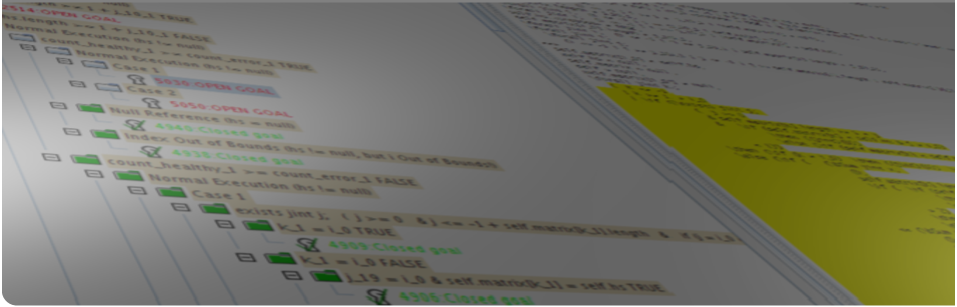
Karlsruhe Institute of Technology

Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2018/2019

Prädikatenlogik: Normalformen

KIT – Institut für Theoretische Informatik



Quiz

Welche der folgenden logischen Folgerungen sind korrekt (für alle A)?

p einstellige Prädikatszeichen
c, d Konstantensymbole $\quad$ x, y, z Variablen

$p(c)$	$\models$	$\forall x\, p(x)$	*nein*
$\forall x\, p(x)$	$\models$	$p(c)$	*ja*
$\forall x \exists y A$	$\models$	$\exists y \forall x A$	*nein*
$\exists x \forall y A$	$\models$	$\forall y \exists x A$	*ja*
	$\models$	$\forall x \exists y A \rightarrow \exists y \forall x A$	*nein*
	$\models$	$\exists x \forall y A \rightarrow \forall y \exists x A$	*ja*

Prädikatenlogische Normalformen

Negationsnormalform

Definition

Eine Formel $A \in For$ heißt

1. eine **Negationsnormalform**, wenn jedes Negationszeichen in A vor einer atomaren Teilformel steht (insbesondere keine Teilformel der Form $\neg\neg B$) und keine Implikation in A vorkommt
2. *bereinigt*, wenn
   - $Frei(A) \cap Bd(A) = \emptyset$
   - die hinter Quantoren stehenden Variablen paarweise verschieden sind.

Theorem

Zu jeder Formel A gibt es eine logisch äquivalente

1. *Formel B in Negationsnormalform.*
2. *bereinigte Formel B.*

Pränexe Normalform

Definition

$A \in For$ heißt eine *Pränexe Normalform*, wenn A die Gestalt hat

$$Q_1 x_1 \dots Q_n x_n B$$

mit $Q_i \in \{\forall, \exists\}$, $x_i \in Var$ und B quantorenfrei. Man nennt B die *Matrix* von A.

Pränexe Normalform

Theorem

Zu jeder Formel A gibt es eine äquivalente in Pränex-Normalform.

Die Pränex-Normalform läßt sich aus A durch sukzessive Anwendung der Tautologien

$$
\begin{array}{ll}
A \wedge QxB \leftrightarrow Qx(A \wedge B)) & x \notin Frei(A) \\
A \vee QxB \leftrightarrow Qx(A \vee B)) & x \notin Frei(A) \\
(A \rightarrow QxB) \leftrightarrow Qx(A \rightarrow B)) & x \notin Frei(A) \\
(\exists xB \rightarrow A) \leftrightarrow \forall x(B \rightarrow A) & x \notin Frei(A) \\
(\forall xB \rightarrow A) \leftrightarrow \exists x(B \rightarrow A) & x \notin Frei(A)
\end{array}
$$

erhalten

Pränexe Normalform

Beispiel

Aus

$$\forall y\ (\forall x(\forall y\ p(x,y)) \rightarrow \exists x\ r(x,y))$$

erhält man sukzessive:

$$\forall y(\forall x(\forall z\ p(x,z)) \rightarrow \exists u\ r(u,y))$$

Pränexe Normalform

Beispiel

Aus

$$\forall y\ (\forall x(\forall y\ p(x,y)) \to \exists x\ r(x,y))$$

erhält man sukzessive:

$$\forall y(\forall x(\forall z\ p(x,z)) \to \exists u\ r(u,y))$$

$$\forall y(\exists x(\forall z\ p(x,z) \to \exists u\ r(u,y)))$$

Pränexe Normalform

Beispiel

Aus

$$\forall y(\ \forall x(\ \forall y\ p(x,y)) \to \exists x\ r(x,y))$$

erhält man sukzessive:

$$\forall y(\ \forall x(\ \forall z\ p(x,z)) \to \exists u\ r(u,y))$$
$$\forall y(\ \exists x(\ \forall z\ p(x,z) \to \exists u\ r(u,y)))$$
$$\forall y(\ \exists x(\ \exists z(\ p(x,z) \to \exists u\ r(u,y))))$$

