Formale Grundlagen der Informatik II
SS 2009

Prof. Dr. Ulrich Kohlenbach
TUD, Fachbereich Mathematik

Inhaltsübersicht

1) **Aussagenlogik AL**
   - Syntax und Semantik der AL
   - Wahrheitsfunktionen („Boolesche" Funktionen)
   - Maximal konsistente Satzmengen und aussagenlogische Vollständigkeit
   - Kompaktheitssatz für AL
   - Beweiskalküle
2) **Prädikatenlogik der 1. Stufe (FO)**
   - Sprache von FO
   - Strukturen und Interpretationen („Modelle")
   - Pränex-, Skolem- und Herbrand-Normalformen

- Beweiskalküle für FO
- Vollständigkeit, Kompaktheit, Satz von Löwenheim-Skolem

3) **Optionale Themen**

- Logik der 2. Stufe
- Algorithmische Aspekte: Satz von Herbrand, Unifikation, Beweiskomplexität, Unentscheidbarkeit
- Konstruktive („intuitionistische") Logik

Literatur

- **Skript von Prof. Dr. M. Otto (SS 2008)**
- **Ebbinghaus, Flum, Thomas: Einführung in die mathematische Logik**, Spektrum 98.
- **U. Schöning: Logik für Informatiker**, Spektrum 2000.

Teil 1: Aussagenlogik, AL

- **Gegenstandsbereich:** Verknüpfungen elementarer Aussagen mittels Boolescher logischer Verknüpfungen.
- **Boolesche Verknüpfungen (Junktoren):** $\neg, \wedge, \vee, \rightarrow, \ldots$
- **Formalisierung komplexerer Eigenschaften**
- **Wahrheitsfunktionale Semantik**
- **Korrekte und vollständige Beweiskalküle**

Syntax der Aussagenlogik AL

Symbole der Sprache: Wahrheitswerte: $0, 1$;

Aussagenvariablen $p, q, r, \ldots, p_1, p_2, \ldots$;

Logische Verknüpfungen: $\neg, \wedge, \vee, \ldots$; Hilfssymbole: $(,)$.

Aussagenlogische Formeln: $\mathrm{AL}(\mathcal{V})$, die Menge der AL-Formeln über einer AL-Variablenmenge $\mathcal{V}$, wird induktiv erzeugt:

atomare Formeln:	0, 1, p in $\mathrm{AL}(\mathcal{V})$ (wobei $p \in \mathcal{V}$).
Negation:	für $\varphi \in \mathrm{AL}(\mathcal{V})$ ist auch $\neg\varphi \in \mathrm{AL}(\mathcal{V})$.
Konjunktion:	für $\varphi, \psi \in \mathrm{AL}(\mathcal{V})$ ist auch $(\varphi \wedge \psi) \in \mathrm{AL}(\mathcal{V})$.
Disjunktion:	für $\varphi, \psi \in \mathrm{AL}(\mathcal{V})$ ist auch $(\varphi \vee \psi) \in \mathrm{AL}(\mathcal{V})$.

Weitere Junktoren (offiziell als Abkürzungen)

z.B. $(\varphi \to \psi) \;:=\; (\neg\varphi \vee \psi)$,

$(\varphi \leftrightarrow \psi) \;:=\; \big((\neg\varphi \wedge \neg\psi) \vee (\varphi \wedge \psi)\big)$.

Meistens: abzählbar unendlich viele Variablen

$$\mathcal{V} = \{p_i : i \geqslant 1\}.$$

Manchmal auch **endliche** Variablenmenge

$$\mathcal{V}_n = \{p_i : 1 \leqslant i \leqslant n\}.$$

Semantik der Aussagenlogik AL

Interpretationen: von **Belegungen** der AL-Variablen zu **Wahrheitswerten** für AL-Formeln $\mathbb{B} = \{0, 1\}$.

$\mathcal{V}$-Interpretation (Belegung):

$$\begin{array}{rcl} \mathfrak{I}\colon \mathcal{V} & \longrightarrow & \mathbb{B} \\ p & \longmapsto & \mathfrak{I}(p) \end{array}$$

$\mathfrak{I}$ interpretiert p als

- "wahr" wenn $\mathfrak{I}(p) = 1$,
- "falsch" wenn $\mathfrak{I}(p) = 0$.

Definition der Semantik von komplexen Formeln

über geg. $\mathcal{V}$-Interpretation $\mathfrak{I}$:

Wahrheitswertfunktion

$$\begin{array}{rcl} {}^{\mathfrak{I}}\colon \mathrm{AL}(\mathcal{V}) & \longrightarrow & \mathbb{B} \\ \varphi & \longmapsto & \varphi^{\mathfrak{I}} \end{array}$$

induktiv über den Aufbau der Formeln $\varphi \in \mathrm{AL}(\mathcal{V})$ definiert bzgl. einer $\mathcal{V}$-Interpretation $\mathfrak{I}$:

atomare Formeln:	$0^{\mathfrak{I}} := 0;\ 1^{\mathfrak{I}} := 1;\ p^{\mathfrak{I}} := \mathfrak{I}(p).$
Negation:	$(\neg\varphi)^{\mathfrak{I}} := 1 - \varphi^{\mathfrak{I}}.$
Konjunktion:	$(\varphi \wedge \psi)^{\mathfrak{I}} := \min(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}}).$
Disjunktion:	$(\varphi \vee \psi)^{\mathfrak{I}} := \max(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}}).$

Modellbegriff

$\mathfrak{I}$ **erfüllt** φ gdw. $\varphi^{\mathfrak{I}} = 1$.

Schreibweise: $\mathfrak{I} \models \varphi$.

Sprechweisen: $\mathfrak{I}$ **erfüllt** φ,

$\mathfrak{I}$ **ist Modell von** φ,

φ **ist wahr unter** $\mathfrak{I}$.

Für **Formelmengen** $\Phi \subseteq \mathrm{AL}(\mathcal{V})$ entsprechend:

$\mathfrak{I} \models \Phi$ gdw. $\mathfrak{I} \models \varphi$ **für alle** $\varphi \in \Phi$.

Semantik und Wahrheitstafeln

Für $\varphi \in \mathrm{AL}_n$ schreiben wir auch $\varphi = \varphi(p_1, \ldots, p_n)$

für $(b_1, \ldots, b_n) \in \mathbb{B}^n$ sei

$$\varphi[b_1, \ldots, b_n] := \begin{cases} \varphi^{\mathfrak{I}} \text{ für Interpretation } \mathfrak{I} \\ \text{mit } (\mathfrak{I}(p_i) = b_i)_{i=1,\ldots,n} \end{cases}$$

der Wahrheitswert von φ auf $(b_1, \ldots, b_n)$.

Wahrheitstafeln: die Wertetabelle der Funktion

$$\begin{array}{ccc} \mathbb{B}^n & \longrightarrow & \mathbb{B} \\ (b_1, \ldots, b_n) & \longmapsto & \varphi[b_1, \ldots, b_n] \end{array}$$

bestimmt die Semantik von φ vollständig!

p	$\neg p$
0	1
1	0

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Grundlegende semantische Begriffe

Folgerungsbeziehung für $\varphi, \psi \in \mathrm{AL}(\mathcal{V})$

$$\varphi \models \psi,$$

in Worten

„ψ folgt aus φ",

ist definiert als: für **alle** $\mathcal{V}$-Interpretationen $\mathfrak{I}$ gilt:

$$\mathfrak{I} \models \varphi \;\Rightarrow\; \mathfrak{I} \models \psi.$$

Entsprechend $\Phi \models \psi$ für Formelmengen Φ.

Allgemeingültigkeit:

$\varphi \in \mathrm{AL}(\mathcal{V})$ ist **allgemeingültig** (in Zeichen: $\models \varphi$), wenn für **alle** $\mathcal{V}$-Interpretationen $\mathfrak{I}$ gilt:

$$\mathfrak{I} \models \varphi.$$

Beispiele

$\varphi \models \varphi \vee \psi, \quad \models \varphi \vee \neg\varphi, \quad \varphi \models (\varphi \wedge \psi) \vee (\varphi \wedge \neg\psi).$

Logische Äquivalenz:

$\varphi, \psi \in \mathrm{AL}(\mathcal{V})$ **logisch äquivalent** (in Zeichen: $\varphi \equiv \psi$), wenn für **alle** $\mathcal{V}$-Interpretationen $\mathfrak{I}$ gilt:

$$\mathfrak{I} \models \varphi \text{ gdw. } \mathfrak{I} \models \psi.$$

Schreibweise: $\varphi \equiv \psi$.

Sämtlich äquivalent: $\varphi \equiv \psi$

$\models \varphi \leftrightarrow \psi$

$\varphi \models \psi$ und $\psi \models \varphi$

Beispiele (vgl. Identitäten in Booleschen Algebren)

$\neg\neg p \equiv p, \quad p \vee 0 \equiv p, \quad p \wedge 0 \equiv 0, \quad \ldots$

$p \vee q \equiv q \vee p, \quad (p \vee q) \vee r \equiv p \vee (q \vee r), \quad \ldots$

$(p \vee q) \equiv \neg(\neg p \wedge \neg q), \quad (p \wedge q) \equiv \neg(\neg p \vee \neg q)$

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r), \quad p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

Erfüllbarkeit

$\varphi \in \mathrm{AL}(\mathcal{V})$ ist **erfüllbar**, wenn es *mindestens eine* $\mathcal{V}$-Interpretation $\mathfrak{I}$ **gibt** mit $\mathfrak{I} \models \varphi$.

Analog für Formelmengen $\Phi \subseteq \mathrm{AL}$:

Φ erfüllbar, wenn $\mathfrak{I} \models \Phi$ für mindestens ein $\mathfrak{I}$.

Also:

φ erfüllbar gdw. $\neg\varphi$ nicht allgemeingültig.

Zentrale Rolle der Erfüllbarkeit (SAT)

- $\models \varphi$ gdw. $\neg\varphi$ **nicht** erfüllbar.
- $\varphi \models \psi$ gdw. $\varphi \wedge \neg\psi$ **nicht** erfüllbar.
- $\Phi \models \psi$ gdw. $\Phi \cup \{\neg\psi\}$ **nicht** erfüllbar.
- $\varphi \equiv \psi$ gdw. **weder** $\varphi \wedge \neg\psi$ **noch** $\neg\varphi \wedge \psi$ erfüllbar.

Satz: $\mathrm{SAT(AL)} = \{\varphi \in \mathrm{AL} : \varphi \text{ erfüllbar } \}$ ist **entscheidbar**.

Beweis: Teste alle endlich vielen Belegungen der AL-Variablen.

Genauer: bei n Aussagenvariablen sind 2^n-viele Belegungen zu betrachten.

AL und Boolesche Funktionen

$\mathcal{B}_n$ die Menge aller n-stelligen Booleschen Funktionen

$$\begin{array}{rcl} f : \mathbb{B}^n & \longrightarrow & \mathbb{B} \\ (b_1, \ldots, b_n) & \longmapsto & f(b_1, \ldots, b_n) \end{array}$$

für $\varphi \in \mathrm{AL}_n$:

$$\left.\begin{array}{rcl} f_\varphi : \mathbb{B}^n & \longrightarrow & \mathbb{B} \\ (b_1, \ldots, b_n) & \longmapsto & \varphi[b_1, \ldots, b_n] \end{array}\right\} \in \mathcal{B}_n$$

Bemerkung: $f_\varphi = f_\psi$ gdw. $\varphi \equiv \psi$

Also: $\mathrm{AL}_n / \equiv \longrightarrow \mathcal{B}_n$ injektiv!

$$\begin{array}{rcl} [\varphi]_\equiv & \longmapsto & f_\varphi \end{array}$$

Fragen

- **Wieviele** n-stellige Boolesche Funktionen gibt es, d.h. was ist die Kardinalität von $\mathcal{B}_n$?
- Ist **jedes** $f \in \mathcal{B}_n$ durch eine AL-Formel $\varphi \in \mathrm{AL}_n$ darstellbar, d.h. ist $[\varphi]_{\equiv} \longmapsto f_\varphi$ **surjektiv**?

Die Antwort auf die erste Frage ist einfach: $|\mathcal{B}_n| = 2^{2^n}$.

Die zweite Frage ist schwieriger zu beantworten.

Disjunktive und konjunktive Normalformen

Nomenklatur: p bzw. $\neg p$ (für $p \in \mathcal{V}$) heißen **Literale**

Disjunktionen von Konjunktionen von Literalen: **DNF-Formeln**

Konjunktionen von Disjunktionen von Literalen: **KNF-Formeln**

Konvention: auch **leere** Disjunktionen/Konjunktionen zulässig, wobei $\bigvee \emptyset \equiv 0$ und $\bigwedge \emptyset \equiv 1$.

Satz (Funktionale Vollständigkeit): Zu jeder Funktion $f \in \mathcal{B}_n$ existiert eine DNF-Formel $\varphi \in \mathrm{AL}_n$ mit $f = f_\varphi$.

Korollar: Zu jedem $\varphi \in \mathrm{AL}_n$ existieren:
DNF-Formel $\varphi_1 \in \mathrm{AL}_n$ mit $\varphi_1 \equiv \varphi$ und KNF-Formel $\varphi_2 \in \mathrm{AL}_n$ mit $\varphi_2 \equiv \varphi$.

Dualität von Konjunktion und Disjunktion

Nützliche Umformungen/Rechenregeln:

$$\neg(\varphi_1 \wedge \varphi_2) \equiv \neg\varphi_1 \vee \neg\varphi_2$$

verallgemeinert zu

$$\neg\Big(\bigwedge \Phi\Big) \equiv \bigvee \Phi^{\neg}, \text{ wobei } \Phi^{\neg} := \big\{\neg\varphi \colon \varphi \in \Phi\big\}.$$

Analog:

$$\neg\Big(\bigvee \Phi\Big) \equiv \bigwedge \Phi^{\neg}.$$

Für KNF $\longleftrightarrow$ DNF (modulo Streichung doppelter Negationen):

$$\neg \underbrace{\bigwedge_{i=1}^{k} \left(\bigvee C_i\right)}_{\text{KNF}} \equiv \underbrace{\bigvee_{i=1}^{k} \left(\bigwedge C_i^{\neg}\right)}_{\text{DNF}^*},$$

wobei $C_1, \ldots, C_k$ (endl.) Mengen von Literalen.

Beispiel für exponentiellen "blow-up"

$\varphi_m = \varphi_m(p_1, \ldots, p_{2m}) := \bigwedge_{i=1}^{m} \neg(p_{2i-1} \leftrightarrow p_{2i}) \qquad \in \mathrm{AL}_{2m}$

- φ_m hat genau 2^m erfüllende Interpretationen in $\mathbb{B}^{2m}$, und:
- KNF von Länge $\sim m$ (linear in m):

  $\varphi_m \equiv \bigwedge_{i=1}^{m} \big((p_{2i-1} \vee p_{2i}) \wedge (\neg p_{2i-1} \vee \neg p_{2i})\big)$

- DNF in Länge $\sim 2m2^m$ (exponentiell in m):

  $\varphi_m \equiv \bigvee \big\{ \varphi_{\mathbf{b}} \colon \mathbf{b} \in \mathbb{B}^{2m}, \varphi_m[\mathbf{b}] = 1 \big\}$

- keine kürzere DNF: { keine kürzeren Disjunktionsglieder! / keine redundanten Disjunktionsglieder!

Vollständige Systeme von Junktoren

Satz: Für $n \geq 1$ ist jede Funktion in $\mathcal{B}_n$ darstellbar durch eine AL_n-Formeln, die nur die Junktoren $\neg$ und $\wedge$ (nur $\neg$ und $\vee$) benutzt.

Beweis: Starte mit Formel in KNF/DNF und eliminiere $\vee$ oder $\wedge$ mit $\varphi_1 \vee \varphi_2 \equiv \neg(\neg\varphi_1 \wedge \neg\varphi_2)$, $\varphi_1 \wedge \varphi_2 \equiv \neg(\neg\varphi_1 \vee \neg\varphi_2)$.

Systeme von Junktoren (Booleschen Funktionen) mit dieser Eigenschaft heißen **vollständig**.

Beispiele vollständiger Systeme

- $|$ mit der Definition $p \mid q := \neg(p \wedge q)$ (NAND; „Sheffer stroke"): benutze z.B.: $\neg p \equiv p \mid p$;
  $p \wedge q \equiv \neg(p \mid q) \equiv (p \mid q) \,\big|\, (p \mid q)$.
- $\rightarrow$ zusammen mit 0 : benutze z.B.: $\neg p \equiv p \rightarrow 0$;
  $p \vee q \equiv \neg p \rightarrow q \equiv (p \rightarrow 0) \rightarrow q$.

