# Formale Grundlagen der Informatik II

**Zusammenfassung der Vorlesung von Prof. Dr. Martin Otto im Sommersemester 2010 an der Technischen Universität Darmstadt**

Dominik Schreiber

mailto:ow91fibo@rbg.informatik.tu-darmstadt.de

Sommer 2010

# Inhaltsverzeichnis

# 1 Aussagenlogik

**Überblick:** Aussagenlogische Formeln ($AL$) sprechen über Tupel von Booleschen Wahrheitswerten und beschreiben Verknüpfungen zwischen aussagenlogischen Variablen. So lassen sich beliebige Informationen (bitweise) erfassen und (auch algorithmisch mittels Kalkülen) analysieren.

## 1.1 Syntax und Semantik

**Überblick:** Die Syntax der AL beschreibt die Regeln zum Erzeugen der aussagenlogische Formelmenge $AL(\mathcal{V})$ (über Variablen aus $\mathcal{V}$). Semantik der AL beschreibt Interpretationen von aussagenlogischen Formeln durch Wahrheitswerte (meist durch *Wahrheitstafeln*).

**Semantik** der AL: für $\mathcal{V}$ (eine Menge aussagenlogischer Variablen) wird $AL(\mathcal{V})$ induktiv erzeugt:

- 0, 1, $p \in \mathcal{V}$ (atomare Formeln)
- $\varphi \in AL(\mathcal{V}) \Rightarrow \neg\varphi \in AL(\mathcal{V})$ (Negation)
- $\varphi, \psi \in AL(\mathcal{V}) \Rightarrow (\varphi \vee \psi), (\varphi \wedge \psi) \in AL(\mathcal{V})$ (Konjunktion, Negation)

**Schreibweisen** der Semantik: sei $\mathcal{V} = \{p_i : i \geq 1\}$ die Standardvariablenmenge oder $\mathcal{V}_n = \{p_1, \ldots, p_n\}$ für $n \in \mathbb{N}$

- $AL := AL(\mathcal{V})$
- $AL_n := AL(\mathcal{V}_n)$
- $(\varphi \rightarrow \psi) := (\neg\varphi \vee \psi)$
- $(\varphi \leftrightarrow \psi) := ((\neg\varphi \wedge \neg\psi) \vee (\varphi \wedge \psi))$
- $\varphi \ldots \psi := (\varphi \ldots \psi)$ (äußere Klammern werden weggelassen)

**Belegung ($\mathcal{V}$-Interpretation)** $\mathcal{J} : \mathcal{V} \rightarrow \mathbb{B} : p \mapsto \mathcal{J}(p)$ – $\mathcal{J}$ interpretiert $p$ als „wahr“, wenn $\mathcal{J}(p) = 1$ und als „falsch“, wenn $\mathcal{J}(p) = 0$.

**Wahrheitswert** einer Formel $\varphi \in AL(\mathcal{V})$ zu gegebener $\mathcal{V}$-Interpretation $\mathcal{J}$ ist $\varphi^{\mathcal{J}} \in \mathbb{B}$.

**Aufbau der Funktion** $^{\mathcal{J}}$ $^{\mathcal{J}} : AL(\mathcal{V}) \rightarrow \mathbb{B} : \varphi \mapsto \varphi^{\mathcal{J}}$ wird induktiv definiert:

- $0^{\mathcal{J}} := 0, 1^{\mathcal{J}} := 1, p^{\mathcal{J}} := \mathcal{J}(p)$ (atomare Formeln)
- $(\neg\varphi)^{\mathcal{J}} := 1 - \varphi^{\mathcal{J}}$ (Negation)
- $(\varphi \wedge \psi)^{\mathcal{J}} := min(\varphi^{\mathcal{J}}, \psi^{\mathcal{J}})$ $(= \varphi^{\mathcal{J}} \cdot \psi^{\mathcal{J}})$(Konjunktion)
- $(\varphi \vee \psi)^{\mathcal{J}} := max(\varphi^{\mathcal{J}}, \psi^{\mathcal{J}})$ $(= \varphi^{\mathcal{J}} + \psi^{\mathcal{J}} - \varphi^{\mathcal{J}} \cdot \psi^{\mathcal{J}})$(Disjunktion)

**Semantik** der AL: sei $\mathcal{J}$ eine $\mathcal{V}$-Interpretation und $\varphi \in AL(\mathcal{V})$. $\mathcal{J}$ *erfüllt / ist Modell von* $\varphi \Leftrightarrow \varphi^{\mathcal{J}} = 1$. Man schreibt $\mathcal{J} \models \varphi$. Entsprechend gilt für die Formelmenge $\Phi \subseteq AL(\mathcal{V})$: $\mathcal{J} \models \Phi \Leftrightarrow \mathcal{J} \models \varphi$ für alle $\varphi \in \Phi$.

**Schreibweisen** Für $\varphi \in AL_n$ schreibt man $\varphi = \varphi(p_1, \ldots, p_n)$. Für $(b_1, \ldots, b_n) \in \mathbb{B}^n$ ist $\varphi[b_1, \ldots, b_n] := \varphi^{\mathcal{J}}$ für die Interpretation $(\mathcal{J}(p_i) = b_i)_{i=1,\ldots,n}$.

**Wertetabellen** beschreiben die Funktion, die $(b_1, \ldots, b_n)$ auf $\varphi[b_1, \ldots, b_n]$ abbildet. Die Semantik einer Formel $\varphi \in AL_n$ wird durch ihre *Wertetabelle* eindeutig beschrieben:

**Negation ($\neg$)** $\neg p$ ist genau dann wahr, wenn $p$ falsch ist:

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

**Konjunktion ($\wedge$)** $p \wedge q$ ist genau dann wahr, wenn sowohl $p$ als auch $q$ wahr sind:

| $p$ | $q$ | $p \wedge q$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

**Disjunktion ($\vee$)** $p \vee q$ ist genau dann wahr, wenn wenigstens einer von $p$ und $q$ wahr ist:

| $p$ | $q$ | $p \vee q$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

**Implikation ($\rightarrow$)** $p \rightarrow q$ ist wahr, wenn $p$ *falsch* oder $q$ wahr ist:

| $p$ | $q$ | $p \rightarrow q$ |
|---|---|---|
| 0 | 0 | **1** |
| 0 | 1 | 1 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

**Biimplikation ($\leftrightarrow$)** $p \leftrightarrow q$ ist wahr, wenn $p = q$ (also beide wahr oder beide falsch)

| $p$ | $q$ | $p \rightarrow q$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

## 1.2 Folgerung, Allgemeingültigkeit, Äquivalenz, Erfüllbarkeit

**Überblick:** Eine Folgerung heißt, dass wann immer die Voraussetzung wahr ist, auch die Konklusion wahr sein muss. Allgemeingültigkeit heißt, dass eine Formel *für alle* möglichen Eingaben (ohne Voraussetzungen) immer wahr ist. Zwei Formeln heißen logisch äquivalent, wenn beide von denselben Interpretationen wahr gemacht werden. Eine Formel(menge) heißt erfüllbar, wenn es eine Interpretation gibt, die sie erfüllt.

**Folgerung** Seien $\varphi, \psi \in AL(\mathcal{V})$ und $\varphi \subseteq AL(\mathcal{V})$. $\psi$ folgt aus $\varphi$ ($\varphi \models \psi$) gdw. für alle $\mathcal{V}$-Interpretationen $\mathcal{J}$ gilt: $\mathcal{J} \models \varphi \Rightarrow \mathcal{J} \models \psi$. Entsprechend ist $\Phi \models \psi$ definiert. Folgerungen weist man mittels Wahrheitstafeln nach (indem man alle Möglichkeiten prüft).

**Allgemeingültigkeit** $\varphi \in AL(\mathcal{V})$ heißt *allgemeingültig* gdw. für alle $\mathcal{V}$-Interpretationen $\mathcal{J}$ gilt: $\mathcal{J} \models \varphi$. Man schreibt $\models \varphi$.

**logische Äquivalenz** $\varphi, \psi \in AL_{\mathcal{V}}$ heißen *logisch äquivalent*, wenn für alle $\mathcal{V}$-Interpretationen $\mathcal{J}$ gilt: $\mathcal{J} \models \varphi \Leftrightarrow \mathcal{J} \models \psi$. Man schreibt $\varphi \equiv \psi$.
Beispielsweise gilt $p \vee q \equiv \neg(\neg p \wedge \neg q)$ und $p \wedge q \equiv \neg(\neg p \vee \neg q)$

**Erfüllbarkeit** $\varphi \in AL(\mathcal{V})$ ist *erfüllbar* gdw. eine Interpretation $\mathcal{J}$ existiert mit $\mathcal{J} \models \varphi$. Analog ist Erfüllbarkeit von Formelmengen definiert.

