\mathtt{f}(t_1, \ldots, t_n) = \mathtt{f}(t_1, \ldots, t_n)$$

Daher oft (zu früh) der Verzicht auf Σ und Schreibweisen $\mathtt{f}$ vs. f.

Herbrand-Algebren

“Syntax = Semantik”

1. Um $\mathtt{f}(t_1, \ldots, t_n)$ zu interpretieren, bestimmt man
2. $\mathcal{H}^{\alpha}.\mathtt{f}(t_1, \ldots, t_n)$. Dazu wertet man aus:
3. $\mathcal{E}^{\alpha}.\mathtt{f}(t_1, \ldots, t_n)$. Man interpretiert $\mathtt{f}$ und die Argumente:
4. $\mathtt{f}_{\mathfrak{h}}(\mathcal{E}^{\alpha}_{\mathfrak{H}}.t_1, \ldots, \mathcal{E}^{\alpha}_{\mathfrak{H}}.t_n)$, was definiert ist als:
5. $\mathtt{f}_{\mathfrak{h}} : \mathrm{Gnd}^n_{\Sigma} \to \mathrm{Gnd}_{\Sigma}$, mit $\mathtt{f}_{\mathfrak{h}}(t_1, \ldots, t_n) = \mathtt{f}(t_1, \ldots, t_n)$
6. Da also auch $t_i \in \mathrm{Gnd}_{\Sigma}$, *sind* diese bereits ausgewertet!
7. d.h. in $\mathfrak{H}$ ist $\mathtt{f}(t_1, \ldots, t_n) \in \mathcal{U}$ wohldefiniert

Substitutionen in Herbrand Modellen*

Kor. $\mathcal{H}^{\alpha\langle x \leftarrow\!\dashv t\rangle}.p = \mathcal{H}^{\alpha}.p\,[x/t]$

Bew.

Wir betrachten $p = \mathtt{p}(x)$.

$$\begin{aligned}
& \mathcal{H}^{\alpha}.p\,[x/t] = \mathbf{1} \\
\iff\ & \mathcal{H}^{\alpha}.\mathtt{p}(x)\,[x/t] = \mathbf{1} \iff \mathcal{H}^{\alpha}.\mathtt{p}(t) = \mathbf{1} \\
\iff\ & \mathcal{E}.t \in \mathtt{p}_{\mathfrak{h}} \iff t \in \mathtt{p}_{\mathfrak{h}} \iff \alpha(x) \in \mathtt{p}_{\mathfrak{h}} \wedge (\alpha(x) = t) \\
\iff\ & \mathcal{H}^{\alpha}_{\mathfrak{H}}.\mathtt{p}(x) \wedge (\alpha(x) = t = \mathcal{E}.t) \iff \mathcal{H}^{\alpha\langle x \leftarrow\!\dashv t\rangle}_{\mathfrak{H}}.\mathtt{p}(x)
\end{aligned}$$

Für komplexe Terme/Formeln Induktion über Aufbau.

8.
NORMALFORMEN IN FOL

8.1 PRENEX UND PRENEX-CNF

Prenex

Def. 52: Prenex-Form

Eine Formel p ist in *Prenex-Form* gdw.

$$p = \mathsf{Q}_1 x_1 : \cdots \mathsf{Q}_n x_n : q$$

und q enthält keine Quantoren. Man nennt q die *Matrix* von p (und $[\mathsf{Q}_i x_i]_n$ das *Präfix*).

Thm. 31: Quantorengesetze

$$\begin{array}{lrcll}
\text{DUA} & \neg\forall x : p & \iff & \exists x : \neg p & \\
\text{EXT} & (\mathsf{Q}x : p \circledast q) & \iff & \mathsf{Q}x : (q \circledast p) & \text{für } x \notin \mathrm{fvr}(q) \\
\text{DST}_\wedge & (\forall x : p \wedge \forall x : q) & \iff & \forall x : (p \wedge q) & \\
\text{DST}_\vee & (\exists x : p \vee \exists x : q) & \iff & \exists x : (p \vee q) & \\
\text{COM}_\mathsf{Q} & \mathsf{Q}x : \mathsf{Q}y : p & \iff & \mathsf{Q}y : \mathsf{Q}x : p &
\end{array}$$

Für $\circledast \in \{\wedge, \vee\}$ und $\mathsf{Q} \in \{\exists, \forall\}$. Beachte Skopus und COM für $\circledast$ in EXT.

Bew. Skopusausweitung (EXT)

Da $x \notin \mathrm{fvr}(q)$, bleibt x in q von $\alpha\langle x \hookleftarrow a\rangle$ für alle a unberührt (Koinzidenzlemma).

Bew. $\wedge$-Distributivität von Quantoren (DST$_\wedge$), $\Longleftarrow$

Einzig zu betrachten wenn $x \in \mathrm{fvr}((p \wedge q))$, sonst triv.

$$
\begin{aligned}
& \mathcal{J}^{\alpha} \models \forall x\colon (p \wedge q) \\
\overset{\mathcal{I}}{\Longleftrightarrow}\quad & \mathcal{J}^{\alpha}.\forall x\colon (p \wedge q) = \mathbf{1} \\
\overset{\forall}{\Longleftrightarrow}\quad & \mathcal{J}^{\alpha\langle x\hookleftarrow a\rangle}.(p \wedge q) = \mathbf{1} \text{ für alle } a \\
\overset{\mathcal{I},\wedge}{\Longleftrightarrow}\quad & (\mathcal{J}^{\alpha\langle x\hookleftarrow a\rangle}.p \text{ für alle } a) \sqcap (\mathcal{J}^{\alpha\langle x\hookleftarrow a\rangle}.q \text{ für alle } a) = \mathbf{1} \\
\overset{\mathcal{B},\sqcap}{\Longleftrightarrow}\quad & (\mathcal{J}^{\alpha\langle x\hookleftarrow a\rangle}.p \text{ für alle } a) = \mathbf{1} \text{ und } (\mathcal{J}^{\alpha\langle x\hookleftarrow a\rangle}.q \text{ für alle } a) = \mathbf{1} \\
\overset{\forall}{\Longleftrightarrow}\quad & \mathcal{J}^{\alpha}.\forall x\colon p \sqcap \mathcal{J}^{\alpha}.\forall x\colon q = \mathbf{1} \\
\overset{\mathcal{I},\wedge}{\Longleftrightarrow}\quad & \mathcal{J}^{\alpha}_{\mathfrak{A}} \models (\forall x\colon p \wedge \forall x\colon q)
\end{aligned}
$$

Quantorengesetze

Kor. $\forall$ ($\exists$) distributiert *nicht* über $\vee$ ($\wedge$)

Bew.

Beachten Sie nun, wie nun langsam die Grenzen zwischen Signatur und Modell verschwimmen:

1. $\forall$ und $\vee$:
   - Es gilt: $\models \forall x\colon (\mathtt{p}(x) \vee \neg\mathtt{p}(x))$
   - Aber: $\not\models (\forall x\colon \mathtt{p}(x) \vee \forall x\colon \neg\mathtt{p}(x))$, z.B. ist $(\forall x\colon 2|x \vee \forall x\colon 2\not|x)$ falsch, weil weder alle Zahlen gerade sind noch sind alle Zahlen ungerade.
2. $\exists$ und $\wedge$:
   - Es gilt: $\models (\exists x\colon \mathrm{prim}(x) \wedge \exists x\colon 42|x)$, denn 7 ist prim und 84 ist ein Vielfaches von 42
   - Aber: $\not\models \exists x\colon (\mathrm{prim}(x) \wedge 42|x)$, denn keine Primzahl ist durch 42 teilbar.

Quantifikation und Subjunktion

Thm. (ctd): Quantorengesetze

$$
\begin{array}{lcll}
(p \longrightarrow \forall x\colon q) & \Longleftrightarrow & \forall x\colon (p \longrightarrow q) & \text{für } x \notin \mathrm{fvr}(p) \\
(\exists x\colon p \longrightarrow q) & \Longleftrightarrow & \forall x\colon (p \longrightarrow q) & \text{für } x \notin \mathrm{fvr}(q) \\
(p \longrightarrow \exists x\colon q) & \Longleftrightarrow & \exists x\colon (p \longrightarrow q) & \text{für } x \notin \mathrm{fvr}(p) \\
(\forall x\colon p \longrightarrow q) & \Longleftrightarrow & \exists x\colon (p \longrightarrow q) & \text{für } x \notin \mathrm{fvr}(q)
\end{array}
$$

Quantoren aus der Konklusion vorziehen: Koinzidenzlemma.
Quantoren aus der Prämisse vorziehen: DUA beachten.

Quantifikation und Subjunktion

Bew. Qx aus der Konklusion "heben"

$$
\begin{aligned}
& \mathcal{J}^{\alpha} \models \forall x\colon (p \longrightarrow q) \\
\overset{\forall}{\iff} \quad & \mathcal{J}^{\alpha\langle x \leftarrow\!\shortmid a\rangle} \models (p \longrightarrow q) \text{ f.a. } a \in \mathcal{U} \\
\overset{\longrightarrow_{\mathrm{i}}}{\iff} \quad & \overline{\mathcal{J}^{\alpha\langle x \leftarrow\!\shortmid a\rangle}.p} \sqcup \mathcal{J}^{\alpha\langle x \leftarrow\!\shortmid a\rangle}.q = \mathbf{1} \text{ f.a. } a \in \mathcal{U} \\
& |\colon\ x \notin \mathrm{fvr}(p) \text{ Koinzidenz Lemma} \\
\iff \quad & \overline{\mathcal{J}^{\alpha}.p} \sqcup \mathcal{J}^{\alpha\langle x \leftarrow\!\shortmid a\rangle}.q = \mathbf{1} \text{ f.a. } a \in \mathcal{U} \\
\overset{\forall}{\iff} \quad & \overline{\mathcal{J}^{\alpha}.p} \sqcup \mathcal{J}^{\alpha}.\forall x\colon q = \mathbf{1} \\
\overset{\longrightarrow}{\iff} \quad & \mathcal{J}^{\alpha} \models (p \longrightarrow \forall x\colon q)
\end{aligned}
$$

$\exists x\colon (p \longrightarrow q) \iff (p \longrightarrow \exists x\colon q)$ analog.