Nicht vollständig sind z.B.: $\{\wedge, \vee\}$ (Monotonie);

$\{\rightarrow\}$ ($0 \in \mathcal{B}_n$ nicht darstellbar).

Aussagenlogischer Kompaktheitssatz (Endlichkeitssatz)

Theorem: Eine beliebige Formelmenge Φ ist genau dann erfüllbar, wenn jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ erfüllbar ist.

Äquivalente Formulierung:

$$\Phi \models \psi \text{ gdw. } \Phi_0 \models \psi \text{ für ein endliches } \Phi_0 \subseteq \Phi$$

(wobei $\Phi \subseteq \mathrm{AL}, \psi \in \mathrm{AL}$).

Korollar: Unerfüllbarkeit einer unendlichen Formelmenge lässt sich durch ein endliches Zertifikat nachweisen.

Beweis des Kompaktheitssatzes

Abzählbarer Fall: $\Phi \subseteq \mathrm{AL}(\mathcal{V})$, $\mathcal{V} = \{p_i : i \geq 1\}$

Sei jedes endliche $\Phi_0 \subseteq \Phi$ erfüllbar.

Konstruiere induktiv $\mathfrak{I}_0, \mathfrak{I}_1, \mathfrak{I}_2, \ldots$ so, dass:

- $\mathfrak{I}_n$ eine $\mathcal{V}_n$-Interpretation.
- $\mathfrak{I}_{n+1}$ verträglich mit $\mathfrak{I}_n$: $\mathfrak{I}_{n+1}(p_i) = \mathfrak{I}_n(p_i)$ für $1 \leq i \leq n$.
- alle endlichen $\Phi_0 \subseteq \Phi$ erfüllbar durch mit $\mathfrak{I}_n$ verträgliche $\mathfrak{I}$.

Dann ist $\mathfrak{I} \models \Phi$ für die Interpretation

$$\begin{array}{rcl} \mathfrak{I} : \mathcal{V} & \longrightarrow & \mathbb{B} \\ p_n & \longmapsto & \mathfrak{I}_n(p_n) \end{array}$$

Übergang von $\mathfrak{I}_n$ zu $\mathfrak{I}_{n+1}$

Nach Voraussetzung ist jedes endliche Φ_0 mit einer mit $\mathfrak{I}_n$ verträglichen Interpretation $\mathfrak{I}$ erfüllbar. Sei $\mathfrak{I}^0_{n+1}$ (bzw. $\mathfrak{I}^1_{n+1}$) die Fortsetzung von $\mathfrak{I}_n$ mit $\mathfrak{I}^0_{n+1}(p_{n+1}) = 0$ (bzw. $\mathfrak{I}^1_{n+1}(p_{n+1}) = 1$). Annahme: für $i \in \{0, 1\}$ existiert endliches $\Phi^i \subseteq \Phi$, das von keiner mit $\mathfrak{I}^i_{n+1}$ verträglichen Interpretation erfüllt wird. Dann wird $\Phi^0 \cup \Phi^1$ von keiner mit $\mathfrak{I}_n$ verträglichen Interpretation erfüllt. Widerspruch!

Beweisprinzip: Lemma von König, d.h. jeder unendliche endlich verzweigte Baum hat einen unendlichen Pfaden.

Konsequenzen des Kompaktheitssatzes

- Lemma von König.
- Ein Graph ist genau dann k-färbbar, wenn jeder endliche Teilgraph k-färbbar ist.
- Ein endliches Domino-System erlaubt genau dann eine Parkettierung der Ebene, wenn sich beliebig große endliche Quadrate parkettieren lassen.

Logikkalküle: Deduktion und Refutation

Logikkalküle: syntaktische Definition **formaler Beweise.**

Formale Beweise: syntaktische Zeichenketten, einfach nachprüfbaren syntaktischen Regeln aufgebaut (Regelsystem: Kalkül).

Ableitung: Erzeugung von (regelkonformen) formalen Beweisen.

Korrespondenz mit Semantik:

- **Korrektheit:** nur semantisch korrekte Sachverhalte sind formal beweisbar.
- **Vollständigkeit:** jeder semantisch korrekte Sachverhalt ist formal beweisbar.

Typen von vollständigen Kalkülen

- **Deduktionskalküle** für alle allgemeingültigen AL-Formeln: Hilbert-Systeme, Sequenzenkalkül.
- **Widerlegungskalkül** für alle unerfüllbaren KNF-Formeln.

Hilbertkalküle

Hilbertkalküle werden durch Angabe von **Axiomen** und **Schlussregeln** bestimmt. Beweise sind endliche Bäume, deren Blätter Axiome und deren Knoten Regelanwendungen sind. Die Wurzel ist die bewiesene Aussage.

Beispiel (Shoenfield 1967) (für das System $\neg, \vee$):

Axiome: alle Aussagen der Form $\neg\varphi \vee \varphi$

Regeln: $\dfrac{\varphi}{\psi \vee \varphi}$, $\dfrac{\varphi \vee \varphi}{\varphi}$, $\dfrac{\varphi \vee (\psi \vee \chi)}{(\varphi \vee \psi) \vee \chi}$, $\dfrac{\varphi \vee \psi \ , \ \neg\varphi \vee \chi}{\psi \vee \chi}$.

$\Phi \vdash \psi$ („Φ beweist ψ"), falls es einen Beweisbaum gibt, dessen Blätter Axiome oder Aussagen in Φ sind und dessen Wurzel ψ ist.

KNF in Klauselform

KNF: Konjunktionen von Disjunktionen von Literalen.

Notation: L für Literal; $\overline{L}$ für komplementäres Literal; $\overline{L} \equiv \neg L$.

Klauseln C: endliche Menge von Literalen. $C = \{L_1, \ldots, L_k\}$ steht dabei für $\bigvee C \equiv L_1 \vee \ldots \vee L_k$.

Bemerkung:

- $\square$ steht für die leere Klausel.
- $\square \equiv \bigvee \emptyset \equiv 0$.

Klauselmengen (endlich): $K = \{C_1, \ldots, C_\ell\}$ steht für $\bigwedge K \equiv C_1 \wedge \ldots \wedge C_\ell$

Bemerkung: $\bigwedge \emptyset \equiv 1$.

endliche Klauselmengen $\approx$ KNF-Formeln

Resolutionskalkül arbeitet mit KNF in Klauselform

Ableitungsziel: Nachweis der Unerfüllbarkeit einer geg. Klauselmenge durch Ableitung der leeren Klausel $\square$

Resolution

Beobachtungen:

- $L, \overline{L} \in C \;\Rightarrow\; C \equiv 1$ **allgemeingültig**.
- $C \equiv 1 \;\Rightarrow\; K \equiv K \setminus \{C\}$.
- $\square \in K \;\Rightarrow\; K \equiv 0$ **unerfüllbar**.

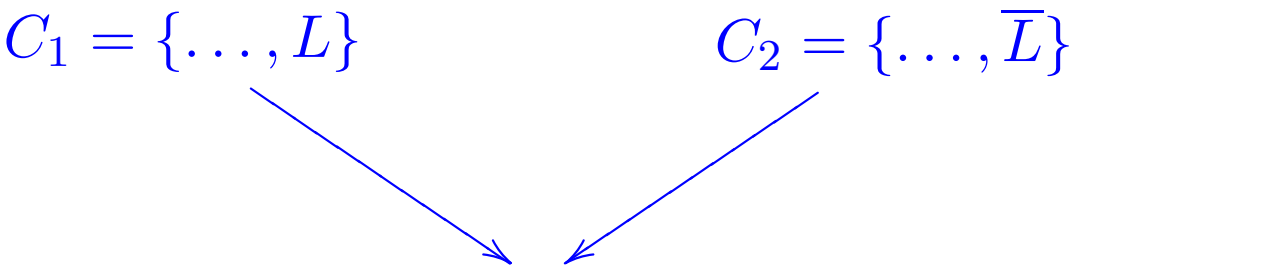
Resolventen:

$$L \in C_1, \overline{L} \in C_2 \;\Rightarrow\; \{C_1, C_2\} \equiv \{C_1, C_2, C\},$$

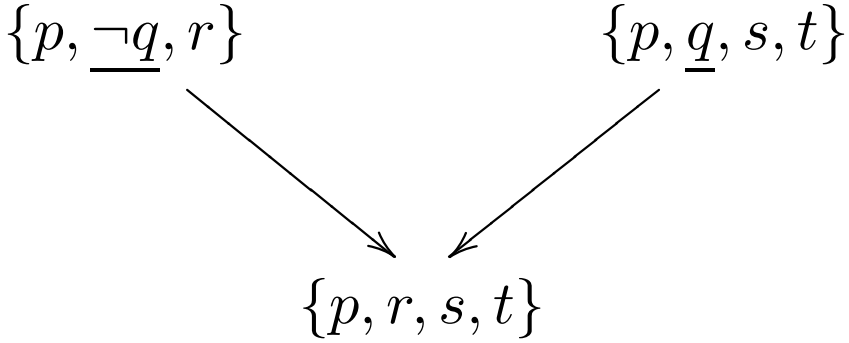
wobei

$$C = \underbrace{(C_1 \setminus \{L\}) \cup (C_2 \setminus \{\overline{L}\})}_{\textit{Resolvente}}$$

Baumdarstellung



Beispiel:



Beweise im Resolutionskakül I

Ableitungsbaum für $\square$:

- Knoten mit Klauseln beschriftet
- $\square$ an der Wurzel
- Resolventen an binären Verzweigungen
- Klauseln aus K an den Blättern.

Beweise im Resolutionskalkül II

Resolutionslemma:

Seien $C_1, C_2 \in K$, C Resolvente von C_1 und C_2. Dann ist $K \equiv K \cup \{C\}$ (also $K \models C$).

Res(K) und Res*(K):

$\mathrm{Res}(K) := K \cup \{C\colon\ C$ Resolvente von Klauseln in $K\ \}$.

Definition: Eine Klausel C heißt (im Resolutionskalkül) **ableitbar** aus K, gdw. $C \in \underbrace{\mathrm{Res} \cdots \mathrm{Res}}_{n\text{-mal}}(K)$ für ein $n \in \mathbb{N}$.

$\mathrm{Res}^*(K)$: die Menge aller aus K ableitbaren Klauseln.

Korrektheit und Vollständigkeit des Resolutionskalküls

Korrektheit: $\square \in \mathrm{Res}^*(K) \Rightarrow K \equiv 0$ unerfüllbar.

(Diese Aussage folgt sofort aus dem Resolutionslemma)

Vollständigkeit: K unerfüllbar $\Rightarrow \square \in \mathrm{Res}^*(K)$.

Beweis der Vollständigkeit

Z.z.: K über $\mathcal{V}_n = \{p_1, \ldots, p_n\}$ unerfüllbar $\Rightarrow$ $\square \in \mathrm{Res}^*(K)$.

Beweis durch Induktion über n.

Induktionsschritt von n nach $n+1$

Aus $K = \{C_1, \ldots, C_k\}$ über $\mathcal{V}_{n+1}$ gewinne K_0 und K_1 über $\mathcal{V}_n$:

K_0 : setze $p_{n+1} := 0$ und vereinfache (streiche p_{n+1} aus allen Klauseln und streiche alle Klauseln, die $\neg p_{n+1}$ enthalten).

K_1 : analog mit $p_{n+1} := 1$.

K unerfüllbar $\Rightarrow$ K_0 und K_1 unerfüllbar

$\Rightarrow$ $\square \in \mathrm{Res}^*(K_0)$ und $\square \in \mathrm{Res}^*(K_1)$.

Dann ist $\square \in \mathrm{Res}^*(K)$ oder $\{p_{n+1}\}, \{\neg p_{n+1}\} \in \mathrm{Res}^*(K)$

und somit ebenfalls $\square \in \mathrm{Res}^*(K)$.

Resolutionsalgorithmus

Eingabe: K [Klauselmenge, endlich]

$R := K$

WHILE $\big(\mathrm{Res}(R) \neq R$ and $\square \notin R\big)$ DO $R := \mathrm{Res}(R)$ OD

IF $\square \in R$ THEN output "unerfüllbar"

ELSE output "erfüllbar"

Hornklauseln

- Interessanter Spezialfall für **KI Anwendungen** (Datenbanken),
- AL-HORN-SAT-Problem **effizient entscheidbar**,
- logische Programmierung (**Prolog**: FO Horn-Formeln)

Definition: Hornklauseln sind Klauseln mit **höchstens einem positiven** Literal.

Beispiel: $C = \{\neg q_1, \ldots, \neg q_r, q\} \equiv \big(q_1 \wedge \ldots \wedge q_r\big) \rightarrow q$;
auch $\square$ ist Hornklausel.

Spezialfälle: C besteht nur aus positivem Literal: **positiv**.

C ohne positive Literale: **negativ**.

Beobachtungen

- Mengen von negativen Hornklauseln trivial erfüllbar $(p_i \mapsto 0)$.
- Mengen von nicht-negativen Hornklauseln besitzen eindeutige **minimale** erfüllende Interpretationen.

Effizienter Horn-Erfüllbarkeitstest: Grundidee

H Hornklauselmenge; $H^- \subseteq H$ negative Klauseln in H

$H_0 := H \setminus H^-$ nicht negative Klauseln

1. Schritt: Berechne minimale Interpretation $\mathfrak{I}_0 \models H_0$.

2. Schritt: Prüfe, ob $\mathfrak{I}_0 \models H^-$.

Korrektheit:

$\mathfrak{I}_0 \models H^- \quad \Rightarrow \quad \mathfrak{I}_0 \models H.$

$\mathfrak{I} \models H \quad \Rightarrow \quad \mathfrak{I} \models H_0$, also $\mathfrak{I}_0 \leq \mathfrak{I}$.

$\mathfrak{I} \models H^- \Rightarrow \mathfrak{I}_0 \models H^-$. Also $\mathfrak{I}_0 \models H$.

Sequenzenkalkül (G. Gentzen 1935)

Sequenzen

$\Gamma \vdash \Delta$, wobei Γ, Δ endliche ungeordnete Listen („Multisets") von AL-Formeln sind. Auch: $\Gamma; \Delta$ oder Γ, Δ).

Bedeutung von $\Gamma \vdash \Delta$: $\bigwedge \Gamma \rightarrow \bigvee \Delta$.

Also: Liste links von $\vdash$ (Antezendent): Konjunktion von Voraussetzungen. Liste rechts von $\vdash$ (Sukzedent): Disjunktion möglicher Konsequenzen.

Somit:

$\Gamma \vdash \Delta$ **allgemeingültig** gdw. $\models \bigwedge \Gamma \rightarrow \bigvee \Delta$ gdw. $\bigwedge \Gamma \models \bigvee \Delta$.

Sequenzenkalkül (G. Gentzen 1935)

Erzeugung **allgemeingültiger Sequenzen** durch

Sequenzenregeln: neue Sequenzen aus bereits abgeleiteten Sequenzen

Format: $\dfrac{\text{Prämissen}}{\text{Konklusion}}$

Beispiele: $\dfrac{}{\Gamma, \varphi \vdash \Delta, \varphi}$ oder $\dfrac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$

AL Sequenzenkalkül $\mathcal{SK}$

(Ax) $\dfrac{}{\Gamma, p \vdash \Delta, p}$ $(p \in \mathcal{V})$

(0-Ax) $\dfrac{}{\Gamma, 0 \vdash \Delta}$ (1-Ax) $\dfrac{}{\Gamma \vdash \Delta, 1}$

($\neg$L) $\dfrac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$ ($\neg$R) $\dfrac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$

($\vee$L) $\dfrac{\Gamma, \varphi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}$ ($\vee$R) $\dfrac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}$

$$(\wedge\mathrm{L})\ \frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta} \qquad (\wedge\mathrm{R})\ \frac{\Gamma \vdash \Delta, \varphi \qquad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$$

$$(\rightarrow \mathrm{L})\ \frac{\Gamma \vdash \Delta, \varphi \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \rightarrow \psi \vdash \Delta} \qquad (\rightarrow \mathrm{R})\ \frac{\Gamma, \varphi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \rightarrow \psi}$$

Übung: Zeige, dass (Ax) für beliebiges φ statt p ableitbar ist.

