

Formale Grundlagen der Informatik II

SS 2012

Prof. Dr. Ulrich Kohlenbach
TUD, Fachbereich Mathematik
Assistenz: Dr. Alexander Kreuzer, Pavol Safarik

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 2010)
- 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):** $\neg, \wedge, \vee, \rightarrow, \dots$
- **Formalisierung komplexerer Eigenschaften**
- **Wahrheitsfunktionale Semantik**
- **Korrekte und vollständige Beweiskalküle**

Syntax der Aussagenlogik AL

Symbole der Sprache: Wahrheitswerte: 0, 1;

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

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

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

atomare Formeln: 0, 1, p in $AL(\mathcal{V})$ (wobei $p \in \mathcal{V}$).

Negation: für $\varphi \in AL(\mathcal{V})$ ist auch $\neg\varphi \in AL(\mathcal{V})$.

Konjunktion: für $\varphi, \psi \in AL(\mathcal{V})$ ist auch $(\varphi \wedge \psi) \in AL(\mathcal{V})$.

Disjunktion: für $\varphi, \psi \in AL(\mathcal{V})$ ist auch $(\varphi \vee \psi) \in AL(\mathcal{V})$.

Weitere Junktoren (offiziell als Abkürzungen)

z.B. $(\varphi \rightarrow \psi) := (\neg\varphi \vee \psi),$
 $(\varphi \leftrightarrow \psi) := ((\neg\varphi \wedge \neg\psi) \vee (\varphi \wedge \psi)).$

Meistens: abzählbar unendlich viele Variablen

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

Manchmal auch **endliche** Variablenmenge

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

Semantik der Aussagenlogik AL

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

\mathcal{V} -Interpretation (Belegung):

$$\begin{array}{lcl} \mathcal{I}: \mathcal{V} & \longrightarrow & \mathbb{B} \\ p & \longmapsto & \mathcal{I}(p) \end{array}$$

\mathcal{I} interpretiert p als $\left\{ \begin{array}{ll} \text{“wahr”} & \text{wenn } \mathcal{I}(p) = 1, \\ \text{“falsch”} & \text{wenn } \mathcal{I}(p) = 0. \end{array} \right.$

Definition der Semantik von komplexen Formeln

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

Wahrheitswertfunktion $\mathfrak{I}: \text{AL}(\mathcal{V}) \longrightarrow \mathbb{B}$

$$\varphi \longmapsto \varphi^{\mathfrak{I}}$$

induktiv über den Aufbau der Formeln $\varphi \in \text{AL}(\mathcal{V})$ 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

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

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

Sprechweisen: \mathcal{I} **erfüllt** φ ,

\mathcal{I} **ist Modell von** φ ,

φ **ist wahr unter** \mathcal{I} .

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

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

Semantik und Wahrheitstafeln

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

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

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

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

Wahrheitstafeln: die Wertetabelle der Funktion

$$\mathbb{B}^n \longrightarrow \mathbb{B}$$

$$(b_1, \dots, b_n) \longmapsto \varphi[b_1, \dots, b_n]$$

bestimmt die Semantik von φ vollständig!

p	$\neg p$	p	q	$p \wedge q$	p	q	$p \vee q$	p	q	$p \rightarrow q$
0	1	0	0	0	0	0	0	0	0	1
1	0	0	1	0	0	1	1	0	1	1
		1	0	0	1	0	1	1	0	0
		1	1	1	1	1	1	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 $\varphi, \psi \in \text{AL}(\mathcal{V})$

$$\varphi \models \psi,$$

in Worten

„ ψ folgt aus φ “,

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

$$\mathcal{I} \models \varphi \Rightarrow \mathcal{I} \models \psi.$$

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

Allgemeingültigkeit:

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

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

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:

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

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

Schreibweise: $\varphi \equiv \psi$.

Sämtlich äquivalent: $\varphi \equiv \psi$

$$\models \varphi \leftrightarrow \psi$$

$$\varphi \models \psi \text{ und } \psi \models \varphi$$

Beispiele (vgl. Identitäten in Booleschen Algebren)

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

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

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

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

Erfüllbarkeit

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

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

Φ erfüllbar, wenn $\mathcal{I} \models \Phi$ für mindestens ein \mathcal{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: $\text{SAT}(\text{AL}) = \{\varphi \in \text{AL} : \varphi \text{ erfüllbar} \}$ 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

$$f : \mathbb{B}^n \longrightarrow \mathbb{B}$$

$$(b_1, \dots, b_n) \longmapsto f(b_1, \dots, b_n)$$

für $\varphi \in \text{AL}_n$:

$$f_\varphi : \mathbb{B}^n \longrightarrow \mathbb{B}$$

$$(b_1, \dots, b_n) \longmapsto \varphi[b_1, \dots, b_n]$$

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

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

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

$$[\varphi]_{\equiv} \longmapsto f_\varphi$$

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 $\varphi \in \text{AL}_n$ 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 $\varphi \in \text{AL}_n$ mit $f = f_\varphi$.

Korollar: Zu jedem $\varphi \in \text{AL}_n$ existieren:

DNF-Formel $\varphi_1 \in \text{AL}_n$ mit $\varphi_1 \equiv \varphi$ und KNF-Formel $\varphi_2 \in \text{AL}_n$ 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

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

Analog:

$$\neg(\bigvee \Phi) \equiv \bigwedge \Phi^\neg.$$

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

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

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

Beispiel für exponentiellen “blow-up”

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

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

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

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

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

- keine kürzere DNF: $\left\{ \begin{array}{l} \text{keine kürzeren Disjunktionsglieder!} \\ \text{keine redundanten Disjunktionsglieder!} \end{array} \right.$

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 $p | q := \neg(p \wedge q)$ (NAND; „Sheffer stroke“): benutze z.B.: $\neg p \equiv p | p$;
 $p \wedge q \equiv \neg(p | q) \equiv (p | q) | (p | q)$.
- \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 $\Phi \subseteq \text{AL}$, $\psi \in \text{AL}$).

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

Beweis des Kompaktheitssatzes

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

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

Konstruiere induktiv $\mathfrak{I}_0, \mathfrak{I}_1, \mathfrak{I}_2, \dots$ 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 $\mathfrak{I}: \mathcal{V} \longrightarrow \mathbb{B}$

$$p_n \longmapsto \mathfrak{I}_n(p_n)$$

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}_{n+1}^0 (bzw. \mathfrak{I}_{n+1}^1) die Fortsetzung von \mathfrak{I}_n mit $\mathfrak{I}_{n+1}^0(p_{n+1}) = 0$ (bzw. $\mathfrak{I}_{n+1}^1(p_{n+1}) = 1$). Annahme: für $i \in \{0, 1\}$ existiert endliches $\Phi^i \subseteq \Phi$, das von keiner mit \mathfrak{I}_{n+1}^i 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: $\frac{\varphi}{\psi \vee \varphi}, \frac{\varphi \vee \varphi}{\varphi}, \frac{\varphi \vee (\psi \vee \chi)}{(\varphi \vee \psi) \vee \chi}, \frac{\varphi \vee \psi, \neg\varphi \vee \chi}{\psi \vee \chi}.$

$\Phi \vdash \psi$ („ 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; \bar{L} für komplementäres Literal; $\bar{L} \equiv \neg L$.