## 1.3 Boolesche Funktionen

**Überblick:** Boolesche Funktionen bilden $n$-Tupel von Wahrheitswerten auf einen einzelnen Wahrheitswert ab. Sie können durch aussagenlogische Formeln dargestellt werden.

**Boolesche Funktion** $f : \mathbb{B}^n \to \mathbb{B} : (b_1, \dots, b_n) \mapsto f(b_1, \dots, b_n)$ ist eine $n$-stellige Boolesche Funktion.

**Menge aller Booleschen Funktionen ($\mathcal{B}_n$)** für $n \in \mathbb{N}$ ist $\mathcal{B}_n$ die Menge aller $n$-stelligen Booleschen Funktionen. Für $n = 0$ ist $\mathbb{B}^0 = \{\square\}$, es gibt also genau zwei Funktionen (eine, die 1 liefert, und eine, die 0 liefert). $|\mathcal{B}_n| = 2^{2^n}$

**Funktionale Vollständigkeit** zu jeder Funktion $f \in \mathcal{B}_n$ gibt es $\varphi \in AL_n$ mit $f = f_\varphi$ (wobei $f_\varphi : \mathbb{B}^n \to \mathbb{B} : (b_1, \dots, b_n) \mapsto \varphi[b_1, \dots, b_n]$).

## 1.4 Normalformen

**Überblick:** Normalformen machen Formeln „greifbarer“, indem sie sie in feste Formen (Disjunktion über Konjunktionen (DNF) oder Konjunktion über Disjunktionen (KNF)) bringen.

**Literal** Aussagenvariablen und ihre Negationen werden Literal genannt (z.B. $p, \neg p$).

**Disjunktive Normalform (DNF)** ist eine *Disjunktion über Konjunktionen* von Literalen ($\bigvee \varphi_i$, wobei $\varphi_i = p_1 \wedge \ldots \wedge p_n$).

**Konjunktive Normalform (KNF)** ist eine *Konjunktion über Disjunktionen* von Literalen ($\bigwedge \varphi_i$, wobei $\varphi_i = p_1 \vee \ldots \vee p_n$).

**leere Konjunktion / Disjunktion** per Konvention ist $\bigvee \emptyset \equiv 0$ und $\bigwedge \emptyset \equiv 1$.

**Formeläquivalenz zu KNF/DNF** zu jeder Formel $\varphi \in AL_n$ gibt es eine äquivalente Formel $\varphi_{KNF} \in AL_n$ in KNF und eine äquivalente Formel $\varphi_{DNF} \in AL_n$ in DNF. Man kann also insbesondere eine Formel in DNF in eine äquivalente Formel in KNF umwandeln und umgekehrt.

## 1.5 Kompaktheitssatz der Aussagenlogik

**Überblick:** Eine unendliche Formelmenge ist erfüllbar, wenn schon jede endliche Teilmenge erfüllbar ist. Ebenso erfüllt eine unendliche Formelmenge eine Formel, wenn es auch eine endliche Teilformelmenge gibt, die die Formel erfüllt.

**Kompaktheitssatz** Sei $\mathcal{V} = \{p_i : 1 \leq i \in \mathbb{N}\}$ und $AL = AL(\mathcal{V})$. Dann gilt für *jede* Formelmenge $\Phi \subseteq AL$:
$\Phi$ ist erfüllbar gdw. jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ ist erfüllbar.

**Erfüllen von Formeln** Für *jede* Formelmenge $\Phi \subseteq AL$ und jede Formel $\psi \in AL$ gilt:
$\Phi \models \psi$ gdw. es gibt eine endliche Teilmenge $\Phi_0 \subseteq \Phi$ mit $\Phi_0 \models \psi$.

**Beweis:**

- $\Rightarrow$ $\Phi \models \psi \Leftrightarrow \Phi \cup \{\neg\psi\}$ ist unerfüllbar. Also existiert $\Phi_0 \subseteq \Phi$ mit $\Phi_0 \cup \{\neg\psi\}$ unerfüllbar (Kompaktheitssatz). Dann existiert ein $\Phi_0 \subseteq \Phi$ mit $\Phi_0 \models \psi$.
- $\Leftarrow$ klar. $\square$

**Lemma von König** als Beispiel für den Kompaktheitssatz: Sei $\mathcal{T}$ ein unendlicher, aber endlich verzweigter (also mit nur endlich vielen Nachfolgern an jedem Knoten) Baum. Dann gibt es in $\mathcal{T}$ einen *unendlich langen Pfad* (von der Wurzel aus).

## 1.6 Logikkalküle

**Überblick:** Logikkalküle liefern formale *korrekte und vollständige* Beweiskonzepte für Folgerungsbeziehungen und Allgemeingültigkeit.

**Korrektheit** *nur* semantisch korrekte Sachverhalte sind formal beweisbar.

**Vollständigkeit** *jeder* semantisch korrekte Sachverhalt ist formal beweisbar.

### 1.6.1 Resolutionskalkül

> **Überblick:** Das Resolutionskalkül liefert den Nachweis der *Unerfüllbarkeit* aussagenlogischer Formeln in KNF. Ist die Klauselmenge endlich, so liefert das Resolutionskalkül auch den Nachweis der Erfüllbarkeit.

**Klauselmenge** alternatives Format für KNF-Formeln. Klauseln werden konjugiert, sind selbst Disjunktionen von Literalen.
**Beispiel:** $K = \{p, \neg q\}, \{q\} \equiv (p \vee \neg q) \wedge q$

**Klausel** endliche Menge von Literalen. $\Box$ ist die *leere Klausel*.

**Resolvente** Seien $C_1, C_2, C_3$ Klauseln. $C$ ist *Resolvente* von $C_1$ und $C_2$, wenn für ein Literal L gilt $L \in C_1, \overline{L} \in C_2$. Dann ist $C = (C_1 \backslash L) \cup (C_2 \backslash \overline{L})$.
**Beispiel**: $\{p, \underline{\neg q}, r\}, \{p, \underline{q}, s, t\} \longrightarrow \{p, r, s, t\}$

**Resolutionslemma** Sei $K$ eine Klauselmenge, die Klauseln $C_1, C_2 \in K$ und $C$ Resolvente von $C_1, C_2$. Dann ist $K \equiv K \cup \{C\}$.

**Resolutionskalkül** $Res(K) := K \cup \{C : C$ Resolvente von Klauseln in K$\}$. $C$ heißt *ableitbar* aus $K$, wenn sie durch iterierte Anwendung von $Res$ auf $K$ gewonnen werden kann (z.B. $Res(Res(K))$). $Res^*(K)$ ist die Menge aller aus K ableitbaren Klauseln. Ist $\Box \in Res^*(K)$, so ist $K$ unerfüllbar.

**Korrektheit** $\Box$ ist nur dann aus $K$ ableitbar, wenn $K$ unerfüllbar

**Vollständigkeit** Ist $K$ unerfüllbar, so lässt sich $\Box$ aus $K$ ableiten

**Beweis im Resolutionskalkül** ist ein Binärbaum, wobei die Knoten mit Klauseln beschriftet sind und

- an den inneren Knoten jeweils eine Resolvente der Klauseln der Nachfolgerknoten steht
- an der Wurzel die leere Klausel $\Box$ steht

ein solcher Beweis zeigt die *Unerfüllbarkeit* der Klauselmenge (der Klauseln an den Blättern).

**Resolutionsalgorithmus** ist die Klauselmenge endlich, so terminiert der Algorithmus (im schlimmsten Fall in Exponentialzeit):

```
boolean unerfüllbar(Klauselmenge K) {
    Klauselmenge R = K;
    while(Res(R) ≠ R && □ ∉ R) R := Res(R);
    return □ ∈ R;
}
```

**Hornklauseln** sind Klauseln mit *höchstens einem positiven Literal*. Die Hornklausel $C = \{\neg p_1, \dots, \neg p_n, q\}$ ist äquivalent zur Implikation $(p_1 \wedge \dots \wedge p_n) \rightarrow q$.

Besteht $C$ aus nur *einem positiven Literal*, so heißt $C$ *positive Hornklausel*. Enthält $C$ *kein positives Literal*, so heißt $C$ *negative Hornklausel*.