Korrektheitssatz: Jede ableitbare Sequenz ist allgemeingültig.

Beweis: Überprüfe, dass für alle Regeln gilt: sind die Prämissen allgemeingültig, so auch die Konklusion.

Bemerkung 1 (Abschwächungslemma): Ist $\Gamma \vdash \Delta$ mit Beweistiefe n ableitbar, so auch $\Gamma, \Gamma' \vdash \Delta, \Delta'$.

Beweis: Induktion über n.

Bemerkung 2 (Inversionslemma): Alle Regeln für $\neg, \vee, \wedge, \rightarrow$ sind auch von unten nach oben gelesen korrekt.
Genauer: Ist die Konklusion (mit Beweis der Tiefe n) herleitbar, dann auch die Prämisse(n) (mit gleicher Tiefe).

Beweis: Induktion über n.

Bemerkung 3 (Kontraktionslemma):
Ist $\Gamma, \varphi, \varphi \vdash \Delta$ (bzw. $\Gamma \vdash \Delta, \varphi, \varphi$) beweisbar (mit Tiefe n), so auch $\Gamma, \varphi \vdash \Delta$ (bzw. $\Gamma \vdash \Delta, \varphi$).

Beweis: Induktion über n.

Man kann die Kontraktionseigenschaft auch direkt in den Kalkül geben, indem man Γ, Δ als Mengen (statt Multisets) nimmt.

Bemerkung: Obige Version des Sequenzenkalküls wird in der Literatur oft als G3c bezeichnet.
Siehe 'A.S. Troelstra, H. Schwichtenberg: Basic Proof Theory. Cambridge Tracts in Theoretical Computer Science 4, 2nd edition, 2000' für weitergehende Information.

Beispiel einer Ableitung

Ableitung der **allgemeingültigen Sequenz**

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

$$\dfrac{\dfrac{\dfrac{}{p \vdash p, \neg q}\,(\mathsf{Ax}) \qquad \dfrac{\dfrac{}{p, q \vdash q}\,(\mathsf{Ax})}{p \vdash q, \neg q}\,(\neg\mathsf{R})}{p \vdash (p \wedge q), \neg q}\,(\wedge\mathsf{R})}{p \vdash (p \wedge q) \vee \neg q}\,(\vee\mathsf{R})$$

Vollständigkeit

Satz: Jede allgemeingültige Sequenz ist ableitbar.

Beweisidee: Systematische Beweissuche rückwärts: zu jeder Formel in einer Konklusions-Sequenz existiert (genau) eine Regel mit Prämissen, in der diese Formel abgebaut ist. In dem rückwärts von der Zielsequenz generiertem Beweisbaum gilt:

Zielsequenz allgemeingültig $\Leftrightarrow$ alle Sequenzen an den Blättern sind allgemeingültig.

Beispiel einer fehlschlagenden Beweissuche

$$\dfrac{\dfrac{\dfrac{}{p \vdash p}(\mathsf{Ax}) \qquad \dfrac{}{\mathbf{p \vdash q}}}{p \vdash p \wedge q}(\wedge\mathsf{R}) \qquad \dfrac{\dfrac{}{\mathbf{p \vdash q}} \qquad \dfrac{}{q \vdash q}(\mathsf{Ax})}{q \vdash p \wedge q}(\wedge\mathsf{R})}{p \vee q \vdash p \wedge q}(\vee\mathsf{L})$$

Die Interpretation liefert $p \mapsto 1\,;\ q \mapsto 0$ ein Gegenbeispiel.

Satz: Der AL Sequenzenkalkül ist korrekt und vollständig für die Ableitung aller allgemeingültigen AL Sequenzen.

Die Schnittregeln CUT

von $\mathcal{SK}^+$ entsteht aus $\mathcal{SK}$ durch Hinzufgung der sogennanten Schnittregel (CUT), die zum modus ponens korrespondiert:

$$\text{(CUT)} \qquad \frac{\Gamma \vdash \Delta, \varphi \qquad \Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta}.$$

Korrektheit nachprüfen!

Anwendung von modus ponens 'schluckt' Hilfsformel φ : problematisch für (rückwärts-) Beweissuche.

CUT kann stets aus Beweisen eliminiert werden (auch algorithmisch, **Schnittelimination**, G. Gentzen), was aber i.a. zu einem **exponentiellen Wachstum** des Beweises führt.

Aus der Schnittregel folgen leicht die folgenden (ebenfalls redundanten Regeln):

$$\text{(Kontradiktion)} \qquad \frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \neg\varphi}{\Gamma \vdash \emptyset}$$

und

$$\text{(Widerspruch)} \qquad \frac{\Gamma, \neg\varphi \vdash \psi \qquad \Gamma, \neg\varphi \vdash \neg\psi}{\Gamma \vdash \varphi}$$

Teil 2: Logik erster Stufe (Prädikatenlogik), FO

Gegenstandsbereich:

S-Strukturen

mit Belegungen für Element-Variablen

Ausdrucksmöglichkeiten:

atomare Aussagen über Terme

Funktionen, Konstanten, Variablen

$\wedge, \vee, \neg$ (wie in AL) aber **zusätzlich**

Quantifizierung $\forall, \exists$ über Elemente

Haupteigenschaften

- Strukturierte Formalisierung komplexerer Eigenschaften: z.B.

$$(\forall n \in \mathbb{N})\,(\exists m \in \mathbb{N})\;(m > n \wedge (\exists k \in \mathbb{N})(2k = m)),$$

  d.h. es gibt unendlich viele gerade Zahlen.

- Modulare Semantik
- Korrekte und vollständige Beweiskalküle
- Die Menge der logisch wahren Sätze ist nicht mehr entscheidbar.
- Schnittelimination im Sequenzenkalkül noch möglich aber von superexponentieller Komplexität $2_{|P|}$, wobei $2_0 := 2$, $2_{n+1} := 2^{2_n}$ und P die Größe des gegebenen Beweises ist.

FO-Sprachen (Signaturen)

Symbole:

$x, y, z, \ldots, x_1, x_2, x_3, \ldots$	Variablensymbole
$c, d, e, \ldots$	Konstantensymbole
$f, g, \ldots$	Funktionssymbole
$P, Q, R, \ldots$	Relationssymbole

Signatur S:

Auswahl von Konstanten-, $\underbrace{\text{Funktions- und Relationssymbolen}}_{\text{mit spezifizierten Stelligkeiten}}$

Strukturen zu Signatur S

S-Struktur:

$\mathcal{A} = (A, c^{\mathcal{A}}, \ldots, f^{\mathcal{A}}, \ldots, R^{\mathcal{A}}, \ldots)$

besteht aus: Trägermenge $A \neq \emptyset$

für $c \in S$: ausgezeichnetes Element $c^{\mathcal{A}} \in A$.

für n-st. $f \in S$: n-st. Funktion $f^{\mathcal{A}}\colon A^n \to A$.

für n-st. $R \in S$: n-st. Relation $R^{\mathcal{A}} \subseteq A^n$.

Beispiel: $\mathcal{N} = \left(\mathbb{N}, +^{\mathcal{N}}, \cdot^{\mathcal{N}}, <^{\mathcal{N}}, 0^{\mathcal{N}}, 1^{\mathcal{N}}\right)$ zu $S = \{+, \cdot, <, 0, 1\}$

Beispiele

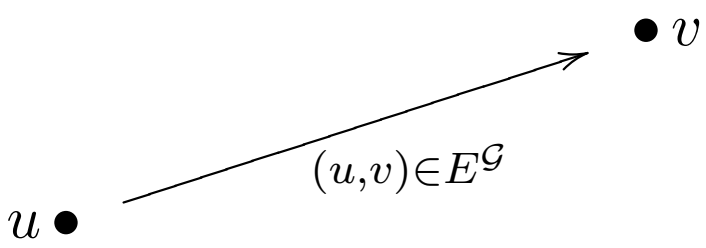
Wortstrukturen zu $S = \{<\} \cup \{P_a : a \in \Sigma\}$

$$w = a_1 \dots a_n \quad \longleftrightarrow \quad \mathcal{W} = \big(\{1, \dots, n\}, <^{\mathcal{W}}, (P_a^{\mathcal{W}})_{a \in \Sigma}\big),$$

$$<^{\mathcal{W}} = \{(i,j) : 1 \le i < j \le n\},$$

$$P_a^{\mathcal{W}} = \{i : a_i = a\}.$$

Graphen zu $S = \{E\}$



$\mathcal{G} = \big(V, E^{\mathcal{G}}\big)$,

mit Knotenmenge V

Kantenrelation $E^{\mathcal{G}} \subseteq V \times V$.

Weitere Beispiele

Transitionssysteme zu $S = \{E_a : a \in \Sigma\}$

$$(\Sigma, Q, \Delta) \quad \longleftrightarrow \quad \mathcal{A} = \big(Q, (E_a^{\mathcal{A}})_{a\in\Sigma}\big),$$
$$E_a^{\mathcal{A}} = \{(q, q') : (q, a, q') \in \Delta\}.$$

Relationale Datenbanken, ...

Terme

Variablen aus $\mathcal{V} := \{x_1, x_2, \ldots\}$ bzw. $\mathcal{V}_n := \{x_1, \ldots, x_n\}$.

Die Menge der **S-Terme** $T(S)$ einer Signatur S (über den Variablen aus $\mathcal{V}$) ist induktiv erzeugt durch:

$x \in T(S)$	für $x \in \mathcal{V}$.
$c \in T(S)$	für $c \in S$.
$ft_1 \ldots t_n \in T(S)$	für $f \in S$ (n-st.), $t_1, \ldots, t_n \in T(S)$.

$T_n(S) \subseteq T(S)$: S-Terme über Variablen aus $\mathcal{V}_n$.

Speziell: $T_0(S)$ sind die **geschlossenen** Terme von S ($= \emptyset$, falls kein Konstantensysmbol in S).

Beispiele wohlgeformter S-Terme

$S = \{f, c\}$, f 2-st.: c, $ffccc$, $fcfcc$, $\ldots$, x_{17}, fx_1c, ffx_5cx_2,

$\ldots$

$S = \{+, \cdot, 0, 1\}$, $+, \cdot$ 2-st.: $\cdot + 11 + +111$,

$+ \cdot + + 111\, x_3\, x_1, \ldots$

Konvention: Funktionsterme mit Klammern, 2-st. auch infix

$\big(((1 + 1) + 1) \cdot x_3 + x_1\big)$ statt $+ \cdot + + 111 x_3 x_1$

Term-Strukturen und Herbrand-Strukturen

Eine S-Struktur $\mathcal{T}$ heißt **Term-Struktur**, wenn gilt:

- $\mathcal{T} = \mathcal{T}(S) = \big(T(S), \ldots, c^{\mathcal{T}(S)}, \ldots, f^{\mathcal{T}(S)}, \ldots, R^{\mathcal{T}(S)}, \ldots\big)$
- $c \in S: \; c^{\mathcal{T}} := c \in T(S)$.
- $f \in S$ (n-st.): $f^{\mathcal{T}} : T(S)^n \longrightarrow T(S)$

  $(t_1, \ldots, t_n) \longmapsto f t_1 \ldots t_n$.
- keine Einschränkungen an $R^{\mathcal{T}}$ für $R \in S$.

Falls S mindestens ein Konstantensymbol enthält, kann man in obiger Definition auch $T_0(S)$ statt $T(S)$ nehmen. Solche Term-Strukturen heißen auch **Herbrand-Strukturen.**

Belegungen

Weisen den Variablensymbolen Elemente einer S-Struktur zu!

Belegung

über S-Struktur $\mathcal{A} = (A, c^{\mathcal{A}}, \ldots, f^{\mathcal{A}}, \ldots)$:

$$\begin{array}{rcl} \beta\colon \mathcal{V} & \longrightarrow & A \\ x & \longmapsto & \beta(x) \end{array}$$

S-Interpretation:

S-Struktur + Belegung $\mathcal{I} = (\mathcal{A}, \beta)$

Semantik von Termen: induktiv über $T(S)$ für gegebene S-Interpretation $\mathfrak{I} = (\mathcal{A}, \beta)$:

Interpretation von $t \in T(S)$: $t^{\mathfrak{I}} \in A$.

- $t = x$ ($x \in \mathcal{V}$ Variable) : $t^{\mathfrak{I}} := \beta(x)$.
- $t = c$ ($c \in S$ Konstante) : $t^{\mathfrak{I}} := c^{\mathcal{A}}$.
- $t = ft_1 \dots t_n$ ($f \in S$, n-st.) : $t^{\mathfrak{I}} := f^{\mathcal{A}}(t_1^{\mathfrak{I}}, \dots, t_n^{\mathfrak{I}})$.

Für jede S-Interpretation $\mathfrak{I} = (\mathcal{A}, \beta)$ ist die Abbildung

$$\begin{aligned} h\colon T(S) &\longrightarrow A \\ t &\longmapsto t^{\mathfrak{I}} \end{aligned}$$

ein Homomorphismus von $\mathcal{T}(S)$ nach $\mathcal{A}$.

Speziell für Term-Strukturen: $t^{\mathfrak{I}} = t$ für $t \in T_0(S)$.

Die Syntax von $\mathrm{FO}(S)$

Induktive Definition der Menge der FO(S) Formeln:

- **atomare Formeln**: für $t_1, t_2 \in T(S)$: $t_1 = t_2 \in \mathrm{FO}(S)$.

  für $R \in S$ (n-st.), $t_1, \ldots, t_n \in T(S)$: $Rt_1 \ldots t_n \in \mathrm{FO}(S)$.

- **AL-Junktoren**: für $\varphi, \psi \in \mathrm{FO}(S)$: $\neg\varphi \in \mathrm{FO}(S)$.

  $(\varphi \wedge \psi) \in \mathrm{FO}(S)$.

  $(\varphi \vee \psi) \in \mathrm{FO}(S)$.

- **Quantifizierung**: für $\varphi \in \mathrm{FO}(S)$, $x \in \mathcal{V}$: $\exists x\varphi \in \mathrm{FO}(S)$.

  $\forall x\varphi \in \mathrm{FO}(S)$.

Logik ohne Gleichheit $\mathrm{FO}^{\neq} \subseteq \mathrm{FO}$: ohne Atome $t_1 = t_2$.

Syntax: freie und gebundene Variablen, Quantorenrang

Freie Variablen

$$\begin{array}{rccl} \text{frei}\colon \mathrm{FO}(S) & \longrightarrow & \mathcal{P}(\mathcal{V}) \\ \varphi & \longmapsto & \text{frei}(\varphi) \subseteq \mathcal{V} \end{array}$$

induktiv: $\text{frei}(\varphi) := \text{var}(\varphi)$ für atomare φ.

$\text{frei}(\neg\varphi) := \text{frei}(\varphi)$.

$\text{frei}(\varphi \wedge \psi) = \text{frei}(\varphi \vee \psi) := \text{frei}(\varphi) \cup \text{frei}(\psi)$.

$\text{frei}(\exists x\varphi) = \text{frei}(\forall x\varphi) := \text{frei}(\varphi) \setminus \{x\}$.

Sätze

Variablen x, die unter den Skopus eines Quantors $\forall x, \exists x$ stehen, werden durch diesen **gebunden**. Eine Variable x kann in einer Formel sowohl frei wie auch gebunden vorkommen:

$$\varphi(x) \wedge \forall x \, \psi(x).$$

$\mathrm{FO}_n(S) := \{\varphi \in \mathrm{FO}(S) \colon \mathrm{frei}(\varphi) \subseteq \mathcal{V}_n\}$.

Schreibweise: $\varphi(x_1, \ldots, x_n)$ für $\varphi \in \mathrm{FO}_n(S)$.

Definition: Formeln φ ohne freie Variablen, d.h. $\varphi \in \mathrm{FO}_0(S)$, heißen **Sätze**.

Bsp: $\text{frei}(0 < fx) = \{x\}$

$\text{frei}(\forall x \neg x = fx) = \emptyset$

$\text{frei}(0 < fx \wedge \forall x \neg x = fx) = \{x\}$

Quantorenrang

$\mathrm{qr}\colon \mathrm{FO}(S) \longrightarrow \mathbb{N}, \quad \varphi \longmapsto \mathrm{qr}(\varphi) \in \mathbb{N}$

induktiv: $\mathrm{qr}(\varphi) = 0$ für atomares φ.

$\mathrm{qr}(\neg\varphi) := \mathrm{qr}(\varphi)$.