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

Bemerkung:

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

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

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

endliche Klauselmengen \approx KNF-Formeln

Resolutionskalkül arbeitet mit KNF in Klauselform

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

Resolution

Beobachtungen:

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

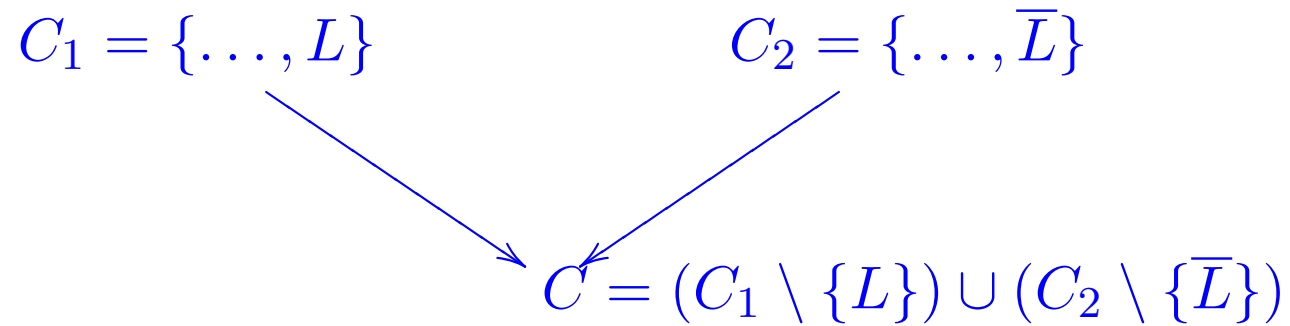
Resolventen:

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

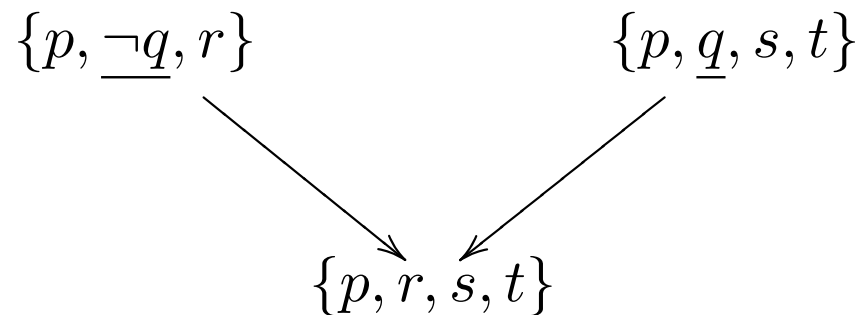
wobei

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

Baumdarstellung



Beispiel:



Beweise im Resolutionskalkül 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 $K \models C$).

$\text{Res}(K)$ und $\text{Res}^*(K)$:

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

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

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

Korrektheit und Vollständigkeit des Resolutionskalküls

Korrektheit: $\square \in \text{Res}^*(K) \Rightarrow K \equiv 0$ unerfüllbar.
(Diese Aussage folgt sofort aus dem Resolutionslemma)

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

Beweis der Vollständigkeit

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

Beweis durch Induktion über n .

Induktionsschritt von n nach $n + 1$

Aus $K = \{C_1, \dots, C_k\}$ 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

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

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

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

Resolutionsalgorithmus

Eingabe: K	[Klauselmenge, endlich]
--------------	-------------------------

$R := K$

WHILE ($\text{Res}(R) \neq R$ and $\square \notin R$) DO $R := \text{Res}(R)$ 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: $C = \{\neg q_1, \dots, \neg q_r, q\} \equiv (q_1 \wedge \dots \wedge q_r) \rightarrow q$;
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 Hornklauselmeng; $H^- \subseteq H$ 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:

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

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

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

Sequenzkalkül (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 (Antezedent): 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:
$$\frac{\text{Prämissen}}{\text{Konklusion}}$$

Beispiele:
$$\frac{}{\Gamma, \varphi \vdash \Delta, \varphi} \quad \text{oder} \quad \frac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$$

AL Sequenzenkalkül \mathcal{SK}

$$(\text{Ax}) \quad \overline{\Gamma, p \vdash \Delta, p} \quad (p \in \mathcal{V})$$

$$(0\text{-Ax}) \quad \overline{\Gamma, 0 \vdash \Delta}$$

$$(1\text{-Ax}) \quad \overline{\Gamma \vdash \Delta, 1}$$

$$(\neg\text{L}) \quad \frac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$$

$$(\neg\text{R}) \quad \frac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$$

$$(\vee\text{L}) \quad \frac{\Gamma, \varphi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}$$

$$(\vee\text{R}) \quad \frac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}$$

$$(\wedge L) \quad \frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}$$

$$(\wedge R) \quad \frac{\Gamma \vdash \Delta, \varphi \quad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$$

$$(\rightarrow L) \quad \frac{\Gamma \vdash \Delta, \varphi \quad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \rightarrow \psi \vdash \Delta}$$

$$(\rightarrow R) \quad \frac{\Gamma, \varphi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \rightarrow \psi}$$

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**

$$\begin{array}{c}
 p \vdash (p \wedge q) \vee \neg q \\
 \\
 \begin{array}{ccc}
 & & (Ax) \quad \frac{}{} \\
 (Ax) \quad \frac{}{} & & \frac{}{} \\
 p \vdash p, \neg q & & (\neg R) \quad \frac{}{} \\
 & & p \vdash q, \neg q \\
 (\wedge R) \quad \frac{}{} & & \\
 & & p \vdash (p \wedge q), \neg q \\
 (\vee R) \quad \frac{}{} & & \\
 & & p \vdash (p \wedge q) \vee \neg q
 \end{array}
 \end{array}$$

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

$$\begin{array}{c}
 \text{(Ax)} \quad \frac{}{p \vdash p} \qquad \text{p} \vdash \text{q} \qquad \text{(Ax)} \quad \frac{}{q \vdash q} \\
 \text{(\wedge R)} \quad \frac{}{p \vdash p \wedge q} \qquad \text{p} \vdash \text{q} \qquad \text{(\wedge R)} \quad \frac{}{q \vdash p \wedge q} \\
 \text{(\vee L)} \quad \frac{}{p \vee q \vdash p \wedge q}
 \end{array}$$

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 Hinzufügung der sogenannten Schnittregel (CUT), die zum modus ponens korrespondiert:

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

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):

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

und

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

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:

$x, y, z, \dots, x_1, x_2, x_3, \dots$ Variablensymbole

c, d, e, \dots Konstantensymbole

f, g, \dots Funktionssymbole

P, Q, R, \dots Relationssymbole

Signatur S :

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

Strukturen zu Signatur S

S -Struktur:

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

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 $f^{\mathcal{A}}: A^n \rightarrow A$.