Quantifikation und Subjunktion

Bew. Qx aus der Prämisse "heben"

$$
\begin{array}{cl}
 & \mathcal{J}^{\alpha} \models \forall x\colon (p \longrightarrow q) \\
\overset{\forall,\rightarrow}{\Longleftrightarrow} & \overline{\mathcal{J}^{\alpha\langle x \leftarrow a\rangle}.p} \sqcup \mathcal{J}^{\alpha\langle x \leftarrow a\rangle}.q = \mathbf{1} \text{ f.a. } a \in \mathcal{U} \\
\overset{\overline{\ },\sqcup}{\Longleftrightarrow} & \mathcal{J}^{\alpha\langle x \leftarrow a\rangle}.p = \mathbf{0} \text{ oder } \mathcal{J}^{\alpha\langle x \leftarrow a\rangle}.q = \mathbf{1} \text{ f.a. } a \in \mathcal{U} \\
\overset{x \notin \mathrm{fvr}(q)}{\Longleftrightarrow} & \mathcal{J}^{\alpha\langle x \leftarrow a\rangle}.p = \mathbf{0} \text{ oder } \mathcal{J}^{\alpha}.q = \mathbf{1} \text{ f.a. } a \in \mathcal{U} \\
\overset{\forall}{\Longleftrightarrow} & \mathcal{J}^{\alpha}.\forall x\colon p = \mathbf{0} \text{ oder } \mathcal{J}^{\alpha}.q = \mathbf{1} \\
\overset{\text{Q}-\text{DUA}}{\Longleftrightarrow} & \mathcal{J}^{\alpha}.\neg\exists x\colon \neg p = \mathbf{0} \text{ oder } \mathcal{J}^{\alpha}.q = \mathbf{1} \\
\overset{\neg}{\Longleftrightarrow} & \mathcal{J}^{\alpha}.\exists x\colon \neg p = \mathbf{1} \text{ oder } \mathcal{J}^{\alpha}.q = \mathbf{1} \\
\overset{\exists}{\Longleftrightarrow} & \mathcal{J}^{\alpha\langle x \leftarrow a\rangle}.\neg p = \mathbf{1} \text{ oder } \mathcal{J}^{\alpha}.q = \mathbf{1} \text{ f.e. } a \in \mathcal{U} \\
\overset{\neg}{\Longleftrightarrow} & \mathcal{J}^{\alpha\langle x \leftarrow a\rangle}.p = \mathbf{0} \text{ oder } \mathcal{J}^{\alpha}.q = \mathbf{1} \text{ f.e. } a \in \mathcal{U} \\
\overset{\exists}{\Longleftrightarrow} & \mathcal{J}^{\alpha}.\exists x\colon p = \mathbf{0} \text{ oder } \mathcal{J}^{\alpha}.q = \mathbf{1} \\
\overset{\sqcup}{\Longleftrightarrow} & \overline{\mathcal{J}^{\alpha}.\exists x\colon p} \sqcup \mathcal{J}^{\alpha}.q = \mathbf{1} \\
\overset{\rightarrow}{\Longleftrightarrow} & \mathcal{J}^{\alpha} \models (\exists x\colon p \longrightarrow q)
\end{array}
$$

$\exists x\colon (p \longrightarrow q) \Longleftrightarrow (\forall x\colon p \longrightarrow q)$ analog.

Generalisierungslemma

Universeller Abschluß

Sei $\mathrm{fvr}(p) = \{x_1, \ldots, x_n\}$. Der *universelle Abschluß von* p ist

$$\forall\!\!\!\forall : p := \forall x_1 : \cdots \forall x_n : p$$

Analog wird der *existentielle Abschluß* $\exists\!\!\!\exists : p$ definiert.

Thm. 32: Generalisierungslemma

$$\mathcal{J}^{\alpha} \models P \text{ gdw. } \mathcal{J}^{\alpha} \models \forall\!\!\!\forall : (P)$$

Bew.

Substitutionslemma.

Quantorengesetze

Kor. Gebundene Umbennung

Für $y \notin \mathrm{var}(p)$, $\mathsf{Q}x : p \Longleftrightarrow \mathsf{Q}y : p\,[x/y]$.

Def. 53: Bereinigte Formeln

p heißt bereinigt, gdw. $\mathrm{fvr}(p) \cap \mathrm{bvr}(p) = \emptyset$ und wenn für $\mathsf{Q}_1 x_1$ und $\mathsf{Q}_2 x_2$ in p ist $x_1 \neq x_2$ (keine mehrfach Quantifizierung).
Formeln können durch (gebundene) Umbenennung bereinigt werden.

Thm. 33: Prenex-Äquivalenz

Für jede (bereinigte) Formel $p \in \mathrm{Fml}_{\mathsf{FOL}}$ existiert eine Formel $q \in \mathrm{Fml}_{\mathsf{FOL}}$ in Prenex-Form mit $p \Longleftrightarrow q$.

Bew. Prenex-Äquivalenz

Strukturelle Induktion; Anwendung der Quantorengesetze.

PCNF

Thm. 34: PCNF-Äquivalenz

Für jede Formel $p \in \mathrm{Fml}_{\mathsf{FOL}}$ existiert eine Formel $q \in \mathrm{Fml}_{\mathsf{FOL}}$ in Prenexform, deren Matrix in CNF ist und für die gilt: $p \iff q$.

Bew.

1. p wird in (geschlossene) bereinigte Prenex-Form gebracht
2. Die (quantorenfreie) Matrix kann wie eine Formel in PRL in CNF/KNF umgeformt werden.

Stand der Dinge:

Eine Formel, die aus einer Sequenz von $\forall$- und $\exists$-Quantoren besteht und einer Matrix, die in CNF ist.
Das sieht schon sehr "normal" aus — nur:

Kann man nicht noch die Quantoren "ordentlich" machen?

8.2
SKOLEMISIERUNG

Skolemisierung

Erfüllungsäquivalenz

Offensichtlich ist $\exists x\colon \mathtt{p}(x) \not\Longleftrightarrow \mathtt{p}(\mathtt{c})$ Aber:

- *Wenn* $\exists x\colon \mathtt{p}(x)$ erfüllt wird für $\alpha \langle x \leftarrow c\rangle$ mit $\mathcal{E}.\mathsf{c} = c$,
- *dann* sind beide Formeln erfüllt.

Skolemfunktionen "bestimmen" genau so ein c für $\exists$-gebundene x.

Def. 54: Skolemisierung

$p = (\forall x_1 : \cdots (\forall x_n : \exists y\colon q) \cdots)$ ist geschlossen und bereinigt; in q kommen keine Quantoren über $x_1, \ldots, x_n$ vor (aber ggf. andere).

- Füge zu Fnc_Σ neu hinzu: $\mathtt{sk}_y$ n-stellig.
- $q\,[y/\mathtt{sk}_y(x_1, \ldots, x_n)]$ ist zulässig (keine neue Bindung!)
- Dann: $p_{\mathtt{sk}} = (\forall x_1 : \cdots \forall x_n\colon q\,[y/\mathtt{sk}_y(x_1, \ldots, x_n)] \cdots)$

Skolemtheorem

hm Erfüllungsäquivalenz von Skolemformen

Sei $\mathtt{sk}_y$, $\Sigma_{\mathtt{sk}_y}$ nach Def. gebildet.

1. $\mathcal{J}^\alpha.p_{\mathtt{sk}} \implies \mathcal{J}^\alpha.p$
2. Jedes Σ-Modell $\mathfrak{A}_\Sigma$ von p (also $\mathcal{J}^\alpha_{\mathfrak{A}} \models p$) kann mit $\Sigma_{\mathtt{sk}_y}$ erweitert werden zu $\mathfrak{A}_{\mathtt{sk}}$ mit $\mathcal{J}^\alpha_{\mathfrak{A}_{\mathtt{sk}}} \models p_{\mathtt{sk}_y}$.

Allein relevant ist die Existenz von $\mathcal{E}^\alpha_{\mathfrak{A}}.\mathtt{sk}_y(x_1, \ldots, x_n)$; der konkrete Wert $\mathcal{E}^\alpha.\mathtt{sk}_y(\cdots) = a$, der $\exists x$ erfüllt, ist irrelevant.

Kor. p ist erfüllbar gdw. $p_{\mathtt{sk}_y}$ erfüllbar ist.

Def. 55: Skolemnormalform

Eine geschlossene Formel p ohne Existenzquantoren in PCNF ist in *Skolemnormalform*:

$$p = \forall x_1 : \cdots \forall x_n : q,\ q \text{ in CNF u. quantorenfrei}, \mathrm{fvr}(p) = \emptyset.$$

Skolemisierung

Zum Sinn von Skolemformen

1. Sei $\mathfrak{A}$ eine Σ-Algebra.
   - Wenn: es ex. $\mathcal{J}_{\mathfrak{A}}^{\alpha} = \langle \mathrm{j}_{\mathfrak{A}}, \alpha \rangle$ mit $\mathcal{J}_{\mathfrak{A}}^{\alpha} \exists x \colon \mathtt{p}(x)$,
   - Dann: es ex. $\mathcal{J}_{\mathfrak{B}}^{\alpha} = \langle \mathrm{j}_{\mathfrak{B}}, \alpha \rangle$ mit $\mathcal{J}_{\mathfrak{B}}^{\alpha} \models \mathtt{p}(\mathtt{sk}_x())$

   und umgekehrt — wobei $\mathfrak{B}$ eine $(\Sigma \cup \{\mathtt{sk}_x\})$-Algebra ist:
   $\mathcal{J}^{\alpha} \models \exists x \colon \mathtt{p}(x) \Longleftrightarrow \mathcal{J}_{\mathtt{sk}} \models \mathtt{p}(\mathtt{sk})$ (mit Σ-Erweiterung)
2. $\exists x \colon \mathtt{prim}(x)$ hat ein Modell, gdw. $\mathtt{prim}(\mathtt{sk}_x)$ ein Modell hat:
   Das ist der Fall, z.B. mit $\mathcal{E}^{\alpha}.\mathtt{sk}_x = 3$ in $\mathbb{N}_0$.
3. $\forall x \colon \exists y \colon x \leq y$ hat ein Modell, gdw. $\forall x \colon x \leq \mathtt{sk}_y(x)$ ein Modell hat:
   Das ist der Fall, z.B. mit $\mathcal{E}^{\alpha}.\mathtt{sk}_y(x) = \alpha(x) + 1$ in $\mathbb{N}_0$.

Skolemisierung

Der Trick mit Skolemtermen

1. Sei $$p = \forall x\colon \forall y\colon \exists k\colon x + k = y.$$

   $+$ sei als Addition auf $\mathbb{Z}$ zu interpretieren.

? Hat p ein Modell?

Skolemisierung

Der Trick mit Skolemtermen

1. Sei $$p = \forall x\colon \forall y\colon \exists k\colon x + k = y.$$
   $+$ sei als Addition auf $\mathbb{Z}$ zu interpretieren.
2. Skolemisierung ergibt: $$p' = \forall x\colon \forall y\colon x + \mathtt{sk}_k(x, y) = y$$

Skolemisierung

Der Trick mit Skolemtermen

1. Sei $p = \forall x\colon \forall y\colon \exists k\colon x + k = y.$

   $+$ sei als Addition auf $\mathbb{Z}$ zu interpretieren.

2. Skolemisierung ergibt: $p' = \forall x\colon \forall y\colon x + \mathtt{sk}_k(x, y) = y$

? Hat p' ein Modell?

Skolemisierung

Der Trick mit Skolemtermen

1. Sei $p = \forall x\colon \forall y\colon \exists k\colon x + k = y.$

   $+$ sei als Addition auf $\mathbb{Z}$ zu interpretieren.