$\mathrm{qr}(\varphi \wedge \psi) = \mathrm{qr}(\varphi \vee \psi) := \max(\mathrm{qr}(\varphi), \mathrm{qr}(\psi))$.

$\mathrm{qr}(\exists x\varphi) = \mathrm{qr}(\forall x\varphi) := \mathrm{qr}(\varphi) + 1$.

Misst die **Quantorschachtelungstiefe!**

Bsp: $\mathrm{qr}(0 < fx) = 0$

$\mathrm{qr}(\forall x \exists y\, (x < y)) = 2$

$\mathrm{qr}(\exists z\, (0 < fz) \wedge \forall x \exists y\, x < y) = 2$

Semantik von FO(S)

Der **Wahrheitswert** $\varphi^{\mathfrak{I}}$ von FO(S)-Formeln φ über S-Interpretation $\mathfrak{I}$ wird induktiv definiert:

atomare φ: $(t_1 = t_2)^{\mathfrak{I}} = 1$ gdw. $t_1^{\mathfrak{I}} = t_2^{\mathfrak{I}}$.

$(Rt_1 \dots t_n)^{\mathfrak{I}} = 1$ gdw. $(t_1^{\mathfrak{I}}, \dots, t_n^{\mathfrak{I}}) \in R^{\mathcal{A}}$.

Negation: $(\neg\varphi)^{\mathfrak{I}} := 1 - \varphi^{\mathfrak{I}}$.

Konjunktion: $(\varphi \wedge \psi)^{\mathfrak{I}} := \min(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$.

Disjunktion: $(\varphi \vee \psi)^{\mathfrak{I}} := \max(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$.

Quantoren: $(\exists x\varphi)^{\mathfrak{I}} = \max\big(\varphi^{\mathfrak{I}[x \mapsto a]} : a \in A\big)$.

$(\forall x\varphi)^{\mathfrak{I}} = \min\big(\varphi^{\mathfrak{I}[x \mapsto a]} : a \in A\big)$.

Sprech- und Schreibweisen für $\varphi^{\mathfrak{I}} = 1$: φ wahr unter $\mathfrak{I}$

$\mathfrak{I}$ erfüllt φ

$\mathfrak{I}$ Modell von φ

$\mathfrak{I} \models \varphi$

Belegungen und freie Variablen: Werte der Belegung $\beta(x) \in A$ über $\mathcal{A}$ nur relevant für $x \in \mathrm{frei}(\varphi)$.

Für **Sätze** φ hängt daher für $\mathfrak{I} = (\mathcal{A}, \beta)$ nur von $\mathcal{A}$ ab:

$$\mathcal{A} \models \varphi \quad \text{:gdw. } (\mathcal{A}, \beta) \models \varphi \text{ für ein/alle } \beta.$$

Semantische Grundbegriffe

Analog zu AL:

Folgerungsbeziehung:

$$\varphi \models \psi : \text{ für alle } \mathfrak{I} \text{ gilt } \big(\mathfrak{I} \models \varphi \Rightarrow \mathfrak{I} \models \psi\big).$$

Logische Äquivalenz: $\varphi \equiv \psi :$ f.a. $\mathfrak{I}$ gilt $\big(\mathfrak{I} \models \varphi \Leftrightarrow \mathfrak{I} \models \psi\big)$.

Erfüllbarkeit: $\varphi \in \mathrm{SAT(FO)}$: es gibt $\mathfrak{I}$ mit $\mathfrak{I} \models \varphi$.

Allgemeingültigkeit: $\models \varphi$: für alle $\mathfrak{I}$ gilt $\mathfrak{I} \models \varphi$.

Äquivalent?

- $\forall x \forall y \varphi(x,y) \equiv \forall y \forall x \varphi(x,y)$?
- $\forall x \varphi \equiv \neg \exists x \neg \varphi$?

Erfüllbar?

- $\forall x \exists y Rxy \wedge \neg \exists y \forall x Rxy$?
- $\forall x \forall y (Rxy \wedge \neg Ryx)$?
- $\forall x \forall y (Rxy \leftrightarrow \neg Ryx)$?

Substitution

Semantisch korrektes Einsetzen von Termen:

Gesucht: für $t \in T(S)$ und $\varphi(x) \in \mathrm{FO}(S)$,
$\varphi' := \varphi(t/x) \in \mathrm{FO}(S)$ so, dass:

$$\mathfrak{I} \models \varphi' \quad \Leftrightarrow \quad \mathfrak{I}[x \mapsto t^{\mathfrak{I}}] \models \varphi.$$

Warnung: Naives Ersetzen von x durch t tut es nicht!

- beachte, dass x frei und gebunden auftreten kann.
- beachte, dass Variablen in t nicht fälschlich gebunden werden.

Bedingung: t muss in φ frei für x sein, d.h. keine Variable in t wird nach der Einsetzung in φ durch einen Quantor in φ gebunden.

Methode: Induktive Definition, die intern gebundene Variablen so umbenennt, dass Konflikte vermieden werden.

Beispiel: $\varphi(x) = \forall y\big(Exy \wedge \exists x \neg Exy\big)$

$$\varphi(fy/x) = ?$$

Negationsnormalform

Eine Formel $\varphi \in \mathrm{FO}(S)$ ist in **Negationsnormalform NNF**, wenn φ aus atomaren und negierten atomaren Formeln mit $\wedge, \vee, \exists, \forall$ aufgebaut ist.

Satz: Zu jedem φ kann man explizit eine Formel $\varphi^* \in$ **NNF** konstruieren, die zu φ logisch äquivalent ist, d.h. $\varphi \equiv \varphi^*$.

Beweis: Übungsaufgabe!

Variationen: Spielsemantik (model checking $\varphi \in$ NNF)

Spiel zwischen **Verifizierer (V)** und **Falsifizierer (F)** zu $\varphi(x_1, \ldots, x_n) \in \mathrm{FO}_n(S)$ über $\mathcal{A}$.

Spielpositionen: $(\psi, \mathbf{a}) \in \mathrm{SF}(\varphi) \times A^n$

Züge in Position $(\psi, \mathbf{a})$, $\mathbf{a} = (a_1, \ldots, a_n)$:

$\psi = \psi_1 \wedge \psi_2$ **F** am Zug

zieht nach $(\psi_1, \mathbf{a})$ oder nach $(\psi_2, \mathbf{a})$.

$\psi = \psi_1 \vee \psi_2$ **V** am Zug

zieht nach $(\psi_1, \mathbf{a})$ oder nach $(\psi_2, \mathbf{a})$.

$\psi = \forall x_i \psi_0$ **F** am Zug

zieht nach einem $(\psi_0, \mathbf{a}[x_i \mapsto a_i'])$.

$\psi = \exists x_i \psi_0$ **V** am Zug

zieht nach einem $(\psi_0, \mathbf{a}[x_i \mapsto a_i'])$.

Spiel-Ende in Positionen $(\psi, \mathbf{a})$, ψ atomar oder negiert atomar.

Gewinner: **V** gewinnt in Endposition $(\psi, \mathbf{a})$, wenn $\mathcal{A} \models \psi[\mathbf{a}]$.

F gewinnt in Endposition $(\psi, \mathbf{a})$, wenn $\mathcal{A} \not\models \psi[\mathbf{a}]$.

Satz: $\mathcal{A} \models \psi[\mathbf{a}] \Leftrightarrow$ **V** hat Gewinnstrategie in Position $(\psi, \mathbf{a})$.

FO **ohne** $=$: $\mathrm{FO}^{\neq}$

- In unserer Behandlung von FO: Gleichheit $R := $ Bestandteil der Logik, d.h. spezielle Interpretion als mengentheoretische Identität auf A in $\mathcal{A}$.
- Alternativ: $=$ ist nicht Bestandteil der Logik ($\mathrm{FO}^{\neq}$). Bei Bedarf Behandlung von $=$ als gewöhnliches binäres Relationssymbol, dass die Gleichheitsaxiome erfüllt: Reflexivität, Symmetrie, Transitivität, Kongruenzrelation bzgl. aller anderen Relations- und Funktionssymbole.

Reduktion von FO auf $\mathrm{FO}^{\neq}$

Idee: modelliere '=' durch interpretierte Relation $\sim$.

$\hat{S} := S \cup \{\sim\}$

Verträglichkeitsbedingungen:

$\sim$ Kongruenzrelation bzgl. aller $R, f \in S$.

Erhalte Modelle $\mathcal{A}_0$ mit **echter Gleichheit** als $\sim$-Quotienten:

$$\mathcal{A}_0 = \mathcal{A}/{\sim^{\mathcal{A}}} = \left(A/{\sim^{\mathcal{A}}}, \ldots, [c^{\mathcal{A}}]_{\sim^{\mathcal{A}}}, \ldots, f^{\mathcal{A}}/{\sim^{\mathcal{A}}}, \ldots, R^{\mathcal{A}}/{\sim^{\mathcal{A}}}\right).$$

$\sim$-Äquivalenzklassen als Elemente.

Erfüllbarkeit universeller Sätze ohne Gleichheit in Herbrand-Modellen

Voraussetzungen:

- S enthalte mindestens ein Konstantensymbol
- $\Phi \subseteq \mathrm{FO}_0^{\neq}(S)$: Menge von **'='-freien reinen $\forall$-Sätzen**

Herbrand-Strukturen $\mathcal{H}$ (Erinnerung):

- S-Termstruktur $\mathcal{T}_0(S)$ über $T_0(S)$ (geschlossene S-Terme) als Trägermenge.
- Interpretation geschlossener Terme durch sich selbst.
- Interpretation von R (n-st.) als Teilmenge von $(T_0(S))^n$.

Herbrand-Strukturen, die Modell einer Satzmenge Φ, sind heißen auch **Herbrand-Modell von Φ**.

Satz über Herbrand-Modelle:

Φ Menge '='-freier reiner $\forall$-Sätze.

Φ erfüllbar $\Leftrightarrow$ es existiert ein Herbrand-Modell

$\mathcal{H} = \left(\mathcal{T}_0(S), (R^{\mathcal{H}})_{R \in S}\right) \models \Phi$.

Beweisidee: "$\Leftarrow$": offensichtlich.

"$\Rightarrow$": geeignete Interpretationen $R^{\mathcal{H}}$ aus geg. Modell $\mathcal{A} \models \Phi$:

$$R^{\mathcal{H}} := \{(t_1, \ldots, t_n) \in (T_0(S))^n : (t_1^{\mathcal{A}}, \ldots, t_n^{\mathcal{A}}) \in R^{\mathcal{A}}\}.$$

□

Verfeinerungen

Sei $\varphi := \forall x_1, \ldots, x_n \varphi_{qf}(x_1, \ldots, x_n) \in \Phi$ (φ_{qf} quantorfrei).
Betrachte die Menge $E(\Phi)$ aller geschlossenen $T_0(S)$-Instanzen

$$\varphi_{qf}(t_1, \ldots, t_n) \qquad (t_1, \ldots, t_n \in T_0(S))$$

für alle $\varphi \in \Phi$.

Satz: Φ hat ein Herbrand-Modell gdw. $E(\Phi)$ im aussagenlogischen Sinne erfüllbar ist gdw. jede endliche Teilmenge von $E(\Phi)$ im aussagenlogischen Sinne erfüllbar ist.

Beweis: Zum Beweis der 1. Äquivalenz: '$\Rightarrow$:' Sei $\mathcal{H}$ ein Herbrand-Modell für Φ. Definiere auf

$$\mathcal{V} := \{p_\alpha : \alpha = R(t_1, \ldots, t_n), R \in S \text{ (n-stell.)}, t_1, \ldots, t_n \in T_0(S)\}$$

$$\mathfrak{I}(p_\alpha) := \begin{cases} 1, & \text{falls } \mathcal{H} \models \alpha \\ 0, & \text{falls } \mathcal{H} \not\models \alpha. \end{cases}$$

'$\Leftarrow$:' Sei $\mathfrak{I}$ eine erfüllende Belegung. Definiere $\mathcal{H}$ durch

$$R^{\mathcal{H}} := \{(t_1, \ldots, t_n) \in T_0(S) : \mathfrak{I}(p_{R(t_1,\ldots,t_n)}) = 1\}$$

Bijektive Korrepondenz $\mathcal{H} \leftrightarrow \mathcal{I}$

Für

$\varphi = \forall x_1 \ldots \forall x_n \, \varphi_{qf}(x_1, \ldots, x_n) = \forall \underline{x} \, \varphi_{qf}(\underline{x}), \quad \xi$ quantorfrei

$\mathcal{H} = \mathcal{H}(\mathcal{I})$:

$\mathcal{H} \models \varphi$ gdw. $\mathcal{H} \models \varphi_{qf}[\underline{t}]$ für alle $\underline{t} = (t_1, \ldots, t_n) \in T_0(S)^n$

gdw. $\mathcal{I} \models \varphi_{qf}(\underline{t})^{\mathrm{AL}}$ für alle $\underline{t} = (t_1, \ldots, t_n) \in T_0(S)^n$

Erhalte $\varphi_{qf}(\underline{t})^{\mathrm{AL}} \in \mathrm{AL}(\mathcal{V})$ aus $\varphi_{qf}(\underline{t})$ durch Ersetzen von Atomen $\alpha = \mathtt{R}\ldots$ durch AL-Variablen $p_\alpha = p_{\mathtt{R}\ldots}$.

Die 2. Äquivalenz folgt aus dem aussagenlogischen Kompaktheitssatz. □

Satz von Herbrand (J. Herbrand 1930)

Satz von Herbrand: Sei $\varphi = \exists \underline{x}\, \varphi_{qf}(\underline{x})$ ein reiner $\exists$-Satz (d.h. φ_{qf} ist quantorfrei) ohne Gleichheit '$=$'. $\underline{x} = x_1, \ldots, x_n$ ist ein Tupel von Variablen. Dann gilt

$$\models \varphi \text{ gdw. } \exists \underline{t}_1, \ldots, \underline{t}_k \in T_0(S) \text{ mit } \bigvee_{i=1}^{k} \varphi_{qf}(\underline{t}_i) \in \text{ TAUT.}$$

Statt $T_0(S)$ genügt es alle aus φ-Material (plus Konstantensymbol c, falls kein Konstantensymbol in φ) bildbaren geschlossenen Terme zu nehmen.

Beweis des Satzes von Herbrand: $\neg\varphi$ ist logisch äquivalent zu dem $\forall$-Satz $\forall \underline{x}\, \neg\varphi_{qf}(\underline{x})$. Wende nun den vorangegangenen Satz auf $\Phi := \{\forall \underline{x}\, \neg\varphi_{qf}(\underline{x})\}$ an. $\square$

Beispiel: Betrachte den logisch wahren Satz

$$\exists x \big(P(x) \vee \neg P(f(x))\big).$$

Für die mit $t_1 := c$ und $t_2 := f(c)$ gebildete Disjunktion gilt

$$\big(P(c) \vee \neg P(f(c))\big) \vee \big(P(f(c)) \vee \neg P(f(f(c)))\big) \in \text{ TAUT}.$$

Pränexe Normalform

Definition: Eine Formel $\varphi \in \mathrm{FO}(S)$ ist in **pränexer Normalform (PNF)**, falls φ die folgende Gestalt hat:

$$\varphi = Q_1 x_{i_1} \dots Q_k x_{i_k} \varphi_{qf}$$

mit $Q_i \in \{\forall, \exists\}, k \in \mathbb{N}, \varphi_{qf}$ quantorfrei.

Beispiele:

$$\exists y(Exy \wedge \forall x(Eyx \to x = y)) \quad \equiv \quad \exists y \forall z\big(Exy \wedge (Eyz \to z = y)\big)$$

$$\exists y \forall x Exy \vee \neg \exists y Exy \quad \equiv \quad \exists y_1 \forall y_2 \forall y_3\big(Ey_2y_1 \vee \neg Exy_3\big)$$

Satz über PNF

Satz über die Pränexnormalform:

Jede FO-Formel ist logisch äquivalent zu einer Formel in PNF.

Beweis: Induktion über $\varphi \in \mathrm{FO}(S)$.

Bemerkung:

1) Die Pränexnormalform ist i.a. nicht eindeutig bestimmt.
2) Die Durchführung der Pränexierung einer Formel erfordert i.a. die Einführung neuer Variablen durch Umbenennung vorhandener Variablen.

Skolemnormalform

Reine $\forall$-Formeln (**Universell-pränexe Formeln**) sind Formeln der Gestalt $\forall x_{i_1} \ldots \forall x_{i_k} \varphi_{qf}$, wobei φ_{qf} quantorenfrei ist.