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

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

Beispiele

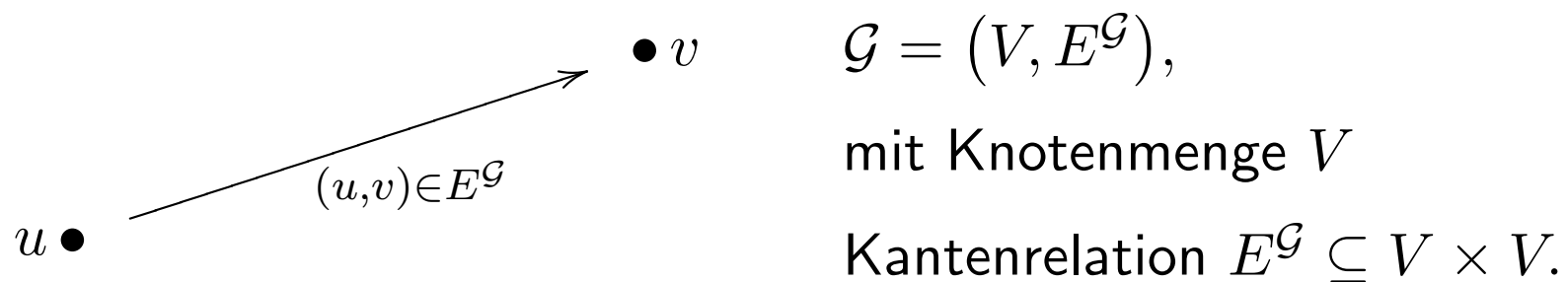
Wortstrukturen zu $S = \{<\} \cup \{P_a : a \in \Sigma\}$

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

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

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

Graphen zu $S = \{E\}$



Weitere Beispiele

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

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

Relationale Datenbanken, ...

Terme

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

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

$$x \in T(S) \quad \text{für } x \in \mathcal{V}.$$

$$c \in T(S) \quad \text{für } c \in S.$$

$$ft_1 \dots t_n \in T(S) \quad \text{für } f \in S \text{ (} n\text{-st.)}, t_1, \dots, t_n \in T(S).$$

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

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

Beispiele wohlgeformter S -Terme

$S = \{f, c\}$, f 2-st.: $c, f f c c c, f c f c c, \dots, x_{17}, f x_1 c, f f x_5 c x_2,$
...

$S = \{+, \cdot, 0, 1\}$, $+, \cdot$ 2-st.: $\cdot + 11 + + 111,$
 $+ \cdot + + 111 x_3 x_1, \dots$

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

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

Term-Strukturen und Herbrand-Strukturen

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

- $\mathcal{T} = \mathcal{T}(S) = (T(S), \dots, c^{\mathcal{T}(S)}, \dots, f^{\mathcal{T}(S)}, \dots, R^{\mathcal{T}(S)}, \dots)$
- $c \in S : c^{\mathcal{T}} := c \in T(S)$.
- $f \in S$ (n-st.) : $f^{\mathcal{T}} : T(S)^n \longrightarrow T(S)$
 $(t_1, \dots, t_n) \longmapsto ft_1 \dots t_n$.
- 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 $\mathcal{A} = (A, c^{\mathcal{A}}, \dots, f^{\mathcal{A}}, \dots)$:

$$\beta: \mathcal{V} \longrightarrow A$$

$$x \longmapsto \beta(x)$$

S -Interpretation:

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

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

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

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

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

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

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 $\text{FO}(S)$

Induktive Definition der Menge der $\text{FO}(S)$ Formeln:

- **atomare Formeln:**
 - für $t_1, t_2 \in T(S)$: $t_1 = t_2 \in \text{FO}(S)$.
 - für $R \in S$ (n -st.), $t_1, \dots, t_n \in T(S)$: $Rt_1 \dots t_n \in \text{FO}(S)$.
- **AL-Junktoren:**
 - für $\varphi, \psi \in \text{FO}(S)$: $\neg\varphi \in \text{FO}(S)$.
 - $(\varphi \wedge \psi) \in \text{FO}(S)$.
 - $(\varphi \vee \psi) \in \text{FO}(S)$.
- **Quantifizierung:**
 - für $\varphi \in \text{FO}(S)$, $x \in \mathcal{V}$: $\exists x\varphi \in \text{FO}(S)$.
 - $\forall x\varphi \in \text{FO}(S)$.

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

Syntax: freie und gebundene Variablen, Quantorenrang

Freie Variablen

$$\text{frei}: \text{FO}(S) \longrightarrow \mathcal{P}(\mathcal{V})$$

$$\varphi \longmapsto \text{frei}(\varphi) \subseteq \mathcal{V}$$

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:

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

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

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

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

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

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

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

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

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

Misst die **Quantorschachtelungstiefe!**

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

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

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

Semantik von $\text{FO}(S)$

Der **Wahrheitswert** $\varphi^{\mathfrak{I}}$ von $\text{FO}(S)$ -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: $(\exists x\varphi)^{\mathfrak{I}} = \max(\varphi^{\mathfrak{I}[x \mapsto a]} : a \in A)$.

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

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 $x \in \text{frei}(\varphi)$.

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

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

Semantische Grundbegriffe

Analog zu AL:

Folgerungsbeziehung:

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

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

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

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

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 $\varphi(x) \in \text{FO}(S)$,
 $\varphi' := \varphi(t/x) \in \text{FO}(S)$ so, dass:

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

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

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

Negationsnormalform

Eine Formel $\varphi \in \text{FO}(S)$ 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 $\varphi^* \in \text{NNF}$ konstruieren, die zu φ logisch äquivalent ist, d.h. $\varphi \equiv \varphi^*$.

Beweis: Übungsaufgabe!

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

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

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

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

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

zieht nach (ψ_1, \mathbf{a}) oder nach (ψ_2, \mathbf{a}) .

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

zieht nach (ψ_1, \mathbf{a}) oder nach (ψ_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 (ψ, \mathbf{a}) , ψ atomar oder negiert atomar.

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

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

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

FO ohne $=$: FO^\neq

- In unserer Behandlung von FO: Gleichheit $R :=$ Bestandteil der Logik, d.h. spezielle Interpretation als mengentheoretische Identität auf A in \mathcal{A} .
- Alternativ: $=$ ist nicht Bestandteil der Logik (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 FO[≠]

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:

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

\sim -Äquivalenzklassen als Elemente.

Erfüllbarkeit universeller Sätze ohne Gleichheit in Herbrand-Modellen

Voraussetzungen:

- S enthalte mindestens ein Konstantensymbol
- $\Phi \subseteq \text{FO}_0^\neq(S)$: 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

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

Beweisidee: " \Leftarrow ": offensichtlich.

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

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

□

Verfeinerungen

Sei $\varphi := \forall x_1, \dots, x_n \varphi_{qf}(x_1, \dots, x_n) \in \Phi$ (φ_{qf} quantorfrei).