**Minimale Belegung** einer Menge nicht-negativer Hornklauseln $H_0$: es gibt eine *eindeutig bestimmte* minimale Belegung $\mathcal{J}_0$ der Variablen in $H_0$, die $H_0$ erfüllt und sich in Polynomialzeit berechnen lässt.

**Einheitsresolution** für Hornklauselmengen ist die Einschränkung des Resolutionskalküls auf Resolutionsschritte, bei denen eine der Eingangsklauseln aus nur einem Literal besteht, *vollständig* und *korrekt*.

### 1.6.2 Sequenzenkalkül

**Überblick:** Das Sequenzenkalkül liefert formale, syntaktische Beweise von Folgerungsbeziehungen (oder allgemeingültigen Implikationen). Es ist nicht auf KNF/Klauselmengen beschränkt und terminiert in der AL.

**Sequenz** ist ein Paar von endlichen Formelmengen $(\Gamma, \Delta)$ mit $\Gamma, \Delta \subseteq AL$, auch als $\Gamma \vdash \Delta$ notiert. Eine Sequenz heißt allgemeingültig, wenn $\bigwedge \Gamma \models \bigvee \Delta$. Die linke Seite einer Sequenz wird als *Konjunktion* gelesen, die rechte als *Disjunktion*. Formelmengen werden als Listen aufgefasst, bei denen die Reihenfolge unwichtig ist. Man schreibt daher auch $\Gamma, \varphi$ statt $\Gamma \cup \{\varphi\}$ oder $\varphi$ statt $\{\varphi\}$.

**Sequenzenkalkül** besteht aus Regeln für die Erzeugung (Ableitung) neuer Sequenzen aus bestehenden (bereits erzeugten) Sequenzen. Man spricht von Prämissen (gegebenen Sequenzen) und Konklusion (abgeleiteter Sequenz) und notiert: $\dfrac{\text{Prämisse}}{\text{Konklusion}}$

**Korrektheit** jede ableitbare Sequenz ist allgemeingültig

**Vollständigkeit** jede allgemeingültige Sequenz ist ableitbar

**Regeln** für beliebige $\Gamma, \Delta, \varphi, \psi$:

**Ax** $\dfrac{}{\Gamma, \varphi \vdash \Delta, \varphi}$

**0-Ax** $\dfrac{}{\Gamma, 0 \vdash \Delta}$

**1-Ax** $\dfrac{}{\Gamma \vdash \Delta, 1}$

$\neg$**L** $\dfrac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$

$\neg$**R** $\dfrac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$

$\vee$**L** $\dfrac{\Gamma, \varphi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}$

$\vee$**R** $\dfrac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}$

$\wedge$**L** $\dfrac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi}$

$\wedge$**R** $\dfrac{\Gamma \vdash \Delta, \varphi \qquad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$

**Beweis** im Sequenzenkalkül: ist ein Baum, dessen Knoten mit Sequenzen beschriftet sind, wobei

- an inneren Knoten Konklusionen von Regeln stehen, deren Prämissen an den Nachfolgerknoten stehen
- an den Blättern Axiome stehen

Dieser Baum beweist die Sequenz, die in der Wurzel steht. Eine Sequenz ist ableitbar gdw. sie in diesem Sinn einen Beweis besitzt.

**Beweissuche** üblicherweise muss man eine gegebene Sequenz auf Axiome zurückführen, quasi den Beweisbaum „rückwärts“ aufbauen. Dies schreibt man „von unten nach oben“ auf, um nach der Suche einen korrekten Beweisbaum zu haben.

**erweiterte Sequenzenkalküle** um typische mathematische Beweisfiguren nachzugestalten wird das Sequenzenkalkül erweitert:

**Schnittregel (modus ponens)** entspricht der Verwendung von „Kettenschlüssen“: $A \Rightarrow B, B \Rightarrow C$, also auch $A \Rightarrow C$.

$$\frac{\Gamma \vdash \varphi \qquad \Gamma', \varphi \vdash \Delta}{\Gamma, \Gamma' \vdash \Delta}$$

**Widerspruchsregel (Kontradiktion)** entspricht dem „indirekten Beweis“ in der Mathematik: weise $A$ nach, indem man zeigt, dass $\neg A$ zum Widerspruch führt. Die Kontradiktionsregel lässt sich aus dem um den modus ponens erweiterten Sequenzenkalkül herleiten.

$$\frac{\Gamma \vdash \varphi \qquad \Gamma' \vdash \neg\varphi}{\Gamma, \Gamma' \vdash \emptyset}$$

# 2 Logik erster Stufe

**Überblick:** Formeln der Logik erster Stufe (first-order logic, *FO*) sprechen über Strukturen mit vorgegebenen Funktionen und Relationen und bekommen an einer Stelle (Tupel von Elementen) in der Struktur einen Wahrheitswert zugewiesen. Elemente können quantifiziert werden. Somit bietet sich ein universelles Format für mathematische Modellierung. Erfüllbarkeit und Allgemeingültigkeit von FO sind im allgemeinen unentscheidbar.

## 2.1 Strukturen, Terme, Belegungen

**Überblick:** Strukturen „implementieren“ Signaturen, indem sie die Konstanten-, Funktions- und Relationssymbole der Struktur interpretieren. Terme können aus Variablen, sowie Konstanten- und Funktionssymbolen der Signatur bestehen.

**Signatur** $S$ ist eine Menge von Konstanten- $(c, d, e, \ldots)$, Funktions- $(f, g, h, \ldots)$ und Relationssymbolen $(P, Q, R, \ldots)$ mit jeweils gegebenen Stelligkeiten. Enthält $S$ keine Funktionssymbole, so heißt $S$ *relationale Signatur*, enthält $S$ keine Relationssymbole, so heißt $S$ *funktionale Signatur*.

**S-Struktur** für Signatur $S$ besteht die *S-Struktur* $\mathcal{A} = (A, c^{\mathcal{A}}, \ldots, f^{\mathcal{A}}, \ldots, R^{\mathcal{A}}, \ldots)$ aus

- der Trägermenge $A \neq \emptyset$
- der Interpretation der Konstantensymbole aus $S$: für jedes Konstantensymbol $c \in S$: ein ausgezeichnetes Element $c^{\mathcal{A}} \in A$
- der Interpretation der Funktionssymbole aus $S$: für jedes $n$-stellige Funktionssymbol $f \in S$: eine $n$-stellige Funktion $f^{\mathcal{A}} : A^n \to A$
- der Interpretation der Relationssymbole aus $S$: für jedes $n$-stellige Relationssymbol $R \in S$: eine $n$-stellige Relation $R^{\mathcal{A}} \subseteq A^n$

**Beispiele:** Graphen, Transitionssysteme, Relationale Datenbanken, Boolesche Algebren, Arithmetik

**S-Terme** die Menge der Terme über der Signatur S (S-Terme), *T(S)*, (mit Variablenmenge V) ist induktiv erzeugt:

- für jede Variable $x \in V$ ist $x \in T(S)$
- für jede Konstante $c \in S$ ist $c \in T(S)$
- für jedes $n$-stellige Funktionssymbol $f \in S$ und $t_1, \ldots, t_n \in T(S)$ ist $f(t_1, \ldots, t_n) \in T(S)$

$T_n(S) \subseteq T(S)$ steht für die Menge aller Terme mit höchstens $n$ Variablen (Variablensymbole aus $V_n = \{x_1, \ldots, x_n\}$). $T_0(S)$ steht für die Menge der *variablenfreien Terme* ($= \emptyset$, wenn $S$ keine Konstanten hat). Funktionen auf $T(S)$ können *induktiv* definiert werden, da auch $T(S)$ induktiv aufgebaut ist.

**Termstrukturen** die Trägermenge einer Termstruktur (*Herbrand-Struktur*) $\mathcal{T} = \mathcal{T}(S)$ zu einer Signatur $S$ ist die Menge aller S-Terme, die Konstanten- und Funktionssymbole in $S$ werden natürlich interpretiert:

- für Konstantensymbol $c \in S$ ist $c^{\mathcal{T}} := c \in T(S)$
- für $n$-stelliges Funktionssymbol $f \in S$ ist $f^{\mathcal{T}} : T(S)^n \to T(S) : (t_1, \ldots, t_n) \mapsto f(t_1, \ldots, t_n)$

**Belegung** eine Funktion $\beta : V \to A$ heißt *Belegung* (für die $x \in V$) in der $S$-Struktur $\mathcal{A} = (A, \ldots)$.

