Warum Prädikatenlogik?

- „Mächtiger“ als die Aussagenlogik
- Die Prädikatenlogik ist die formale Sprache der Mathematik und Informatik.
- Ein Computer der „denkt“, denkt in der Regel in der Sprache der Prädikatenlogik
- Die Prädikatenlogik ist eine *wesentliche Grundlage* für
  - Künstliche Intelligenz (siehe `www.cis.TUGraz.at/igi/lehre/EKI/`)
  - Softwaretechnologie (z.B: automatische Programmverifikation)
  - Datenbanken
  - Maschinelles Beweisen (siehe TI 2)
  - Maschinelles Lernen (z.B: first odrer logic programming)
  - Hardware Verifikation
- Die Prädikatenlogik ist bisher dauerhafter als jede Programmiersprache geblieben. (Welche 70 Jahre alte Programmiersprache gibt es?)

Prädikatenlogik: Erweiterung der Aussagenlogik

In der Aussagenlogik ist es nicht möglich auszudrücken, daß gewisse

- „Objekte“ in gewissen Beziehungen (Relationen) zueinander stehen,
- daß eine Eigenschaft *für alle* Objekte gilt,
- oder daß ein Objekt mit einer bestimmten Eigenschaft *existiert*.

Beispiel:

Für alle $\varepsilon > 0$ gibt es ein n_0, sodaß für alle $n \geq n_0$ gilt: $\mathrm{abs}(f(n) - a) < \varepsilon$.

Die wesentlichen Bestandteile hier sind die sprachlichen Konstrukte „für alle“ und „es gibt“, sowie die Verwendung von *Funktionen* (abs,f,$-$) und *Relationen* ($\geq$, $>$, $<$). Die Objekte sind in diesem Beispiel Zahlen.

Elemente der Prädikatenlogik

Man verwendet für beliebige $i \in \mathbb{N}$ die Symbole

- x_i für Variablen (dies sind *Variablen für Objekte*),
- Symbole f_i^k für *k-stellige Funktionen* ($k \in \mathbb{N} \cup \{0\}$),
- Symbole P_i^k für *k-stellige Prädikate* ($k \in \mathbb{N} \cup \{0\}$),
- einem Symbol “=”für ein 2-stelliges Prädikat (“Gleichheitszeichen”),
- sowie die *Quantoren* $\exists$ (Existenzquantor), $\forall$ (Allquantor).

Anmerkungen:

- Neben x_i verwenden wir auch x, y, z, u, v (auch mit Indizes) als Variablen
- 0-stellige Funktionssymbole spielen die Rolle von *Konstanten*.

Definition eines Terms

Mittels Funktionszeichen (möglicherweise hintereinandergeschaltet) angewendet auf Variablen für Objekte können neue formale Bezeichnungen für Objekte erzeugt werden, die als *Terme* bezeichnet werden:

Definition eines Terms

1. Jede Variable x_i ist ein *Term*.
2. Falls f_i^k ein Symbol für eine k-stellige Funktion ist, und $t_1, \ldots, t_k$ sind Terme, so ist auch $f_i^k(t_1, \ldots, t_k)$ ein *Term*.

Beispiel: $f_7^3(x_2, f_1^1(x_3), f_5^0)$ ist ein Term, und f_5^0 ist eine Konstante.

Definition einer Formel

1. Falls $t_1, \ldots, t_k$ Terme sind und P_i^k ein Symbol für ein k-stelliges Prädikat ist, so ist $P_i^k(t_1, \ldots, t_k)$ eine *Formel* (*atomare Formeln*).
2. Falls F eine Formel ist, so ist auch $\neg F$ eine *Formel*.
3. Falls F, G Formeln sind, so sind auch $(F \wedge G)$ und $(F \vee G)$ *Formeln.*
4. Falls x_i eine Variable und F eine Formel ist, so sind auch $\exists x_i F$ und $\forall x_i F$ *Formeln.*