2. Skolemisierung ergibt: $p' = \forall x\colon \forall y\colon x + \mathtt{sk}_k(x, y) = y$

3. p' hat ein Modell, gdw. es eine Interpretation des Skolemterms gibt, die die Formel wahr macht.
   Gesucht ist also $\mathfrak{j}(\mathtt{sk}_k) = f$ so daß:

   $$x + f(x, y) = y, \text{ für alle } a, b \text{ als Werte für } x, y$$

Skolemisierung

Der Trick mit Skolemtermen

1. Sei $$p = \forall x\colon \forall y\colon \exists k\colon x + k = y.$$
   $+$ sei als Addition auf $\mathbb{Z}$ zu interpretieren.
2. Skolemisierung ergibt: $$p' = \forall x\colon \forall y\colon x + \mathtt{sk}_k(x, y) = y$$
3. p' hat ein Modell, gdw. es eine Interpretation des Skolemterms gibt, die die Formel wahr macht.
   Gesucht ist also $\mathtt{j}(\mathtt{sk}_k) = f$ so daß:
   $$x + f(x, y) = y, \text{ für alle } a, b \text{ als Werte für } x, y$$
4. Da $+$ normale Addition sein soll, setze (für $\mathbb{Z}$):
   $$f(a, b) = b - a$$
   mit der Subtraktion auf $\mathbb{Z}$.

Der Trick mit Skolemtermen

1. Sei $$p = \forall x\colon \forall y\colon \exists k\colon x + k = y.$$
   $+$ sei als Addition auf $\mathbb{Z}$ zu interpretieren.
2. Skolemisierung ergibt: $$p' = \forall x\colon \forall y\colon x + \mathtt{sk}_k(x, y) = y$$
3. p' hat ein Modell, gdw. es eine Interpretation des Skolemterms gibt, die die Formel wahr macht.
   Gesucht ist also $\mathfrak{j}(\mathtt{sk}_k) = f$ so daß:
   $$x + f(x, y) = y, \text{ für alle } a, b \text{ als Werte für } x, y$$
4. Da $+$ normale Addition sein soll, setze (für $\mathbb{Z}$):
   $$f(a, b) = b - a$$
   mit der Subtraktion auf $\mathbb{Z}$.
5. Natuerlich ist $a + f(a, b) = a + (b - a) = b$ für alle a, b wahr!

Beispiel.

p' = Jeder Bauer hat einen Esel oder ein Pferd, den er gern hat.

$$
\begin{aligned}
& \forall x\colon (\mathtt{f}(x) \longrightarrow \exists y\colon (((\mathtt{h}(y) \vee \mathtt{d}(y)) \wedge \mathtt{o}(x,y)) \wedge \mathtt{l}(x,y))) \\
\overset{\text{EXT}}{\Longleftrightarrow} \quad & \forall x\colon \exists y\colon (\mathtt{f}(x) \longrightarrow (((\mathtt{h}(y) \vee \mathtt{d}(y)) \wedge \mathtt{o}(x,y)) \wedge \mathtt{l}(x,y))) \\
\overset{\mathtt{sk}}{\Longleftrightarrow} \quad & \forall x\colon (\mathtt{f}(x) \longrightarrow (((\mathtt{h}(\mathtt{sk}_y(x)) \vee \mathtt{d}(\mathtt{sk}_y(x))) \wedge \mathtt{o}(x,\mathtt{sk}_y(x))) \wedge \mathtt{l}(x,\mathtt{sk}_y(x)))) \\
\overset{\forall:,\rightarrow}{\Longleftrightarrow} \quad & \forall\!\!\!\forall : (\neg\mathtt{f}(x) \vee (((\mathtt{h}(\mathtt{sk}_y(x)) \vee \mathtt{d}(\mathtt{sk}_y(x))) \wedge \mathtt{o}(x,\mathtt{sk}_y(x))) \wedge \mathtt{l}(x,\mathtt{sk}_y(x)))) \\
\overset{\text{DST}}{\Longleftrightarrow} \quad & ((\neg\mathtt{f}(x) \vee \mathtt{l}(x,\mathtt{sk}_y(x))) \wedge (\neg\mathtt{f}(x) \vee ((\mathtt{h}(\mathtt{sk}_y(x)) \vee \mathtt{d}(\mathtt{sk}_y(x))) \wedge \mathtt{o}(x,\mathtt{sk}_y(x))) \\
\overset{\text{DST}}{\Longleftrightarrow} \quad & ((\neg\mathtt{f}(x) \vee \mathtt{l}(x,\mathtt{sk}_y(x))) \wedge \\
& ((\neg\mathtt{f}(x) \vee (\mathtt{h}(\mathtt{sk}_y(x)) \vee \mathtt{d}(\mathtt{sk}_y(x)))) \wedge (\neg\mathtt{f}(x) \vee \mathtt{o}(x,\mathtt{sk}_y(x)))))) \\
\overset{\text{CNF}}{\Longleftrightarrow} \quad & \{\{\sim\mathtt{f}(x), \mathtt{l}(x,\mathtt{sk}_y(x))\}, \\
& \{\sim\mathtt{f}(x), \mathtt{h}(\mathtt{sk}_y(x)), \mathtt{d}(\mathtt{sk}_y(x))\}, \\
& \{\sim\mathtt{f}(x), \mathtt{o}(x,\mathtt{sk}_y(x))\}\}
\end{aligned}
$$

Skolem & Erfüllbarkeitsäquivalenz

Bew. Erfüllungsäquivalenz von Skolemformen

(ausgelassen)

Skolemisierte Literalmengen

Kor.

Zwei Klauseln C_1, C_2 in Skolemnormalform können durch eine Umbennung υ *variablenfremd* gemacht werden, so daß $\mathrm{var}(C_1\upsilon) \cap \mathrm{var}(C_2) = \emptyset$.

Def. 56: Grundinstanzen

Sei P eine Menge geschlossener, universell quantifizierter Formeln p in Pränexform mit Matrix q. Die Menge

$$\mathrm{gnd}(P) := \{q\,[x_i/t_i] \,\|\, \forall x_1 \colon \cdots \forall x_n \colon q \in P \ \wedge \ t_i \in \mathrm{Gnd}_\Sigma\}$$

ist die Menge der *Grundinstanzen von* P.

Thm. 35: Syntax und Semantik von Grundliteralmengen

Seien l_i Grundliterale.

$\bigwedge l_i$	hat ein Modell gdw.	für alle i, j ist $l_i \neq \sim l_j$
$\bigwedge l_i$	ist (allgemein-) gültig gdw.	$\mathbf{1} = \mathbf{0}$
$\bigvee l_i$	hat ein Modell gdw.	$\mathbf{1} = \mathbf{1}$
$\bigvee l_i$	ist (allgemein-) gültig gdw.	für ein Paar i, j ist $l_i = \sim l_j$

Eine Konjunktion ist *erfüllbar*, wenn sie *kein* komplementäres Paar enthält; eine Disjunktion ist *gültig*, wenn sie *ein* komplementäres Paar enthält.

Skolemtheorem, Kompaktheitstheorem

Thm. 36: Skolemtheorem

P hat ein Modell	gdw.	P hat ein Herbrand-Modell
gdw.		gdw.
$\mathrm{gnd}(P)$ hat ein Modell	gdw.	$\mathrm{gnd}(P)$ hat ein Herbrand-Modell

Thm. 37: Kompaktheitstheorem

Sei P eine Menge geschlossener Formeln. P ist erfüllbar gdw. jede endliche Teilmenge von P erfüllbar ist.

9.1.
RESOLUTIONSKALKÜL FÜR FOL

MGU

Def. 57: Unifikatoren, Unifikation, MGU, μ

Seien V, W Teilmengen von Ter oder Fml.

1. $W\sigma := \{w\sigma \parallel w \in W\}$
2. σ heißt *Unifikator von W*, gdw. $c(W\sigma) = 1$.
3. μ heißt *allgemeinster Unifikator (mgu) von W* gdw.:

$$\forall\sigma\colon \exists\vartheta\colon (\, c(W\sigma) = 1 \longrightarrow \sigma = \mu\vartheta).$$

4. V ist allgemeiner als W ($V \preceq W$), gdw. es ex. σ mit $V\sigma = W$.
5. Seien P, Q Klauselmengen. P subsumiert Q ($P \Subset Q$), gdw. es ex. σ mit $P\sigma \subseteq Q$.

Thm. 38: Unifikationsalgorithmus

Wenn existent, kann man μ algorithmisch bestimmen (Robinson).

Unifikationsalgorithmus

Seien v, w variablenfremde Terme (quantorenfreie Formeln), $\mathtt{Op} \in \mathrm{Fnc} \cup \mathrm{Prd}$ oder Junktoren.

$\mathtt{Unif}(v, w) \to (\mathrm{Ter}^{\mathrm{Var}})$

$\quad$ LET μ:=$\emptyset$;

$\quad$ IF $v = w \vee v\mu = w\mu$ THEN;

$\quad\quad$ RETURN μ;

$\quad$ ELSE;

$\quad\quad$ IF $v \in \mathrm{Var} \wedge w \in \mathrm{Gnd} \cup \mathrm{Var}$ THEN; $^{(*)}$

$\quad\quad\quad$ RETURN $\mu \cup \{v/w\}$; $^{(*)}$

$\quad\quad$ ELSIF $v = \mathtt{Op}(v_1, \ldots, v_n) \wedge w = \mathtt{Op}(w_1, \ldots, w_n)$ THEN;

$\quad\quad\quad$ FORALL $i \in \{1, \ldots n\}$ DO;

$\quad\quad\quad\quad$ LET μ:=$\mu \cup \bigcup_{1 \leq i \leq n} \mathtt{Unif}(v_i, w_i)$;

$\quad\quad\quad$ DONE;

$\quad\quad$ ELSE;

$\quad\quad\quad$ ABORT err;

$\quad\quad$ ENDIF;

$\quad$ ENDIF;

$^{(*)}$ oder umgekehrt. Für quantifizierte Formeln existiert ein iterativer präfixbasierter Algorithmus.

RES

"Sprache der Resolution"

Wir nehmen für eine Formelmenge an, sie sei in eine erfüllungsäquivalente skolemisierte PCNF P überführt (Klauselmenge $\forall\!\!\!\forall : \{\{l_{1,1}, \ldots, l_{1,n_1}\}, \ldots, \{l_{m,1}, \ldots, l_{m,n_m}\}\}$).

Def. 58: Die Resolutionsregel

Gegeben seien zwei variablenfremde Klauseln.

$$\frac{\{l_1, \ldots, \sim l, \ldots, l_m\} \qquad \{l'_1, \ldots, l', \ldots, l'_n\}}{\{l_1, \ldots, l_m, l'_1, \ldots, l'_n\}\,\mu}\ \mathrm{RES}$$

mit $l\mu = l'\mu$.

Varianten: Resolution mehrerer Literalpaare, beliebigen Unifikatoren, keine Unifikation ($\mathrm{RES}_{\mathsf{PRL}}$).