- nicht jede Formel ist logisch äquivalent

  zu universell-pränexer Formel, z.B. $\varphi = \forall x \exists y \, Exy$

- aber jede Formel ist **erfüllbarkeitsäquivalent**

  zu einer geeigneten universell-pränexen Formel.

Idee: neue Funktionen, die potentielle Existenzbeispiele liefern

[im Semantik Spiel: $\exists$-Züge für $\mathbf{V}$]

Beispiel

$\varphi = \forall x \exists y\, E(x,y) \quad \longmapsto \quad \varphi' = \forall x\, E(x, f(x))$ (für *neues* f)

dann gilt:

(i) $\mathcal{A}' = (A, E^{\mathcal{A}}, \ldots, f^{\mathcal{A}'}) \models \varphi' \;\Rightarrow\; \mathcal{A} = (A, E^{\mathcal{A}}, \ldots) \models \varphi$

(ii) $\mathcal{A} = (A, E^{\mathcal{A}}, \ldots) \models \varphi \;\Rightarrow$

es gibt eine Interpretation von f über A so, dass

$$\mathcal{A}' = (A, E^{\mathcal{A}}, \ldots, f^{\mathcal{A}'}) \models \varphi'$$

Satz über die Skolemnormalform

Satz: Jedes $\varphi \in \mathrm{FO}$ ist **erfüllbarkeitsäquivalent** zu einer $\forall$-Formel φ^S (in einer erweiterten Signatur), der sogenannten Skolemnormalform (Vorsicht: nicht eindeutig).

Beweis: Man erhält φ^S aus einer zu φ logisch äquivalenten Formel φ^{pr} in PNF (x_i, y_j auch Tupel von Variablen):

$$\varphi^{pr} \equiv \forall x_1 \exists y_1 \ldots \forall x_n \exists y_n \varphi_{qf}(x_1, y_1, \ldots, x_n, y_n)$$

durch Substitution von **Skolemfunktionstermen** die für existentiell abquantifizierten Variablen:

$$\varphi^S :\equiv \forall x_1 \ldots \forall x_n \, \varphi_{qf}(x_1, f_1(x_1), \ldots, x_n, f_n(x_1, \ldots, x_n)).$$

φ^S impliziert logisch triviallerweise φ^{pr} (und damit φ). Umgekehrt gilt nur, dass die Erfüllbarkeit von φ die Erfüllbarkeit von φ^S impliziert. Sei $\mathcal{A} \models \varphi^{pr}$. Erweitere $\mathcal{A}$ zu einer Struktur $\mathcal{A}^S$ der um $f_1, \ldots, f_n$ erweiterten Signatur durch Interpretation der f_i als geeignete Auswahlfunktionen. Dann gilt $\mathcal{A}^S \models \varphi^S$ und damit die Erfüllbarkeit von φ^S. □

Bemerkung: Stets $\varphi^S \models \varphi$, aber i.a. nicht $\varphi \models \varphi^S$.

Herbrandnormalform

Satz: Jedes $\varphi \in \mathrm{FO}$ ist **gültigkeitsäquivalent** zu einer reinen $\exists$-Formel φ^H (in einer erweiterten Signatur), der sogenannten Herbrandnormalform.

Beweis: Man erhält φ^H aus einer zu φ logisch äquivalenten Formel in PNF (x_i, y_j auch Tupel von Variablen):

$$\exists x_1 \forall y_1 \ldots \exists x_n \forall y_n \varphi_{qf}(x_1, y_1, \ldots, x_n, y_n)$$

durch Substitution von **Herbrandfunktionstermen** für die universell abquantifizierten Variablen:

$$\exists x_1 \ldots \exists x_n \, \varphi_{qf}(x_1, f_1(x_1), \ldots, x_n, f_n(x_1, \ldots, x_n)).$$

$$\models \varphi \Leftrightarrow \models \varphi^H$$

folgt aus dem Satz über die Skolemnormalform, da φ^H die Negation der Skolemnormalform (einer Pränexnormalform) der Negation von φ ist. $\square$

Bemerkung: Stets $\varphi \models \varphi^H$, aber i.a. nicht $\varphi^H \models \varphi$.

Satz: Sei Γ eine Menge von PNF-Formeln, φ in PNF.
$\Gamma^S := \{\psi^S : \psi \in \Gamma\}$. Dann gilt

$$\Gamma^S \models \varphi^H \text{ gdw. } \Gamma \models \varphi.$$

Erfüllbarkeit: Reduktion auf AL

Reduktion:

$\Phi \subseteq \mathrm{FO}(S)$ (bel. Formelmenge)

$\Big\}$ erf.-äquiv. (neue Konst. statt freien Var.)

$\Phi' \subseteq \mathrm{FO}_0(S_1)$ (Satzmenge)

$\Big\}$ erf.-äquiv. (Vorschalten $=$-Ax.)

$\Phi'' \subseteq \mathrm{FO}_0^{\neq}(S_2)$ (gleichheitsfrei)

$\Big\}$ erf.-äquiv. (Skolemnormalform)

$\Phi''' \subseteq \mathrm{FO}_0^{\neq}(S_3)$ (universell(-pränex))

Φ erfüllbar $\Leftrightarrow$ Φ''' erfüllbar $\Leftrightarrow$ Φ''' in Herbrand-Modell erfüllbar

Bedingungen an Herbrand-Modell lassen sich in AL kodieren!

Erfüllbarkeit: Reduktion auf AL (fortges.): o.B.d.A.:

$\Phi \subseteq \mathrm{FO}_0^{\neq}(S)$, universell-pränex, S habe Konstanten

Φ erfüllbar $\Leftrightarrow$ Φ hat ein Herbrand-Modell

$$\mathcal{H} = \left(\mathcal{T}_0(S), (R^{\mathcal{H}})_{R \in S}\right) \models \Phi$$

$\Leftrightarrow$ für alle $R \in S$ (n-st.) existieren $R^{\mathcal{H}} \subseteq T_0(S)^n$,

sodass $\mathcal{H} = \left(\mathcal{T}_0(S), (R^{\mathcal{H}})_{R \in S}\right) \models \Phi$

$\mathcal{V} := \{p_\alpha : \alpha = \mathtt{Rt_1} \ldots \mathtt{t_n}; R \in S; t_1, \ldots, t_n \in$
$T_0(S)$ für n-stelliges $R\}$

$\mathcal{V}$-Interpretationen $\mathcal{I}$ beschreiben mögliche $\mathcal{H}$

Beispiel

$S = \{R, Q, f\}$ R (2-st.), Q (1-st.), Relationssymbole

f (1-st.), Funktionssymbol

Behauptung:

$$\Phi: \begin{cases} \varphi_1 = \forall x \forall y \big(Rxy \rightarrow (Qx \leftrightarrow \neg Qy)\big) \\ \varphi_2 = \forall x (Rxfx \vee Rfxx) \\ \varphi_3 = \forall x \forall y \big(\neg Rxy \rightarrow Rxffy\big) \end{cases}$$

ist **unerfüllbar**.

$S_c := S \cup \{c\}$

$T_0(S_c) = \{c, fc, ffc, fffc, \ldots\} = \{f^n c \colon n \in \mathbb{N}\}$

Fortsetzung des Beispiels

AL-Variablen für die Reduktion:

$q_n \quad (= p_{\mathtt{Qf^n c}})$ für die Atome $Qf^n c$, $(n \in \mathbb{N})$,

$r_{\ell,m} \quad (= p_{\mathtt{Rf^\ell cf^m c}})$ für die Atome $Rf^\ell c f^m c$, $(\ell, m \in \mathbb{N})$.

zugeh. AL-Formeln

$$\begin{cases} [\![\varphi_1]\!]^{\mathrm{AL}} = \{r_{\ell,m} \to (q_\ell \leftrightarrow \neg q_m) : \ell, m \in \mathbb{N}\} \\ [\![\varphi_2]\!]^{\mathrm{AL}} = \{r_{\ell,\ell+1} \vee r_{\ell+1,\ell} : \ell \in \mathbb{N}\} \\ [\![\varphi_3]\!]^{\mathrm{AL}} = \{\neg r_{\ell,m} \to r_{\ell,m+2} : \ell, m \in \mathbb{N}\} \end{cases}$$

Unerfüllbarkeit von Φ folgt aus Unerfüllbarkeit von

$$r_{0,0} \rightarrow (q_0 \leftrightarrow \neg q_0),$$

$$r_{0,1} \rightarrow (q_0 \leftrightarrow \neg q_1),$$

$$r_{1,0} \rightarrow (q_1 \leftrightarrow \neg q_0),$$

$$r_{0,2} \rightarrow (q_0 \leftrightarrow \neg q_2),$$

$$r_{1,2} \rightarrow (q_1 \leftrightarrow \neg q_2), \quad r_{0,1} \vee r_{1,0},$$

$$\underbrace{r_{2,1} \rightarrow (q_2 \leftrightarrow \neg q_1),}_{\in [\![\varphi_1]\!]^{\mathrm{AL}}} \quad \underbrace{r_{1,2} \vee r_{2,1}\,,}_{\in [\![\varphi_2]\!]^{\mathrm{AL}}} \quad \underbrace{\neg r_{0,0} \rightarrow r_{0,2}}_{\in [\![\varphi_3]\!]^{\mathrm{AL}}}$$

Kompaktheitssatz (Endlichkeitssatz):

Version 1: (Erfüllbarkeit)

Für $\Phi \subseteq \mathrm{FO}$ sind äquivalent:

(i) Φ erfüllbar.

(ii) Jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ ist erfüllbar.

Version 2: (Folgerungsbeziehung)

Für $\Phi \subseteq \mathrm{FO}, \varphi \in \mathrm{FO}$ sind äquivalent:

(i) $\Phi \models \varphi$.

(ii) $\Phi_0 \models \varphi$ für eine endliche Teilmenge $\Phi_0 \subseteq \Phi$.

Version 1 $\Leftrightarrow$ Version 2 (zur Übung!)

Version 1 für universell-pränexes $\Phi \subseteq \mathrm{FO}_0^{\neq}$: Reduktion auf AL

Konsequenzen des Endlichkeitssatzes

Beliebig große endliche Modelle $\Rightarrow$ unendliche Modelle: zu Φ

betrachte $\Phi \cup \{\exists x_1 \ldots \exists x_n \bigwedge_{1 \leq i < j \leq n} \neg x_i = x_j : n \geq 1\}$

Unendliche Modelle $\Rightarrow$ beliebig große unendliche Modelle: zu Φ

betrachte $\Phi \cup \{\neg c_i = c_j : i \neq j; i, j \in I\}$

für neue Konstanten $(c_i)_{i \in I}$

$\Rightarrow$ keine unendliche Struktur in FO bis auf Isomorphie charakterisierbar

Nichtstandardmodelle

Z.B. $\mathcal{N}^*$ zu $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$

Nichtstandardmodell der Arithmetik mit

'unendlich großen natürlichen Zahlen.'

Betrachte alle $\mathbb{N}$-wahren Sätze in der Sprache der Arithmetik erster Stufe plus allen Sätzen der Form $c \neq 0, c \neq 1, c \neq 2, \ldots$ (c neue Konstante). Für jede endliche Teilmenge hiervon ist $\mathcal{N}$ ein Modell (bei geeigneter Interpretation von c). Also hat die gesamte Menge ein Modell $\mathcal{N}^*$, dass nicht zu $\mathcal{N}$ isomorph sein kann.

Logik-Kalküle

Syntaktische Beweiskalküle: Beweise der Unerfüllbarkeit (Resolution) bzw. der Allgemeingültigkeit (Hilbertkalküle, Sequenzenkalkül).

Erweiterung des Kalküls von J.S. Shoenfield auf $\neg, \vee, \forall$

Axiome: alle Instanzen von $\neg\varphi \vee \varphi$ und $\forall x\, \varphi \rightarrow \varphi(t/x)$.

Regeln: $\dfrac{\varphi}{\psi \vee \varphi}$, $\dfrac{\varphi \vee \varphi}{\varphi}$, $\dfrac{\varphi \vee (\psi \vee \chi)}{(\varphi \vee \psi) \vee \chi}$, $\dfrac{\varphi \vee \psi \ ,\ \neg\varphi \vee \chi}{\psi \vee \chi}$

und $\dfrac{\varphi \vee \psi}{\forall x\, \varphi \vee \psi}$, falls $x \notin$ frei(ψ).

Alternativ für $\exists$: $\varphi(t/x) \rightarrow \exists x \varphi$ und $\dfrac{\varphi \rightarrow \psi}{\exists x\, \varphi \rightarrow \psi}$ falls $x \notin$ frei(ψ)

mit $\varphi \rightarrow \psi := \neg\varphi \vee \psi$.

Erweiterung um Gleichheitsaxiome

$$x = x \text{ (Reflexivität)},$$

$$x = y \rightarrow y = x \text{ (Symmetrie)},$$

$$x = y \wedge y = z \rightarrow x = z \text{ (Transitivität)},$$

$$x_1 = y_1 \wedge \ldots \wedge x_n = y_n \rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n),$$

$$x_1 = y_1 \wedge \ldots \wedge x_n = y_n \rightarrow (P(x_1, \ldots, x_n) \rightarrow P(y_1, \ldots, y_n)).$$

Bemerkung: Die Gleichheitsaxiome implizieren:

$$x_1 = y_1 \wedge \ldots \wedge x_n = y_n \rightarrow t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n)$$

und

$$x_1 = y_1 \wedge \ldots \wedge x_n = y_n \rightarrow (\varphi(x_1, \ldots, x_n) \rightarrow \varphi(y_1, \ldots, y_n))$$

für **beliebige** Terme t und Formeln φ.

Symmetrie und Transitivität folgen tatsächlich bereits aus den anderen Axiomen.

Grundinstanzen-Resolution (GI-Resolution):

Gegenstand: $\mathrm{FO}^{\neq}$-Klauselmengen K

(universelle $\mathrm{FO}^{\neq}$-Satzmengen Φ)

Beweisziel: Ableitung der (unerfüllbaren) leeren Klausel $\square$

Korrektheit: $\square$ ableitbar aus $K \Rightarrow K$ unerfüllbar.

Vollständigkeit: K unerfüllbar $\Rightarrow \square$ ableitbar aus K.

FO-Klauselmengen

Universelle (skolemisierte) $\mathrm{FO}^{\neq}$-Sätze in Klauselform:

$$\forall x_1 \ldots \forall x_k \, \xi \;\equiv\; \forall x_1 \ldots \forall x_k \underbrace{\bigwedge_{C \in K} \bigvee C}_{\text{q-fr. Kern in KNF}}$$

$\xi \equiv K$ für endliche Klauselmenge K über $\mathrm{FO}^{\neq}$-Literalen

$\mathrm{FO}^{\neq}$-Literale:

relationale Atome oder negierte relationale Atome λ, $\overline{\lambda} \equiv \neg\lambda$

$\mathrm{FO}^{\neq}$-Klauseln: endliche Mengen C von $\mathrm{FO}^{\neq}$-Literalen

für $C = \{\lambda_1, \ldots, \lambda_k\}$: $C \equiv \bigvee C = \bigvee_{i=1,\ldots,k} \lambda_i$

$\mathrm{FO}^{\neq}$-Klauselmengen: Mengen K von $\mathrm{FO}^{\neq}$-Klauseln

Klauselmengen und universell-pränexe Sätze

Semantisch identifiziere Klauselmenge mit Satzmenge:

$$K \quad \equiv \quad \{\underbrace{\forall x_1 \ldots \forall x_n}_{\text{alle Variablen in } C} \bigvee C : C \in K\}$$

$$\left(\quad \equiv \quad \underbrace{\forall x_1 \ldots \forall x_n}_{\text{alle Variablen in } K} \bigwedge_{C \in K} \bigvee C \qquad \text{für endliches } K \right)$$

Korrespondenzen

endliche $\mathrm{FO}^{\neq}$ Klauselmengen	!	universell-pränexe $\mathrm{FO}^{\neq}$-Sätze
$\mathrm{FO}^{\neq}$ Klauselmengen	!	universell-pränexe $\mathrm{FO}^{\neq}$-Satzmengen

Übersetzungs-Beispiel

$\varphi = \forall x \forall y \big(Rxy \rightarrow (Qx \leftrightarrow \neg Qy) \big)$

relevante Atome: $\alpha = Rxy$, $\beta_1 = Qx$ und $\beta_2 = Qy$

$\varphi = \forall x \forall y \big(\alpha \rightarrow (\beta_1 \leftrightarrow \neg \beta_2) \big)$

Kern von φ in KNF (z.B.):

$$\underbrace{(\neg\alpha \vee \beta_1 \vee \neg\beta_1)}_{\equiv 1} \wedge (\neg\alpha \vee \beta_1 \vee \beta_2) \wedge (\neg\alpha \vee \neg\beta_2 \vee \neg\beta_1) \wedge \underbrace{(\neg\alpha \vee \neg\beta_2 \vee \beta_2)}_{\equiv 1}$$

$$K = \big\{ \{\neg\alpha, \beta_1, \beta_2\}, \{\neg\alpha, \neg\beta_1, \neg\beta_2\} \big\}$$

$$= \big\{ \{\neg Rxy, Qx, Qy\}, \{\neg Rxy, \neg Qy, \neg Qx\} \big\}$$

Grundinstanzen-Resolution (GI)

Übertragung von AL-Resolution gemäß Reduktionsansatz

ähnlich wie schon für andere Erfüllbarkeitsargumente

Grundinstanzen einer Klausel C über Literalen $\lambda \in \mathrm{FO}_n^{\neq}$:

$$C(t_1/x_1, \ldots, t_n/x_n) := \{\lambda(t_1/x_1, \ldots, t_n/x_n) \colon \lambda \in C\}$$

mit $t_i \in T_0(S)$

Grundinstanzenmenge einer Klauselmenge K:

$$\mathrm{GI}(K) := \{C(t_1/x_1, \ldots) \colon C \in K, t_i \in T_0(S)\}$$

- es gilt $K \models \mathrm{GI}(K)$.

und aus dem **Satz von Herbrand**:

- K und $\mathrm{GI}(K)$ **erfüllbarkeitsäquivalent**.