Betrachte die Menge $E(\Phi)$ aller geschlossenen $T_0(S)$ -Instanzen

$$\varphi_{qf}(t_1, \dots, t_n) \quad (t_1, \dots, t_n \in T_0(S))$$

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

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

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

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

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

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

Für

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

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

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

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

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

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 '='. $\underline{x} = x_1, \dots, x_n$ ist ein Tupel von Variablen. Dann gilt

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

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

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

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

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

Satz von Herbrand für offene Theorien

Eine Menge Γ von S -Sätzen (in der Logik mit Gleichheit $=$) heißt *offen*, falls jeder Satz in Γ ein reiner \forall -Satz

$\forall y_1, \dots, y_m \psi_{qf}(y_1, \dots, y_m)$ ist.

Satz: Sei $\varphi = \exists \underline{x} \varphi_{qf}(\underline{x})$ ein reiner \exists -Satz (d.h. φ_{qf} ist quantorfrei). Dann gilt

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

Tatsächlich ist $\bigvee_{i=1}^k \varphi_{qf}(\underline{t}_i)$ sogar eine tautologische Folgerung aus endlich vielen geschlossenen Instanzen von $=$ - und Γ -Axiomen.

Statt $T_0(S)$ genügen alle aus φ, Γ gebildeten geschl. Terme.

Beweis

Betrachte „ $=$ “ als gewöhnliches binäres Relationssymbol, dass durch den \forall -Abschluss E der Gleichheitsaxiome axiomatisiert wird. Wende nun den Satz über Herbrand-Modelle an auf $\Phi := \Gamma \cup E \cup \{\forall \underline{x} \neg \varphi_{qf}(\underline{x})\}$.

Pränexe Normalform

Definition: Eine Formel $\varphi \in \text{FO}(S)$ 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 $Q_i \in \{\forall, \exists\}$, $k \in \mathbb{N}$, φ_{qf} quantorfrei.

Beispiele:

$$\begin{aligned} \exists y (Exy \wedge \forall x (Eyx \rightarrow x = y)) &\equiv \exists y \forall z (Exy \wedge (Eyz \rightarrow z = y)) \\ \exists y \forall x Exy \vee \neg \exists y Exy &\equiv \exists y_1 \forall y_2 \forall y_3 (Ey_2 y_1 \vee \neg Exy_3) \end{aligned}$$

Satz über PNF

Satz über die Pränexnormalform:

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

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

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 $\forall x_{i_1} \dots \forall x_{i_k} \varphi_{qf}$, 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 \forall]

Beispiel

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

dann gilt:

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

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

es gibt eine Interpretation von f über A so, dass

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

Satz über die Skolemnormalform

Satz: Jedes $\varphi \in \text{FO}$ 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):

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

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

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

φ^S impliziert logisch trivialerweise 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, \dots, 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 . \square

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

Herbrandnormalform

Satz: Jedes $\varphi \in \text{FO}$ 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):

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

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

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

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

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

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

$\left\{ \begin{array}{l} \text{erf.-äquiv. (neue Konst. statt freien Var.)} \end{array} \right.$

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

$\left\{ \begin{array}{l} \text{erf.-äquiv. (Vorschalten } \neg\text{-Ax.)} \end{array} \right.$

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

$\left\{ \begin{array}{l} \text{erf.-äquiv. (Skolemnormalform)} \end{array} \right.$

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

$$\Phi \text{ erfüllbar} \Leftrightarrow \Phi''' \text{ erfüllbar} \Leftrightarrow \Phi''' \text{ in Herbrand-Modell erfüllbar}$$

Bedingungen an Herbrand-Modell lassen sich in AL kodieren!

Erfüllbarkeit: Reduktion auf AL

(fortges.): o.B.d.A.:

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

S habe Konstanten

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

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

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

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

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

\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:

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

ist **unerfüllbar**.

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

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

Fortsetzung des Beispiels

AL-Variablen für die Reduktion:

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

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

zugeh. AL-Formeln

$$\left\{ \begin{array}{l} \llbracket \varphi_1 \rrbracket^{\text{AL}} = \{ r_{\ell, m} \rightarrow (q_\ell \leftrightarrow \neg q_m) : \ell, m \in \mathbb{N} \} \\ \llbracket \varphi_2 \rrbracket^{\text{AL}} = \{ r_{\ell, \ell+1} \vee r_{\ell+1, \ell} : \ell \in \mathbb{N} \} \\ \llbracket \varphi_3 \rrbracket^{\text{AL}} = \{ \neg r_{\ell, m} \rightarrow r_{\ell, m+2} : \ell, m \in \mathbb{N} \} \end{array} \right.$$

Unerfüllbarkeit von Φ folgt aus Unerfüllbarkeit von

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

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

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

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

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

$$\underbrace{r_{2,1} \rightarrow (q_2 \leftrightarrow \neg q_1)}_{\in \llbracket \varphi_1 \rrbracket^{\text{AL}}} \quad \underbrace{r_{1,2} \vee r_{2,1}}_{\in \llbracket \varphi_2 \rrbracket^{\text{AL}}} \quad \underbrace{\neg r_{0,0} \rightarrow r_{0,2}}_{\in \llbracket \varphi_3 \rrbracket^{\text{AL}}}$$

Kompaktheitssatz (Endlichkeitssatz):**Version 1:** (Erfüllbarkeit)

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

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

Version 2: (Folgerungsbeziehung)

Für $\Phi \subseteq \text{FO}, \varphi \in \text{FO}$ 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 $\Phi \subseteq \text{FO}_0^\neq$: Reduktion auf AL

Konsequenzen des Endlichkeitssatzes

Beliebig große endliche Modelle \Rightarrow unendliche Modelle: zu Φ

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

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 $c \neq 0, c \neq 1, c \neq 2, \dots$ (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: $\frac{\varphi}{\psi \vee \varphi}, \frac{\varphi \vee \varphi}{\varphi}, \frac{\varphi \vee (\psi \vee \chi)}{(\varphi \vee \psi) \vee \chi}, \frac{\varphi \vee \psi, \neg\varphi \vee \chi}{\psi \vee \chi}$

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

Alternativ für \exists : $\varphi(t/x) \rightarrow \exists x \varphi$ und $\frac{\varphi \rightarrow \psi}{\exists x \varphi \rightarrow \psi}$ falls $x \notin \text{frei}(\psi)$
mit $\varphi \rightarrow \psi := \neg\varphi \vee \psi$.

Alternativer Hilbertkalkül für $\{\wedge, \rightarrow, \vee, \perp, \forall, \exists\}$ **Logische Axiomschemata** ($\neg\varphi := \varphi \rightarrow \perp$):

- (i) $\varphi \rightarrow (\psi \rightarrow \varphi)$,
- (ii) $(\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$,
- (iii) $\varphi \rightarrow \varphi \vee \psi$, (iv) $\psi \rightarrow \varphi \vee \psi$,
- (v) $(\varphi \rightarrow \chi) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\varphi \vee \psi \rightarrow \chi))$,
- (vi) $\varphi \wedge \psi \rightarrow \varphi$, (vii) $\varphi \wedge \psi \rightarrow \psi$,
- (viii) $\varphi \rightarrow (\psi \rightarrow \varphi \wedge \psi)$,
- (x) $\perp \rightarrow \varphi$, (xi) $\neg\neg\varphi \rightarrow \varphi$,
- (xii) $\forall x \varphi \rightarrow \varphi[t/x]$, (xiii) $\varphi[t/x] \rightarrow \exists x \varphi$,

wobei in (xii), (xiii) der Term t frei für x in φ sein muss.