Pränexe Normalform

Beispiel

Aus

$$\forall y \; (\forall x(\forall y \; p(x, y)) \to \exists x \; r(x, y))$$

erhält man sukzessive:

$$\forall y(\forall x(\forall z \; p(x, z)) \to \exists u \; r(u, y))$$

$$\forall y(\exists x(\forall z \; p(x, z) \to \exists u \; r(u, y)))$$

$$\forall y(\; \exists x(\; \exists z(p(x, z) \to \exists u \; r(u, y))))$$

$$\forall y(\; \exists x(\; \exists z(\; \exists u(p(x, z) \to r(u, y)))))$$

Pränexe Normalform

Beispiel

Aus

$$\forall y\ (\forall x(\forall y\ p(x,y)) \to \exists x\ r(x,y))$$

erhält man sukzessive:

$$\forall y(\forall x(\forall z\ p(x,z)) \to \exists u\ r(u,y))$$
$$\forall y(\exists x(\forall z\ p(x,z) \to \exists u\ r(u,y)))$$
$$\forall y(\ \exists x(\ \exists z(\ p(x,z) \to \exists u\ r(u,y))))$$
$$\forall y\ \exists x\ \exists z\ \exists u(\ p(x,z) \to r(u,y))$$

Pränexe Normalform

Eindeutigkeit?

Abhängig von der Reihenfolge der angewandten Äquivalenzen kann man z. B. aus

$$\forall x p(x) \to \forall y q(y)$$

sowohl $\exists x \forall y (p(x) \to q(y))$

als auch $\forall y \exists x (p(x) \to q(y))$

erhalten.

Quantoren gegen Funktionszeichen

Darstellung mit Existenzquantor

1. $\forall x \exists y (y \doteq x + x)$
2. $\forall x \exists y (x < y)$
3. $\forall x \forall y \exists z (x < y \rightarrow x + z \doteq y)$

Darstellung mit Funktionszeichen

1. $\forall x (do(x) \doteq x + x)$
2. $\forall x (x < gr(x))$
3. $\forall x \forall y (x < y \rightarrow x + \mathit{diff}(x, y) \doteq y)$

Noch einmal die Funktionszeichen mit ihren Interpretationen

Darstellung mit Funktionszeichen

1. $\forall x(do(x) \doteq x + x)$
2. $\forall x(x < gr(x))$
3. $\forall x \forall y(x < y \rightarrow x + diff(x, y) \doteq y)$

Interpretationen

1. $do^{\mathcal{N}_1}(d) = d + d$ (einzige Möglichkeit)
2. etwa: $gr^{\mathcal{N}_2}(d) = d + 1$
3. etwa:
   $$diff^{\mathcal{N}_3}(d_1, d_2) = \begin{cases} d_2 - d_1 \text{ falls } d_1 < d_2 \\ 0 \text{ sonst} \end{cases}$$

   Der Wert im Fall $d_2 \leq d_1$ ist willkürlich gewählt.

Skolem-Normalform

Definition

Eine Formel ist in *Skolem-Normalform*, wenn sie

- geschlossen ist
- die Gestalt $\forall x_1 \ldots \forall x_n B$ hat mit quantorenfreiem B
- die Matrix B in KNF ist.

Skolem-Normalform

Theorem

Zu jedem $A \in For_\Sigma$ gibt es eine endliche Erweiterung Σ_{sk} von Σ und eine Formel $A_{sk} \in For_{\Sigma_{sk}}$ mit

- *A_{sk} ist in Skolem-Normalform*
- *A_{sk} hat ein Modell genau dann, wenn A ein Modell hat.*

A_{sk} läßt sich aus A algorithmisch erhalten.

Skolem-Normalform

Allgemeine Konstruktionsvorschrift

0. All-Abschluss der freien Variablen
1. Transformation in pränexe Normalform: $Q_1 x_1 \ldots Q_n x_n B$
2. Skolemisierung
   (a) Signatur-Erweiterung von Σ zu Σ_{sk}:
   Für jedes i, $1 \leq i \leq n$, so daß $Q_i = \exists$ wird ein neues k-stelliges Funktionszeichen f_i hinzugefügt, wobei k die Anzahl der Q_j mit $Q_j = \forall$ und $j < i$

   (b) Für alle $Q_i = \exists$:
   - Lasse $\exists x_i$ weg
   - Substituiere x_i in B durch $f_i(\bar{x}_i)$, wobei $\bar{x}_i$ das Tupel aller Variablen x_j mit $1 \leq j < i$ und $Q_j = \forall$ ist.
3. Transformation der Matrix der Formal in KNF.