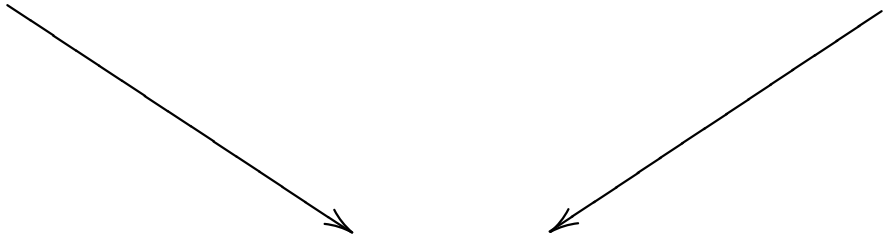
GI-Resolution: Resolventen

C_1, C_2, C Klauseln von variablenfreien $\mathrm{FO}^{\neq}(S)$-Literalen

C ist **Resolvente** von C_1 und C_2 (bezüglich des Literals λ), wenn

$$\lambda \in C_1, \quad \overline{\lambda} \in C_2, \quad \text{und } C = (C_1 \setminus \{\lambda\}) \cup (C_2 \setminus \{\overline{\lambda}\})$$

$$C_1 = \{\lambda_1, \ldots, \lambda_k, \underline{\lambda}\} \qquad C_2 = \{\lambda'_1, \ldots, \lambda'_\ell, \overline{\lambda}\}$$



$$C = \{\lambda_1, \ldots, \lambda_k, \lambda'_1, \ldots, \lambda'_\ell\}$$

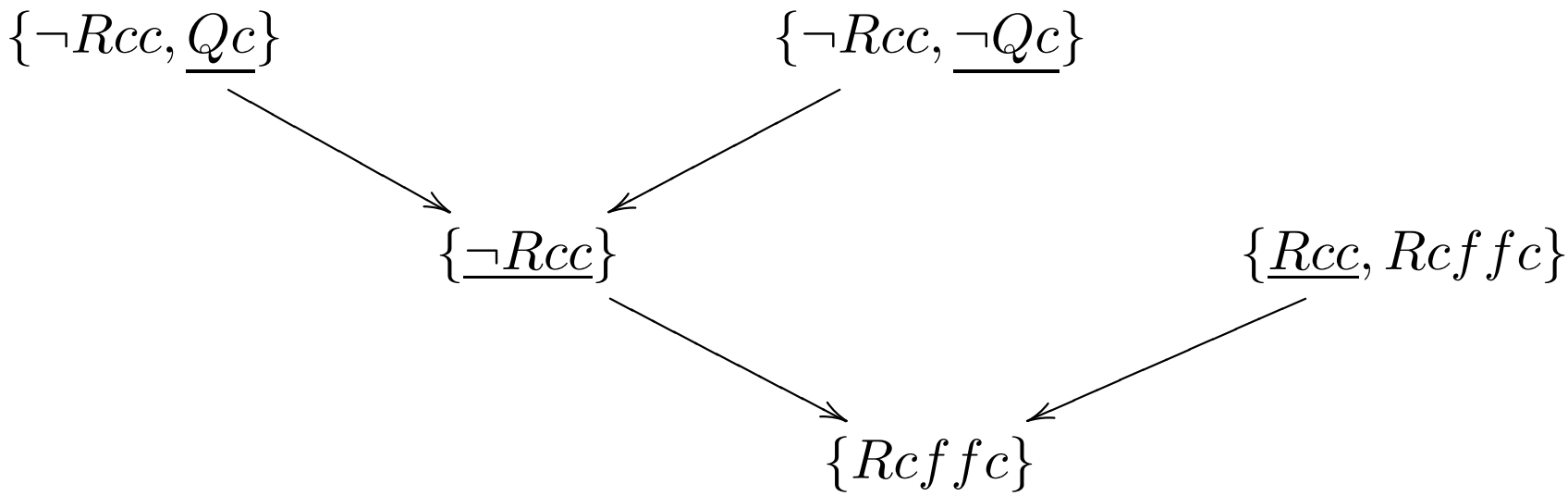
Zu Klauselmenge K über variablenfreien $\mathrm{FO}^{\neq}(S)$-Literalen:

$\mathrm{Res}^*(K) =$ Abschluß von K unter Resolventenbildung

Beispiel

Über Grundinstanzen von

$\{\neg Rxy, Qx, Qy\}$, $\{\neg Rxy, \neg Qx, \neg Qy\}$ und $\{Rxx, Rxffx\}$:



$$\left.\begin{array}{c} \forall x \forall y \big(\neg Rxy \vee Qx \vee Qy \big) \\ \forall x \forall y \big(\neg Rxy \vee \neg Qx \vee \neg Qy \big) \\ \forall x \big(Rxx \vee Rxffx \big) \end{array}\right\} \models Rcffc$$

Resolutionssatz

Korrektheit und **Vollständigkeit** von GI-Resolution für die Unerfüllbarkeit von universell-pränexen $\mathrm{FO}^{\neq}(S)$-Satzmengen in Klauselform:

Resolutionssatz: Für $\mathrm{FO}^{\neq}(S)$-Klauselmengen K sind äquivalent:

(i) K unerfüllbar.

(ii) $\mathrm{GI}(K)$ unerfüllbar.

(iii) $\square \in \mathrm{Res}^*(\mathrm{GI}(K))$.

Beweis:

$(iii) \Rightarrow (i)$: $C \in \mathrm{Res}^*(\mathrm{GI}(K))$ impliziert, dass $K \models C$

$\square \equiv 0$ unerfüllbar.

$(i) \Leftrightarrow (ii)$: Erfüllbarkeitsäquivalenz (Herbrand).

$(ii) \Rightarrow (iii)$: Vollständigkeit von AL Resolution $+$ Reduktion.

Allgemeinere Resolution: Termunifikation

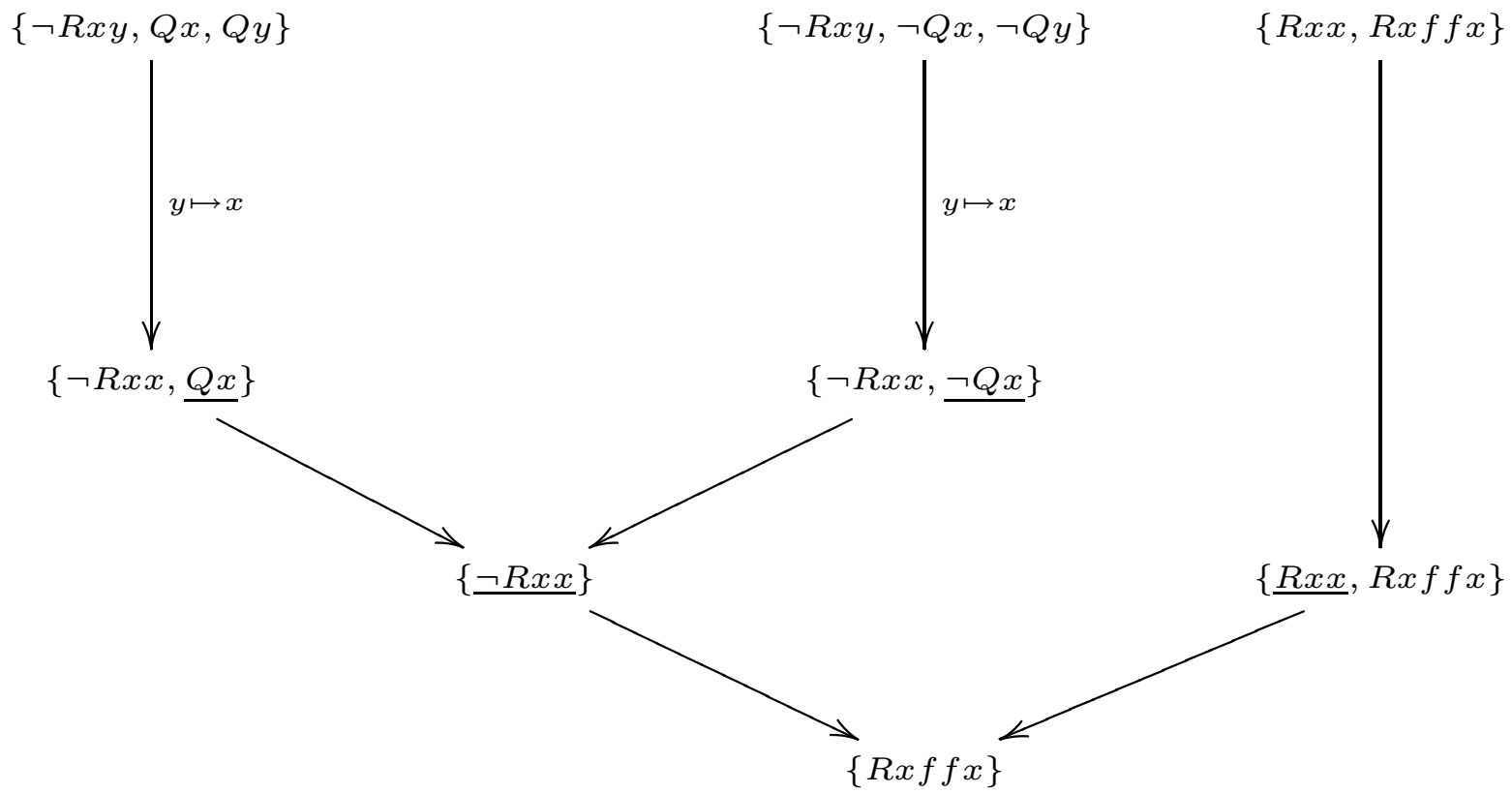
Idee: nicht notwendig zu Grundinstanzen absteigen

Resolution nach Substitution von Termen mit Variablen

Substitutionsinstanz zu $\sigma = (t_1, \ldots, t_n) \in T(S)^n$:
$C^\sigma = \{\lambda^\sigma : \lambda \in C\} = \{\lambda(t_1/x_1, \ldots, t_n/x_n) : \lambda \in C\}$

Resolution von C_1 und C_2 zu C falls für geeignete σ_1 und σ_2:
$\lambda \in C_1^{\sigma_1}, \overline{\lambda} \in C_2^{\sigma_2}, C = (C_1^{\sigma_1} \setminus \{\lambda\}) \cup (C_2^{\sigma_2} \setminus \{\overline{\lambda}\})$

Beispiel



$\forall x \forall y (\neg Rxy \vee Qx \vee Qy), \forall x \forall y (\neg Rxy \vee \neg Qx \vee \neg Qy), \forall x (Rxx \vee Rxffx) \models \forall x Rxffx$

Sequenzenkalkül

Allgemeingültigkeitsbeweise (für bel. FO-Formeln/Sätze)

Gegenstand: FO-**Sequenzen** $\Gamma \vdash \Delta$

für endliche Γ, Δ Multisets aus $\mathrm{FO}(S)$

$\Gamma \vdash \Delta$ **allgemeingültig** wenn $\bigwedge \Gamma \models \bigvee \Delta$

Beweisziel: Ableitung allgemeingültiger Sequenzen

Korrektheit: Jede ableitbare Sequenz ist allgemeingültig.

Vollständigkeit: Jede allgemeingültige Sequenz ist ableitbar.

(schwache Form, wird später verschärft)

Sequenzenkalkül: Regeln und Korrektheit

Format von **Sequenzenregeln** (wie in AL): $\frac{\textbf{Prämissen}}{\textbf{Konklusion}}$

Konklusionen von Regeln ohne Prämisssen: **Axiome**

Ableitbare Sequenzen:

ausgehend von Axiomen (in endlich vielen Schritten) durch Anwendung von Sequenzenregeln erzeugte Sequenzen

Korrektheit:

Jede ableitbare Sequenz ist allgemeingültig.

Die **Korrektheit** olgt aus der Korrektheit der einzelnen Regeln:

- die Axiome sind allgemeingültige Sequenzen.
- für Regeln mit Prämissen:

  Prämissen allgemeingültig $\Rightarrow$ Konklusion allgemeingültig.

Regeln des Sequenzenkalküls

FO Sequenzenkalkül $\mathcal{SK}$, drei Gruppen von Regeln:

- **AL Regeln** (wie AL-Sequenzenkalkül).
- **Quantorenregeln (neu)**: Einführung von $\forall$ oder $\exists$ links/rechts.

  $(\forall\mathrm{L})$, $(\forall\mathrm{R})$, $(\exists\mathrm{L})$, $(\exists\mathrm{R})$.
- **Gleichheitsregeln (neu)**: Umgang mit Term-Gleichheiten.

  $(=)$, (Sub).

AL + Quantorenregeln: vollständiger Beweiskalkül $\mathcal{SK}^{\neq}$ für $\mathrm{FO}^{\neq}$.

$\mathcal{SK}^{\neq}$ + Gleichheitsregeln: vollständiger Beweiskalkül $\mathcal{SK}$ für FO.

Zusätzlich (nicht notwendig aber natürlich) in $\mathcal{SK}^{+}$:

- **Schnittregel** (modus ponens, Kettenschluss)

Sequenzenkalkül: Quantorenregeln

$$(\forall\mathrm{L})\quad \frac{\Gamma, \forall x\varphi, \varphi(t/x) \vdash \Delta}{\Gamma, \forall x\varphi \vdash \Delta} \qquad (\forall\mathrm{R})\quad \frac{\Gamma \vdash \Delta, \varphi(y/x)}{\Gamma \vdash \Delta, \forall x\varphi}$$

falls y nicht in Γ, Δ, φ

$$(\exists\mathrm{L})\quad \frac{\Gamma, \varphi(y/x) \vdash \Delta}{\Gamma, \exists x\varphi \vdash \Delta} \qquad (\exists\mathrm{R})\quad \frac{\Gamma \vdash \Delta, \exists x\varphi, \varphi(t/x)}{\Gamma \vdash \Delta, \exists x\varphi}$$

falls y nicht in Γ, Δ, φ

Korrektheit prüfen!

Sequenzenkalkül: Gleichheitsregeln

$$(=) \quad \frac{\Gamma, t = t \vdash \Delta}{\Gamma \vdash \Delta}$$

$$\text{(Sub)} \quad \frac{\Gamma, \varphi(t'/x), t = t', \varphi(t/x) \vdash \Delta}{\Gamma, t = t', \varphi(t'/x) \vdash \Delta}$$

Es ist tatsächlich ausreichend, diese Regeln for alle atomaren Formeln P statt φ zu fordern.

Übung: Zeige, dass

$$\Gamma, t = t', \varphi(t/x) \vdash \Delta, \varphi(t'/x)$$

ableitbar ist (siehe S. Negri, J. van Plato: Structural Proof Theory, CUB 2001).