Logische Regeln:

$$\frac{\varphi \quad , \quad \varphi \rightarrow \psi}{\psi},$$

$$\frac{\varphi \rightarrow \psi}{\varphi \rightarrow \forall x \psi},$$

$$\frac{\psi \rightarrow \varphi}{\exists x \psi \rightarrow \varphi},$$

wobei in den letzten beiden Regeln x nicht frei in φ vorkommen darf.

Erweiterung um Gleichheitsaxiome

$$x = x \text{ (Reflexivität),}$$

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

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

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

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

Bemerkung: Die Gleichheitsaxiome implizieren:

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

und

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

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

Symmetrie und Transitivität folgen tatsächlich bereits aus den anderen Axiomen (wenn man '=' als Relationssymbol P zuläßt).

Grundinstanzen-Resolution (GI-Resolution):

Gegenstand: FO^\neq -Klauselmengen K

(universelle 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) FO[≠]-Sätze in Klauselform:

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

$\xi \equiv K$ für endliche Klauselmengen K über FO[≠]-Literalen

FO[≠]-Literale:

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

FO[≠]-Klauseln: endliche Mengen C von FO[≠]-Literalen

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

FO[≠]-Klauselmengen: Mengen K von FO[≠]-Klauseln

Klauselmengen und universell-pränexe Sätze

Semantisch identifiziere Klauselmengen mit Satzmenge:

$$K \equiv \left\{ \underbrace{\forall x_1 \dots \forall x_n}_{\text{alle Variablen in } C} \vee C : C \in K \right\}$$

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

Korrespondenzen

endliche	!	universell-pränexe
FO^\neq Klauselmengen		FO^\neq -Sätze

FO^\neq Klauselmengen	!	universell-pränexe
		FO^\neq -Satzmengen

Übersetzungs-Beispiel

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

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

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

Kern von φ in KNF (z.B.):

$$(\neg \alpha \vee \beta_1 \vee \beta_2) \wedge (\neg \alpha \vee \neg \beta_2 \vee \neg \beta_1)$$

$$\begin{aligned} K &= \{ \{ \neg \alpha, \beta_1, \beta_2 \}, \{ \neg \alpha, \neg \beta_1, \neg \beta_2 \} \} \\ &= \{ \{ \neg Rxy, Qx, Qy \}, \{ \neg Rxy, \neg Qy, \neg Qx \} \} \end{aligned}$$

Grundinstanzen-Resolution (GI)

Übertragung von AL-Resolution gemäß Reduktionsansatz
ähnlich wie schon für andere Erfüllbarkeitsargumente

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

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

mit $t_i \in T_0(S)$

Grundinstanzenmenge einer Klauselmenge K :

$$\text{GI}(K) := \{C(t_1/x_1, \dots) : C \in K, t_i \in T_0(S)\}$$

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

und aus dem **Satz von Herbrand**:

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

GI-Resolution: Resolventen

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

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

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

$$C_1 = \{\lambda_1, \dots, \lambda_k, \underline{\lambda}\}$$

$$C_2 = \{\lambda'_1, \dots, \lambda'_\ell, \bar{\lambda}\}$$

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

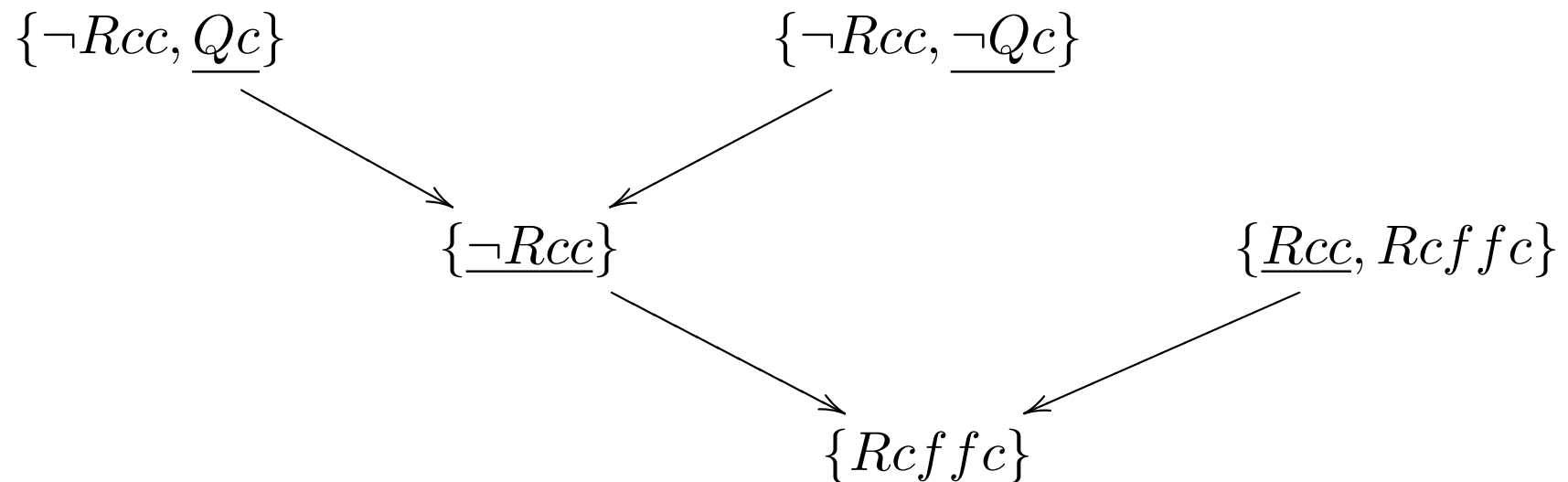
Zu Klauselmengemenge K über variablenfreien $\text{FO}^\neq(S)$ -Literalen:

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

Beispiel

Über Grundinstanzen von

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



$$\left. \begin{array}{l} \forall x \forall y (\neg Rxy \vee Qx \vee Qy) \\ \forall x \forall y (\neg Rxy \vee \neg Qx \vee \neg Qy) \\ \forall x (Rxx \vee Rxf fx) \end{array} \right\} \models Rcf fc$$

Resolutionssatz

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

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

- (i) K unerfüllbar.
- (ii) $\text{GI}(K)$ unerfüllbar.
- (iii) $\square \in \text{Res}^*(\text{GI}(K))$.