Resolution

Anwendung des Resolutionskalküls

Sei P eine Klauselmenge. Wir schreiben für resolvierbare $C_1, C_2 \in P$ die Ableitung einer Resolvente R durch RES als $C_1, C_2 \vdash R$.
Man definiert $\mathrm{Res} : \wp(\mathrm{Fml}) \to \wp(\mathrm{Fml})$ als

$$\begin{array}{rcl} \mathrm{Res}(P) & := & P \cup \{R \,\|\, \exists C_i, C_j : (C_i, C_j \in P \wedge C_i, C_j \vdash R)\} \\ \mathrm{Res}^*(P) & = & \bigcup_{i \in \mathbb{N}_0} \mathrm{Res}^i(P). \end{array}$$

Thm. 39: Erfüllbarkeitsbeweis

$$\begin{array}{llll} \bigwedge P \in \mathrm{Fml} & \text{ist unerfüllbar} & \text{gdw.} & \oslash \in \mathrm{Res}^*(P) \\ \bigwedge P \in \mathrm{Fml} & \text{ist erfüllbar} & \text{gdw.} & \oslash \notin \mathrm{Res}^*(P). \end{array}$$

Beispiel

Beispiel: Menschen sind sterblich und Anton ist ein Mensch

$P = \{p, q\}$ mit

$$\begin{array}{lcl} p & = & \forall x\colon (\mathtt{hmn}(x) \longrightarrow \mathtt{mrt}(x)) & \iff & \{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\} \\ q & = & \mathtt{hmn}(\mathtt{anton}) & \iff & \{\ \ \mathtt{hmn}(\mathtt{anton})\} \end{array}$$

Dann

$$\mathrm{Res}^0(P) \quad ==$$

Beispiel

Beispiel: Menschen sind sterblich und Anton ist ein Mensch

$P = \{p, q\}$ mit

$$
\begin{array}{rcl}
p & = & \forall x \colon (\mathtt{hmn}(x) \longrightarrow \mathtt{mrt}(x)) \quad \Longleftrightarrow \quad \{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\} \\
q & = & \mathtt{hmn}(\mathtt{anton}) \quad \Longleftrightarrow \quad \{\ \mathtt{hmn}(\mathtt{anton})\}
\end{array}
$$

Dann

$$\mathrm{Res}^0(P) \quad == \quad \mathrm{Res}^0(\{\{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\}, \{\mathtt{hmn}(\mathtt{anton})\}\})$$

Beispiel

Beispiel: Menschen sind sterblich und Anton ist ein Mensch

$P = \{p, q\}$ mit

$$
\begin{array}{lcl}
p & = & \forall x\colon (\mathtt{hmn}(x) \longrightarrow \mathtt{mrt}(x)) \iff \{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\} \\
q & = & \mathtt{hmn}(\mathtt{anton}) \iff \{\ \mathtt{hmn}(\mathtt{anton})\}
\end{array}
$$

Dann

$$
\begin{array}{lcl}
\mathrm{Res}^0(P) & = & \mathrm{Res}^0(\{\{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\}, \{\mathtt{hmn}(\mathtt{anton})\}\}) \\
\mathrm{Res}^1(P) & = & \mathrm{Res}^0(P) \cup \{\{\mathtt{mrt}(x)\,[x/\mathtt{anton}]\}\})
\end{array}
$$

Beispiel

Beispiel: Menschen sind sterblich und Anton ist ein Mensch

$P = \{p, q\}$ mit

$$\begin{array}{lcll} p & = & \forall x\colon (\mathtt{hmn}(x) \longrightarrow \mathtt{mrt}(x)) & \iff \{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\} \\ q & = & \mathtt{hmn}(\mathtt{anton}) & \iff \{\ \mathtt{hmn}(\mathtt{anton})\} \end{array}$$

Dann

$$\begin{array}{lcl} \mathrm{Res}^0(P) & = & \mathrm{Res}^0(\{\{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\}, \{\mathtt{hmn}(\mathtt{anton})\}\}) \\ \mathrm{Res}^1(P) & = & \mathrm{Res}^0(P) \cup \{\{\mathtt{mrt}(x)\,[x/\mathtt{anton}]\}\}) \\ & = & \{\{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\}, \{\mathtt{hmn}(\mathtt{anton})\}, \{\mathtt{mrt}(x)\,[x/\mathtt{anton}]\}\} \end{array}$$

Beispiel

Beispiel: Menschen sind sterblich und Anton ist ein Mensch

$P = \{p, q\}$ mit

$$
\begin{array}{rcl}
p & = & \forall x\colon (\mathtt{hmn}(x) \longrightarrow \mathtt{mrt}(x)) \quad \Longleftrightarrow \quad \{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\} \\
q & = & \mathtt{hmn}(\mathtt{anton}) \quad \Longleftrightarrow \quad \{\ \mathtt{hmn}(\mathtt{anton})\}
\end{array}
$$

Dann

$$
\begin{array}{rcl}
\mathrm{Res}^0(P) & = & \mathrm{Res}^0(\{\{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\}, \{\mathtt{hmn}(\mathtt{anton})\}\}) \\
\mathrm{Res}^1(P) & = & \mathrm{Res}^0(P) \cup \{\{\mathtt{mrt}(x)\,[x/\mathtt{anton}]\}\}) \\
 & = & \{\{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\}, \{\mathtt{hmn}(\mathtt{anton})\}, \{\mathtt{mrt}(x)\,[x/\mathtt{anton}]\}\} \\
 & = & \{\{\sim\mathtt{hmn}(x), \mathtt{mrt}(x)\}, \{\mathtt{hmn}(\mathtt{anton})\}, \{\mathtt{mrt}(\mathtt{anton})\}\} \not\ni \emptyset
\end{array}
$$

Keine weitere Resolution möglich: $\mathrm{Res}^*(P) = \mathrm{Res}^1(P)$.

Beispiel: Widerlegungsbeweis

Beispiel: $\{p, q\} \mathrel{|}\!\approx$ Anton ist sterblich

Die These laute also $r = \texttt{mrt}(\texttt{anton})$. Es ergibt sich als negierte Form:

$$\sim r \quad = \quad \sim\texttt{mrt}(\texttt{anton}) \quad \iff \quad \{\sim\texttt{mrt}(\texttt{anton})\}$$

Dann

$$\begin{tikzcd}
\{\sim\texttt{hmn}(x), \texttt{mrt}(x)\} \arrow[dr, dash, "\mu"'] & & \{\texttt{hmn}(\texttt{anton})\} \arrow[dl, dash, "\mu"] & \{\sim\texttt{mrt}(\texttt{anton})\} \arrow[ddl, dash] \\
& \{\texttt{mrt}(\texttt{anton})\} \arrow[dr, dash] & & \\
& & \emptyset &
\end{tikzcd}$$

mit $\mu = [x/\texttt{anton}]$.

RES— Korrektheit & Vollständigeit

Thm. 40: RES ist deduktiv korrekt

$$p \in \mathrm{Res}^*(P) \Longrightarrow P \mathrel{|\!\approx} p$$

Thm. 41: RES als Widerlegungskalkül ist korrekt

$$\oslash \in \mathrm{Res}^*(P) \Longrightarrow P \text{ ist unerfüllbar.}$$

Thm. 42: RES als Widerlegungskalkül ist vollständig

$$P \text{ hat kein Modell } \Longrightarrow \oslash \in \mathrm{Res}^*(P)$$

Korrektheit von **RES**

Bew. $p \in \mathrm{Res}^*(P) \Longrightarrow P \mathrel{|\!\approx} p$

Man beweist die Korrektheit der Regelanwendung.

- Gelte $\mathcal{J} \models C \cup \{l\}$ u. $\mathcal{J} \models C' \cup \{\sim l'\}$, mit $l \notin C$, $\sim l' \notin C'$.
- Dann $\mathcal{J}^\alpha \models (\bigvee C \vee l)$ u. $\mathcal{J}^\alpha \models (\bigvee C' \vee \neg l')$. Sei $l\mu = l'\mu$.
- Man betrachtet vier mögliche Fälle:
  1. $\mathcal{J}^\alpha \models (\bigvee C)$. Dann natürlich auch $\mathcal{J}^\alpha \models (\bigvee C \vee \bigvee C')\,\mu$.
  2. $\mathcal{J}^\alpha \models (\bigvee C')$. Dann natürlich auch $\mathcal{J}^\alpha \models (\bigvee C \vee \bigvee C')\,\mu$.
  3. $\mathcal{J}^\alpha \models l$. Dann natürlich $\mathcal{J}^\alpha \not\models \neg l'$. Da aber $\mathcal{J}^\alpha \models (\bigvee C' \vee \neg l')\,\mu$, muß $\mathcal{J}^\alpha \models (\bigvee C')\mu$. Dann siehe 2.
  4. $\mathcal{J}^\alpha \models \neg l'$. Dann natürlich $\mathcal{J}^\alpha \not\models l$. Da aber $\mathcal{J}^\alpha \models (\bigvee C \vee l)\,\mu$, muß $\mathcal{J}^\alpha \models (\bigvee C)\mu$. Dann siehe 1.

Korrektheit von **RES**

Bew. $\oslash \in \mathrm{Res}^*(P) \Longrightarrow P$ unerfüllbar.

1. Sei $\oslash \in \mathrm{Res}^*(P)$.
2. Nach Korrektheit von Res, gilt also $P \approx\!\!\!\models \emptyset$.
3. Da $\emptyset$ unerfüllbar, $P \approx\!\!\!\models \mathsf{F}$, d.h.

$$
\begin{array}{ll}
 & \mathcal{J}^{\alpha} \models P \Longrightarrow \mathcal{J}^{\alpha} \models \mathsf{F} \\
\text{gdw} & \mathcal{J}^{\alpha} \models P \Longrightarrow \mathsf{F} \\
\text{gdw} & \mathcal{J} \not\models P
\end{array}
$$

4. Also kann es kein Modell von P geben, d.h.
5. P ist unerfüllbar.

Vollständigkeit von **RES**

Bew. P unerfüllbar $\Longrightarrow \oslash \in \mathrm{Res}^*(P)$

Beweis sehr technisch.
Zuerst eine Induktion über die Mächtigkeit der Klauseln für den Fall dass P keine Variablen entält.
Danach eine Konstruktion durch Lifting der Grundinstanzen zur Herleitung von $\oslash$ auf bel. Klauseln mit passenden mgus.
Siehe Literatur, Skript oder ggf. Folgevorlesung.

Algorithmische Varianten von **RES**

Lineare Resolution: Man konstruiert $P \vdash^* p$ mit:

1. $r_0, r'_0 \in P$
2. $\{r_i, r'_i\} \vdash r_{i+1}$ mit $r'_i \in P \cup \{r_j \parallel 0 \leq j < i\}$

Suchraum kleiner; geschickte Wahl von r_0, r'_i nötig.

Eingaberesolution: Man konstruiert $P \vdash^* p$ mit:

1. $r_0, r'_0 \in P$
2. $\{r_i, r'_i\} \vdash r_{i+1}$ mit $r'_i \in P$

Suchraum noch kleiner, aber nicht mehr widerlegungsvollständig:

$$\{\{p, q\}, \{\sim p, q\}, \{p, \sim q\}, \{\sim p, \sim q\}\} \not\vdash \emptyset$$

aber

$$\{\{p, q\}, \{\sim p, q\}, \{p, \sim q\}, \{\sim p, \sim q\}\} \mathrel{|}\!\!\approx \mathsf{F}$$

Eine Teilmenge von FOL

Das Problem

Man hat ein Beweisverfahren, das

- korrekt bzgl. der logischen Sprache ist, aber
- nicht vollständig bzgl. der logischen Sprache ist.