Sequenzenkalkül: Schnittregel (optional)

(Schnittregel (CUT)) $$\frac{\Gamma \vdash \Delta, \varphi \qquad \Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta}$$

Schnitteliminationssatz (G. Gentzen 1935): Jeder Beweis im Sequenzenkalkül mit Schnittregel läßt sich in einen Beweis ohne Gebrauch der Schnittregel umformen.

Beweis: Sehr kompliziert (Gegenstand der sognannten **Beweistheorie**).

Bemerkung: Resultierender Beweis i.a. **extrem lang**: Es gibt Beweise B mit Schnitt der Größe $|B|$, so dass jeder schnittfreie Beweis derselben Konklusion $\geq 2_{|B|}$ groß ist, wobei $2_0 := 1$ und $2_{n+1} := 2^{2_n}$ (Statman 1979).

Korrektheit und Vollständigkeit

Ableitbarkeit aus Theorie $\Phi \subseteq \mathrm{FO}_0$:

φ ableitbar aus Φ $[\Phi \vdash \varphi]$ gdw.

für geeignetes $\Gamma_0 \subseteq \Phi$ (Voraussetzungen) ist $\Gamma_0 \vdash \varphi$ ableitbar.

Φ konsistent (widerspruchsfrei) gdw. *nicht* $\Phi \vdash \emptyset$.

Vollständigkeit (starke Form)

$$\Phi \models \varphi \;\Rightarrow\; \Phi \vdash \varphi$$

$$\Phi \text{ konsistent} \;\Rightarrow\; \Phi \text{ erfüllbar}$$

Korrektheit

$$\Phi \vdash \varphi \;\Rightarrow\; \Phi \models \varphi$$

$$\Phi \text{ erfüllbar} \;\Rightarrow\; \Phi \text{ konsistent}$$

Gödelscher Vollständigkeitssatz (K. Gödel 1929)

Satz (Vollständigkeit des Sequenzenkalküls $\mathcal{SK}^+$):

Für jede Satzmenge $\Phi \subseteq \mathrm{FO}_0(S)$
und jeden Satz $\varphi \in \mathrm{FO}_0(S)$ gelten:

- $\Phi \models \varphi$ gdw. $\Phi \vdash \varphi$, hier „$\vdash$" Herleitbarkeit in $\mathcal{SK}^+$
- Φ erfüllbar gdw. Φ konsistent.

Zentrale Folgerungen

- **Kompaktheitssatz** (wesentlich neuer Zugang)
- **Allgemeingültigkeit rekursiv aufzählbar**
  (aber: nicht entscheidbar!)
- (aus dem Beweis) Jede konsistente Satzmenge über einer abzählbaren Sprache hat bereits ein abzählbares Modell (Satz von Löwenheim-Skolem).

Vollständigkeitsbeweis (Idee)

Zu zeigen:

$$\text{Konsistenz} \Rightarrow \text{Erfüllbarkeit}$$

$$\left.\begin{array}{r}\text{nicht-Ableitbarkeit}\\ \text{best. Sequenzen}\end{array}\right\} \Rightarrow \text{Existenz eines Modells}$$

Henkin-Theorien 1 (L. Henkin 1949)

Sei Φ eine konsistente Satzmenge und T die von Φ axiomatisierte Theorie, d.h. $T := \{\varphi : \Phi \vdash \varphi\}$.

Definition: Eine Theorie T^{Henkin} heißt **Henkin-Theorie**, falls zu jedem Satz $\exists x\, \varphi(x)$ eine Konstante c existiert mit $\forall x\, \neg\varphi \vee \varphi(c/x) \in T^{\text{Henkin}}$ (inhaltlich: $\exists x\, \varphi \rightarrow \varphi((c/x))$.

Zu T sei T^* die wie folgt axiomatisierte erweiterte Theorie: für jeden Satz $\exists x\, \varphi(x)$ aus $\mathcal{L}(T)$ fügen wir ein neues Konstantensymbol c_φ zur Sprache hinzu mit dem neuen Axiom

$$\forall x\, \neg\varphi \vee \varphi(c_\varphi/x).$$

Henkin-Theorien 2

Lemma 1: T^* ist **konservativ** über T, d.h. falls ψ ein Satz in $\mathcal{T}(T)$ ist, d.h. ohne neue Konstanten c_φ (für irgendein φ), so gilt

$$T^* \vdash \psi \quad \Rightarrow \quad T \vdash \psi.$$

Definition: Sei T wie zuvor. Definiere

$$T_0 := T,\ T_{n+1} := (T_n)^*;\ \ T_\omega := \bigcup_{n\in\mathbb{N}} T_n.$$

Lemma 2: T_ω ist eine Henkin-Theorie und ist konservativ über T.

T_ω heißt **Henkin-Erweiterung von Φ**.

Henkin-Theorien 3

Lemma 3 (Lindenbaum): Jede konsistente Theorie ist in einer maximal-konsistenten Theorie enthalten.

Lemma 4: Sei T_ω^M eine maximal-konsistente Erweiterung von T_ω. Dann ist T_ω^M ebenfall eine Henkin-Theorie.

T_ω^M heißt **maximal-konsistente Henkin-Erweiterung von** Φ (nicht eindeutig bestimmt).

Henkin-Methode

Zu konsistentem Φ finde maximal-konsistente Henkin-Erweiterung T_ω^M von Φ.

$\mathrm{FO}^{\neq}$ (**ohne Gleichheit**): Herbrand-Modell aus Henkin-Theorie T_ω^M.

FO (**mit Gleichheit**): Quotienten bzgl. der in T_ω^M postulierten Gleichheitsrelation auf $T_0(S)$.

Unentscheidbarkeit von SAT(FO)

Satz von Church und Turing, 1936: SAT(FO) ist unentscheidbar (und somit nach Post nicht rekursiv aufzählbar).

Beweis: Reduktion des Halteproblems für Turing-Maschinen auf SAT(FO): FO ausreichend ausdrucksstark für Kodierung des Verhaltens von TM (in einzelnen Sätzen).

Finde berechenbare Zuordnung

$$\mathcal{M}, w \quad \longmapsto \quad \varphi_{\mathcal{M},w} \in \mathrm{FO}_0(S_{\mathcal{M}}),$$

$$\varphi_{\mathcal{M},w} \text{ erfüllbar gdw. } w \xrightarrow{\mathcal{M}} \infty.$$

Idee: $\varphi_{\mathcal{M},w}$ besagt, dass die Konfigurationenfolge in der Berechnung von $\mathcal{M}$ auf w nicht abbricht.

Reduktion des Halteproblems auf SAT(FO)

Zu $\mathcal{M} = (\Sigma, Q, q_0, \delta, q^+, q^-)$: wähle als Signatur $S_{\mathcal{M}}$:

succ	Nachfolgerfunktion, 1-st.	(Schritt-/Positionszähler)
pred	Vorgängerfunktion, 1-st.	
0	Konstante	
R_a	2-st. Relation für $a \in \Sigma \cup \{\Box\}$	(Bandbeschriftung)
Z_q	1-st. Relation für $q \in Q$	(Zustände)
K	2-st. Relation	(Kopfpositionen)

Intendierte Interpretation über $\mathbb{Z}$

$(t,i) \in R_a$: in Konfiguration C_t steht ein a in Zelle i.

$t \in Z_q$: in Konfiguration C_t ist $\mathcal{M}$ im Zustand q.

$(t,i) \in K$: in Konfiguration C_t steht der Kopf bei Zelle i.

$\varphi_{\mathcal{M},w} := \varphi_0 \wedge \varphi_{\text{start}} \wedge \varphi_\delta \wedge \varphi_\infty$ $\mathcal{M} = (\Sigma, Q, q_0, \delta, q^+, q^-)$,
$w = a_1 \dots a_n$, wobei

$$\varphi_0 := \begin{cases} \forall x\ (\text{pred succ}\, x = x \ \wedge\ \text{succ pred}\, x = x) & \\ \forall t \forall y\ \neg(R_a t y \wedge R_{a'} t y) & \text{für } a \neq a' \\ \forall t\ \neg(Z_q t \wedge Z_{q'} t) & \text{für } q \neq q' \\ \forall t \forall y \forall y'\ ((K t y \wedge K t y') \rightarrow y = y') & \end{cases}$$

$$\varphi_{\mathsf{start}} := K00 \wedge Z_{q_0}0 \wedge \left[\begin{array}{l} \bigwedge_{i=1}^{n} R_{a_i} 0\, \mathsf{succ}^i\, 0 \\ \wedge \forall y \left((\bigwedge_{i=1}^{n} \neg y = \mathsf{succ}^i\, 0) \rightarrow R_\Box 0 y \right) \end{array}\right]$$

$$\varphi_\delta := \forall t \forall t' \left(t' = \mathsf{succ}\, t \rightarrow \psi(t,t') \right) \text{ wobei } \psi(t,t') \text{ Konj. der Form.}$$

$\forall y \big((Z_q t \wedge Kty \wedge R_b ty) \rightarrow (Z_{q'} t' \wedge Kt' \mathsf{succ}\, y \wedge R_{b'} t' y) \big)$ für $\delta(q,b) = (b', >, q')$

$\forall y \big((Z_q t \wedge Kty \wedge R_b ty) \rightarrow (Z_{q'} t' \wedge Kt' \mathsf{pred}\, y \wedge R_{b'} t' y) \big)$ für $\delta(q,b) = (b', <, q')$

$\forall y \big((Z_q t \wedge Kty \wedge R_b ty) \rightarrow (Z_{q'} t' \wedge Kt' y \wedge R_{b'} t' y) \big)$ für $\delta(q,b) = (b', \circ, q')$

$\forall y, y' \big((Kty \wedge y \neq y') \rightarrow \bigwedge_a (R_a ty' \leftrightarrow R_a t' y') \big)$

$$\varphi_\infty := \forall t\, \neg (Z_{q^+} t \vee Z_{q^-} t)$$

- $w \xrightarrow{\mathcal{M}} \infty \;\Rightarrow\; \varphi_{\mathcal{M},w}$ erfüllbar,
- $w \xrightarrow{\mathcal{M}} \mathrm{STOP} \;\Rightarrow\; \varphi_{\mathcal{M},w}$ unerfüllbar.

Weitere zentrale Unentscheidbarkeitsaussagen

FINSAT(FO): Sätze, die in **endlichen** Modellen erfüllbar sind

beachte: FINSAT(FO) ist rekursiv aufzählbar.

Variation der Reduktion aus Church/Turing liefert:

Satz von Traktenbrot: FINSAT(FO) ist unentscheidbar.

Sätze von K. Gödel und A. Tarski

$\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$, $\quad \mathrm{Th}(\mathcal{N}) := \{\varphi \in \mathrm{FO}_0 : \mathcal{N} \models \varphi\}$

die erststufige Theorie der Arithmetik.

Satz von Tarski (1933):

$\mathrm{Th}(\mathcal{N})$ ist nicht arithmetisch definierbar, also nocht nicht einmal semi-entscheidbar.

1. Unvollständigkeitssatz von Gödel (1931):

Keine rekursiv aufzählbare Axiomatisierung der Zahlentheorie beweist alle $\mathcal{N}$-wahren Sätze.

Beide Sätze basieren auf unterschiedlichen formalisierten Versionen der **Lügner-Antinomie!**

Semantische Antinomien: die Lügner-Antinomie (Eubulides 4.Jh.v.C.)

Dieser Satz ist falsch!

Vorbereitung: Primitiv-rekursive Funktionen

Definition 1 Eine Funktion $f : \mathbb{N} \times \ldots \times \mathbb{N} \to \mathbb{N}$ heißt **primitiv-rekursiv**, falls f durch einfache Rekursionen aus $(\underline{x} = x_1, \ldots, x_k)$:

$$N(x) = 0,\ S(x) = x + 1,\ P_i^k(\underline{x}) = x_i \text{ (Ausgangsfunktionen)}$$

hervorgeht. Beispiele:

(i) $x + 0 := x,\ x + (y + 1) := (x + y) + 1$ (Addition),

(ii) $x \cdot 0 := 0,\ x \cdot (y + 1) := x \cdot y + x$ (Multiplikation).

Formalisierte Zahlentheorie der 1. Stufe: Peano Arithmetik PA

- Alle Axiome und Regeln der Logik (der 1. Stufe).
- Axiome der Gleichheit.
- Nachfolgeraxiome: $x + 1 = y + 1 \rightarrow x = y,\ x + 1 \neq 0$.
- Definierende Axiome für die prim.-rek. Funktionszeichen.
- Axiomschema der Induktion

$$\textbf{IA:}\ \ \varphi(0) \wedge \forall x\big(\varphi(x) \rightarrow \varphi(x+1)\big) \rightarrow \forall x\, \varphi(x)$$

für alle Formeln $\varphi(x)$ von $\mathcal{L}$(PA).

Gödelisierung

Prim.-rek. Folgenkodierung: Endliche Folgen natürlicher Zahlen $\langle x_1, \ldots x_n \rangle$ können durch Zahlen prim.-rek. kodiert werden.

Bäume werden als Folgen (und damit Zahlen) kodiert.

Terme, Formeln, Beweise sind endliche Bäume. Daher:
Es gibt prim.rek. Prädikat $Bew_{\mathrm{PA}}(x, y)$ mit $Bew_{\mathrm{PA}}(x, y)$ gdw.

„x ist Kode eines PA-Beweises des Satzes mit Kode y".

Wir schreiben $\lceil \varphi \rceil$ für den Kode des Satzes φ.

Das Fixpunktlemma

Fixpunktlemma: $\Phi(x)$ sei eine Formel von $\mathcal{L}$(PA). Dann kann man einen Satz $\varphi \in \mathcal{L}$(PA) **konstruieren** mit

$$\mathcal{N} \models \varphi \text{ genau dann, wenn } \mathcal{N} \models \Phi(\lceil \varphi \rceil),$$

d.h. φ sagt über sich selbst aus, Φ zu erfüllen.

Definition (Wahrheitsprädikat): Eine Formel $W(x) \in \mathcal{L}$(PA) ist ein **Wahrkeitsprädikat** für die Zahlentheorie, falls für alle Sätze $\varphi \in \mathcal{L}$(PA) gilt

$$\mathcal{N} \models \varphi \text{ genau dann, wenn } \mathcal{N} \models W(\lceil \varphi \rceil).$$

„Wahrheit" ist kompliziert!

Satz (A. Tarski, 1933): Es gibt kein Wahrheitsprädikat $W(x)$ in $\mathcal{L}$(PA) für die Zahlentheorie der ersten Stufe.

Beweis: Angenommen $W(x)$ sei Wahrheitsprädikat.
Fixpunktlemma (angewendet auf $\neg W(x)$) liefert **„Lügner"-Satz** L mit

$$\mathcal{N} \models L \text{ gdw. } \mathcal{N} \models \neg W(\lceil L \rceil) \text{ gdw. } \mathcal{N} \not\models W(\lceil L \rceil).$$

Andererseit (W Wahrkeitsprädikat)

$$\mathcal{N} \models L \text{ genau dann, wenn } \mathcal{N} \models W(\lceil L \rceil), \text{ also}$$

$$\mathcal{N} \models W(\lceil L \rceil) \text{ genau dann, wenn } \mathcal{N} \not\models W(\lceil L \rceil)$$

Widerspruch!

Gödels 1. Unvollständigkeitssatz

Satz (K. Gödel 1931): Sei $\mathcal{T}$ eine Erweiterung von PA um eine rekursiv aufzählbare Menge von ($\mathcal{N}$)-wahren Axiomen. Dann gibt es einen **wahren Satz** $\varphi \in \mathcal{L}(\mathsf{PA})$, der in $\mathcal{T}$ **nicht beweisbar** ist:

$$\mathcal{N} \models \varphi, \text{ aber } \mathcal{T} \nvdash \varphi.$$

Beweisskizze: Sei S_1 die Menge aller **wahren Sätze**, d.h.

$$S_1 = \{\varphi \in \mathcal{L}(\mathsf{PA}) : \mathcal{N} \models \varphi\}$$

und S_2 die Menge aller **$\mathcal{T}$-beweisbaren Sätze**, d.h.

$$S_2 := \{\varphi \in \mathcal{L}(\mathsf{PA}) : \mathcal{T} \vdash \varphi\}$$

Da $\mathbb{N} \models \mathcal{T}$, gilt $S_2 \subseteq S_1$. Es gibt ein **Beweisbarkeitsprädikat** $B_{\mathcal{T}} :\equiv \exists x\, Bew_{\mathcal{T}}(x, y)$, aber **kein Wahrheitsprädikat** W.
Also $S_1 \neq S_2$ und somit existiert ein Satz $\varphi \in S_1 \setminus S_2$. $\dashv$

Formalisierte Widerspruchfreiheit (Konsistenz):

$$\mathrm{KON}_{\mathcal{T}} := \neg B_{\mathcal{T}}(\lceil 0 = 1 \rceil)$$

(„0=1 ist in $\mathcal{T}$ nicht beweisbar")

Gödels 2. Unvollständigkeitssatz: $\mathcal{T}$ ist genau dann konsistent, wenn $\mathcal{T} \nvdash \mathrm{KON}_{\mathcal{T}}$, d.h. genau dann, wenn $\mathcal{T}$ **nicht** seine eigene Konsistenz beweist.