Beispiel für eine Formel: $\forall x \exists y(P^1(y) \vee \exists z P^2(z, f^2(x, y)))$

Bemerkungen:

1. Man bezeichnet die nach 1. in Definition 1.2.2 gebildeten Formeln als *atomare Formeln*.
2. $F \rightarrow G$ ist eine Abkürzung für $\neg F \vee G$, wie in der Booleschen Logik.
3. $F \leftrightarrow G$ ist eine Abkürzung für $(F \rightarrow G) \wedge (G \rightarrow F)$, wie in der Booleschen Logik.

Freie / Gebundene Variablen

Definition: Ein *Auftreten* einer Variablen x_i in einer Formel F wird als *gebunden* bezeichnet, falls es innerhalb einer Teilformel der Form $\exists x_i G$ oder $\forall x_i G$ von F liegt. Andernfalls wird dieses Auftreten von x_i in F als *frei* bezeichnet.

Durch den ersten Quantor in einer Teilformel $\exists x_i G$ oder $\forall x_i G$ werden alle Auftreten von x_i in G gebunden, die frei in G auftreten.

Beispiel:

$$F :\equiv (f(x_j) = x_i \vee \exists\, x_i(P(f(x_i))))$$
$$\qquad\qquad\quad \uparrow \qquad \uparrow \qquad \uparrow$$

freies gebundenes Auftreten von x_i in der Formel F.

Eine Formel ohne freie Variablen wird als *Aussage* bezeichnet. Man kann die Variablen $a, b, c, \ldots$ der Booleschen Logik als Variablen auffassen die für beliebige Aussagen stehen.

Freie / Gebundene Variablen

Übung 43: Man gebe sämtliche Teilformeln und Terme an, die in der Formel

$$F = ((Q(x) \vee \exists x \forall y(P(f(x), z) \wedge Q(a))) \vee \forall z R(x, z, g(x)))$$

enthalten sind. Welche Teilformeln sind Aussagen? Für jedes Vorkommen einer Variablen bestimme man, ob es frei oder gebunden ist. Wie lautet die Matrix von F ?

43. Teilformeln:

$((Q(x) \vee \exists x \forall y(P(f(x), z) \wedge Q(a))) \vee \forall z R(x, z, g(x)))$
$(Q(x) \vee \exists x \forall y(P(f(x), z) \wedge Q(a)))$
$\forall z R(x, z, g(x))$
$Q(x)$
$\exists x \forall y(P(f(x), z) \wedge Q(a))$
$\forall y(P(f(x), z) \wedge Q(a))$
$(P(f(x), z) \wedge Q(a))$
$P(f(x), z)$
$Q(a)$
$R(x, z, g(x))$

Terme:

$x,\ y,\ z,\ a,\ f(x),\ g(x)$

Die folgenden Vorkommen von Variablen sind frei (die anderen sind somit gebunden):

$((Q(x) \vee \exists x \forall y(P(f(x), z) \wedge Q(a))) \vee \forall z R(x, z, g(x)))$
$\qquad\quad \uparrow \qquad\qquad\quad \uparrow \qquad\qquad\quad \uparrow \quad \uparrow$

Semantik der Prädikatenlogik (Definition Struktur)

Definition einer Struktur: Eine *Struktur* $\mathcal{A}$ is ein Paar $(U_\mathcal{A}, I_\mathcal{A})$. Dabei ist $U_\mathcal{A}$ eine Menge (das *"Universum"* der Struktur, die Variablen x_i laufen über die Elemente von $U_\mathcal{A}$), und $I_\mathcal{A}$ ist eine Abbildung (*"Interpretation"*)

- die einigen k-stelligen Prädikatssymbolen P_i^k jeweils eine beliebige Teilmenge $P_i^{k,\mathcal{A}} \subseteq (U_\mathcal{A})^k$ (d.h. k-stellige Relationen über $U_\mathcal{A}$) zuordnet,
- die einigen k-stelligen Funktionssymbolen f_i^k jeweils eine beliebige k-stellige Funktion $f_i^{k,\mathcal{A}} : (U_\mathcal{A})^k \rightarrow U_\mathcal{A}$ zuordnet,
- und die einigen Variablen x_i beliebige Elemente $x_i^\mathcal{A}$ in $U_\mathcal{A}$ zuordnet.

