Der Satz von Herbrand

Def: Eine $\mathcal{L}$-Formel ist in pränexer Normalform, falls die Gestalt hat

$Q_1 v_{i_1} \ldots Q_n v_{i_n} \psi$ mit $Q_i \in \{\exists, \forall\}$ und ψ quantorenfrei,

d.h. in ψ kommt kein Quantor vor.

Satz: Jede Formel ist zu einer Formel in pränexer Normalform äquivalent.

Beweis: Zeige: bis auf Äquivalenz sind die pränexen Formeln unter $\exists, \wedge, \neg$ abgeschlossen

$\exists$ trivial: d.h. wenn φ in pränexer NF, dann auch $\exists v_i \varphi$

$\neg$ einfach: Wenn $\neg Q_1 v_{i_1} \ldots Q_n v_{i_n} \psi \sim \bar{Q}_1 v_{i_1} \ldots \bar{Q}_n v_{i_n} \neg \psi$

wobei $\bar{\exists} = \forall$, $\bar{\forall} = \exists$

$\wedge$ ist etwas trickreich $(Q_1 v_1 \varphi \wedge \psi)$ geht ebenso für $\vee$

$\sim (Q_1 v_k \varphi \frac{v_k}{v_1} \wedge \psi)$ wobei v_k in ψ nicht vorkommt

$\sim Q_1 v_k (\varphi \frac{v_k}{v_1} \wedge \psi)$ da v_k in ψ nicht vorkommt!

Bsp: $(\exists v_0 \forall v_1 \, R v_0 v_1 \to \forall v_1 \exists v_0 \, R v_0 v_1)$

$\sim (\neg \exists v_0 \forall v_1 \, R v_0 v_1 \vee \forall v_1 \exists v_0 \, R v_0 v_1)$

$\sim (\underbrace{\forall v_0 \exists v_1 \neg R v_0 v_1}_{\text{pränex}} \vee \underbrace{\forall v_1 \exists v_0 \, R v_0 v_1}_{\text{pränex}})$

$\sim (\forall v_0 \exists v_1 \neg R v_0 v_1 \vee \forall v_2 \exists v_3 \, R v_3 v_2)$

$\sim \forall v_0 (\exists v_1 \neg R v_0 v_1 \vee \forall v_2 \exists v_3 \, R v_3 v_2)$

$\sim \forall v_0 \exists v_1 (\neg R v_0 v_1 \vee \dots)$

$\vdots$

$\sim \forall v_0 \exists v_1 \forall v_2 \exists v_3 (\underbrace{\neg R v_0 v_1 \vee R v_3 v_2}_{(R v_0 v_1 \to R v_3 v_2)})$

Def: Eine $\mathcal{L}$-Formel φ heißt

universell, falls φ in pränexer NF ist und kein Existenzquantor in φ vorkommt

existentiell, ——— " ——— kein Allquantor — " —

(Bem: quantorenfreie Formeln sind universell & existentiell)

Satz (a) Eine $\mathcal{L}$-Aussage φ in pränexer NF kann auf algorithmische Weise zu einer universellen $\mathcal{L}^*$-Aussage φ^* gemacht werden mit:

- $\mathcal{L}^*$ ist $\mathcal{L} \cup \{$ zusätzliche Konstanten und Funktionszeichen $\}$
- φ ist erfüllbar $\Leftrightarrow$ φ^* erfüllbar

(b) $\mathcal{L}$-Aussage φ in pränexer NF kann algorithmisch zu existentieller $\mathcal{L}^*$-Aussage φ_* gemacht werden mit: $\models \varphi \Leftrightarrow \models \varphi_*$

Beweis: Wenn φ $\exists v_i \, \varphi'$, dann neue Konstante c und betrachte $\varphi' \frac{c}{v_i}$
$c \notin \mathcal{L}$

Wenn φ $\exists v_i \, \exists v_j \, \varphi''$, dann 2 neue Konstanten c, d
und betrachte $\varphi'' \frac{c}{v_i} \frac{d}{v_j}$.
$c \notin \mathcal{L}$, $d \notin \mathcal{L} \cup \{c\}$

Wenn φ $\forall v_i \, \exists v_j \, \varphi'''$, dann neues 1-stelliges Funktionszeichen $f \notin \mathcal{L}$
und betrachte $\forall v_i \, \varphi''' \frac{f v_i}{v_j}$

$\forall v_i \, \exists v_j \, R v_i v_j$ zu $R v_i f v_i$

eliminiere nach und nach von außen nach innen alle Existenzquantoren.