**Interpretation** eine $S$-Struktur $\mathcal{A}$ und eine Belegung $\beta$ bilden eine *S-Interpretation* $\mathcal{J} = (\mathcal{A}, \beta)$.

**Semantik** von Termen: für eine gegebene $S$-Interpretation $\mathcal{J} = (\mathcal{A}, \beta)$ als Interpretation von $t \in T(S)$ wird induktiv über den Aufbau der $S$-Terme das von $t$ bezeichnete Element $t^{\mathcal{J}} \in A$ definiert:

- für $t = x$ ($x \in V$ Variable): $t^{\mathcal{J}} := \beta(x)$.
- für $t = c$ ($c \in S$ Konstantensymbol): $t^{\mathcal{J}} := c^{\mathcal{A}}$.
- für $t = f(t_1, \dots, t_n)$ ($f \in S$ $n$-stelliges Funktionssymbol): $t^{\mathcal{J}} := f^{\mathcal{A}}(t_1^{\mathcal{J}}, \dots, t_n^{\mathcal{J}})$.

## 2.2 Syntax, Semantik

> **Überblick:** Die Syntax von Formeln in $FO(S)$ besteht aus atomaren Formeln, Negation, Konjunktion, Disjunktion *und Quantoren.* Variablen können frei oder (durch Quantoren) gebunden sein. Eine $S$-Interpretation $\mathcal{J}$ erfüllt eine Formel $\varphi \in FO(S)$ gdw. $\varphi^{\mathcal{J}} = 1$.

**Syntax** $FO(S)$, die Menge der Formeln der Logik erster Stufe zur Signatur $S$ wird *induktiv* erzeugt:

**Atomare Formeln** für $t_1, t_2 \in T(S)$ ist $t_1 = t_2 \in FO(S)$ (Gleichheit), für $n$-stelliges Relationssymbol $R \in S$ und $t_1, \dots, t_n \in T(S)$ ist $R(t_1, \dots, t_n) \in FO(S)$ (Relationen)

**Negation** für $\varphi \in FO(S)$ ist $\neg\varphi \in FO(S)$

**Konjunktion, Disjunktion** für $\varphi, \psi \in FO(S)$ sind $(\varphi \wedge \psi), (\varphi \vee \psi) \in FO(S)$

**Quantoren** für $\varphi \in FO(S)$ und $x \in V$ sind $\exists x\varphi \in FO(S)$ (existentielle Quantifizierung) und $\forall x\varphi FO(S)$ (universelle Quantifizierung).

Quantifizierungen ($\exists x\varphi$, $\forall x\varphi$) *binden* die Variable $x$.

**Freie Variablen** sind alle Variablen, die nicht durch einen Quantor gebunden werden. Formeln ohne freie Variablen heißen *Sätze*. Man schreibt $FO_n(S) := \{\varphi \in FO(S) : frei(\varphi) \subseteq V_n\}$ für Formeln mit höchstens $n$ freien Variablen. Für $\varphi \in FO_n(S)$ schreibt man auch $\varphi = \varphi(x_1, \dots, x_n)$ um freie Variablen auszuzeichnen.

**Quantorenrang** ist die maximale Schachtelung von Quantoren in einer Formel. Induktiv definiert man $qr(\varphi) \in \mathbb{N}$ für $\varphi, \psi \in FO(S)$:

- $qr(\varphi) = 0$ für atomare $\varphi$
- $qr(\neg\varphi) := qr(\varphi)$
- $qr(\varphi \wedge \psi) = qr(\varphi \vee \psi) := max(qr(\varphi), qr(\psi))$
- $qr(\exists x\varphi) = qr(\forall x\varphi) := qr(\varphi) + 1$

Formeln mit $qr(\varphi) = 0$ heißen *quantorenfrei.*

**Semantik** bezüglich einer $S$-Interpretation $\mathcal{J}$ wird jeder $FO(S)$-Formel $\varphi$ ein Wahrheitswert $\varphi^{\mathcal{J}} \in \mathbb{B}$ zugewiesen. Die Funktion $^{\mathcal{J}} : FO(S) \to \mathbb{B} : \varphi \mapsto \varphi^{\mathcal{J}}$ wird induktiv definiert:

**Atomare Formeln** $(t_1 = t_2)^{\mathcal{J}} = 1$ gdw. $t_1^{\mathcal{J}} = t_2^{\mathcal{J}}$, $(R(t_1, \dots, t_n))^{\mathcal{J}} = 1$ gdw. $(t_1^{\mathcal{J}}, \dots, t_n^{\mathcal{J}}) \in R^{\mathcal{A}}$

**Negation** $(\neg\varphi)^{\mathcal{J}} := 1 - \varphi^{\mathcal{J}}$

**Konjunktion** $(\varphi \wedge \psi)^{\mathcal{J}} := min(\varphi^{\mathcal{J}}, \psi^{\mathcal{J}})$

**Disjunktion** $(\varphi \vee \psi)^{\mathcal{J}} := max(\varphi^{\mathcal{J}}, \psi^{\mathcal{J}})$

**Quantoren** $(\exists x\varphi)^{\mathcal{J}} := max(\varphi^{\mathcal{J}[x\mapsto a]} : a \in A)$, $(\forall x\varphi)^{\mathcal{J}} := min(\varphi^{\mathcal{J}[x\mapsto a]} : a \in A)$.

$\mathcal{J}$ *erfüllt/ist Modell von* $\varphi$ gdw. $\varphi^{\mathcal{J}} = 1$. Man schreibt $\mathcal{J} \models \varphi$. Analog gilt für Formelmengen $\Phi \subseteq FO(S)$: $\mathcal{J} \models \Phi$ gdw. $\mathcal{J} \models \varphi$ für alle $\varphi \in \Phi$.
**Beispiel:** $\forall x \forall y(Exy \leftrightarrow Eyx) \wedge \forall x(\neg Exx \wedge \exists y Exy)$
mit $E$ zweistelligem Relationssymbol. Beschreibt (in Graphen) einen ungerichteten Graph ohne Schlaufen und ohne isolierte Knoten.

## 2.3 Semantische Grundbegriffe

**Überblick:** Folgerung, Allgemeingültigkeit, logische Äquivalenz und Erfüllbarkeitsäquivalenz werden analog zur Aussagenlogik definiert.

**Folgerungsbeziehung ($\varphi \models \psi$)** für $\varphi, \psi \in FO(S)$ ist $\psi$ die *logische Folgerung* von $\varphi$ ($\varphi \models \psi$) gdw. für alle $S$-Interpretationen $\mathcal{J}$ gilt, dass $\mathcal{J} \models \varphi \Rightarrow \mathcal{J} \models \psi$ (also dass alle Interpretationen, die $\varphi$ erfüllen auch $\psi$ erfüllen). Analog ist $\Phi \models \psi$ definiert.

**Allgemeingültigkeit ($\models \varphi$)** $\varphi \in FO(S)$ heißt *allgemeingültig* gdw. für alle $S$-Interpretationen $\mathcal{J}$ gilt, dass $\mathcal{J} \models \varphi$.

**logische Äquivalenz ($\varphi \equiv \psi$)** $\varphi, \psi \in FO(S)$ heißen *(logisch) äquivalent* gdw. für alle $S$-Interpretationen $\mathcal{J}$ gilt, dass $\mathcal{J} \models \varphi \Leftrightarrow \mathcal{J} \models \psi$. Man schreibt $\varphi \equiv \psi$.

**Erfüllbarkeitsäquivalenz** schwächere Äquivalenz, $\varphi, \psi$ heißen *erfüllbarkeitsäquivalent* gdw. $\varphi$ erfüllbar $\Leftrightarrow \psi$ erfüllbar.

## 2.4 Semantikspiel

**Überblick:** Im Semantikspiel nehmen der *Verifizierer* und der *Falsifizierer* eine FO-Formel „auseinander“, um so ihre Erfüllbarkeit zu zeigen (oder sie zu widerlegen).