Beweis:

$(iii) \Rightarrow (i)$: $C \in \text{Res}^*(\text{GI}(K))$ 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

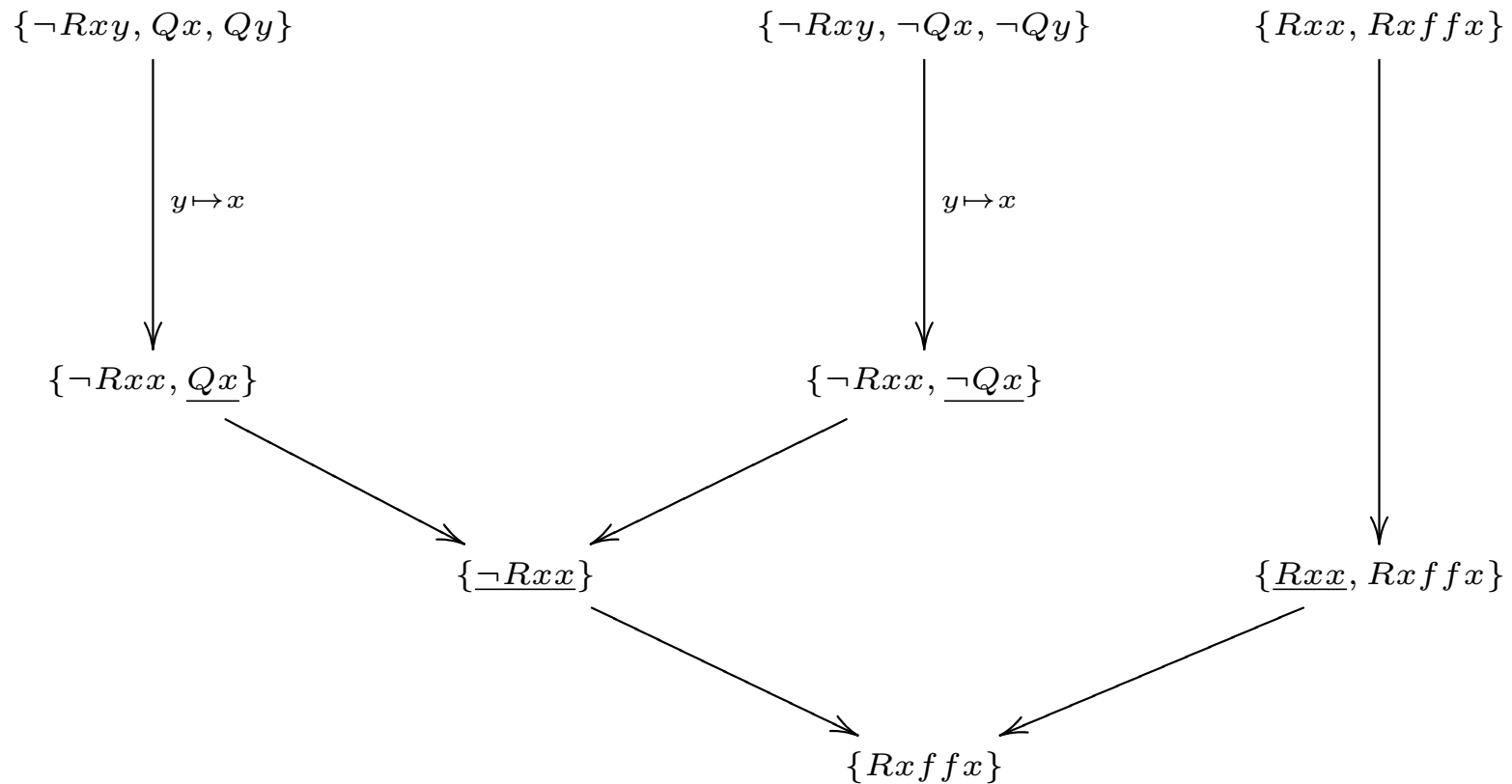
Substitutionsinstanz zu $\sigma = (t_1, \dots, t_n) \in T(S)^n$:

$$C^\sigma = \{\lambda^\sigma : \lambda \in C\} = \{\lambda(t_1/x_1, \dots, t_n/x_n) : \lambda \in C\}$$

Resolution von C_1 und C_2 zu C falls für geeignete σ_1 und σ_2 :

$$\lambda \in C_1^{\sigma_1}, \bar{\lambda} \in C_2^{\sigma_2}, C = (C_1^{\sigma_1} \setminus \{\lambda\}) \cup (C_2^{\sigma_2} \setminus \{\bar{\lambda}\})$$

Beispiel



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

Sequenzkalkül

Allgemeingültigkeitsbeweise (für bel. FO-Formeln/Sätze)

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

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

$\Gamma \vdash \Delta$ **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)

Sequenzkalkül: Regeln und Korrektheit

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

Konklusionen von Regeln ohne Prämissen: **Axiome**

Ableitbare Sequenzen:

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

Korrektheit:

Jede ableitbare Sequenz ist allgemeingültig.

Die **Korrektheit** folgt 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.
 $(\forall L)$, $(\forall R)$, $(\exists L)$, $(\exists R)$.
- **Gleichheitsregeln (neu)**: Umgang mit Term-Gleichheiten.
 $(=)$, (Sub) .

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

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

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

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

Sequenzkalkül: Quantorenregeln

(O.B.d.A.: y frei für x in φ wenn wir schreiben $\varphi(y/x)$)

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

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

falls y nicht in $\Gamma, \Delta, \forall x\varphi$

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

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

falls y nicht in $\Gamma, \Delta, \exists\varphi$

Korrektheit prüfen!

Sequenzkalkül: 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 für 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)

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

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 sogenannten **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 $\Phi \subseteq \text{FO}_0$:

φ

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

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

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

Vollständigkeit (starke Form)

Korrektheit

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

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

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

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

Gödelscher Vollständigkeitssatz (K. Gödel 1929)

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

Für jede Satzmenge $\Phi \subseteq \text{FO}_0(S)$

und jeden Satz $\varphi \in \text{FO}_0(S)$ gelten:

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

Bemerkung zu Herbrand und Vollständigkeit

Die Existenz eines vollständigen Kalküls ist bereits implizit im Satz von Herbrand und der Existenz eines vollständigen Kalküls für die Aussagenlogik (Resolution): Sei Φ eine beliebige Satzmenge und φ ein Satz. Sei Φ^S die Menge der Skolemnormalformen $\forall x \psi_{qf}^S(x)$ (x auch Tupel) der Sätze $\psi \in \Phi$ und φ^H die Herbrandnormalform von φ . Mit dem Satz von Herbrand (für offene Theorien) folgt:

$$\Phi \models \varphi \Leftrightarrow \bigwedge_{j=1}^k \bigwedge_{i=1}^n \psi_{qf,j}^S(s_i) \rightarrow \bigvee_{l=1}^m \varphi_{qf}^H(t_l) \in \text{TAUT}$$

für geeignetes $\{\psi_1, \dots, \psi_k\} \subseteq \Phi$ und Termtupel s_i, t_l .

Ersetze nun in der Tautologie alle Terme, die mit einer Skolem- oder Herbrand-Funktion beginnen, ihrer Größe nach durch neue Variablen. Die entstehende aussagenlogische Formel ist weiterhin eine Tautologie, aus der man durch geeignete Quantoreinführungsregeln und Kontraktion

$$\bigwedge_{j=1}^k \psi_j \rightarrow \varphi$$

ableiten kann (Details nicht ganz einfach).