Also:

$$P \vdash^* p \Longrightarrow P {\mid\!\approx} p \text{ aber } P {\mid\!\approx} p \not\Longrightarrow P \vdash^* p$$

Idee

Man schränke die Menge möglicher P und p so ein, daß auch

$$P {\mid\!\approx} p \Longrightarrow P \vdash^* p$$

Def. 59: Hornklauseln

C heißt *Hornklausel*, wenn sie *höchstens ein positives* Literal enthält. Man unterscheidet die *leere Klausel*, *Fakten*, *Regeln* und *Zielklauseln*: Fakten und Regeln bilden zusammen ein *logisches Programm* P.

Erfüllbarkeit von Programen und Zielklauseln

Thm. 43: Grundlagen der **SLD** Widerlegung

$P \approx \exists : (g_1 \wedge \cdots \wedge g_n) \Longleftrightarrow P \cup \{\{\sim g_1, \ldots, \sim g_n\}\}$ ist unerfüllbar.

In anderer Schreibweise: $P \cup \{ \text{:-}\ g_1, \ldots, g_n\} \vdash_{\mathbf{SLD}} \oslash$.

Zur logischen Programmierung

- Sei P ein log. Programm, mit $P \approx dbl(x, y)$ gdw. $2x = y$.
- Die Frage "Gibt es eine Zahl y mit $y = 2x \cdot 3$?" ist eine Frage nach der *Unerfüllbarkeit* der Aussage "$\forall y \colon \neg dbl(3, y))$".
- Die Herleitung von $\oslash$ beweist dann die Existenz von $y = 2 \cdot 3$. Aus den Substitutionen kann man eine erfüllende Belegung, $\alpha(y) = 6$, ableiten.

Funktionsweise der **SLD**-Resolution

"S, L, D"

Resolviere schrittweise je *das erste* Literal aus der Zielklausel entlang eines *linearen* Resolutionsbaumes.

$P = \{\texttt{grk}(\texttt{sokrates}), (\texttt{grk}(x) \longrightarrow \texttt{hum}(x)), (\texttt{hum}(y) \longrightarrow \texttt{mrt}(y))\}$

$\texttt{?-mrt}(\texttt{sokrates})$ — $\texttt{mrt}(x)$:- $\texttt{hum}(x)$

$[x/\texttt{sokrates}]$

$\texttt{?-hum}(\texttt{sokrates})$ — $\texttt{hum}(y)$:- $\texttt{grk}(y)$

$[y/\texttt{sokrates}]$

$\texttt{?-grk}(\texttt{sokrates})$ — $\texttt{grk}(\texttt{sokrates})$

$\emptyset$

$\oslash$

Implementation der **SLD**Resolution

Logische Programmierung / Prolog

1. Eine Zielklausel $g =$ `?-`$g_1, g_2, \ldots g_n$. wird mit g_1' `:-` $b_1, \ldots, b_m$ zu `?-`$b_1, \ldots, b_m, g_2, \ldots g_n.\mu$ resolviert.
2. Der SLD-Beweis wird auf der Herbrand-Basis von P geführt.
3. Führt eine SLD-Sequenz *nicht* zu $\oslash$, werden weitere *Alternativen* versucht.
4. SLD-Sequenzen können schlimmstenfalls unendlich sein.
5. Endet *keine* SLD-Sequenz in $\oslash$ ($P \cup \{\sim g\} \not\vdash \oslash$), wird angenommen, daß $P \approx \sim g$.
6. Es kann nicht bewiesen, daß etwas *nicht* gilt — es kann nur nachgewiesen, daß etwas nicht bewiesen werden kann.

Beispiele

```
% Sokrates ist ein Grieche: grk(sokrates)

grk(sokrates).

% Alle Griechen sind Menschen:
% ALL X: (grk(X) -> hmn(X)) <=> (grk(X) -> hmn(X))
%    <=> (-grk(X) | hmn(X))  <=> {~grk(X) , hmn(X)}

hmn(X) :- grk(X).

% Alle Menschen sind sterblich:
% ALL X: (hmn(X) -> mrt(X)) <=> (hmn(X) -> mrt(X))
%    <=> (-hmn(X) | mrt(X))  <=> {~hmn(X) , mrt(X)}

mrt(X) :- hmn(X).

% Ist sokrates sterblich? : ?- mrt(sokrates).
```

Beispiele

```
strasse(bonn, koeln).
strasse(bonn, koblenz).
strasse(koeln, wuppertal).
strasse(koeln, duesseldorf).
strasse(wuppertal, bielefeld).
strasse(wuppertal, muenster).
strasse(muenster, osnabrueck).

% ALL X: tour(X,X)

tour(X, X).

% \ALL X,Y: (tour(Z,Y) & strasse(X,Y)) -> tour(X,Y).

tour(X, Z) :-
    strasse(X, Y), tour(Y, Z).
```

Beispiele

```
% Leere und einelementige Listen sind sortiert:

qsort([],[]). qsort([X], [X]).

% Angenommen,
%   Man habe eine Liste geteilt in zwei Listen,
%       deren erste nur Elemente =< einem Pivotelement sind
%       und deren zweite nur Elemente > enthaelt,
%   und zu diesen beiden Listen Less und Greater jeweils
%       sortierte Varianten vorliegen,
% Dann ist das Aneinanderhaengen dieser beiden listen
% eine sortierte Version der urspruenglich geteilten liste.

qsort([Head, Pivot|Tail],Sorted):-
        split(Pivot,[Head|Tail],Less,Greater),
        qsort(Less,SortedLess),
        qsort(Greater,SortedGreater),
        append(SortedLess,[Pivot|SortedGreater],Sorted).
```

10.
SEQUENZENKALKÜL

Sequenzenkalkül

Sequenzen

"Wenn *dies* eine korrekter Schluss ist, dann auch *jenes*".

1. Beginne mit leeren Schlüssen d.h. *Axiomen*
2. Erweitere diese, bis der gewünschte Schluss dargestellt ist.

Oft sich eine umgekehrte Vorgehensweise (Dekomposition) an.

Darstellungsweise

Ein korrekter Schluss von P auf Q wird dargestellt als:

$$P \Vdash Q.$$

Man leitet aus der Korrektheit (Ableitbarkeit) eines Schlusses die Korrektheit eines weiteren Schlusses ab:

$$P \Vdash Q \quad \vdash \quad P' \Vdash Q'.$$

Die Sprache der Sequenzen

Def. 60: PRL/FOL -Sequenzen

Die Sprache der Sequenzen ist die Menge

$$\mathrm{Fml}_{\mathsf{LK}} := \{P \Vdash Q \,\|\, P, Q \text{ finite and } P, Q \subseteq \mathrm{Fml}\}$$

wobei $\Vdash$ ein neues Symbol ist und $P \cup Q \neq \emptyset$.
$P \subseteq \mathrm{Fml}$ heißt *Antezedent* (oder *Prämisse*) und $Q \subseteq \mathrm{Fml}$ heißt *Sukzedent* (oder *Conclusion*).
Alternativ kann man auch definieren

$$\mathrm{Fml}_{\mathsf{LK}} = (\wp(\mathrm{Fml}) \times \{\Vdash\} \times \wp(\mathrm{Fml})) - \{\Vdash\}\,.$$

Anmerkung.

1. Genau genommen handelt es sich bei P und Q um *Folgen*.
2. Wir definieren **LK** zunächst für PRL und erweitern dann auf FOL.

Def. 61: Gültigkeitsbegriff für Sequenzen

Eine Sequenz $s = P \Vdash Q \in L_{\mathbf{LK}}$ *gilt unter/in* $\mathcal{G}$, gdw.

$$\mathcal{G}^{\alpha}_{\mathfrak{G}} \models P \Vdash Q \qquad \text{gdw.} \qquad \mathcal{J}^{\alpha} \models \bigwedge P \implies \mathcal{J}^{\alpha} \models \bigvee Q$$

wobei $\mathfrak{G} = \mathfrak{A} \times \mathfrak{A}$ mit einer Σ-Algebra $\mathfrak{A}$ (d.h. $\mathcal{G} \in \mathfrak{A}^{\mathrm{Fml}} \times \mathfrak{A}^{\mathrm{Fml}}$).
$\mathcal{J} = \langle \mathfrak{j}, \alpha \rangle$ ist die kanonische Interpretation in $\mathfrak{A}$; d.h.

$$\mathcal{G}^{\alpha}.P \Vdash Q \;=\!=\; \overline{\mathcal{J}^{\alpha}.\bigwedge P} \sqcup \mathcal{J}^{\alpha}.\bigvee Q$$

In Worten:

Eine Sequenz ist gültig, wenn aus der Gütligkeit der Konjunktion ihrer Antezedentien logisch die Gültigkeit der Disjunktion ihrer Sukzedentien folgt.

Sequenzen

Der Linguistentrick für Sequenzen

$$s' = (P \Vdash Q)' \Longleftrightarrow \overline{(\bigwedge P)'} \sqcup (\bigvee Q)'.$$

$$\models s \iff \prod_{p \in P} p' \sqsubseteq \bigsqcup_{q \in Q} q'$$

Notationsvereinbaruung

Wir schreiben $P^{\wedge}$ und $Q^{\vee}$ für $\bigwedge P$ und $\bigvee Q$.

LK- Axiom

Def. 62: LK- Axiom

$$\overline{\quad p \Vdash p \quad}\ \textsc{axm}.$$

Bew. $\textsc{axm}$ ist korrekt bzgl. PRL und FOL

$$\begin{aligned} \mathcal{G} \models p \Vdash p \quad & \text{gdw} \quad \mathcal{I} \models p \Longrightarrow \mathcal{I} \models p \\ & \text{gdw} \quad \mathsf{T} \\ & \text{gdw} \quad \mathcal{J} \models p \Longrightarrow \mathcal{J} \models p \end{aligned}$$

LK-Strukturregeln

Def. 63: LK-Strukturregeln

$$\frac{P \Vdash Q}{p, P \Vdash Q}\,\text{WKL} \qquad \frac{P \Vdash Q}{P \Vdash Q, q}\,\text{WKR}$$

$$\frac{p, p, P \Vdash Q}{p, P \Vdash Q}\,\text{IDL} \qquad \frac{P \Vdash Q, p, p}{P \Vdash Q, p}\,\text{IDR}$$

$$\frac{P, p, q, P' \Vdash Q}{P, q, p, P' \Vdash Q}\,\text{CHL} \qquad \frac{P \Vdash Q, p, q, Q'}{P \Vdash Q, q, p, Q'}\,\text{CHR}$$

Ausserdem gilt die CUT-Regel:

$$\frac{P \Vdash Q, p \qquad p, R \Vdash S}{P, R \Vdash Q, S}\,\text{CUT}$$

LK-Strukturregeln

Bew. $\textsc{ID}x$ und $\textsc{CH}x$ sind korrekt bzgl. PRL und FOL

Folgt aus Idempotenz und Kommutativität von $\sqcap$ und $\sqcup$ in $\mathcal{B}$.