Wenn l $\underbrace{\text{Allquantoren}}_{\forall v_{i_1} \dots \forall v_{i_l}}$ links von $\exists v_j$ stehen, ersetze v_j durch $f v_{i_1} \dots v_{i_l}$

Endergebnis ist φ^*, $\mathcal{L}^* = \mathcal{L} \cup$ alle zusätzlichen Zeichen

φ^* erfüllbarkeitsäquivalent mit φ ?

Sei $\mathfrak{M} \models \varphi$, f neues ℓ-stelliges Funktionszeichen

für $m_1, \dots, m_\ell \in M$ betrachte Belegung β mit $\beta(v_{i_k}) = m_k$

$\mathfrak{M} \models \exists v_j \, \chi(v_{i_1}, \dots, v_{i_n}) \, [\beta]$ da φ erfüllbar

$\varphi = \forall v_{i_1} \dots \forall v_{i_n} \exists v_j \, \tilde{\chi}$

dann existiert wegen Erfüllbarkeit ein $m \in M$ mit

$\mathfrak{M} \models \chi(v_{i_1}, \dots, v_{i_n}, v_j) \, [\beta \frac{m}{v_j}]$

Definiere $f^{\mathfrak{M}}(m_1, \dots, m_\ell) = m$ und

$\mathfrak{M}$ mit der $f^{\mathfrak{M}}$ wird zu $\mathcal{L}^*$-Struktur $\mathfrak{M}^*$

mit $\mathfrak{M}^* \models \varphi^*$

Umgekehrt: falls $\mathfrak{M}^* \models \varphi^*$, dann ist $f^{\mathfrak{M}^*}(m_1, \dots, m_\ell)$ „Beweis"

für die Gültigkeit von „$\exists v_j$"

φ^* heißt <u>Skolem-Normal</u>form von φ, oder Skolemisierung,

die zusätzlichen Zeichen heißen Skolem-<u>Konstanten</u> und <u>Skolem-Funktionen</u>.

(b) φ ist allgemeingültig $\iff$ $\neg\varphi$ nicht erfüllbar

$\iff$ $(\neg\varphi)^*$ nicht erfüllbar

$\iff$ $\neg(\neg\varphi)^*$ allgemeingültig

$\iff$ φ_* ist $\neg(\neg\varphi)^*$ in pränexe Normalform gebracht

$$\neg \forall v_{i_1} \ldots \forall v_{i_n} \psi \rightsquigarrow \exists v_{i_1} \ldots \exists v_{i_n} \neg \psi$$

φ_* heißt <u>Herbrand-Normalform</u> von φ

<u>Achtung</u>: * die pränexe NF einer Formel ist nicht eindeutig

* Skolem- und Herbrand-NF einer Formel in pränexer NF sind dagegen durch das Verfahren im wesentlichen eindeutig.

Bsp: a) $\forall v_0 \exists v_1 \forall v_2 \exists v_3 (Rv_0v_1 \to Rv_3v_2) = \varphi$

$\varphi^* = \forall v_0 \forall v_2 (Rv_0 fv_0 \to R\, gv_0v_2\, v_2)$ $\quad$ $\left.\begin{array}{l} f \text{ einstellig} \\ g \text{ zweistellig} \end{array}\right\}$ neu

$\varphi_* = ?$ $\quad \neg\varphi \sim \exists v_0 \forall v_1 \exists v_2 \forall v_3 \neg(Rv_0v_1 \to Rv_3v_2)$

$(\neg\varphi)^* = \forall v_1 \forall v_3 \neg(Rcv_1 \to Rv_3hv_1)$ $\quad$ $\left.\begin{array}{l} c \text{ Konstante} \\ h \text{ einstellig} \end{array}\right\}$ neu

$\varphi_* = \exists v_1 \exists v_3 (Rcv_1 \to Rv_3hv_1)$

b) $\exists v_0 \forall v_1 \forall v_2 \exists v_3 \exists v_4 \chi = \varphi$

$\varphi^* = \forall v_1 \forall v_2\, \chi \frac{c}{v_0} \frac{fv_1v_2}{v_3} \frac{gv_1v_2}{v_4}$ $\quad$ f, g neu

Def: Ein $\mathcal{L}$-Term heißt <u>geschlossen</u> („closed"), falls in dem Term keine Individuenvariablen vorkommen

$f v_i c$ nicht geschlossen
$f f c c c$ geschlossen (f zweistellig)