**Spieler** **V**erifizierer gegen **F**alsifizierer

**Spielpositionen** $(\psi, a) \in SF(\varphi) \times A^n$ (wobei $SF(\varphi)$ die Menge aller Subformeln von $\varphi$ ist)

**Züge** in Position $(\psi, a), a = (a_1, \ldots, a_n)$:

- $\psi = \psi_1 \wedge \psi_2$ **F** zieht nach $(\psi_1, a)$ oder $(\psi_2, a)$
- $\psi = \psi_1 \vee \psi_2$ **V** zieht nach $(\psi_1, a)$ oder $(\psi_2, a)$

- $\psi = \forall x_i \psi_0$ **F** zieht nach irgendeinem $(\psi_0, a^{'})$ mit $a^{'} = (a_1, \ldots, a_i^{'}, \ldots, a_n)$
- $\psi = \exists x_i \psi_0$ **V** zieht nach irgendeinem $(\psi_0, a^{'})$ mit $a^{'} = (a_1, \ldots, a_i^{'}, \ldots, a_n)$

**Spielende** in Positionen $(\psi, a)$ wo $\psi$ atomar oder negiert atomar

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

**Ziel** der Verifizierer will zeigen, dass eine gegebene FO-Formel erfüllbar ist, der Falsifizierer will dies widerlegen.

## 2.5 FO ohne Gleichheit

**Überblick:** In $FO^{\neq}$ gibt es keine Termgleichheit als atomare Formel. Stattdessen nimmt man zur Signatur eine zweistellige Äquivalenzrelation hinzu, die Gleichheit modelliert.

**FO ohne Gleichheit ($FO^{\neq}(S)$)** $\subseteq FO(S)$ ist wie $FO(S)$ aufgebaut, lediglich die Termgleichheit in den atomaren Formeln fehlt. Die Semantik überträgt sich von $FO(S)$.

**Äquivalenzrelation** als Modellierung von Gleichheit: man nimmt zur Signatur $S$ ein zweistelliges Relationssymbol (z.B. $\sim$), das Gleichheit modelliert (dies ist nicht so stark wie Gleichheit, reicht aber in den meisten Fällen aus).

## 2.6 Normalformen

**Überblick:** Jede FO-Formel ist logisch äquivalent zu einer FO-Formel in *pränexer Normalform* (bei der die Quantoren vor dem aussagenlogischen Anteil stehen) und erfüllbarkeitsäquivalent zu einer FO-Formel in *universell-pränexer Normalform* (Skolemnormalform, bei der zusätzlich Existenzaussagen durch Skolemfunktionen ersetzt wurden).

**Pränexe Normalform (PNF)** FO-Formeln in *pränexer Normalform* sind von der Form $Q_1 x_{i_1} \ldots Q_k x_{i_k} \varphi$, wobei $k \in \mathbb{N}, Q_i \in \{\forall, \exists\}$. Hierbei heißt $\varphi$ auch *quantorenfreier Kern* der Formel und $Q_1 x_{i_1} \ldots Q_k x_{i_k}$ ihr *Quantorenpräfix*. Anschaulich stehen in einer solchen Formel die Quantoren allesamt *vor* dem aussagenlogischen Anteil. Jede FO-Formel ist äquivalent zu einer Formel in pränexer Normalform.

**FO $\rightarrow$ PNF** um eine zu einer FO-Formel äquivalente Formel in pränexer Normalform zu finden muss man

1. gebundene Variablen *eindeutig* umbenennen (für jede gebundene Variable einen bis dahin unbenutzten Namen einführen)
2. danach kann man die Quantoren einfach vor den AL-Anteil schreiben

**Substitution ($\varphi(t/x)$)** induktiv werden Variablen so umbenannt, dass keine Konflikte mit gebundenen Variablen mehr auftreten:

**quantorenfreie $\varphi$, atomare** jedes Vorkommen von $x$ in $\varphi$ kann durch $t$ ersetzt werden

**Negation, Konjunktion, Disjunktion** $(\neg\varphi)(t/x) := \neg(\varphi(t/x))$, $(\varphi_1 \wedge \varphi_2)(t/x) := \varphi_1(t/x) \wedge \varphi_2(t/x)$, $(\varphi_1 \vee \varphi_2)(t/x) := \varphi_1(t/x) \vee \varphi_2(t/x)$

**Quantifizierung** sei $\varphi = Qy\psi$, $i \geq 1$ minimal und $x_i$ eine bisher unbenutzte Variable und $\hat{\psi} := \psi(x_i/y)$. Dann ist $\varphi(t/x) := Qx_i(\hat{\psi}(t/x))$. Anschaulich arbeitet man sich „von innen nach außen" und ersetzt dabei die vorkommenden gebundenen Variablen durch bisher unbenutzte.

**Skolemisierung** um Existenzaussagen zu umgehen erweitert man die Signatur $S$ um eine $n$-stellige (entsprechend der Anzahl der Allquantoren) *Skolemfunktion* $f$, wobei $f$ entsprechend der übergebenen Argumente genau das $x$ liefert, das $\exists x$ geliefert hätte. Eine skolemisierte Formel $\varphi^{'}$ ist *erfüllbarkeitsäquivalent* (Achtung: *nicht* logisch äquivalent) zur nicht skolemisierten „Ursprungsformel" $\psi$. Es gilt $\psi^{'} \models \psi$.
**Beispiel:** $\psi = \forall x \exists y \varphi(x, y)$ ist erfüllbar gdw. $\psi^{'} := \forall x \varphi(x, f(x))$ erfüllbar.

**Skolemnormalform** jede FO-Formel $\varphi \in FO(S)$ ist *erfüllbarkeitsäquivalent* zu einer *universell-pränexen* Formel $\varphi^{'} = \forall x_{i_1} \dots \forall x_{i_k} \psi$ mit quantorenfreiem „AL-Anteil" $\psi$ (in einer erweiterten Signatur).

**FO $\rightarrow$ Skolemnormalform** um eine zu einer FO-Formel $\varphi$ erfüllbarkeitsäquivalente Formel in Skolemnormalform $\psi$ zu finden muss man $\varphi$

- in pränexe Normalform bringen
- skolemisieren (Existenzaussagen durch Skolemfunktionen ersetzen)

## 2.7 Satz von Herbrand

**Überblick:** Eine Menge $\Phi \subseteq FO_0^{\neq}(S)$ von universellen, gleichheitsfreien Sätzen ist erfüllbar gdw. ein Herbrand-Modell $\mathcal{H} = (\mathcal{T}_0(S), (R^{\mathcal{H}})_{R \in S})$ existiert mit $\mathcal{H} \models \Phi$.

**Satz von Herbrand** sei $\Phi \subseteq FO_0^{-}(S)$ eine Menge von *universellen, gleichheitsfreien Sätzen*. Dann gilt:
$\Phi$ erfüllbar gdw.
$\Phi$ hat ein Herbrand-Modell $\mathcal{H} = (\mathcal{T}_0(S), (R^{\mathcal{H}})_{R \in S}) \models \Phi$, wobei Trägermenge, Funktions- und Konstanteninterpretation wie in $\mathcal{T}_0(S)$ (2.1) und die Relationssymbole $R \in S$ werden geeignet interpretiert. O.b.d.A hat $S$ mindestens ein Konstantensymbol (ansonsten ist $T_0(S) = \emptyset$).

## 2.8 Reduktion von FO auf AL

**Überblick:** Durch den Kompaktheitssatz der FO (2.9) und Übertragung auf den Kompaktheitssatz der AL (1.5) lässt sich das Erfüllbarkeitsproblem von FO-Satzmengen auf das Erfüllbarkeitsproblem von AL-Satzmengen reduzieren.

**Reduktion auf AL** sei $\Phi \subseteq FO_0^{\neq}(S)$ eine Menge von universellen, gleichheitsfreien Sätzen. Dann gilt:

$$\Phi \text{ erfüllbar gdw. } [\![\Phi]\!]^{AL} \text{ erfüllbar.}$$

$[\![\Phi]\!]^{AL}$ ist dabei definiert als $[\![\Phi]\!]^{AL} := \bigcup_{\varphi \in \Phi} [\![\varphi]\!]^{AL} \subseteq AL(\mathcal{V})$, wobei $\varphi = \forall x_1 \dots \forall x_k \xi(x_1, \dots x_k)$ ein universell-pränexer Satz und $[\![\varphi]\!]^{AL} := \{\xi(t)^{AL} : t \in T_0(S)^k\}$ ist.