Beispiel 1

Gegeben:

$$\forall x(\exists y(p(y)) \land \exists z(q(x,z)))$$

Pränex Normalform:

$$\forall x \exists y \exists z(p(y) \land q(x,z))$$

Skolem Normalform:

$$\forall x(p(f_1(x)) \land q(x, f_2(x)))$$

Beispiel 2

Gegeben:

$$\exists x(p(w,x) \vee \forall y(q(w,x,y) \wedge \exists z\, r(y,z)))$$

All-Abschluß:

$$\forall w\ \exists x(p(w,x) \vee \forall y(q(w,x,y) \wedge \exists z r(y,z)))$$

Beispiel 2

Gegeben:

$$\exists x(p(w,x) \vee \forall y(q(w,x,y) \wedge \exists z\, r(y,z)))$$

All-Abschluß:

$$\forall w\ \exists x(p(w,x) \vee \forall y(q(w,x,y) \wedge \exists z r(y,z)))$$

Pränex Normalform:

$$\forall w\ \exists x\ \forall y\ \exists z(p(w,x) \vee (q(w,x,y) \wedge r(y,z)))$$

Beispiel 2

Gegeben:

$$\exists x(p(w,x) \vee \forall y(q(w,x,y) \wedge \exists z\, r(y,z)))$$

All-Abschluß:

$$\forall w\, \exists x(p(w,x) \vee \forall y(q(w,x,y) \wedge \exists z r(y,z)))$$

Pränex Normalform:

$$\forall w\, \exists x\, \forall y\, \exists z(p(w,x) \vee (q(w,x,y) \wedge r(y,z)))$$

Skolemisierung:

$$\forall w\, \forall y(p(w,f_1(w)) \vee (q(w,f_1(w),y) \wedge r(y,f_2(w,y))))$$

Beispiel 2

Gegeben:

$$\exists x(p(w,x) \vee \forall y(q(w,x,y) \wedge \exists z\, r(y,z)))$$

All-Abschluß:

$$\forall w\, \exists x(p(w,x) \vee \forall y(q(w,x,y) \wedge \exists z r(y,z)))$$

Pränex Normalform:

$$\forall w\, \exists x\, \forall y\, \exists z(p(w,x) \vee (q(w,x,y) \wedge r(y,z)))$$

Skolemisierung:

$$\forall w\, \forall y(p(w,f_1(w)) \vee (q(w,f_1(w),y) \wedge r(y,f_2(w,y))))$$

Matrix in KNF, Skolem Normalform:

$$\begin{aligned}\forall w\, \forall y(\ & (p(w,f_1(w)) \vee q(w,f_1(w),y)) \quad \wedge \\ & (p(w,f_1(w)) \vee r(y,f_2(w,y))))\end{aligned}$$

Definition

Grundinstanzen

Sei $A := \forall x_1 \ldots \forall x_n B$
mit quantoremfreiem B eine geschlossenen Formel.
Eine **Grundinstanz** von A ist eine Formel

$$\{x_1/t_1, \ldots, x_n/t_n\}(B)$$

mit Grundtermen $t_1, \ldots, t_n$.
Ist M eine Menge geschlossener, universell quantifizierter Formeln, so sei

$$\text{Grundinstanzen}(M)$$

die Menge aller Grundinstanzen aller Formeln in M.

Herbrand-Strukturen

Definition

Die Signatur Σ enthalte mindestens eine Konstante.
Eine Interpretation (D, I) von Σ heißt *Herbrand-Interpretation* oder *Herbrand-Struktur*, wenn

1. $D = Term^0_\Sigma$ = Menge der Grundterme.
2. $I(f)(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$
   für alle Funktionssymbole $f \in \Sigma$
   und beliebige Grundterme $t_1, \ldots, t_n$.

In einer Herbrand-Struktur wird jeder Grundterm t als er selbst interpretiert,

$$val_{D,I}(t) = t$$

Spielraum für *verschiedene* Herbrand-Strukturen gibt es nur bei der Interpretation der Prädikatsymbole.