<u>Satz von Herbrand:</u>

Sei $\mathcal{L}$ eine Sprache mit mindestens einer Konstanten
$\varphi = \exists v_1 \dots \exists v_k \psi$ sei existentielle Formel mit quantorenfreiem ψ

Dann ist φ genau allgemeingültig, wenn es ein $N \in \mathbb{N}$ gibt und geschlossene $\mathcal{L}$-Terme $\tau_{11}, \dots \tau_{1k}, \dots, \tau_{N1}, \dots, \tau_{Nk}$ so, dass

$$\left(\psi \frac{\tau_{11}}{v_1} \dots \frac{\tau_{1k}}{v_k} \vee \psi \frac{\tau_{21}}{v_1} \dots \frac{\tau_{2k}}{v_k} \vee \dots \vee \frac{\tau_{N1}}{v_1} \dots \frac{\tau_{Nk}}{v_k} \right)$$ allgemeingültig ist.

Bem: Falls in ψ kein Gleichheitszeichen vorkommt, ist die Frage, ob

$\left(\psi \frac{\tau_{11}}{v_1} \dots \quad \vee \dots \vee \psi \frac{\tau_{N1}}{v_1} \dots \right)$ allgemeingültig ist, ein rein aussagenlogisches

Problem (ersetze atomare Formeln durch Aussagenvariablen und teste, ob das Ergebnis eine Tautologie ist).

Bem (vgl. Übung): man sich immer auf Formel ohne Gleichheitszeichen zurückziehen.

Beweis von Satz von Herbrand:

klar: $\psi \frac{\tau_1}{v_1} \dots \frac{\tau_k}{v_k} \models \exists v_1 \dots \exists v_k \psi$

$$\left(\psi \frac{\tau_{11}}{v_1} \dots \frac{\tau_{1k}}{v_k} \vee \dots \vee \psi \frac{\tau_{N1}}{v_1} \dots \frac{\tau_{Nk}}{v_k}\right) \models \exists v_1 \dots \exists v_k \psi$$

Also: falls $\downarrow$ allgemeingültig, dann auch $\uparrow$

Also Annahme: φ ist allgemeingültig, aber für alle Termeinsetzungen ist $\psi\frac{\bar{\tau}}{\dots} \vee \dots$ nicht allgemeingültig,

d.h. $\neg\left(\psi\frac{\tau_{11}}{v_1}\dots \vee \dots \vee \psi\frac{\tau_{n1}}{v_1}\dots\right)$ ist erfüllbar

$$\sim \left(\neg\psi\frac{\tau_{11}}{v_1}\dots\frac{\tau_{1k}}{v_k} \wedge \dots \wedge \neg\psi\frac{\tau_{n1}}{v_1}\dots\frac{\tau_{nk}}{v_k}\right)$$

Also: $\underbrace{\left\{\neg\psi\frac{\tau_1}{v_1}\dots\frac{\tau_k}{v_k} \;\middle|\; \tau_i \text{ geschlossene } \mathcal{L}\text{-Terme}\right\}}_{=\Psi}$ ist endlich erfüllbar (jede endl. Konjunktion ist erfüllbar)

Kompaktheitssatz: Ψ ist erfüllbar und hat also ein Modell $\mathfrak{M}$

$$M_0 = \{\tau^{\mathfrak{M}} \mid \tau \text{ geschlossener } \mathcal{L}\text{-Term}\}$$

M_0 ist unter den $\underbrace{f^{\mathfrak{M}}}_{n\text{-stellig}}$ für $f \in \mathcal{L}$ abgeschlossen, denn

$$f^{\mathfrak{M}}(\tau_1^{\mathfrak{M}}, \dots, \tau_n^{\mathfrak{M}}) = (f\tau_1\dots\tau_n)^{\mathfrak{M}}$$

also ist M_0 Universum einer Unterstruktur $\mathfrak{M}_0$ von $\mathfrak{M}$

In $\mathfrak{M}_0$ gilt $\neg\psi\frac{\tau_1}{v_1}\ldots\frac{\tau_k}{v_k}$ für alle geschlossenen $\mathcal{L}$-Terme τ_i

denn: $\mathfrak{M} \models \underbrace{\neg\psi\frac{\tau_1}{v_1}\ldots\frac{\tau_k}{v_k}}_{\text{quantorenfreie Formel}}$

Bem: Wenn χ quantorenfrei, $\mathfrak{M}_0 \subseteq \mathfrak{M}$, dann $\mathfrak{M} \models \chi \Rightarrow \mathfrak{M}_0 \models \chi$

denn dies gilt per Definition für alle atomaren Formeln

der Unterstruktur!