Mit diesen Regeln (plus Resolution) folgt also

$$\Phi \vdash \varphi.$$

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:

Konsistenz	\Rightarrow	Erfüllbarkeit
nicht-Ableitbarkeit	$\left. \vphantom{\begin{matrix} \text{nicht-Ableitbarkeit} \\ \text{best. Sequenzen} \end{matrix}} \right\} \Rightarrow$	Existenz eines Modells
best. Sequenzen		

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 φ ein Satz in $\mathcal{L}(T)$ ist, d.h. ohne neue Konstanten c_ψ (für irgendein ψ), so gilt

$$T^* \vdash \varphi \Rightarrow T \vdash \varphi.$$

Definition: Sei T wie zuvor. Definiere

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

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 ebenfalls 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 .

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

$$\begin{aligned}\mathcal{M}, w &\longmapsto \varphi_{\mathcal{M}, w} \in \text{FO}_0(S_{\mathcal{M}}), \\ \varphi_{\mathcal{M}, w} &\text{ erfüllbar gdw. } w \xrightarrow{\mathcal{M}} \infty.\end{aligned}$$

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 $a \in \Sigma \cup \{\square\}$ (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

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

$$\begin{aligned}
\varphi_{\text{start}} &:= K00 \wedge Z_{q_0}0 \wedge \left[\begin{array}{l} \bigwedge_{i=1}^n R_{a_i}0 \text{succ}^i 0 \\ \wedge \forall y \left(\left(\bigwedge_{i=1}^n \neg y = \text{succ}^i 0 \right) \rightarrow R_{\square}0y \right) \end{array} \right] \\
\varphi_{\delta} &:= \forall t \forall t' (t' = \text{succ } t \rightarrow \psi(t, t')) \text{ wobei } \psi(t, t') \text{ Konj. der Form.} \\
&\quad \forall y ((Z_q t \wedge Kty \wedge R_b ty) \rightarrow (Z_{q'} t' \wedge Kt' \text{succ } y \wedge R_{b'} t' y)) \text{ f\"ur } \delta(q, b) = (b', >, q') \\
&\quad \forall y ((Z_q t \wedge Kty \wedge R_b ty) \rightarrow (Z_{q'} t' \wedge Kt' \text{pred } y \wedge R_{b'} t' y)) \text{ f\"ur } \delta(q, b) = (b', <, q') \\
&\quad \forall y ((Z_q t \wedge Kty \wedge R_b ty) \rightarrow (Z_{q'} t' \wedge Kt' y \wedge R_{b'} t' y)) \text{ f\"ur } \delta(q, b) = (b', \circ, q') \\
&\quad \forall y, y' ((Kty \wedge y \neq y') \rightarrow \bigwedge_a (R_a ty' \leftrightarrow R_a t' y')) \\
\varphi_{\infty} &:= \forall t \neg (Z_{q^+} t \vee Z_{q^-} t)
\end{aligned}$$

- $w \xrightarrow{\mathcal{M}} \infty \Rightarrow \varphi_{\mathcal{M},w}$ erfüllbar,
- $w \xrightarrow{\mathcal{M}} \text{STOP} \Rightarrow \varphi_{\mathcal{M},w}$ 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

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

die erststufige Theorie der Arithmetik.

Satz von Tarski (1933):

$\text{Th}(\mathcal{N})$ ist nicht arithmetisch definierbar, also noch 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 $f : \mathbb{N} \times \dots \times \mathbb{N} \rightarrow \mathbb{N}$ heißt **primitiv-rekursiv**, falls f durch einfache Rekursionen aus $(\underline{x} = x_1, \dots, x_k)$:

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

hervorgeht. Beispiele:

- (i) $x + 0 := x, \quad x + (y + 1) := (x + y) + 1$ (Addition),
- (ii) $x \cdot 0 := 0, \quad x \cdot (y + 1) := x \cdot y + x$ (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**

$$\mathbf{IA:} \quad \varphi(0) \wedge \forall x (\varphi(x) \rightarrow \varphi(x + 1)) \rightarrow \forall x \varphi(x)$$

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

Gödelisierung

Prim.-rek. Folgenkodierung: Endliche Folgen natürlicher Zahlen $\langle x_1, \dots, x_n \rangle$ 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 $Bew_{PA}(x, y)$ mit $Bew_{PA}(x, y)$ 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 $\mathcal{L}(\text{PA})$. Dann kann man einen Satz $\varphi \in \mathcal{L}(\text{PA})$ **konstruieren** mit

$$\text{PA} \vdash \varphi \leftrightarrow \Phi(\ulcorner \varphi \urcorner).$$

Insbesondere:

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

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

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

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

„Wahrheit“ ist kompliziert!

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

Beweis: Angenommen $W(x)$ sei Wahrheitsprädikat.

Fixpunktlemma (angewendet auf $\neg W(x)$) liefert **„Lügner“-Satz** L mit

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

Andererseits (W Wahrheitsprädikat)

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

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

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** $\varphi \in \mathcal{L}(\text{PA})$, der in \mathcal{T} **nicht beweisbar** ist:

$$\mathcal{N} \models \varphi, \text{ aber } \mathcal{T} \not\vdash \varphi.$$

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

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

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

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

Da $\mathbb{N} \models \mathcal{T}$, gilt $S_2 \subseteq S_1$. Es gibt ein **Beweisbarkeitsprädikat** $B_{\mathcal{T}} := \exists x \text{Bew}_{\mathcal{T}}(x, y)$, aber **kein Wahrheitsprädikat** W .

Also $S_1 \neq S_2$ und somit existiert ein Satz $\varphi \in S_1 \setminus S_2$. \dashv

Formalisierte Widerspruchsfreiheit (Konsistenz):

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

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

Gödels 2. Unvollständigkeitssatz: \mathcal{T} ist genau dann konsistent, wenn $\mathcal{T} \not\vdash \text{KON}_{\mathcal{T}}$, 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 Verifikation, 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 $ML(S)$ sprechen über einzelne Zustände in Σ -Transitionssystemen mit atomaren

Zustandseigenschaften $p_i ! P_i$

Syntax von $ML(S)$

atomare Formeln: \perp, \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 $ML(S)$ als Fragment von $FO(S)$

$$\begin{aligned}\Box_a \varphi(x) &\equiv \forall y (E_a xy \rightarrow \varphi(y)) : \quad \forall y ((x \xrightarrow{a} y) \rightarrow \varphi(y)) \\ \Diamond_a \varphi(x) &\equiv \exists y (E_a xy \wedge \varphi(y)) : \quad \exists y ((x \xrightarrow{a} y) \wedge \varphi(y))\end{aligned}$$

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 SAT(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 \perp .
- (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 $\varphi \rightarrow \psi$ 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 $\wedge, \vee, \rightarrow, \perp, \exists, \forall$.

Abkürzungen:

$$\neg\varphi := \varphi \rightarrow \perp, \varphi \leftrightarrow \psi := (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi).$$

Sequenzkalkül \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.

Ein Hilbert-Kalkül H_i für IL: streiche aus bisherigem alternativen Hilbert-Kalkül das Schema: $\neg\neg\varphi \rightarrow \varphi$.