Dem 2-stelligen Prädikatssymbol "=" wird in jeder Struktur $\mathcal{A}$ stets die Menge $\{\langle x, x\rangle | x \in U_\mathcal{A}\}$ zugeordnet.

Definition: Man sagt, daß $\mathcal{A} = (U_\mathcal{A}, I_\mathcal{A})$ eine *zu einer Formel F passende Struktur* ist, falls $I_\mathcal{A}$ für alle in in F vorkommenden Prädikatensymbole, Funktionssymbole und freien Variablen definiert ist.

Beispiel für eine Struktur

Beispiel: $F = \forall x P(x, f(x)) \wedge Q(g(a, z))$ ist eine Formel. Hierbei ist P ein zweistelliges und Q ein einstelliges Prädikatsymbol und f ein einstelliges, g ein zweistelliges und a ein nullstelliges Funktionssymbol. Die Variable z kommt in F frei vor. Eine zu F passende Struktur ist z.B. $\mathcal{A} = (U_\mathcal{A}, I_\mathcal{A})$ mit

$$
\begin{aligned}
U_\mathcal{A} &= \{0, 1, 2, \ldots\} = \mathbb{N}, \\
I_\mathcal{A}(P) &= P^\mathcal{A} = \{(m, n) \mid m, n \in U_\mathcal{A} \text{ und } m < n\}, \\
I_\mathcal{A}(Q) &= Q^\mathcal{A} = \{n \in U_\mathcal{A} \mid n \text{ ist Primzahl }\} \\
I_\mathcal{A}(f) &= f^\mathcal{A} = \text{ die Nachfolgerfunktion auf } U_\mathcal{A}, \\
&\quad \text{also } f^\mathcal{A}(n) = n + 1, \\
I_\mathcal{A}(g) &= g^\mathcal{A} = \text{ die Additionsfunktion auf } U_\mathcal{A}, \\
&\quad \text{also } g^\mathcal{A}(m, n) = m + n, \\
I_\mathcal{A}(a) &= a^\mathcal{A} = 2, \\
I_\mathcal{A}(z) &= z^\mathcal{A} = 3.
\end{aligned}
$$

Semantik der Prädikatenlogik, 1
(Interpreation einer Formel)

Sei $\mathcal{A}$ eine zu F passende Struktur, so wird jedem in F auftretenden Term t ohne gebundene Variablen aufgrund der folgenden Regeln ein Element $\mathcal{A}(t) \in U_\mathcal{A}$ zugeordnet:

- Falls t eine Variable x_i ist, dann ist $\mathcal{A}(t) := x_i^\mathcal{A}$.
- Falls t von der Form $f_i^k(t_1, \ldots, t_k)$ ist, so ist $\mathcal{A}(t) := f_i^{k,\mathcal{A}}(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_k))$.

Semantik der Prädikatenlogik, 2

Weiters ordnet $\mathcal{A}$ der Formel F einen Wahrheitswert $\mathcal{A}(F) \in \{0, 1\}$ zu:

1. Falls F eine atomare Formel $P_i^k(t_1, \ldots, t_k)$ ist, so ist
$$\mathcal{A}(F) = \begin{cases} 1 & , \text{ falls } \langle \mathcal{A}(t_1), \ldots, \mathcal{A}(t_k) \rangle \in P_i^{k,\mathcal{A}} \\ 0 & , \text{ sonst .} \end{cases}$$
2. Falls F von der Form $\neg G$ ist, so ist
$$\mathcal{A}(F) = 1 - \mathcal{A}(G).$$
3. Falls F von der Form $G \wedge H$ ist, so ist
$$\mathcal{A}(F) = \mathcal{A}(G)\mathcal{A}(H).$$
4. Falls F die Form $\forall x_i G$ hat, so ist $\mathcal{A}(F) = 1$ falls für alle $d \in U_\mathcal{A}$ gilt: $\mathcal{A}_{[x_i/d]}(G) = 1$.
5. Falls F die Form $\exists x_i G$ hat, so ist $\mathcal{A}(F) = 1$, falls es mindestens ein $d \in U_\mathcal{A}$ gibt, sodaß $\mathcal{A}_{[x_i/d]}(G) = 1$.

Hierbei ist $\mathcal{A}_{[x_i/d]}$ eine leicht veränderte Struktur, die zwar dasselbe Universum $U_\mathcal{A}$ wie die Struktur $\mathcal{A}$ besitzt, aber der Variablen x_i anstatt $x_i^\mathcal{A}$ das Element $d \in U_\mathcal{A}$ zuordnet, und sonst genau dieselben Zuordnungen wie $\mathcal{A}$ trifft.

Erfüllbar, Allgemeingültig und Unerfüllbar

- Eine Formel F der Prädikatenlogik heißt *erfüllbar*, falls es eine zu F passende Struktur $\mathcal{A}$ gibt mit $\mathcal{A}(F) = 1$. [Man sagt dann, daß $\mathcal{A}$ ein Modell von F ist, geschrieben: $\mathcal{A} \models F$.]
- F heißt *allgemeingültig*, falls $\mathcal{A}(F) = 1$ für jede zu F passende Struktur (Schöning sagt stattdessen “gültig”).
- F heißt *unerfüllbar* , falls es *keine* zu F passende Struktur $\mathcal{A}$ gibt, sodaß $\mathcal{A}(F) = 1$.

Bemerkung: Wie in der Booleschen Logik gilt auch in der Prädikatenlogik für jede Formel F: F ist allgemeingültig genau dann wenn $\neg F$ nicht erfüllbar ist.

Erfüllbar / Allgemeingültig: Beispiel 1

Behauptung: $\forall x P(x)$ ist erfüllbar, aber nicht allgemeingültig.

Um zu beweisen, daß $\forall x P(x)$ erfüllbar ist, betrachte eine beliebige Struktur

$$\mathcal{A} = (U_{\mathcal{A}}, I_{\mathcal{A}}) \text{ mit } P^{\mathcal{A}} := U_{\mathcal{A}}.$$

Dann gilt $\mathcal{A} \models \forall x P(x)$, d.h. $\mathcal{A}$ ist ein Modell der Formel $\forall x P(x)$.

Um zu beweisen, daß $\forall x P(x)$ nicht allgemeingültig ist, betrachte eine beliebige Struktur

$$\mathcal{A} = (U_{\mathcal{A}}, I_{\mathcal{A}}) \text{ mit } P^{\mathcal{A}} \subsetneq U_{\mathcal{A}}.$$

Sei c in $U_{\mathcal{A}} - P^{\mathcal{A}}$. Dann gilt $\mathcal{A}(\forall x P(x)) = 0$ weil $\mathcal{A}_{[x/c]}(P(x)) = 0$. (Letzteres folgt aus $c \notin P^{\mathcal{A}}$).

Äquivalenz und Implikation

Implikation: Wir schreiben $F \Rightarrow G$ ("*F impliziert G*") falls für *jede* zu F und G passende Struktur $\mathcal{A}$ gilt: Falls $\mathcal{A}(F) = 1$, so ist auch $\mathcal{A}(G) = 1$.

Äquivalenz: Wir schreiben $F \Leftrightarrow G$ ("*F äquivalent G*") falls für *jede* zu F und G passende Struktur $\mathcal{A}$ gilt: $\mathcal{A}(F) = \mathcal{A}(G)$.