Bew. $\textsc{WKR}$ ist korrekt bzgl. PRL und FOL

$$\begin{aligned}
\mathcal{G}^\alpha \models P \Vdash Q \quad &\overset{\mathcal{G}}{\Longleftrightarrow} \quad \mathcal{J}^\alpha \models P^\wedge \Longrightarrow \mathcal{J}^\alpha \models Q^\vee \\
&\Longrightarrow \quad \mathcal{J}^\alpha \models P^\wedge \Longrightarrow \mathcal{J}^\alpha \models \left(Q^\vee \vee q\right) \\
&\overset{\mathcal{G}}{\Longleftrightarrow} \quad \mathcal{G}^\alpha \models P \Vdash Q, q
\end{aligned}$$

Algebraisch argumentiert man: $P^\sqcap \leq Q^\sqcup \Longrightarrow P^\sqcap \leq Q^\sqcup \sqcup q$.

Bew. $\textsc{WKL}$ ist korrekt bzgl. PRL und FOL

Algebraisch argumentiert man: $P^\sqcap \leq Q^\sqcup \Longrightarrow P^\sqcap \sqcap p \leq Q^\sqcup$.

LK-Strukturregeln

Bew. CUT ist korrekt bzgl. PRL und FOL

Seien die Prämissen der CUT-Regel erfüllt:

$$(a.)\ P^{\sqcap} \sqsubseteq Q^{\sqcup} \sqcup p' \text{ und } (b.)\ p' \sqcap R^{\sqcap} \sqsubseteq S^{\sqcup}$$

Vermittels der Rangierregel SHN erhält man:

$$(c.)\ P^{\sqcap} \sqcap \overline{p'} \sqsubseteq Q^{\sqcup} \text{ und } (d.)\ R^{\sqcap} \sqsubseteq S^{\sqcup} \sqcup \overline{p'}$$

Man rechnet:

$$\begin{aligned}
P^{\sqcap} \sqcap R^{\sqcap} &\overset{(a.)}{\sqsubseteq} (Q^{\sqcup} \sqcup p') \sqcap \mathrm{R} \\
&\overset{(d.)}{\sqsubseteq} (Q^{\sqcup} \sqcup p') \sqcap (S^{\sqcup} \sqcup \overline{p'}) \\
&\overset{\text{DST}}{=\!=} ((Q^{\sqcup} \sqcap S^{\sqcup}) \sqcup (p' \sqcap S^{\sqcup})) \sqcup ((Q^{\sqcup} \sqcap \overline{p'}) \sqcup (p' \sqcap \overline{p'})) \\
&\overset{\text{NTR,ASC}}{=\!=} (Q^{\sqcup} \sqcap S^{\sqcup}) \sqcup (p' \sqcap S^{\sqcup}) \sqcup (Q^{\sqcup} \sqcap \overline{p'}) \\
&\overset{\text{ITN}}{\sqsubseteq} Q^{\sqcup} \sqcup S^{\sqcup} \sqcup Q^{\sqcup} \\
&\overset{\text{COM,IDM}}{=\!=} Q^{\sqcup} \sqcup S^{\sqcup}
\end{aligned}$$

Def. 64: LK-Junktorregeln (a)

$$\frac{P \Vdash Q, p}{\neg p, P \Vdash Q}\,\mathrm{NIL} \qquad \frac{p, P \Vdash Q}{P \Vdash Q, \neg p}\,\mathrm{NIR}$$

$$\frac{p, q, P \Vdash Q}{(p \wedge q)\,, P \Vdash Q}\,\mathrm{CIL} \qquad \frac{P \Vdash Q, p, q}{P \Vdash Q, (p \vee q)}\,\mathrm{DIR}$$

$$\frac{q, P \Vdash Q \qquad R \Vdash S, p}{(p \longrightarrow q)\,, P, R \Vdash Q, S}\,\mathrm{IIL} \qquad \frac{p, P \Vdash Q, q}{P \Vdash Q, (p \longrightarrow q)}\,\mathrm{IIR}$$

Beispiel

Vor den Beweisen ein kleines Beispiel: $\textsc{h}1$ (PRL)

Wir zeigen:

$$\Vdash (p \longrightarrow (q \longrightarrow p)) \text{ ist eine gültige Sequenz.}$$

Das einfache Besipiel ist problemlos “top-down” zu bewerkstelligen:

$$\begin{array}{c|rcl|l}
1 & p & \Vdash & p & \textsc{axm} \\
2 & p, q & \Vdash & p & \textsc{wkl}(1) \\
3 & p & \Vdash & (q \longrightarrow p) & \textsc{iir}(2) \\
4 & & \Vdash & (p \longrightarrow (q \longrightarrow p)) & \textsc{iir}(3)
\end{array}$$

LK-Junktorregeln

Bew. Korrektheit der Junktorregeln (a): NIL, CIL, IIR

$$\frac{P \Vdash Q, p}{\neg p, P \Vdash Q}\ \mathrm{NIL} \qquad \frac{p, P \Vdash Q}{P \Vdash Q, \neg p}\ \mathrm{NIR} \frac{p, q, P \Vdash Q}{(p \wedge q)\,, P \Vdash Q}\ \mathrm{CIL} \qquad \frac{p, P \Vdash Q, q}{P \Vdash Q, (p \longrightarrow q)}\ \mathrm{IIR}$$

1. NIL und NIR: SHN.
2. CIL und DIR: asc von $\sqcap$ und $\sqcup$.
3. IIR: SHN, DIR, $(\neg p \vee q) \Longleftrightarrow (p \longrightarrow q)$.

Bew. Korrektheit der Junktorregeln (a)

$$\frac{q, P \Vdash Q \qquad R \Vdash S, p}{(p \longrightarrow q)\,, P, R \Vdash Q, S}\ \textsc{iil}$$

4. IIL:
   4.1 Mit SHN wird das zweite Antezedens zu $\neg p, R \Vdash S$.
   4.2 Die rechten Seiten werden nach oben abgeschätzt:

   $$q, P \Vdash Q, S \text{ und } \neg p, R \Vdash Q, S$$

   4.3 Die linken Seiten werden nach unten abgeschätzt:

   $$q, P, R \Vdash Q, S \text{ und } \neg p, P, R \Vdash Q, S$$

   4.4 und man erhält:

   $$(\neg p \vee q)\,, P, R, \Vdash Q, S \overset{\longrightarrow}{\Longleftrightarrow} (p \longrightarrow q)\,, P, R \Vdash Q, S$$

   Für den letzten Schritt s. Beweis zu DIL

LK-Junktorregeln

Def. 65: **LK**-Junktorregeln (b)

$$\frac{P \Vdash Q, p \qquad P \Vdash Q, q}{P \Vdash Q, (p \wedge q)}\ \textsc{cir} \qquad\qquad \frac{p, P \Vdash Q \qquad q, P \Vdash Q}{(p \vee q)\,, P \Vdash Q}\ \textsc{dil}$$

Bew. Korrektheit der Junktorregeln (b)

Seien die Antezedetien gültige Sequenzen. Dann gilt für $\textsc{cir}$:

$$\begin{aligned} P^{\sqcap} \sqsubseteq Q^{\sqcup} \sqcup p' \wedge P^{\sqcap} \sqsubseteq Q^{\sqcup} \sqcup q' \quad &\overset{\mathscr{B}}{\Longrightarrow} \quad P^{\sqcap} \sqsubseteq (Q^{\sqcup} \sqcup p') \sqcap (Q^{\sqcup} \sqcup q') \\ &\overset{\text{DST}}{\Longrightarrow} \quad P^{\sqcap} \sqsubseteq Q^{\sqcup} \sqcup (p' \sqcap q') \end{aligned}$$

und $P \Vdash Q, (p \wedge q)$ ist eine gültige Sequenz.
Die Korrektheit von $\textsc{dil}$ wird analog gezeigt.

PRL-Korrektheit von **LK**

Kor.

LK ist als PRL-Kalkül korrekt.

LK für FOL

Benötigt sind noch korrekte Regeln für quantifizierte Formeln.

Vollständigkeit

Zu zeigen bleibt dann die Vollständigkeit von **LK**.

Dies wird durch die *Simulation* eines bekannten vollständigen Kalküls in **LK** bewiesen.

LK- Quantorenregeln

Def. 66: LK-Quantorenregeln

$$\frac{p\,[x/t]\,, P \Vdash Q}{\forall x\colon p, P \Vdash Q}\,\textsc{all} \qquad \frac{P \Vdash Q, p\,[x/t]}{P \Vdash Q, \exists x\colon p}\,\textsc{exr}$$

vorausgesetzt, daß $p\,[x/t]$ jeweils zulässig ist (oder: $t \in \mathrm{Gnd}$)

$$\frac{P \Vdash Q, p\,[x/y]}{P \Vdash Q, \forall x\colon p}\,\textsc{alr} \qquad \frac{p\,[x/y]\,, P \Vdash Q}{\exists x\colon p, P \Vdash Q}\,\textsc{exl}$$

vorausgesetzt, daß $p\,[x/y]$ jeweils zulässig ist und

- $y \notin \mathrm{fvr}(P \Vdash Q, \forall x\colon p)$ für $\textsc{alr}$ und
- $y \notin \mathrm{fvr}(\exists x\colon p, P \Vdash Q)$ für $\textsc{exl}$.

(oder: $y \in \mathrm{Con}$ (!) kommt nicht "unterm Strich vor").

LK- Quantorenregeln

Bew. Korrektheit von $\textsc{All}$

Sei das Antezedens erfüllt, d.h. eine gültige Sequenz:

$$\mathcal{G}^{\alpha} \models p\,[x/t]\,, P \Vdash Q \text{ gdw. } \mathcal{J}^{\alpha} \models \big(p\,[x/t] \wedge P^{\wedge}\big) \Longrightarrow \mathcal{J}^{\alpha} \models Q^{\vee}$$

Zz: *Wenn* die Prämisse des Sukzedens erfüllt ist, dann auch die Konklusion.

$$\begin{aligned}
\mathcal{J}^{\alpha}_{\mathfrak{A}} \models \big(\forall x : p \wedge P^{\wedge}\big) \quad & \overset{\forall}{\Longrightarrow} \quad \mathcal{J}^{\alpha\langle x \leftarrow a\rangle}_{\mathfrak{A}} \models p \wedge P^{\wedge}, \text{ für alle } a \in \mathcal{U} \\
& \overset{\forall t' = a}{\Longrightarrow} \quad \mathcal{J}^{\alpha\langle x \leftarrow t'\rangle}_{\mathfrak{A}} \models p \wedge P^{\wedge} \\
& \overset{\text{Subst.}}{\Longrightarrow} \quad \mathcal{J}^{\alpha}_{\mathfrak{A}} \models p\,[x/t] \wedge P^{\wedge} \\
& \overset{\text{Ann.}}{\Longrightarrow} \quad \mathcal{J}^{\alpha}_{\mathfrak{A}} \models Q^{\vee}
\end{aligned}$$

Also ist $\forall x : p, P \Vdash Q$ eine gültige Sequenz.

Beachte: Zulässigkeit von $p\,[x/t]$ im Schritt 3.