Axiome von H_i :

- (i) $\varphi \rightarrow (\psi \rightarrow \varphi)$,
- (ii) $(\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$,
- (iii) $\varphi \rightarrow \varphi \vee \psi$, (iv) $\psi \rightarrow \varphi \vee \psi$,
- (v) $(\varphi \rightarrow \chi) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\varphi \vee \psi \rightarrow \chi))$,
- (vi) $\varphi \wedge \psi \rightarrow \varphi$, (vii) $\varphi \wedge \psi \rightarrow \psi$,
- (viii) $\varphi \rightarrow (\psi \rightarrow \varphi \wedge \psi)$,
- (x) $\perp \rightarrow \varphi$,
- (xi) $\forall x \varphi \rightarrow \varphi[t/x]$, (xii) $\varphi[t/x] \rightarrow \exists x \varphi$,

wobei in $(xi), (xii)$ der Term t frei für x in φ sein muss.

Logische Regeln von H_i :

$$\frac{\varphi \quad , \quad \varphi \rightarrow \psi}{\psi},$$

$$\frac{\varphi \rightarrow \psi}{\varphi \rightarrow \forall x \psi},$$

$$\frac{\psi \rightarrow \varphi}{\exists x \psi \rightarrow \varphi},$$

wobei in den letzten beiden Regeln x nicht frei in φ vorkommen darf.

Gleichheitsaxiome: wie für FO.

Ein vollständiger Kalkül H für FO entsteht aus H_i durch Hinzufügung des Schemas vom ausgeschlossenen Dritten

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

oder von

$$\neg\neg\varphi \rightarrow \varphi.$$

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

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

Satz (Gödel 1933): Γ, φ sei aus doppelt negierten atomaren Formeln $\neg\neg R(t_1, \dots, t_n), \neg\neg s = t$ mittels $\wedge, \rightarrow, \perp, \forall$ aufgebaut. Dann gilt $\Gamma \vdash_H \varphi$ gdw. $\Gamma \vdash_{H_i} \varphi$.

Da sich in klassischer Logik **jede** Formel logisch äquivalent in obiger Form schreiben läßt, ergibt dies eine **Einbettung** von FO in IL: IL ist eine **Verfeinerung** von FO!

IL läßt sich in einer Erweiterung von FO um einen Modaloperator („S4“) einbetten (Gödel 1933).

Die „mögliche Welten“-Semantik (Kripke 1959) für S4 induziert dann eine vollständige Semantik für IL (Kripke 1962).

Ausblick: entscheidbare Theorien

Beispiele:

entscheidbar	dagegen unentscheidbar
MSO-Theorie von Bäumen (Rabin)	Graphentheorie, FO
FO-Th(\mathbb{R} , +, ·, 0, 1, <) (Tarski)	FO-Th(\mathbb{N} , +, ·, 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. $\varphi(\mathbf{x}) \in \text{FO}(S)$ mit $\text{qr}(\varphi) \leq q$:

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

insbesondere für $q = 0$, $\mathbf{m} = (m_1, \dots, m_k)$, $\mathbf{m}' = (m'_1, \dots, m'_k)$

$\mathcal{W}, \mathbf{m} \equiv_0 \mathcal{W}', \mathbf{m}'$ 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

Die 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 $\mathbf{m} = (m_1, \dots, m_k)$ und $\mathbf{m}' = (m'_1, \dots, m'_k)$
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 $\mathcal{W}, \mathbf{m} \not\equiv_0 \mathcal{W}', \mathbf{m}'$

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

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 $\mathbf{m} = (m_1, \dots, m_k)$ in \mathcal{W} und $\mathbf{m}' = (m'_1, \dots, m'_k)$ in \mathcal{W}' sind äquivalent:

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

(i) \Rightarrow (ii):

Beweis per Induktion über q .

$q = 0$: trivial.

Induktionsschritt $q \rightsquigarrow q + 1$:

Angenommen $\mathcal{W}, \mathbf{m} \not\equiv_{q+1} \mathcal{W}', \mathbf{m}'$,

d.h. es existiert ein φ mit $qr(\varphi) = q + 1$,

$\mathcal{W} \models \varphi(\mathbf{m})$ und $\mathcal{W}' \not\models \varphi(\mathbf{m}')$. (oder umgekehrt)

Gilt $\varphi \equiv \neg\varphi_1$, $\varphi \equiv \varphi_1 \vee \varphi_2$, $\varphi \equiv \varphi_1 \wedge \varphi_2$,

dann kann φ durch φ_1 oder φ_2 ersetzt werden. (warum?).

Wir können also annehmen, dass $\varphi \equiv \exists z\psi(\mathbf{x}, z)$.

Es gibt ein Element m in \mathcal{W} mit $\mathcal{W} \models \psi(\mathbf{m}, m)$

und für alle m' in \mathcal{W}' gilt $\mathcal{W}' \not\models \psi(\mathbf{m}', m')$. (oder umgekehrt)

Markiert **I** zuerst m , erreicht man nach der ersten Runde eine Konfiguration mit $\mathcal{W}, \mathbf{m} \not\equiv_q \mathcal{W}', \mathbf{m}'$.

Nach Induktionshypothese hat **I** also eine Gewinnstrategie.

(ii) \Rightarrow (i):

Beweisidee: Zeige induktiv, dass die Aussage

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

mit einer Formel φ mit $qr(\varphi) = q$ ausgedrückt werden kann.

Beispiel

Sei $\mathcal{O}_n := (\{1, \dots, n\}, <)$.

Für $n, n' \geq 2^q - 1$ gilt $\mathcal{O}_n \equiv_q \mathcal{O}_{n'}$.

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.

AL Sequenzenkalkül \mathcal{SK}

$$(\text{Ax}) \quad \overline{\Gamma, p \vdash \Delta, p} \quad (p \in \mathcal{V})$$

$$(0\text{-Ax}) \quad \overline{\Gamma, 0 \vdash \Delta}$$

$$(1\text{-Ax}) \quad \overline{\Gamma \vdash \Delta, 1}$$

$$(\neg\text{L}) \quad \frac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$$

$$(\neg\text{R}) \quad \frac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$$

$$(\vee\text{L}) \quad \frac{\Gamma, \varphi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}$$

$$(\vee\text{R}) \quad \frac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}$$

$$(\wedge L) \quad \frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}$$

$$(\wedge R) \quad \frac{\Gamma \vdash \Delta, \varphi \quad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$$

$$(\rightarrow L) \quad \frac{\Gamma \vdash \Delta, \varphi \quad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \rightarrow \psi \vdash \Delta}$$

$$(\rightarrow R) \quad \frac{\Gamma, \varphi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \rightarrow \psi}$$

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

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.
 $(\forall L), (\forall R), (\exists L), (\exists R)$.
- **Gleichheitsregeln (neu)**: Umgang mit Term-Gleichheiten.
 $(=), (Sub)$.

AL + Quantorenregeln: vollständiger Beweiskalkül \mathcal{SK}^\neq für 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

(O.B.d.A.: y frei für x in φ wenn wir schreiben $\varphi(y/x)$)

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

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

falls y nicht in $\Gamma, \Delta, \forall x\varphi$

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

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

falls y nicht in $\Gamma, \Delta, \exists\varphi$

Sequenzenkalkül: Gleichheitsregeln

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

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

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.