Einige Äquivalenzen

Für beliebige Formeln F, G und Variablen x, y gilt:

1. $\neg \forall x F \Leftrightarrow \exists x \neg F$
   $\neg \exists x F \Leftrightarrow \forall x \neg F$

2. Falls x nicht frei vorkommt in G, so gilt:
$$\begin{aligned} (\forall x F \wedge G) &\Leftrightarrow \forall x (F \wedge G) \\ (\forall x F \vee G) &\Leftrightarrow \forall x (F \vee G) \\ (\exists x F \wedge G) &\Leftrightarrow \exists x (F \wedge G) \\ (\exists x F \vee G) &\Leftrightarrow \exists x (F \vee G) \quad . \end{aligned}$$

3. Es gilt stets
$$\begin{aligned} \forall x F \wedge \forall x G &\Leftrightarrow \forall x (F \wedge G) \\ \exists x F \vee \exists x G &\Leftrightarrow \exists x (F \vee G) \quad . \end{aligned}$$

4. Es gilt stets
$$\begin{aligned} \forall x \forall y F &\Leftrightarrow \forall y \forall x F \\ \exists x \exists y F &\Leftrightarrow \exists y \exists x F \quad . \end{aligned}$$

Es gelten zusätzlich die Äquivalenzen der Aussagenlogik.

Bereinigte Formel

Anmerkung: Falls x_j nicht in G auftritt, so ist $\exists x_i G$ ($\forall x_i G$) äquivalent zu $\exists x_j G[x_i/x_j]$ ($\forall x_j G[x_i/x_j]$), wobei $G[x_i/x_j]$ diejenige Formel ist die man aus G erhält, wenn man jedes freie Auftreten von x_i in G durch x_j ersetzt ("gebundene Umbenennung"). Durch mehrfache gebundene Umbenennung kann man zu jeder Formel F eine äquivalente Formel H erzeugen in der

- alle Quantoren *verschiedene* Variablen binden.
- keine Variable sowohl frei als auch gebunden in H auftritt.

Man nennt eine Formel H mit diesen Eigenschaften *bereinigt*.

Eine Normalform: Die Pränexform

Definition: F ist in *Pränexform* falls F die Form

$$Q_1 x_{i_1} Q_2 x_{i_2} \dots Q_n x_{i_n} G$$

hat, wobei $Q_j \in \{\exists, \forall\}$, $x_{i_j} \in \{x_i | i \in \mathbb{N}\}$, und in G kein Quantor vorkommt. In diesem Fall besteht G aus atomaren Formeln der Struktur $P^k(t_1, \dots, t_k)$, die durch $\neg, \wedge, \vee$ verknüpft sind.

Umformen in Pränexform: Ein Beispiel

Beispiel:

$$\begin{aligned}
&(\neg(\exists x P(x,y) \vee \forall z Q(z)) \wedge \exists w P(f(a,w))) \\
&\quad \equiv ((\neg\exists x P(x,y) \wedge \neg\forall z Q(z)) \wedge \exists w P(f(a,w))) \text{ (de Morgan)} \\
&\quad \equiv ((\forall x \neg P(x,y) \wedge \exists z \neg Q(z)) \wedge \exists w P(f(a,w)) \text{ (wegen 1.)} \\
&\quad \equiv (\exists w P(f(a,w)) \wedge (\forall x \neg P(x,y) \wedge \exists z \neg Q(z))) \text{ (Kommutativität)} \\
&\quad \equiv \exists w (P(f(a,w)) \wedge \forall x (\neg P(x,y) \wedge \exists z \neg Q(z))) \text{ (wegen 2.)} \\
&\quad \equiv \exists w (\forall x (\exists z \neg Q(z) \wedge \neg P(x,y)) \wedge P(f(a,w))) \text{ (Kommutativität)} \\
&\quad \equiv \exists w (\forall x \exists z (\neg Q(z) \wedge \neg P(x,y)) \wedge P(f(a,w))) \text{ (wegen 2.)} \\
&\quad \equiv \exists w \forall x \exists z (\neg Q(z) \wedge \neg P(x,y) \wedge P(f(a,w))) \text{ (wegen 2.)}
\end{aligned}$$

Bemerkungen zur Pränexform

Die Umformung einer Formel F in Pränexform ist nicht eindeutig.