**Beispiel** Zur Signatur $S = \{R/2, Q/1, f/1\}$ folgende universelle, gleichheitsfreie Sätze:

- $\varphi_1 = \forall x \forall y (Rxy \rightarrow (Qx \leftrightarrow \neg Qy))$
- $\varphi_2 = \forall x (Rxfx \vee Rfxx)$
- $\varphi_3 = \forall x \forall y (\neg Rxy \rightarrow Rxffy)$

Behauptung: $\Phi = \{\varphi_1, \varphi_2, \varphi_3\}$ unerfüllbar. Sei $S_c := S \cup \{c\}$ (damit $S$ eine Konstante enthält). $T_0(S_c)$ (die Trägermenge der zugehörigen Herbrand-Struktur) ist $\{f^n(c) : n \in \mathbb{N}\}$ und als AL-Variablen sei $q_n = p_{Q(f^n(c))}$ für Atome $Q(f^n(c))$ $(n \in \mathbb{N})$ und $r_{l,m} = p_{R(f^l(c), f^m(c))}$ für Atome $R(f^l(c), f^m(c))$ $(l, m \in \mathbb{N})$. So erhält man aus $\varphi_i$:

- $[\![\varphi_1]\!]^{AL} = \{r_{l,m} \rightarrow (q_l \leftrightarrow \neg q_m) : l, m \in \mathbb{N}\}$
- $[\![\varphi_2]\!]^{AL} = \{r_{l,l+1} \vee r_{l+1,l} : l \in \mathbb{N}\}$
- $[\![\varphi_3]\!]^{AL} = \{\neg r_{l,m} \rightarrow r_{l,m+2} : l, m \in \mathbb{N}\}$

Die Menge $[\![\Phi]\!]^{AL} = \{[\![\varphi_1]\!]^{AL}, [\![\varphi_2]\!]^{AL}, [\![\varphi_3]\!]^{AL}\}$ ist unerfüllbar. Also ist auch $\Phi = \{\varphi_1, \varphi_2, \varphi_3\}$ unerfüllbar.

## 2.9 Kompaktheitssatz

**Überblick:** Ähnlich wie in der Aussagenlogik (1.5) gilt: Eine (unendliche) FO-Formelmenge ist genau dann erfüllbar, wenn jede endliche Teilmenge erfüllbar ist. Außerdem erfüllt sie eine FO-Formel genau dann, wenn schon eine endliche Teilmenge diese erfüllt.

**Kompaktheitssatz** für *jede* Formelmenge $\Phi \subseteq FO$ gilt:
$\Phi$ erfüllbar gdw. jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ erfüllbar.

**Erfüllen von Formeln** für *jede* Formelmenge $\Phi \subseteq FO$ und Formel $\psi \in FO$ gilt:
$\Phi \models \psi$ gdw. eine endliche Teilmenge $\Phi_0 \subseteq \Phi$ erfüllt $\psi$ ($\Phi_0 \models \psi$).

**Beispiel: Nichtstandardmodell** der Arithmetik der natürlichen Zahlen: die Struktur $\mathcal{N}^* = (\mathbb{N}^*, +^*, \cdot^*, 0^*, 1^*, <^*)$ erfüllt genau dieselben $FO(\{+, \cdot, 0, 1, <\})$-Sätze wie $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$ (ist also im Rahmen von $FO(\{+, \cdot, 0, 1, <\})$ nicht von ihr zu unterscheiden), ist aber *nicht isomorph* dazu (also doch wesentlich verschieden): Jedes Element aus $\mathcal{N}$ (also alle $n \in \mathbb{N}$) sind Interpretationen variablenfreier $S$-Terme. Sei $t_n := \sum_1^n 1$ und $\varphi_n(x) := t_n < x$. Weiterhin sei $\Phi := \{\varphi \in FO_0(S) : \mathcal{N} \models \varphi\} \cup \{\varphi_n : n \in \mathbb{N}\}$ die unendliche Formelmenge. $\Phi$ ist erfüllbar, da jedes $\Phi_0 \subseteq \Phi$ nur endlich viele $\varphi_n(x)$ enthält und man in $\mathcal{N}$ eine Belegung für $x$ findet, die die endlich vielen Forderungen wahr macht (nach Kompaktheitssatz ist dann $\Phi$ erfüllbar). Jedes Modell von $\Phi$ muss

1. alle $FO(S)$-Sätze erfüllen, die in $\mathcal{N}$ gelten (also genau dieselben)
2. für die Belegung von $x$ ein Element besitzen, das im Sinne von $<$ größer als alle $t_n$ ist (also so etwas wie eine „unendliche natürliche Zahl").

Aus 2. folgt, dass jedes so gewonnene $\mathcal{N}^*$ nicht zu $\mathcal{N}$ isomorph sein kann, aber wegen 1. bezüglich $FO(S)$ von $\mathcal{N}$ ununterscheidbar ist.

## 2.10 Logikkalküle

**Überblick:** Ähnlich wie in der Aussagenlogik (1.6) gibt es auch in der FO-Logik Kalküle, namentlich das Resolutionskalkül, zum Beweis der Unerfüllbarkeit, und das Sequenzenkalkül, zum Nachweis von Folgerungsbeziehungen, um systematisch FO-Aussagen nachzuweisen.

### 2.10.1 Resolutionskalkül

**Überblick:** Aus FO-Formeln in Skolemnormalform lassen sich Klauseln bilden, die mittels der Grundinstanzen-Resolution oder Resolution durch Unifikation auf Unerfüllbarkeit überprüft werden können.

**FO-Formel → Klausel** sei $\varphi = \forall x_1 \ldots \forall x_n \xi(x_1, \ldots, x_n)$ ein universell-pränexer Satz und $\xi \in FO_n^{\neq}(S)$ quantorenfrei (also eine AL-Formel aus Atomen $\alpha = Rt$ mit Relationssymbolen $R \in S$ und Tupeln von Termen $t_i \in T_n(S)$). $\xi$ kann man als Formel in $AL(\{\alpha_1, \ldots \alpha_n)$ auffassen und in KNF bzw. Klauselform bringen.

**Literal** ist eine (negiert) atomare $FO^{\neq}(S)$-Formel $\lambda = \alpha$ oder $\lambda = \neg\alpha$ mit $\alpha = R(t_1, \ldots, t_n)$ ($R \in S$ ein $n$-stelliges Relationssymbol und $t_i \in T_n(S)$).

**Klausel C** endliche Menge von $FO^{\neq}(S)$-Literalen, logisch mit der *Disjunktion* $\bigvee C$ ihrer Literale identifiziert.

**Klauselmenge K** Menge von $FO^{\neq}(S)$-Klauseln. Endliche $K$ werden logisch mit der *Konjunktion* $\bigwedge_{C \in K} \bigvee C$ ihrer Literale identifiziert.

Mit der $FO^{\neg}(S)$-Klausel $C$ assoziiert man den *universell-pränexen* Satz $C \equiv \forall \mathbf{x} \bigvee C \in FO_0^{\neq}(S)$ (mit $\forall \mathbf{x}$ dem universellen Abquantifizieren *aller* in $C$ enthaltenen Variablen). ebenso assoziiert man mit der Klauselmenge $K$ die Menge der $FO^{\neq}(S)$-Sätze $K \equiv \{\forall x \bigvee C : C \in K\} \subseteq FO_0^{\neq}$.

**Grundinstanz** zu einer $FO^{\neq}(S)$-Klausel $C$ über Literalen $\lambda \in FO_n^{\neq}(S)$ und variablenfreien Termen $t_1, \ldots, t_n \in T_0(S)$ ist $C(t_1/x_1, \ldots, t_n/x_n) := \{\lambda(t_1/x_1, \ldots, t_n/x_n) : \lambda \in C\}$ eine *Grundinstanz* von $C$. Zu einer Klauselmenge $K$ erhält man $GI(K)$ (die Menge aller Grundinstanzen), indem man alle Grundinstanzen aller Klauseln zusammenfasst: $GI(K) := \{C(t_1/x_1, \ldots) : C \in K, t_i \in T_0(S)\}$. Es gilt $K \models GI(K)$, außerdem ist jedes Modell von $GI(K)$ ein Herbrand-Modell (2.7) von $K$.

**GI-Resolution** für Klauseln $C_1, C_2, C$ von variablenfreien $FO^{\neq}(S)$-Literalen ist $C$ eine *Resolvente* von $C_1, C_2$ bezüglich des Literals $\lambda$, wenn $\lambda \in C_1, \overline{\lambda} \in C_2$ und $C = (C_1 \backslash \{\lambda\}) \cup (C_2 \backslash \{\overline{\lambda}\})$. Man sagt, $C$ ist aus $C_1, C_2$ ableitbar.