LK- Quantorenregeln

Bew. Korrektheit von ALR

Übung, Hausaufgabe oder Klausur

Bew. Korrektheit von EXL

Übung, Hausaufgabe oder Klausur

Bew. Korrektheit von EXR

Übung, Hausaufgabe oder Klausur

Beispiel: $\mathcal{I} \models ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$ (PRL)

Wir zeigen:

$$\mathcal{G} \models\!\Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$$

Beispiel: $\mathcal{I} \models ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$ (PRL)

Wir zeigen:

$$\mathcal{G} \models\Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$$

1. Um letztendlich $\Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$ herzuleiten, braucht man IIR. Dies erfordert zuvor die Herleitung von:

$$(\neg p \vee q) \Vdash (p \longrightarrow q) \overset{\text{IIR}}{\vdash} \Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$$

Beispiel: $\mathcal{I} \models ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$ (PRL)

Wir zeigen:

$$\mathcal{G} \models\Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$$

1. Um letztendlich $\Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$ herzuleiten, braucht man IIR. Dies erfordert zuvor die Herleitung von:
$$(\neg p \vee q) \Vdash (p \longrightarrow q) \overset{\text{IIR}}{\vdash} \Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$$
2. Auch dazu bietet sich IIR an. Das erfordert:
$$(\neg p \vee q)\,, p \Vdash q \overset{\text{IIR}}{\vdash} (\neg p \vee q) \Vdash (p \longrightarrow q)$$

Beispiel: $\mathcal{I} \models ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$ (PRL)

Wir zeigen:

$$\mathcal{G} \models\Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$$

1. Um letztendlich $\Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$ herzuleiten, braucht man IIR. Dies erfordert zuvor die Herleitung von:
   $$(\neg p \vee q) \Vdash (p \longrightarrow q) \overset{\text{IIR}}{\vdash} \Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$$
2. Auch dazu bietet sich IIR an. Das erfordert:
   $$(\neg p \vee q)\,, p \Vdash q \overset{\text{IIR}}{\vdash} (\neg p \vee q) \Vdash (p \longrightarrow q)$$
3. Die Disjunktion links wurde offensichtlich mit DIL eingeführt:
   $$\neg p, p \Vdash q \text{ und } q, p \Vdash q \overset{\text{DIL}}{\vdash} (\neg p \vee q)\,, p \Vdash q$$

Beispiel: $\mathcal{I} \models ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$ (PRL)

Wir zeigen:

$$\mathcal{G} \models\Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$$

1. Um letztendlich $\Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$ herzuleiten, braucht man IIR. Dies erfordert zuvor die Herleitung von:
   $$(\neg p \vee q) \Vdash (p \longrightarrow q) \overset{\text{IIR}}{\vdash} \Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$$
2. Auch dazu bietet sich IIR an. Das erfordert:
   $$(\neg p \vee q)\,, p \Vdash q \overset{\text{IIR}}{\vdash} (\neg p \vee q) \Vdash (p \longrightarrow q)$$
3. Die Disjunktion links wurde offensichtlich mit DIL eingeführt:
   $$\neg p, p \Vdash q \text{ und } q, p \Vdash q \overset{\text{DIL}}{\vdash} (\neg p \vee q)\,, p \Vdash q$$
4. (a.) Die Rückführung auf positive Atome erfordert NIL:
   $$\overset{\text{AXM}}{\vdash} p \Vdash p \overset{\text{WKR}}{\vdash} p \Vdash q, p \overset{\text{NIL}}{\vdash} \neg p, p \Vdash q$$

Beispiel: $\mathcal{I} \models ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$ (PRL)

Wir zeigen:

$$\mathcal{G} \models\Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$$

1. Um letztendlich $\Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$ herzuleiten, braucht man IIR. Dies erfordert zuvor die Herleitung von:
   $$(\neg p \vee q) \Vdash (p \longrightarrow q) \overset{\text{IIR}}{\vdash} \Vdash ((\neg p \vee q) \longrightarrow (p \longrightarrow q))$$
2. Auch dazu bietet sich IIR an. Das erfordert:
   $$(\neg p \vee q)\,, p \Vdash q \overset{\text{IIR}}{\vdash} (\neg p \vee q) \Vdash (p \longrightarrow q)$$
3. Die Disjunktion links wurde offensichtlich mit DIL eingeführt:
   $\neg p, p \Vdash q$ und $q, p \Vdash q \overset{\text{DIL}}{\vdash} (\neg p \vee q)\,, p \Vdash q$
4. (a.) Die Rückführung auf positive Atome erfordert NIL:
   $$\overset{\text{AXM}}{\vdash} p \Vdash p \overset{\text{WKR}}{\vdash} p \Vdash q, p \overset{\text{NIL}}{\vdash} \neg p, p \Vdash q$$
   (b.) Es reicht Einführung von q und WKR zum Hinzufügen von q:
   $$\overset{\text{AXM}}{\vdash} p \Vdash p \overset{\text{WKR}}{\vdash} p \Vdash q, p$$

Der sterbliche Sokrates — Ohne Quantoren

Sei $P = \{\mathtt{hum}(\mathtt{skr}), \forall x \colon (\mathtt{hum}(x) \longrightarrow \mathtt{mrt}(x))\}$ und $Q = \{\mathtt{mrt}(\mathtt{skr})\}$.
Zuerst müssen die entsprechenden *atomaren* Formeln her:

$$\overset{\text{AXM}}{\vdash}\mathtt{hum}(\mathtt{skr}) \Vdash \mathtt{hum}(\mathtt{skr}) \text{ und } \overset{\text{AXM}}{\vdash}\mathtt{mrt}(\mathtt{skr}) \Vdash \mathtt{mrt}(\mathtt{skr})$$

Wieder gehen wir rückwärts vor:

$$\mathtt{hum}(\mathtt{skr}), \forall x \colon (\mathtt{hum}(x) \longrightarrow \mathtt{mrt}(x)) \Vdash \mathtt{mrt}(\mathtt{skr})$$

kann nur mit ALL erzeugt werden:

$$\frac{\mathtt{hum}(\mathtt{skr}), (\mathtt{hum}(x) \longrightarrow \mathtt{mrt}(x))\,[x/\mathtt{skr}] \Vdash \mathtt{mrt}(\mathtt{skr})}{\mathtt{hum}(\mathtt{skr}), \forall x \colon (\mathtt{hum}(x) \longrightarrow \mathtt{mrt}(x)) \Vdash \mathtt{mrt}(\mathtt{skr})}\ \text{ALL}$$

So daß $\mathtt{hum}(\mathtt{skr}), (\mathtt{hum}(\mathtt{skr}) \longrightarrow \mathtt{mrt}(\mathtt{skr})) \Vdash \mathtt{mrt}(\mathtt{skr})$ herzuleiten bleibt (IIL).

Der sterbliche Sokrates — Ohne Quantoren

$$\frac{q, P \Vdash Q \qquad R \Vdash S, p}{P, R, (p \longrightarrow q) \Vdash Q, S} \quad \leftrightarrow \quad \frac{q, P \Vdash Q \qquad R \Vdash S, p}{\underbrace{\mathtt{hum}(\mathtt{skr})}_{P=R}, (\underbrace{\mathtt{hum}(\mathtt{skr})}_{p} \longrightarrow \underbrace{\mathtt{mrt}(\mathtt{skr})}_{q}) \Vdash \underbrace{\mathtt{mrt}(\mathtt{skr})}_{S=Q}}$$

Eingesetzt müssen also abgeleitet werden (mit $\textsc{wk}x$):

$$\frac{\mathtt{mrt}(\mathtt{skr}) \Vdash \mathtt{mrt}(\mathtt{skr})}{\underbrace{\mathtt{mrt}(\mathtt{skr})}_{q}, \underbrace{\mathtt{hum}(\mathtt{skr})}_{P} \Vdash \underbrace{\mathtt{mrt}(\mathtt{skr})}_{Q}} \quad \text{und} \quad \frac{\mathtt{hum}(\mathtt{skr}) \Vdash \mathtt{hum}(\mathtt{skr})}{\underbrace{\mathtt{hum}(\mathtt{skr})}_{R} \Vdash \underbrace{\mathtt{mrt}(\mathtt{skr})}_{S}, \underbrace{\mathtt{hum}(\mathtt{skr})}_{p}}$$

Diese Sequenzen haben wir direkt zu Beginn per Axiom AXM erzeugt.
Man beachte, daß die Herleitung nicht wie wegen MP durch CUT sondern durch IIL gelingt.

Beispiel: Ein **LK**-Beweis für DUA

Zu zeigen sei: $\exists x\colon \neg \mathtt{p}(x) \Longrightarrow \neg\forall x\colon \mathtt{p}(x)$.

Ax_1	$\mathtt{p}(\mathtt{a})$	$\Vdash$	$\mathtt{p}(\mathtt{a})$	AXM
1		$\Vdash$		
2		$\Vdash$		
3		$\Vdash$		
4		$\Vdash$		
5	$\exists x\colon \neg\mathtt{p}(x)$	$\Vdash$	$\neg\forall x\colon \mathtt{p}(x)$	

Beispiel: Ein **LK**-Beweis für DUA

Zu zeigen sei: $\exists x : \neg \mathtt{p}(x) \Longrightarrow \neg \forall x : \mathtt{p}(x)$.

Ax_1	$\mathtt{p}(\mathtt{a})$	$\Vdash$	$\mathtt{p}(\mathtt{a})$	AXM
1		$\Vdash$		
2		$\Vdash$		
3		$\Vdash$		
4	$\neg \mathtt{p}(\mathtt{a})$	$\Vdash$	$\neg \forall x : \mathtt{p}(x)$	
5	$\exists x : \neg \mathtt{p}(x)$	$\Vdash$	$\neg \forall x : \mathtt{p}(x)$	EXL(4)

Beispiel: Ein **LK**-Beweis für DUA

Zu zeigen sei: $\exists x\colon \neg\mathtt{p}(x) \Longrightarrow \neg\forall x\colon \mathtt{p}(x)$.

Ax_1	$\mathtt{p(a)}$	$\Vdash$	$\mathtt{p(a)}$	$\textsc{axm}$
1	$\forall x\colon \mathtt{p}(x)$	$\Vdash$	$\mathtt{p(a)}$	$\textsc{all}(\mathrm{Ax}_1)$
2		$\Vdash$		
3		$\Vdash$		
4	$\neg\mathtt{p(a)}$	$\Vdash$	$\neg\forall x\colon \mathtt{p}(x)$	
5	$\exists x\colon \neg\mathtt{p}(x)$	$\Vdash$	$\neg\forall x\colon \mathtt{p}(x)$	$\textsc{exl}(4)$

Beispiel: Ein **LK**-Beweis für DUA

Zu zeigen sei: $\exists x\colon \neg \mathtt{p}(x) \Longrightarrow \neg\forall x\colon \mathtt{p}(x)$.

Ax_1	$\mathtt{p}(\mathtt{a})$	$\Vdash$	$\mathtt{p}(\mathtt{a})$	AXM
1	$\forall x\colon \mathtt{p}(x)$	$\Vdash$	$\mathtt{p}(\mathtt{a})$	ALL(Ax_1)
2	$\neg\mathtt{p}(\mathtt{a}), \forall x\colon \mathtt{p}(x)$	$\Vdash$		NIL(1)
3		$\Vdash$		
4	$\neg\mathtt{p}(\mathtt{a})$	$\Vdash$	$\neg\forall x\colon \mathtt{p}(x)$	
5	$\exists x\colon \neg\mathtt{p}(x)$	$\Vdash$	$\neg\forall x\colon \mathtt{p}(x)$	EXL(4)

Beispiel: Ein **LK**-Beweis für DUA

Zu zeigen sei: $\exists x\colon \neg \mathtt{p}(x) \Longrightarrow \neg\forall x\colon \mathtt{p}(x)$.