Satz von HERBRAND

Theorem

Σ enthalte mindestens eine Konstante, und es sei M eine Menge geschlossener, universell quantifizierter Formeln. Ferner enthalte keine Formel in M das Gleichheitssymbol $\doteq$. Dann sind äquivalente Aussagen

1. *M hat ein Modell*
2. *M hat ein Herbrand-Modell*
3. *Grundinstanzen(M) hat ein Modell*
4. *Grundinstanzen(M) hat ein Herbrand-Modell.*

Beweisübersicht

1. M hat ein Modell
2. M hat ein Herbrand-Modell
3. Grundinstanzen(M) hat ein Modell
4. Grundinstanzen(M) hat ein Herbrand-Modell.

Die Implikationen $4 \Rightarrow 3$ und $2 \Rightarrow 1$ sind trivial;
ebenso wegen der Allgemeingültigkeit von

$$\forall x_1 \ldots \forall x_n B \to \{x_1/t_1, \ldots, x_n/t_n\}(B)$$

die Implikationen $1 \Rightarrow 3$ und $2 \Rightarrow 4$.
Es genügt zusätzlich noch zu zeigen, daß $3 \Rightarrow 2$.

Beweis

Es sei $\mathcal{D}$ ein Modell von Grundinstanzen(M).

Wir definieren eine Herbrand-Interpretation $\mathcal{H} = (Term^0_\Sigma, J)$.

$$J(p) \quad := \quad \{(t_1, \ldots, t_n) \mid \quad t_i \in Term^0_\Sigma, val_\mathcal{D}(p(t_1, \ldots, t_n)) = W\}$$

für Prädikatsymbole p einer Stelligkeit n.

Für jedes geschlossene Atom A gilt also $val_\mathcal{H}(A) = val_\mathcal{D}(A)$
Durch Induktion beweist man diese Relation für alle geschlossenen, quantorenfreien Formeln A.

Für $\forall x_1 \ldots \forall x_n B \in M$ gilt

$val_\mathcal{D}(\{x_1/t_1, \ldots, x_n/t_n\}B) = W$ für alle Grundinstanzen $t_1, \ldots, t_n$
$val_\mathcal{H}(\{x_1/t_1, \ldots, x_n/t_n\}B) = W$ für alle Grundinstanzen $t_1, \ldots, t_n$
$val_\mathcal{H}(\forall x_1 \ldots \forall x_n B) = W$

(letzter Schritt verwendet Substitutionstheorem)

Einschub: Endlichkeitssatz (Kompaktheitssatz) der Aussagenlogik

Theorem

Sei U eine unendliche Menge aussagenlogischer Formeln.

U ist genau dann unerfüllbar, wenn
es eine endliche Teilmenge $E \subset U$ gibt, die unerfüllbar ist.

Beweis später

Satz von HERBRAND
2. Form

Sei ϕ eine quantorenfreie Formel ohne Gleichheit mit (nur) einer freien Variablen x. Dann gilt

1. $\exists x \phi$ ist allgemeingültig

   gdw

   es gibt ein $n \in \mathbb{N}$ und Grundterme $t_1, \ldots, t_n$, so dass

   $\phi(t_1) \vee \ldots \vee \phi(t_n)$

   allgemeingültig ist.

2. $\forall x \phi$ ist unerfüllbar

   gdw

   es gibt ein $n \in \mathbb{N}$ und Grundterme $t_1, \ldots, t_n$, so dass

   $\phi(t_1) \wedge \ldots \wedge \phi(t_n)$

   unerfüllbar ist.

Beweis der 2. Form des Satzes von HERBRAND

(2. Form folgt aus 1. Form des Satzes + Endlichkeitssatz)

1.:

$\exists x \phi$ ist allgemeingültig

$\Leftrightarrow$ $\neg \exists x \phi$ ist unerfüllbar

$\Leftrightarrow$ $\forall x \neg \phi$ ist unerfüllbar

$\Leftrightarrow$ $\{\neg \phi(t) \mid t$ Grundterm$\}$ ist unerfüllbar

$\Leftrightarrow$ es gibt ein n und $t_1, \ldots, t_n$ so daß
$\{\neg \phi(t_1), \ldots, \neg \phi(t_n)\}$ ist unerfüllbar
(Anwendung des Endlichkeitssatzes der Aussagenlogik)

$\Leftrightarrow$ $\neg \phi(t_1) \wedge \ldots \wedge \neg \phi(t_n)$ ist unerfüllbar

$\Leftrightarrow$ $\phi(t_1) \vee \ldots \vee \phi(t_n)$ ist allgemeingültig

2.: Analog