Beispiel: Zum Beispiel sind $\exists x \forall y (F \vee G)$ und $\forall y \exists x (F \vee G)$ beides Pränexformen der Formel $\exists x F \vee \forall y G$ – vorausgesetzt, daß x nicht in G und y nicht in F auftritt. In diesem Spezialfall sind dann auch $\exists x \forall y (F \vee G)$ und $\forall y \exists x (F \vee G)$ äquivalent, obwohl dies im Allgemeinen nicht gilt.

Um nachzuweisen, daß solche Formeln im Allgemeinen nicht äquivalent sind, betrachte zum Beispiel die konkreten Formeln $\exists x \forall y (x > y \vee x = y)$ und $\forall y \exists x (x > y \vee x = y)$, sowie die Struktur $\mathcal{A}$ mit $U_{\mathcal{A}} = \mathbb{N}$, die dem Prädikatssymbol $>$ die Menge $\{\langle x, y \rangle : x > y\} \subseteq \mathbb{N} \times \mathbb{N}$ zuordnet. Es gilt dann

$$\mathcal{A} \models \forall y \exists x (x > y \vee x = y) \quad , \quad \text{aber nicht } \mathcal{A} \models \exists x \forall y (x > y \vee x = y).$$

Logisches Folgern in der Prädikatenlogik

Wir schreiben $F \Rightarrow G$ (“F *impliziert* G”) falls für *jede* zu F und G passende Struktur $\mathcal{A}$ gilt: Falls $\mathcal{A}(F) = 1$, so ist auch $\mathcal{A}(G) = 1$.

Bemerkungen

- In der VO „Theoretischen Informatik 2“ werden Herleitungskalküle besprochen werden, mit deren Hilfe ein Rechner in einigen Fällen verifizieren kann, daß $F \Rightarrow G$ (“maschinelles Beweisen”).
- Wir können hier nur eine sehr einfache Regel vorstellen, mit deren Hilfe man manchmal die Gültigkeit der Implikation $F \Rightarrow G$ für Formeln F und G der Prädikatenlogik aus der Gültigkeit einer Implikation $F' \Rightarrow G'$ für gewisse andere Formeln F', G' der Booleschen Logik folgen kann.

Logisches Folgern: Beispiel

Nehmen wir an, daß F und G in Pränexform sind, daß beide genau denselben Quantorenblock haben, und daß $\tilde{F}$ und $\tilde{G}$ die auf die Quantorenblöcke in F und G folgenden aussagenlogischen Verknüpfungen von atomaren Formeln sind.

Wir ersetzen jetzt jede atomare Formel in $\tilde{F}$ und $\tilde{G}$ durch eine andere Boolesche Variable, wobei aber mehrmals auftretende identische atomare Formeln durch identische Boolesche Variablen ersetzt werden. Wir nennen die auf diese Weise aus $\tilde{F}$ und $\tilde{G}$ hervorgehenden Booleschen Formeln F' und G'.

Falls für diese Booleschen Formeln $F' \Rightarrow G'$ gilt, so gilt auch in der Prädikatenlogik $F \Rightarrow G$.

Beispiel: Es gilt in der Prädikatenlogik

$$\forall x\, \exists y(P^2(x,y)) \Rightarrow\ \forall x\, \exists y(P^2(x,y) \vee x = y)$$

weil

$$a \Rightarrow a \vee b$$

in der Booleschen Logik gilt.