Ax_1	$\mathtt{p}(\mathtt{a})$	$\Vdash$	$\mathtt{p}(\mathtt{a})$	$\textsc{axm}$
1	$\forall x\colon \mathtt{p}(x)$	$\Vdash$	$\mathtt{p}(\mathtt{a})$	$\textsc{all}(\mathrm{Ax}_1)$
2	$\neg\mathtt{p}(\mathtt{a}), \forall x\colon \mathtt{p}(x)$	$\Vdash$		$\textsc{nil}(1)$
3	$\forall x\colon \mathtt{p}(x), \neg\mathtt{p}(\mathtt{a})$	$\Vdash$		$\textsc{chl}(2)$
4	$\neg\mathtt{p}(\mathtt{a})$	$\Vdash$	$\neg\forall x\colon \mathtt{p}(x)$	$\textsc{nir}(3)$
5	$\exists x\colon \neg\mathtt{p}(x)$	$\Vdash$	$\neg\forall x\colon \mathtt{p}(x)$	$\textsc{exl}(4)$

Der sterbliche Sokrates

$$\mathcal{G} \models \forall x\colon (\texttt{hum}(x) \longrightarrow \texttt{mrt}(x)), \texttt{hum}(\texttt{skr}) \Vdash \texttt{mrt}(\texttt{skr})$$

Darstellung als invertierter "Baum":

$$\begin{array}{c|c}
\multicolumn{2}{c}{\forall x\colon (\texttt{hum}(x) \longrightarrow \texttt{mrt}(x)), \texttt{hum}(\texttt{skr}) \Vdash \texttt{mrt}(\texttt{skr})} \\
\hline
\multicolumn{2}{c}{(\texttt{hum}(\texttt{skr}) \longrightarrow \texttt{mrt}(\texttt{skr})), \texttt{hum}(\texttt{skr}) \Vdash \texttt{mrt}(\texttt{skr})} \\
\hline
\texttt{hum}(\texttt{skr}) \Vdash \texttt{mrt}(\texttt{skr}), \texttt{hum}(\texttt{skr}) & \texttt{hum}(\texttt{skr}) \Vdash \texttt{mrt}(\texttt{skr}), \texttt{hum}(\texttt{skr}) \\
\hline
\texttt{hum}(\texttt{skr}) \Vdash \texttt{hum}(\texttt{skr}) & \texttt{hum}(\texttt{skr}) \Vdash \texttt{hum}(\texttt{skr}) \\
\hline
 &
\end{array}$$

Sequenzenkalkül - Quellen & Theorembeweiser

Literatur

- Bücher, Skripte, etc.
  1. Ebbinghaus/Flum/Thomas, *Mathematical Logic*, Springer, 1994.
  2. Ben-Ari, *Mathematical Logic for Computer Science*, 3rd ed., Springer, 2012.
- Online Tutorials
  - `http://logitext.mit.edu/tutorial`
  - `http://sakharov.net/sequent.html`

Online Theorembeweiser

1. Sequenzenkalkül für PRL: `https://www.nayuki.io/page/propositional-sequent-calculus-prover`

10.3
LITERATUR ZUR PRL/FOL **SEMANTIK**

FOL-Semantik in der Literatur

Die FOL-Semantik ist prinzipiell festgelegt und überall gleich

Dennoch gibt es viele verschiedene Notationen und kleine Unterschiede in der Auslegung der Begrifflichkeiten "Modell", "Interpretation", "Erfüllung", "Gültigkeit", "Wahrheit", usw.

Konvention

1. Eine *Interpretation* ist ein Vorgang. $\mathcal{I} : \Sigma \to \mathfrak{A}$ *interpretiert* die Symbole aus Σ als Objekte, Relationen und Funktionen aus und auf $\mathcal{U}$.
2. Eine Interpretation legt implizit ein pot. Modell $\mathfrak{A}$ fest und wird durch α in $\mathcal{E}$ parametrisiert.
3. $\mathfrak{A}$ hat die *Modelleigenschaft*, wenn sie bzgl. $\mathcal{I}$ *Erfüllungseigenschaften* der interpretierten Formeln aufweist.

Konkordanztabelle

Literatur

1. Schöning, *Logik für Informatiker*, BI, 1989.
2. Rautenberg, *Einführung in die Mathematische Logik*, Vieweg+Teubner, 2008 (1996).
3. Ebbinghaus, Flum, Thomas, *Mathematical Logic* (2 ed.), Springer, 1994
4. Sperschneider, Antoniou, *Logic. A foundation for Computer Science*, Addison-Wesley, 1991.
5. Ben-Ari, *Mathematical Logic for Computer Science* (3 ed.), Springer, 2012 (Prentice-Hall, 1993).
6. Enderton, *A Mathematical Introduction to Logic*, AP, 2001 (1972).
7. Huth, Ryan, *Logic in Computer Science*", CUP, 2002 (2000).

Konkordanztabelle Bezeichnungen/Notationen

	Symbole, Notation						Signatur	Σ-Algebra
	x	t	p	P	$\mathtt{p}$	$\mathtt{f}$	Σ	$\mathfrak{A}$, $\mathfrak{A}$, $\mathfrak{H}$
1.	x	t	F		P	f	"zu F passende ...	... Struktur $\mathcal{A}$"
2.	x	t	φ	X		f	L bestimmt $\mathcal{L}$	$\mathcal{L}$-Struktur $\mathcal{A}$
3.	x, v	t	φ	Φ			S determines FOL	S-structure $\mathfrak{A}$
4.	X	t	φ	M	p	f	Σ	$\boldsymbol{A}$
5.	x	t	A	U	p	f	$\mathcal{P}, \mathcal{A}, \mathcal{V}$	$\mathcal{I}_A$
6.	x	t	α		p	f		structure $\mathfrak{A}$

3.: $\mathfrak{A} = (A, \mathfrak{a})$

4.: $\boldsymbol{A}$ genannt Σ-*interpretation* oder Σ-*algebra*

5.: $\mathcal{I}_A = \left(D, \{R_i\}_m, \{F_i^{n_i}\}_l, \{d_j\}_k\right)$ genannt *Interpretation*.

Konkordanztabelle Bezeichnungen/Notationen

	Domäne* $\mathcal{U}$	Termsubst. $\sigma = [x/t]$	Belegung $\alpha : \mathrm{Var} \to \mathcal{U}$	α-Substitution $\alpha \langle x \leftarrow\!\shortmid a \rangle$
1.	Grundmenge $U_{\mathcal{A}}$	$sub = [x/t]$	$I_{\mathcal{A}}$	$\mathcal{A}_{[x/a]}$
2.	Träger A	$\frac{t}{x}$	w	w^a_x
3.	domain A	$\frac{t}{x}$	β	$\beta\frac{a}{x}$
4.	domain $\mathrm{dom}(\boldsymbol{A})$	$\sigma = \{X/t\}$	sta	$\mathrm{sta}(X/a)$
5.	domain D	$\theta = \{x \leftarrow t\}$	$\sigma_{\mathcal{I}_A}$	$\sigma_{\mathcal{I}_A}[x \leftarrow d]$
6.	universe $\vert\mathfrak{A}\vert$	α^x_t	s	$s(x \vert d)$

1.: $U_{\mathcal{A}}$ auch: Grundbereich, Individuenbereich, Universum

6.: $|\mathfrak{A}|$ auch: *domain*

* Wir verwenden den Begriff *Domäne* für das Universum einer einsortigen Signatur; also der Trägermenge der Σ-Algebra $\mathfrak{A}$.

Konkordanztabelle Bezeichnungen/Notationen

	Termauswertung	Wahr-/Gültigkeit*
	$\mathcal{E}^{\alpha}_{(\mathfrak{A})}.t$ bzw. t'	$\mathcal{I}^{(\alpha)}_{(\mathfrak{A})}.p \quad :\Longleftrightarrow \quad \mathcal{I}^{\alpha}_{(\mathfrak{A})}.p = \mathbf{1}$
1.	$\mathcal{A}(t)$	$\mathcal{A}(F)$
2.	$t^{\mathcal{M}}$	$\mathcal{M} \models \varphi$ oder $\mathcal{A} \models \varphi[w]$
3.	$\mathfrak{I}(t) = t^{\mathfrak{A}}$	$\mathfrak{I} \models \varphi$
4.	$\mathrm{val}_{\boldsymbol{A},\mathrm{sta}}(\mathrm{t})$	$\boldsymbol{A} \models_{(\mathrm{sta})} \varphi$
5.	$\mathcal{D}_{\mathcal{I}}(t)$	$\mathcal{I} \models A \quad :\Longleftrightarrow \quad v_{\mathcal{I}}(A) = T$
6.	$\bar{s}(t)$	$\models_{\mathfrak{A}} \varphi[s]$

$^{*)}$. $p' \quad :\Longleftrightarrow \quad \mathcal{I}^{\alpha}_{\mathfrak{A}}.p$

2. $\mathcal{M} = (\mathcal{A}, w)$ Modell für φ (in $\mathcal{A}$ unter w).

$\models$ heißt *Modellrelation* oder *satisfaction relation*.

Konkordanztabelle Bezeichnungen/Notationen

1.

2. a. $\mathcal{M}$ erfüllt φ gdw. $\mathcal{M}$ ist ein Modell für φ gdw. $\mathcal{M} \models \varphi$. $^{(*)}$
   b. $\mathcal{A}$ erfüllt φ gdw. in $\mathcal{A}$ gilt φ gdw. $\mathcal{M} \models \varphi$ für alle w.

3. a. $\mathfrak{I}$ is a model of φ gdw. $\mathfrak{I}$ satisfies φ gdw. φ holds in $\mathfrak{I}$ gdw. $\mathfrak{I} \models \varphi$. $^{(**)}$
   b. ... for all interpretations ...$^{(**)}$

4. a. φ is valid in $\boldsymbol{A}$ in state sta : $\boldsymbol{A} \models_{\mathrm{sta}} \varphi$
   b. $\boldsymbol{A}$ is a model of φ, $\boldsymbol{A} \models \varphi$ iff $\boldsymbol{A} \models_{\mathrm{sta}} \varphi$ for all φ is valid in $\boldsymbol{A}$ in state sta.

5. a. A is true under $\mathcal{I}_A$ and σ_{I_A} iff $v_{\sigma_{\mathcal{I}_A}}(A) = T$.
   b. **For closed** A**,** $v_{\sigma_{\mathcal{I}_A}} = v_{\mathcal{I}}$**:** A is true in $\mathcal{I}$ gdw. $\mathcal{I}$ is a model for A gdw. $v_{\mathcal{I}}(A) = T$, Notation: $\mathcal{I} \models A$.

6. a. $\mathfrak{A}$ satisfies φ with s gdw. $\models_{\mathfrak{A}} \varphi[s]$.
   b. $\mathfrak{A}$ is a model of p *oder* φ is true in $\mathfrak{A}$ gdw. $\models_{\mathfrak{A}} \varphi$

$^{(*)}$ Belegung w ist in $\mathcal{M}$ integriert festgelegt. $^{(**)}$ Belegung β ist in $\mathfrak{I}$ integriert festgelegt.