und setzt sich über die Junktoren zu beliebigen quantorenfreien Formeln fort

In $\mathfrak{M}_0$ sind aber alle Elemente von der Form $\tau^{\mathfrak{M}_0}$

d.h. $\mathfrak{M}_0 \models \forall v_1\ldots\forall v_k\,\neg\psi(v_1\ldots v_k) \sim \neg\exists v_1\ldots\exists v_k\,\psi = \neg\varphi$

Widerspruch zur Allgemeingültigkeit! $\boxtimes$

Bsp: $\exists v_1 \exists v_3 (R c v_1 \to R v_3 h v_1)$

$\sim \exists v_1 \exists v_3 (\neg R c v_1 \vee R v_3 h v_1)$

geschlossene Terme: c, hc, hhc, $\vdots$

$v_1 \rightsquigarrow c$, $v_3 \rightsquigarrow c$

$v_1 \rightsquigarrow hc$, $v_3 \rightsquigarrow c$

$v_1 \rightsquigarrow c$, $v_3 \rightsquigarrow hc$

$$(\neg Rcc \vee \underline{Rchc}) \vee (\underline{\neg Rchc} \vee Rchhc) \vee (\neg Rcc \vee Rhchc)$$

$\sim \top$

Um mit Herbrand-Methode Allgemeingültigkeit zu testen, wendet man auf die Termeinsetzungen am besten die Resolutionsmethode an (bzw. Variante)

Dazu sollte man versuchen, durch geschickte Termeinsetzungen gleiche atomare Formeln zu erreichen. Dies geschieht durch <u>Unifikation</u>.

Gegeben Menge von Paaren von Termen $P = \{(\tau_1,\tau_1'),\dots,(\tau_n,\tau_n')\}$ $\quad \tau_i,\tau_i'$ $\mathcal{L}$-Terme

Unifikation von P ist eine Menge von Ersetzungen $\frac{\sigma_i}{v_i}$, σ_i $\mathcal{L}$-Terme, $i=1,\dots,k$

so dass

$$\tau_1 \frac{\sigma_1}{v_1} \cdots \frac{\sigma_k}{v_k} = \tau_1' \frac{\sigma_1}{v_1} \cdots \frac{\sigma_k}{v_k}$$
$$\vdots$$
$$\tau_n \frac{\sigma_1}{v_1} \cdots \frac{\sigma_k}{v_k} = \tau_n' \frac{\sigma_1}{v_1} \cdots \frac{\sigma_k}{v_k}$$

__Beispiel__ $\quad f, g$ zweistellig, h einstellig

$\tau_1 = f\, v_1\, g\, v_2 v_3 \qquad f(v_1, g(v_2, v_3))$

$\tau_1' = f\, h v_3\, v_4$

$\rightsquigarrow$ $f\, h v_3\, g v_2 v_3$

unifizierter Term

$\xrightarrow{\frac{h v_5}{v_3}}$

$f\, h h v_5\, g v_2 h v_5$

eine Unifikation durch $\frac{h v_3}{v_1} \; \frac{g v_2 v_3}{v_4}$

andere Möglichkeit $\frac{h v_5}{v_3} \; \frac{h h v_5}{v_1} \; \frac{g v_2 h v_5}{v_4}$

Satz: Wenn Paare von Termen unifiziert werden können, dann durch eine minimale Unifikation („Haupt-Unifikator"). Jede andere Unifikation entsteht aus der Hauptunifikation durch weitere Termersetzungen.

(ohne Beweis)

Algorithmus (entscheidet, ob Paare unifizierbar sind und findet Haupt-Unifikator)

Induktion über Aufbau der Terme

Start P, schaue τ_i, τ_i' an.

$\frac{\tau_i'}{v_j}$ ein Ersetzung gut

v_i $\quad f v_i$ nicht unifizierbar

Symmetrisch in τ_i, τ_i'

- Falls $\tau_i = f v_1 \dots v_k$ und τ_i' beginnt mit $g \neq f$: nicht unifizierbar!
  Falls — " — $\tau_i' \; f g_1 \dots g_k$, ersetze P durch $P \setminus \{(\tau_i, \tau_i')\} \cup \{(v_1, g_1), \dots, (v_k, g_k)\}$
- Falls $\tau_i = v_j$ und v_j kommt in τ_i' vor, $\tau_i' \neq v_j$: nicht unifizierbar
- Falls $\tau_i = v_j$ und v_j kommt in τ_i' nicht vor