- **Abschluss von K ($Res^*(K)$)** unter Hinzunahme von Resolventen: $K$ zusammen mit allen Klauseln, die man durch iterierte Resolutionsschritte aus $K$ gewinnen kann.
- **Korrektheit** ist $\Box$ aus $GI(K)$ ableitbar ($\Box \in Res^*(GI(K))$), dann ist $K$ *unerfüllbar*.
- **Vollständigkeit** ist $K$ unerfüllbar, so ist $\Box$ aus $GI(K)$ ableitbar ($\Box \in Res^*(GI(K))$).
- **Resolutionssatz** für GI-Resolution: für $FO^{\neq}(S)$-Klauselmengen $K$ gilt: $K$ unerfüllbar gdw. $GI(K)$ unerfüllbar gdw. $\Box \in Res^*(GI(K))$.

**Unifikation** erkenne, wann bestimmte Terme in Klauselmengen durch geeignete Substitutionen (von Termen) syntaktisch gleich gemacht werden können. Diese „Spezialisierungen“ sind quasi „Klassen von GI-Instanzen“.

- **Simultane Substitution** Sei $\sigma = (t_1, \ldots, t_n) \in T(S)^n$ die Operation der simultanen Substitution von $S$-Termen $t_1, \ldots, t_n$ für die Variablen $x_1, \ldots, x_n$.
- **Substitutionsinstanz eines Literals** Sei $\lambda^\sigma := \lambda(t_1/x_1, \ldots, t_n/x_n)$ die $\sigma$-Substitutionsinstanz des Literals $\lambda$.
- **Substitutionsinstanz einer Klausel** Sei $C^\sigma := \{\lambda_1^\sigma : \lambda \in C\}$ die $\sigma$-Substitutionsinstanz der Klausel $C$.

**Resolution durch Unifikation** für Klauseln $C_1, C_2, C$ von $FO^{\neq}(S)$-Literalen ist $C$ eine *Resolvente* von $C_1, C_2$ bzgl. des Literals $\lambda$, wenn *für geeignete Substitutionen* $\sigma_1, \sigma_2$ gilt: $\lambda \in C_1^{\sigma_1}, \overline{\lambda} \in C_2^{\sigma_2}$ und $C = (C_1^{\sigma_1} \backslash \{\lambda\}) \cup (C_2^{\sigma_2} \backslash \{\overline{\lambda}\})$.

- **Resolutionssatz** Für $FO^{\neq}(S)$-Klauselmengen $K$ gilt: $K$ unerfüllbar gdw. $\Box \in Res^*(K)$.
- **Resolutionsalgorithmus** der Unifikation: nutze jeweils die *allgemeinste unifizierende Substitution* (um jeweils die logisch stärkste Resolvente zu erhalten).

### 2.10.2 Sequenzenkalkül

**Überblick:** Ähnlich dem Sequenzenkalkül der Aussagenlogik (1.6.2) gibt es ein FO-Sequenzenkalkül, das Folgerungsbeziehungen nachweist. Die Regeln des AL-Sequenzenkalküls werden dafür um Regeln für Quantoren und Gleichheit erweitert. Für die Vollständigkeit dieses Kalküls gibt es neben dem Gödelschen Vollständigkeitssatz, aus dem die Aufzählbarkeit der FO-Allaussagen folgt, auch noch Beweise über Hintikka- und Henkin-Konstruktionen.

**FO-Sequenz** ist ein *Paar von endlichen FO-Satzmengen*, $(\Gamma, \Delta)$ mit $\Gamma, \Delta \in FO_0(S)$, auch als $\Gamma \vdash \Delta$ notiert. $\Gamma \vdash \Delta$ heißt *allgemeingültig*, wenn $\bigwedge \Gamma \models \bigvee \Delta$. Die linke Seite der Sequenz wird als *Konjunktion* gelesen, die rechte als *Disjunktion*.

**Ableitbarkeit** eine Sequenz heißt *ableitbar* im Sequenzenkalkül, wenn sie (in endlich vielen Schritten) durch Anwendung der Sequenzenregeln (ausgehend von Axiomen – Regeln ohne Prämisse) als Konklusion gewonnen werden kann.

**Sequenzenregeln** der FO-Sequenzenkalkül ($\mathcal{SK}$) hat drei Gruppen von Regeln: *aussagenlogische Regeln* (1.6.2), *Quantorenregeln* und *Gleichheitsregeln*, wobei die aussagenlogischen Regeln mit den Quantorenregeln ein vollständiges Beweiskalkül für $FO^{\neq}$ bilden. Zu beachten ist, dass die Quantorenregeln teilweise nur unter bestimmten Voraussetzungen ($c \notin \Gamma, \Delta, \varphi(x)$) gelten.

**Al-Regeln** es gelten zu den Regeln des AL-Sequenzenkalküls (1.6.2) äquivalente Regeln:

$$\textbf{Ax}\ \frac{}{\Gamma, \varphi \vdash \Delta, \varphi}$$

$$\neg\textbf{L}\ \frac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$$

$$\neg\textbf{R}\ \frac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$$

$$\vee\textbf{L}\ \frac{\Gamma, \varphi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}$$

$$\vee\textbf{R}\ \frac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash, \Delta, \varphi \vee \psi}$$

$$\wedge\textbf{L}\ \frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}$$

$$\wedge\textbf{R}\ \frac{\Gamma \vdash \Delta, \varphi \qquad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$$

**Quantorenregeln** bei $\forall$**R** und $\exists$**L** darf das verallgemeinerte $c$ *nicht* in $\Gamma, \Delta, \varphi(x)$ vorkommen.

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

$$\forall\textbf{R}\ \frac{\Gamma \vdash \Delta, \varphi(c/x)}{\Gamma \vdash \Delta, \forall x \varphi(x)}$$
(wenn $c \notin \Gamma, \Delta, \varphi(x)$)

$$\exists\textbf{L}\ \frac{\Gamma, \varphi(c/x) \vdash \Delta}{\Gamma, \exists x \varphi(x) \vdash \Delta}$$
(wenn $c \notin \Gamma, \Delta, \varphi(x)$)

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

**Gleichheitsregeln** analoge Regeln für $t' = t$ statt $t = t'$ gelten ebenfalls. **Sub-L/R** entsprechen der Substitution von $t$ bzw. $t'$ für $x$ in $\varphi(x)$.

$$= \frac{\Gamma, t = t \vdash \Delta}{\Gamma \vdash \Delta} \qquad \textbf{Sub-R}\ \frac{\Gamma \vdash \Delta, \varphi(t/x)}{\Gamma, t = t' \vdash \Delta, \varphi(t'/x)}$$

$$\textbf{Sub-L}\ \frac{\Gamma, \varphi(t/x) \vdash \Delta}{\Gamma, t = t', \varphi(t'/x) \vdash \Delta}$$

**Optional: Schnittregeln** analog zu *modus ponens* und *Kontradiktion* in der AL kann auch das FO-Sequenzenkalkül $\mathcal{SK}$ erweitert werden zu $\mathcal{SK}^+$:

$$\textbf{modus ponens}\ \frac{\Gamma \vdash \varphi \qquad \Gamma', \varphi \vdash \Delta}{\Gamma, \Gamma' \vdash \Delta} \quad \textbf{Kontradiktion}\ \frac{\Gamma \vdash \varphi \qquad \Gamma' \vdash \neg\varphi}{\Gamma, \Gamma' \vdash \emptyset}$$

**Nachweis im Sequenzenkalkül** verläuft ähnlich wie in der Aussagenlogik (1.6.2). Man sucht durch „sinnvolles Raten" des richtigen nächsten Schritts nach einem Ableitungsbaum der nachzuweisenden Formel aus Axiomen.

**Korrektheit** jede ableitbare Sequenz ist allgemeingültig.

**Vollständigkeit** hier existieren mehrere Vollständigkeitsaussagen und -beweise:

**Gödelscher Vollständigkeitssatz** (Vollständigkeit des Sequenzenkalküls): für jede Satzmenge $\Phi \subseteq FO_0(S)$ und jeden Satz $\varphi \in FO_0(S)$ gelten:

- $\Phi \models \varphi$ gdw. $\Phi \vdash \varphi$ (Ableitbarkeit von $\Phi \vdash \varphi \longleftrightarrow$ Folgerung von $\Phi \models \varphi$)
- $\Phi$ erfüllbar gdw. $\Phi$ konsistent (Konsistenz $\longleftrightarrow$ Erfüllbarkeit)

*Konsistenz* heißt, dass für kein $\Gamma_0 \subseteq \Phi$ die Sequenz $\Gamma_0 \vdash \emptyset$ ableitbar ist. $\Gamma \vdash \Delta$ ist im $\mathcal{SK}$ ableitbar aus $\Phi$, wenn eine Sequenz $\Gamma_0, \Gamma \vdash \Delta$ mit $\Gamma_0 \subseteq \Phi$ im $\mathcal{SK}$ ableitbar ist.