Ausblick: entscheidbare Fragmente von FO

über relationalen Signaturen ist SAT z.B. entscheidbar für:

- pränexe $\exists^*\forall^*$-Sätze
- pränexe gleichheitsfreie $\exists^*\forall\forall\exists^*$-Sätze
- pränexe $\exists^*\forall\exists^*$-Sätze
- FO-Sätze mit nur zwei Variablensymbolen

Ausblick: Andere Logiken (Beispiele)

Angewandte Modallogiken:

Anwendungen in der Wissensrepräsentation, KI

Fragment(e) von FO: eingeschränkte Quantifizierung

längs Kanten in Transitionssystemen;

Formeln mit einer freien Variablen

SAT entscheidbar

Temporallogiken LTL, CTL, μ-Kalkül

Anwendungen in Verfikation, model checking für

Transitionssysteme, (verzweigte) Prozesse, etc.

SAT entscheidbar, für viele Zwecke ausdrucksstärker als FO

ML: Modallogik

Hier über Σ-Transitionssystemen,
zu $S = \{E_a : a \in \Sigma\} \cup \{P_i : 1 \leq i \leq n\}$

Formeln von $\mathrm{ML}(S)$ sprechen über einzelne Zustände in Σ-Transitionssystemen mit atomaren Zustandseigenschaften p_i ! P_i

Syntax von $\mathrm{ML}(S)$

atomare Formeln: $\bot$, $\top$, p_i (wie AL_n)

AL Junktoren $\wedge, \vee, \neg$ wie üblich

modale Quantifizierung: $\Box_a\varphi$, $\Diamond_a\varphi$ für jedes $a \in \Sigma$

Semantik von $\mathrm{ML}(S)$ als Fragment von $\mathrm{FO}(S)$

$$\Box_a\varphi(x) \equiv \forall y\big(E_a xy \to \varphi(y)\big) : \quad \forall y\big((x \xrightarrow{a} y) \to \varphi(y)\big)$$

$$\Diamond_a\varphi(x) \equiv \exists y\big(E_a xy \wedge \varphi(y)\big) \quad : \quad \exists y\big((x \xrightarrow{a} y) \wedge \varphi(y)\big)$$

Monadische Logik zweiter Stufe: MSO

Monadische zweite Stufe MSO:

- Quantifizierung auch über alle Teilmengen der Trägermenge
- es existiert *kein* vollständiges Beweissystem
- Allgemeingültigkeit nicht einmal rekursiv aufzählbar

aber $\mathrm{SAT}(\mathrm{MSO})$ entscheidbar über interessanten Strukturklassen: z.B. Wortmodelle, lineare Ordnungen, Bäume

enger Zusammenhang mit Automatentheorie

Satz von Büchi: Reguläre Sprachen = MSO definierbare Wortmodellklassen.

Konstruktive („intuitionistische") Logik (L.E.J. Brouwer, A. Heyting)

Die Brouwer-Heyting-Kolmogorov ('BHK') Interpretation der logischen Konstanten (intendierte „konstruktive" Semantik):

(i) Es gibt keine Konstruktion (konstruktiven Beweis) für $\bot$.

(ii) Eine Konstruktion für $\varphi \wedge \psi$ ist ein Paar (q, r) von Konstruktionen, wobei q Konstruktion für φ und r Konstruktion für ψ ist.

(iii) Eine Konstruktion für $\varphi \vee \psi$ ist ein Paar (n, q), wobei $n \in \mathbb{N}$ und q Konstruktion für φ ist, falls $n = 0$, und für ψ, falls $n \neq 0$.

(iv) Eine Konstruktion p für $\varphi \to \psi$ ist ein Programm, das jede Konstruktion q für φ in eine Konstruktion $p(q)$ für ψ überführt.

(v) Eine Konstruktion für $\forall x\, \varphi(x)$ ist ein Programm p, das jedes Element d (des intendierten Universums) in eine Konstruktion $p(d)$ für $\varphi(d)$ überführt.

(vi) Eine Konstruktion für $\exists x\, \varphi(x)$ ist ein Paar (d, q), wobei d ein Element des Universums ist und q eine Konstruktion für $\varphi(d)$.

Beweiskalküle für intuitionistische Prädikatenlogik IL

Als logische Konstanten benötigen wir $\wedge, \vee, \rightarrow, \bot, \exists, \forall$.

Abkürzungen:

$\neg A :\equiv A \rightarrow \bot$, $A \leftrightarrow B :\equiv (A \rightarrow B) \wedge (B \rightarrow A)$.

Sequenzenkalkül $\mathcal{SK}_i$ für IL: Wie $\mathcal{SK}$, aber mit der Bedingung, dass der Kontext Δ so ist, dass rechts von $\vdash$ stets höchstens eine Formel steht.

Axiome von IL:

(i) $\varphi \vee \varphi \to \varphi, \quad \varphi \to \varphi \wedge \varphi;$

(ii) $\varphi \to \varphi \vee \psi, \quad \varphi \wedge \psi \to \varphi;$

(iii) $\varphi \vee \psi \to \psi \vee \varphi, \quad \varphi \wedge \psi \to \psi \wedge \varphi;$

(iv) $\bot \to \varphi;$

(v) $\forall x\, \varphi \to \varphi(t/x), \quad \varphi(t/x) \to \exists x\, \varphi,$
wobei t frei für x in φ.

Regeln von IL:

(i)

$$\frac{\varphi\,,\ \varphi \to \psi}{\psi}, \quad \frac{\varphi \to \psi\,,\ \psi \to \chi}{\varphi \to \chi};$$

(ii)

$$\frac{\varphi \wedge \psi \to \chi}{\varphi \to (\psi \to \chi)}, \quad \frac{\varphi \to (\psi \to \chi)}{\varphi \wedge \psi \to \chi};$$

(iii)

$$\frac{\varphi \to \psi}{\chi \vee \varphi \to \chi \vee \psi}$$

(iv)

$$\frac{\psi \to \varphi}{\psi \to \forall x\, \varphi}, \quad \frac{\varphi \to \psi}{\exists x\, \varphi \to \psi}, \text{ wobei } x \text{ nicht frei in } \psi.$$

Gleichheitsaxiome: wie für FO.

Gewöhnliche Logik FO ensteht aus IL durch Hinzufgung des Schemas vom ausgeschlossenen Dritten

$$\varphi \vee \neg\varphi.$$

Beispiele: konstruktiv beweisbar: $(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$,
jedoch **nicht** $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$.

Konstruktiv: $\neg\exists x\, \varphi(x) \leftrightarrow \forall x\, \neg\varphi(x)$,
jedoch **nicht**: $\neg\forall x\, \varphi(x) \to \exists x\, \neg\varphi(x)$.

Satz (Gödel 1933): Γ, φ sei aus doppelt negierten atomaren Formeln $\neg\neg R(t_1, \ldots, t_n), \neg\neg s = t$ mittels $\wedge, \to, \bot, \forall$ aufgebaut.
Dann gilt $\Gamma \vdash \varphi$ gdw. $\Gamma \vdash_{\mathrm{IL}} \varphi$.

Ausblick: entscheidbare Theorien

Beispiele:

entscheidbar	dagegen unentscheidbar
MSO-Theorie von Bäumen (Rabin)	Graphentheorie, FO
FO-Th$(\mathbb{R}, +, \cdot, 0, 1, <)$ (Tarski)	FO-Th$(\mathbb{N}, +, \cdot, 0, 1, <)$
FO-Th$(\mathbb{N}, +, 0, 1, <)$ (Presburger)	
FO-Theorie abelscher Gruppen	Gruppentheorie, FO

Ausblick: Ausdrucksstärke verschiedener Logiken

Welche Struktureigenschaften können in gegebener Logik formalisiert werden?

Welche Eigenschaften sind nicht ausdrückbar?

z.B. *nicht* in FO: Endlichkeit der Trägermenge

Zusammenhang von (endlichen) Graphen

gerade Länge endlicher linearer Ordnungen

...

Fragen der Ausdrucksstärke

Kernfrage: Welche Logik wofür?

Z.B. bei der Wahl einer Logik als Sprache für

Spezifikation, Verifikation, Deduktion

Wissensrepräsentation, Datenbankabfragen

Kriterien: algorithmische Eigenschaften

beweistheoretische Eigenschaften

Ausdrucksstärke

- wie kann man analysieren, was ausdrückbar ist?
- wie erkennt/beweist man, dass etwas *nicht* ausdrückbar ist?

Ehrenfeucht-Fraïssé Spiele

(vgl. Semantikspiel zwischen Verifizierer und Falsifizierer)

Idee: Spielprotokoll für zwei Spieler **I** und **II**

zum Vergleich zweier Strukturen so, dass

$\mathcal{A}$ und $\mathcal{B}$ ähnlich (ununterscheidbar in L)

wenn Spieler **II** Gewinnstrategie hat.

Spieler **II** muss in der jeweils anderen Struktur nachmachen,

was **I** in einer der Strukturen vorgibt

Spieler **I** versucht das Spiel auf Unterschiede zu lenken,

die das für **II** unmöglich machen

Verwendung

Wenn $\mathcal{A}$ und $\mathcal{B}$ ununterscheidbar in L,
aber verschieden hinsichtlich Eigenschaft E,
dann lässt sich E *nicht* in L ausdrücken

Klassisches Ehrenfeucht-Fraïssé Spiel für FO

Fixiere feste endliche relationale Signatur S

zB für Wortstrukturen zu Alphabet Σ: $S = \{<\} \cup \{P_a : a \in \Sigma\}$

Ununterscheidbarkeitsgrade $\mathcal{W}, \mathbf{m} \equiv_q \mathcal{W}', \mathbf{m}'$

f.a. $\varphi(\mathbf{x}) \in \mathrm{FO}(S)$ mit $\mathrm{qr}(\varphi) \leq q$:

$\mathcal{W} \models \varphi[\mathbf{m}] \quad \Leftrightarrow \quad \mathcal{W}' \models \varphi[\mathbf{m}']$

insbesondere für $q = 0$, $\mathbf{m} = (m_1, \ldots, m_k)$, $\mathbf{m}' = (m'_1, \ldots, m'_k)$
$\mathcal{W}, \mathbf{m} \equiv_0 \mathcal{W}', \mathbf{m}'$ gdw. $\rho : (m_i \mapsto m'_i)_{1 \leq i \leq k}$ lokaler Isomorphismus

Spielidee: **I** markiert zukzessive Elemente in $\mathcal{W}$ oder $\mathcal{W}'$,

II antwortet in der jeweils anderen Struktur,

II muss $\mathcal{W}, \mathbf{m} \equiv_0 \mathcal{W}', \mathbf{m}'$ gewährleisten

Diee Spiele $G^q(\mathcal{W}, \mathcal{W}')$ und $G^q(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$

Konfigurationen:

$(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ mit $\mathbf{m} = (m_1, \ldots, m_k)$ und $\mathbf{m}' = (m'_1, \ldots, m'_k)$ wenn in $\mathcal{W}$ und $\mathcal{W}'$ jeweils k Elemente markiert sind

Zugabtausch in einer Runde:

I markiert in $\mathcal{W}$ oder in $\mathcal{W}'$ ein weiteres Element,

II ein Element in der jeweils anderen Struktur

von

$(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$

zu Nachfolgekonfiguration

$(\mathcal{W}, \mathbf{m}, m_{k+1}; \mathcal{W}', \mathbf{m}', m'_{k+1})$

Gewinnbedingung:

II verliert wenn $\mathcal{W}, \mathbf{m} \not\equiv_0 \mathcal{W}', \mathbf{m}'$

$\boldsymbol{G^q(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')}$:

Spiel über q Runden mit Startkonfiguration $(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$

Ehrenfeucht-Fraïssé Satz

Für alle $q \in \mathbb{N}$, S-Strukturen $\mathcal{W}$ und $\mathcal{W}'$ mit Parametern $\mathbf{m} = (m_1, \ldots, m_k)$ in $\mathcal{W}$ und $\mathbf{m}' = (m'_1, \ldots, m'_k)$ in $\mathcal{W}'$ sind äquivalent:

(i) **II** hat Gewinnstrategie in $G^q(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$

(ii) $\mathcal{W}, \mathbf{m} \equiv_q \mathcal{W}', \mathbf{m}'$

Beweis per Induktion über q. Strategieanalyse!

$q = 0$: trivial.

Gewinnstrategie für eine Runde verlangt gerade Übereinstimmung hinsichtlich Existenzbeispielen für z in allen Formeln $\exists z\varphi(\mathbf{x}, z)$ mit quantorenfreiem φ (warum?)

Gewinnstrategie für $q + 1$ Runden verlangt analog, in der ersten Runde, Übereinstimmung hinsichtlich aller Formeln $\exists z\varphi(\mathbf{x}, z)$ mit $\mathrm{qr}(\varphi) \leq q$

Zusammenfassung

Syntax der Aussagenlogik und der Prädikatenlogik

- AL, FO, Terme, freie Variablen, Formeln etc.
- Normalformen für aussagenlogische Äquivalenz: **DNF, KNF**.
- Normalformen für prädikatenlogische Äquivalenz: **pränexe Normalform**.
- Erfüllbarkeitsnormalform: **Skolemnormalform**.
- Gültigkeitsnormalform: **Herbrandnormalform**.
- **Beweiskalküle:** Hilbertkalküle, Resolutionskalkül, Sequenzenkalkül.

Semantik der Aussagenlogik und der Prädikatenlogik

- Aussagenlogik: **Belegungen** und **Wahrheitsfunktionen**.
- **Strukturen** und **Interpretationen** zu Signaturen
- **Interpretation von Termen** in Interpretationen.
- **Wahrheit** von Formeln (Sätzen) in Interpretationen (Strukturen).
- Modellbeziehung: $\Gamma \models \varphi$.

Lernziele

- Zentrale Begriffe/Konzepte inhaltlich beherrschen und im Kontext sinnvoll anwenden können.
- Zentrale Sätze und Resultate kennen und anwenden können.

Zentrale Sätze

- Kompaktheit (Endlichkeitssätze).
- Satz über Herbrand-Modelle.
- Sätze über Skolem- und Herbrandnormalform.
- Satz von Herbrand.
- Reduktionen von FO auf AL.
- Korrektheits- und Vollständigkeitsaussagen zu Kalkülen.
- Entscheidbarkeit und Unentscheidbarkeit.
- Nichtdefinierbarkeit (Tarski) und Unvollständigkeit (Gödel).

Wiederholung: Beispiele

AL-Formeln auswerten (systematisch: Wahrheitstafel)

AL-Formeln auf Folgerung bzw. Äquivalenz untersuchen

natürlichsprachliche Bedingungen in AL formalisieren

Unerfüllbarkeit mittels Resolution nachweisen

Allgemeingültigkeit formal im Sequenzenkalkül nachweisen

Folgerungsbeziehungen reduzieren auf Unerfüllbarkeit/Allgemeingültigkeit

Kompaktheitssatz anwenden

Kalküle rechtfertigen (z.B. Korrektheit von Regeln)

Wiederholung: Beispiele

Umgang mit Strukturen

auch spezielle Strukturen und Klassen wie z.B.

Graphen, Transitionssysteme, relationale DB-Strukturen,

Wortmodelle, linear-temporale Abfolgen, $\mathcal{N}$

Auswerten von Termen und Formeln in Strukturen

PNF, Skolemisieren, Substitutionen ausführen

Herbrandmodelle beschreiben/untersuchen

Unerfüllbarkeit durch Reduktion auf AL nachweisen

GI-Resolution und Sequenzenkalkül in Beispielen

etc.