**Folgerung: Kompaktheitssatz** $\Phi \models \varphi \iff \Phi_0 \models \varphi$ für eine endliche Teilmenge $\Phi_0 \subseteq \Phi$ (2.9) folgt aus dem Vollständigkeitssatz mit $\Phi \vdash \varphi \iff \Phi_0 \vdash \varphi$ für eine endliche Teilmenge $\Phi_0 \subseteq \Phi$.

**Folgerung: Aufzählbarkeit der Allgemeingültigkeit** dass die Menge der allgemeingültigen $\varphi \in FO_0(S)$ ($\emptyset \models \varphi$) rekursiv aufzählbar ist folgt ebenfalls aus dem Vollständigkeitssatz mit der Erkenntnis, das man für jede feste endliche Signatur $S$ alle ableitbaren Sequenzen $\Gamma \vdash \varphi$ aufzählen kann, also insbesondere also auch alle $\emptyset \vdash \varphi$.

**Hintikka-Konstruktion** ist $\Gamma \vdash \Delta$ *nicht* aus $\Phi$ ableitbar, so ist $\Phi \cup \Gamma \cup \Delta^\neg$ erfüllbar (mit $\Delta^\neg = \{\neg\varphi : \varphi \in \Delta\}$), also gilt $\Phi \models \bigwedge \Gamma \rightarrow \bigvee \Delta$ *nicht*.
Für eine Hintikka-Menge $\hat{\Phi} \in FO^{\neq}(S)$ gelten folgende Abschlusseigenschaften:

- für kein $\varphi$ ist $\varphi \in \hat{\Phi}$ *und* $\neg\varphi \in \hat{\Phi}$ (Konsistenzbedingung)
- ist $\varphi \in \hat{\Phi}, \varphi = \varphi_1 \vee \varphi_2$, so ist $\varphi_1 \in \hat{\Phi}$ und/oder $\varphi_2 \in \hat{\Phi}$
- ist $\varphi \in \hat{\Phi}, \varphi = \varphi_1 \wedge \varphi_2$, so ist $\varphi_1, \varphi_2 \in \hat{\Phi}$

- ist $\varphi \in \hat{\Phi}, \varphi = \exists x\psi(x)$, so existiert ein $c \in S$, sodass $\psi(c/x) \in \hat{\Phi}$ (Existenzbeispiele)
- ist $\varphi \in \hat{\Phi}, \varphi = \forall x\psi(x)$, so ist $\psi(t/x) \in \hat{\Phi}$ für jeden Term $t \in T_0(S)$

und zusätzlich für $\hat{\Phi} \in FO(S)$:

- für alle $t \in T_0(S)$ ist $t = t \in \hat{\Phi}$ (Termgleichheit)
- ist $\varphi \in \hat{\Phi}, \varphi = \psi(t/x)$ und $t = t' \in \hat{\Phi}$ oder $t' = t \in \hat{\Phi}$, dann ist auch $\psi(t'/x) \in \hat{\Phi}$

Sei $\hat{\Phi} \subseteq FO(S)$ eine Hintikka-Menge (die diesen Abschlusseigenschaften genügt) und sei $\mathcal{H} = \mathcal{H}(\hat{\Phi})$ die Herbrand-Struktur (als Modell für $\Phi \cup \Gamma \cup \Delta^{\neg}$) mit Trägermenge $T_0(S)$ mit folgender Interpretation der $n$-stelligen Relationssymbole in S: $R^{\mathcal{H}} := \{(t_1, \ldots, t_n) \in T_0(S)^n : R(t_1, \ldots, t_n) \in \hat{\Phi}\}$. Dann ist $\mathcal{H} \models \hat{\Phi}$, es gilt also für alle $\varphi \in \hat{\Phi} : \mathcal{H} \models \varphi$.

**Henkin-Konstruktion** ist eine vereinfachte Hintikka-Konstruktion im Sequenzenkalkül *mit Schnittregel*. *Konsistenz von* $\Phi$ heißt nun entsprechend, dass für kein $\Gamma \subseteq \Phi$ die Sequenz $\Gamma \vdash \emptyset$ (in $\mathcal{SK}^+$) ableitbar ist. Ist $\Phi \subseteq FO_0(S)$ konsistent bzgl. $\mathcal{SK}^+$, dann ist $\Phi$ erfüllbar. $\hat{\Phi}$ ist eine *Henkin-Menge*, wenn gilt:

- für jedes $\varphi \in FO_0(S) : \varphi \in \hat{\Phi} \Leftrightarrow \neg\varphi \notin \hat{\Phi}$. (Maximale Konsistenz)
- für jedes $\psi(x) \in FO(S)$ existiert ein Term $t \in T_0(S)$ mit $(\forall x(\neg\psi(x) \vee \psi(t/x))) \in \hat{\Phi}$. (Existenzbeispiele)

Sei $\hat{\Phi}$ eine Henkin-Menge. Dann ist die 2-stellige Relation $\sim$, $t \sim t'$ gdw $t = t' \in \hat{\Phi}$, eine Äquivalenzrelation auf $T_0(S)$. Die Relationen/Funktionen der durch $\hat{\Phi}$ definierten Herbrand-Struktur $\mathcal{H}(\hat{\Phi})$ alle mit $\sim$ verträglich, und die *Quotientenstruktur* (deren Elemente die $\sim$-Äquivalenzklassen der Terme $t \in T_0(S)$ sind) ist ein Modell von $\hat{\Phi}$.

## 2.11 Unentscheidbarkeit

**Überblick:** $UNSAT(FO(S))$ und die Menge der allgemeingültigen $FO(S)$-Sätze sind aufzählbar, $SAT(FO(S))$ ist unentscheidbar.

**Aufzählbar** sind (für ein endliches oder aufzählbares $S$) nach dem Gödelschen Vollständigkeitssatz die Menge der *allgemeingültigen* $FO(S)$-Sätze ($VAL(FO)$) und das Komplement der erfüllbaren Sätze (da $\varphi \notin SAT(FO(S))$ gdw. $\neg\varphi$ allgemeingültig) $UNSAT(FO(S))$ (die Menge der *unerfüllbaren* $FO(S)$-Sätze).

**Halteproblem → FO-Erfüllbarkeit** sei $\mathcal{M}, w \longmapsto \varphi_{\mathcal{M},w}$ eine berechenbare Abbildung, die jeder DTM $\mathcal{M}$ und jedem Wort $w \in \Sigma^*$ einen Satz $\varphi_{\mathcal{M},w}$ zuordnet, sodass $w \xrightarrow{\mathcal{M}} \infty$ gdw. $\varphi_{\mathcal{M},w}$. Dann ist $\langle\mathcal{M}\rangle \in H$ ($H$ sei das Halteproblem) gdw. $\varphi_{\mathcal{M},w} \notin$

$SAT(FO)$ für $w = \langle \mathcal{M} \rangle$. Wäre die Erfüllbarkeit von $SAT(FO)$ entscheidbar, so auch das Halteproblem. Somit folgt der:

**Satz von Church/Turing** das Erfüllbarkeitsproblem für FO ist unentscheidbar.

**FINSAT(FO)** die Menge aller $FO(S)$-Sätze die ein *endliches* Modell besitzen ($FINSAT(FO)$) ist

- aufzählbar (indem man systematisch alle endlichen $S$-Strukturen $\mathcal{A}$ generiert und jeweils $\mathcal{A} \models \varphi$ testet)
- unentscheidbar (*Satz von Traktenbrot*). Daraus folgt, dass die Menge aller über endlichen Strukturen allgemeingültigen $FO(S)$-Sätze nicht aufzählbar ist und es also keinen Beweiskalkül für Allgemeingültigkeit in endlichen Strukturen geben kann.

**Satz von Traktenbrot** $FINSAT(FO)$ ist unentscheidbar.

**Satz von Tarski** die $FO$-Theorie der Arithmetik, also die Menge $Th(\mathcal{N})$ aller in $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$ wahren $FO(S_{ar})$-Sätze ist unentscheidbar (und nicht aufzählbar).

**Äquivalenzklassen** „modulo logischer Äquivalenz“: