

THEORETISCHE INFORMATIK 2

185.183

B. Gramlich, A. Leitsch

Termine:

- Vorlesungszeit: Block 8.10.02 – 12.12.02
 - Dienstag 17:15 – 18:45, EI 7
 - Donnerstag 18:45 – 20:15, EI 7
- Prüfungen:
 - Teil 1: 22.11.02, 16:15 – 17:45
 - Teil 2: 13.12.02, 14:15 – 15:45

Skriptum:

- 1. Teil: 15.10.2002, 16:45, EI 7
- 2. Teil: Anfang/Mitte November

Informationen: <http://www.logic.at/lvas/185183/>

Achtung: Parallelveranstaltung!

Leiter der LVA: Matthias Baaz, Arnold Beckmann

Zeit: Block im Jänner und Anfang Februar

Details: siehe <http://www.logic.at/lvas/185183/>

INHALT:

- Deduktion in der Prädikatenlogik
- Formale Aspekte von Programmiersprachen
- Berechenbarkeit und Entscheidbarkeit
- Komplexitätstheorie

DIE PRÄDIKATENLOGIK

- Aussagenlogik: eine Sprachebene
- Prädikatenlogik: 2 Sprachebenen, Terme, Formeln, stärkere Ausdruckskraft

Beispiel:

Alle Menschen sind sterblich
Sokrates ist ein Mensch

Sokrates ist sterblich

(ist ein) Mensch, (ist) sterblich: Prädikat,
Sokrates: Subjekt.

Schluss nicht aussagenlogisch repräsentierbar:

$$\frac{A \quad B}{C}$$

Formalisierung als Schluss:

$$\frac{(\forall x)(M(x) \supset S(x))}{S(s)} \quad M(s)$$

M, S : Prädikatsymbole,

x : (Individuen-) Variable,

s : Konstantensymbol,

\forall : Quantor.

- Terme: x, s ,
- Formeln: $M(s), S(s), (\forall x)(M(x) \supset S(x))$

Formalisierung als Formel:

$$(M(s) \wedge (\forall x)(M(x) \supset S(x))) \supset S(s).$$

Beispiel:

Väter von Menschen sind Menschen.

$$(\forall x)(M(x) \supset M(f(x))).$$

f : Funktionssymbol,

x : Variable, M : Prädikatsymbol.

Terme: $x, f(x)$,

Formeln:

$$M(x), M(f(x)), (M(x) \supset M(f(x))), \\ (\forall x)(M(x) \supset M(f(x))).$$

Terme: T

- (T1) Variablen sind Terme ($V \subseteq T$)
- (T2) Konstantensymbole sind Terme ($KS \subseteq T$)
- (T3) Für alle $n \geq 1$ gilt: Sind $t_1, \dots, t_n \in T$ und ist $f \in FS_n$, so ist $f(t_1, \dots, t_n) \in T$.
(aus n Termen werden mittels n -stelliger Funktionssymbole neue Terme erzeugt).

Formeln:

- (PL1) Für alle $n \geq 0$ gilt: Ist $P \in PS_n$ und sind $t_1, \dots, t_n \in T$, dann ist $P(t_1, \dots, t_n) \in PL$; eine Formel dieser Gestalt wird auch *Atomformel* genannt.
- (PL2) Ist $A \in PL$, so auch $\neg A \in PL$.
- (PL3) Sind $A, B \in PL$, dann ist $(A \wedge B) \in PL$.
- (PL4) Sind $A, B \in PL$, dann ist $(A \vee B) \in PL$.
- (PL5) Sind $A, B \in PL$, dann ist $(A \supset B) \in PL$.
- (PL6) Ist $A \in PL$ und $x \in V$ dann ist $(\forall x)A \in PL$.
- (PL7) Ist $A \in PL$ und $x \in V$ dann ist $(\exists x)A \in PL$.

Teilformeln:

- Ist $A \in \text{PL}$ dann ist A Teilformel von A .
- Ist $A = (B \circ C)$ für $\circ \in \{\wedge, \vee, \supset\}$ dann sind B und C Teilformeln von A .
- Ist $A = \neg B$ dann ist B Teilformel von A .
- Ist $A = (Qx)B$ für $Q \in \{\forall, \exists\}$ und ist $x \in V$ dann ist B Teilformel von A .

Eine Variable kann in einer Formel *frei* oder *gebunden* vorkommen:

- x in $(\exists y)P(x, y)$ frei,
- x in $(\forall x)(\exists y)P(x, y)$ gebunden,
- x in $(\forall x)Q(x) \wedge (\exists y)P(x, y)$ frei und gebunden.

frei vorkommende Variablen: $\text{FV}(A)$.

Sei t ein Term, dann bezeichnet $V(t)$ die Menge der in t vorkommenden Variablen.

- Ist $A : P(t_1, \dots, t_n)$ eine Atomformel dann ist $\text{FV}(A) = V(t_1) \cup \dots \cup V(t_n)$.
- $\text{FV}(A \circ B) = \text{FV}(A) \cup \text{FV}(B)$ für $\circ \in \{\wedge, \vee, \supset\}$,
- $\text{FV}(\neg A) = \text{FV}(A)$,
- $\text{FV}((Qx)A) = \text{FV}(A) - \{x\}$.

$x \in \text{FV}(A)$: x *kommt* in A *frei* vor.

x *kommt* in A *gebunden* vor: Es gibt Teilformel $(Qx)B$ von A gibt mit $Q \in \{\forall, \exists\}$.

A *geschlossen*: $\text{FV}(A) = \emptyset$.

Beispiele: (Terme, Formeln)

Sei $f \in \text{FS}_2$, dann ist $f(x, a)$ ein Term.
Ebenso sind x, a und $f(f(x, a), x)$ Terme.
 $f(f, f), f(x)$ und $f(x, a)$ sind keine Terme.

Seien $P \in \text{PS}_1$ und $Q \in \text{PS}_2$.
Dann sind $P(f(x, a))$ und $Q(y, f(y, a))$ Atomformeln.

$\neg P(f(x, a)),$
 $(P(f(x, a)) \supset Q(y, f(y, a))),$
 $\neg(P(f(x, a)) \supset Q(y, f(y, a))),$
 $(\forall x)\neg(P(f(x, a)) \supset Q(y, f(y, a)))$ und
 $A = (\exists y)(\forall x)\neg(P(f(x, a)) \supset Q(y, f(y, a)))$ sind Formeln;
 $P(x) \vee Q(x, x) \wedge P(a)$ ist keine Formel (Klammern fehlen);
 $(\forall x)(\exists x)P(x)$ ist eine Formel.

Beispiele:

Teilformeln:

Sei $A = (\exists y)(\forall x)\neg(P(f(x, a)) \supset Q(y, f(y, a)))$.

- $((\forall x)\neg(P(f(x, a)) \supset Q(y, f(y, a))))$ und
 - $\neg(P(f(x, a)) \supset Q(y, f(y, a)))$ sind Teilformeln von A .
 - $\neg P(f(x, a))$ ist keine Teilformel von A .
- $\text{FV}((\forall x)\neg(P(f(x, a)) \supset Q(y, f(y, a)))) = \{y\}$.

Substitutionen:

Sei $A = (\forall x)(P(x, y) \supset Q(x, y)) \wedge R(x)$ und $t = f(a)$. Dann ist

$A(x/t) = (\forall x)(P(x, y) \supset Q(x, y)) \wedge R(f(a)),$
 $A(y/t) = (\forall x)(P(x, f(a)) \supset Q(x, f(a)) \wedge R(x)).$

Man beachte, dass bei $A(x/t)$ nur die *freien* Vorkommen von x ersetzt werden!

Signatur:

$FS(F)$: Menge der Funktionssymbole in F ;
analog: $KS(F)$, $PS_i(F)$ und $PS(F)$ definiert.

Signatur von F :

$$\Sigma(F) = FS(F) \cup KS(F) \cup PS(F).$$

Umgekehrt:

$$\Sigma \subseteq KS \cup FS \cup PS:$$

PL-Formeln über Σ : $PL[\Sigma]$.

Terme über Σ : $T[\Sigma]$.

Beispiele:

$$F = P(f(x, a)): \Sigma(F) = \{P, f, a\}.$$

$$(\exists y)(\forall x)(P(x) \supset P(f(y, x))), P(a) \vee P(f(a, a)) \in PL[F]$$

$$P(b), Q(x, y) \notin PL[F].$$

$\Sigma = \{f, a, b\}$:

$$\begin{aligned} T_0 &= V \cup \{a, b\}, \\ T_{n+1} &= T_n \cup \{f(t_1, t_2) \mid t_1 \in T_n, t_2 \in T_n\}, \\ T(\Sigma) &= \cup_{i=0}^{\infty} T_i. \end{aligned}$$

SEMANTIK:

Interpretation:

Eine *Interpretation* einer Formel F in PL ist ein Tupel $\mathcal{M} = (D, \Phi, I)$ mit folgenden Eigenschaften:

- 1) D ist eine nichtleere Menge, der Bereich (domain) von \mathcal{M} .
- 2) Φ ist eine Abbildung mit Definitionsbereich $\Sigma(F)$, sodass gilt:
 - 2.1) $\Phi(c) \in D$ für $c \in KS(F)$.
 - 2.2) Für $f \in FS_n(F)$ ist $\Phi(f)$ eine Funktion vom Typ $D^n \rightarrow D$.
 - 2.3) Für $P \in PS_n(F)$ ist $\Phi(P)$ ein n -stelliges Prädikat über D (d.h. eine Funktion vom Typ $D^n \rightarrow \{\mathbf{t}, \mathbf{f}\}$). Für $n = 0$ definieren wir $\Phi(\top) = \mathbf{t}$ und $\Phi(\perp) = \mathbf{f}$.
- 3) I ist eine Funktion vom Typ $V \rightarrow D$, die Variablenumgebung (environment).

Semantik der Terme:

$F \in \text{PL}$.

Ist \mathcal{M} eine Interpretation von F , so definieren wir folgende Semantikfunktion $t_{\mathcal{M}} : T[F] \rightarrow D$.

(T1S) $t_{\mathcal{M}}(x) = I(x)$ für $x \in V$

(T2S) $t_{\mathcal{M}}(c) = \Phi(c)$ für $c \in \text{KS}(F)$

(T3S.) $t_{\mathcal{M}}(f(t_1, \dots, t_n)) = \Phi(f)(t_{\mathcal{M}}(t_1), \dots, t_{\mathcal{M}}(t_n))$
für alle Terme $f(t_1, \dots, t_n) \in T[F]$.

Beispiel:

$F = P(x) \supset P(f(x, x))$.

$\Sigma(F) = \{P, f\}$,

$T(F) = \cup_{i=0}^{\infty} T_i$ mit $T_0 = V$,

$T_{n+1} = \{f(t_1, t_2) \mid t_1, t_2 \in T_n\} \cup T_n$ für $n \in \mathbb{N}$.

Sei $\mathcal{M} = (\mathbb{N}, \Phi, I)$, mit \mathbb{N} die Menge der natürlichen Zahlen.

$\Phi(P) =$ das Prädikat „gerade“ ($n \rightarrow [n = 0 \bmod 2]$)

$\Phi(f) = +$

$I(x) = 0$ und $I(v) = 1$ für alle $v \in V - \{x\}$.

Wir erkennen intuitiv (für die mathematische Interpretation fehlt uns noch die Auswertungsfunktion für Formeln), dass F unter \mathcal{M} bedeutet:

„Ist x gerade, dann auch $x + x$ “.

Der Term t , mit $t = f(x, f(x, y))$ ist in $T[F]$.
 „Wert“ von t :

$$\begin{aligned} t_{\mathcal{M}}(f(x, f(x, y))) &= t_{\mathcal{M}}(x) + t_{\mathcal{M}}(f(x, y)). \\ t_{\mathcal{M}}(x) &= I(x) = 0. \\ t_{\mathcal{M}}(f(x, y)) &= t_{\mathcal{M}}(x) + t_{\mathcal{M}}(y) = \\ &= I(x) + I(y) = \\ &= 0 + 1 = 1. \end{aligned}$$

Es folgt

$$t_{\mathcal{M}}(t) = 0 + 1 = 1.$$

Äquivalenz von Interpretationen:

Begriff nötig für Quantorensemantik.

Zwei Interpretationen \mathcal{M}, \mathcal{N} einer Formel F heißen *äquivalent modulo* x_1, \dots, x_k

$$(\mathcal{M} \sim \mathcal{N} \text{ mod } x_1, \dots, x_k),$$

wenn es D, Φ, I, J gibt mit

$$\mathcal{M} = (D, \Phi, I), \mathcal{N} = (D, \Phi, J) \text{ und } I(v) = J(v)$$

für $v \in V - \{x_1, \dots, x_k\}$

(I und J unterscheiden sich *höchstens* auf der Menge $\{x_1, \dots, x_k\}$).

Ist \mathcal{M} äquivalent zu \mathcal{N} modulo x , so schreiben wir auch $\mathcal{M} \sim_x \mathcal{N}$ statt $\mathcal{M} \sim \mathcal{N} \text{ mod } x$.

Semantik von PL:

Sei F eine prädikatenlogische Formel und \mathcal{M} eine Interpretation von F . Wir definieren eine Auswertungsfunktion $v_{\mathcal{M}}$, die PL - Formeln Wahrheitswerte zuordnet.

$$v_{\mathcal{M}} : \text{PL}[F] \rightarrow \{\mathbf{t}, \mathbf{f}\}.$$

Sei $\mathcal{M} = (D, \Phi, I)$.

PLS1. Ist A eine Atomformel in $\text{PL}(F)$ der Gestalt

$$\begin{aligned} &P(t_1, \dots, t_n), \text{ dann gilt} \\ &v_{\mathcal{M}}(A) = \Phi(P)(t_{\mathcal{M}}(t_1), \dots, t_{\mathcal{M}}(t_n)). \end{aligned}$$

PLS2. $v_{\mathcal{M}}(\neg A) = \text{not}(v_{\mathcal{M}}(A))$

PLS3. $v_{\mathcal{M}}((A \wedge B)) = \text{and}(v_{\mathcal{M}}(A), v_{\mathcal{M}}(B))$

PLS4. $v_{\mathcal{M}}((A \vee B)) = \text{or}(v_{\mathcal{M}}(A), v_{\mathcal{M}}(B))$

PLS5. $v_{\mathcal{M}}((A \supset B)) = \text{impl}(v_{\mathcal{M}}(A), v_{\mathcal{M}}(B))$

PLS6. $v_{\mathcal{M}}((\forall x)A) = \mathbf{t}$ genau dann, wenn für alle \mathcal{N} mit $\mathcal{N} \sim_x \mathcal{M}$ gilt $v_{\mathcal{N}}(A) = \mathbf{t}$.

PLS7. $v_{\mathcal{M}}((\exists x)A) = \mathbf{t}$ genau dann, wenn es ein \mathcal{N} mit $\mathcal{N} \sim_x \mathcal{M}$ gibt mit $v_{\mathcal{N}}(A) = \mathbf{t}$.

Modell:

Eine Interpretation \mathcal{M} von F heißt *Modell* von F , wenn $v_{\mathcal{M}}(F) = \mathbf{t}$ gilt.

Beispiel:

Sei $F = (\forall x)(P(x) \supset P(f(x, y)))$, $\mathcal{M} = (\mathbb{N}, \Phi, I)$ mit $\mathbb{N} = \text{Menge der natürlichen Zahlen}$, $\Phi(P) = \text{„ist gerade“}$, $\Phi(f) = +$ und $I(x) = 0$, $I(y) = 2$, $I(v) = 0$ für $v \in V - \{x, y\}$.

$$\mathcal{M}_x^* = \{\mathcal{N} \mid \mathcal{N} \sim_x \mathcal{M}\}.$$

$$v_{\mathcal{M}}(F) = \mathbf{t} \iff$$

Für alle $\mathcal{N} \in \mathcal{M}_x^*$ gilt

$$v_{\mathcal{N}}(P(x) \supset P(f(x, y))) = \mathbf{t} \iff$$

Für alle $\mathcal{N} \in \mathcal{M}_x^*$ gilt

$$\text{impl}(v_{\mathcal{N}}(P(x)), v_{\mathcal{N}}(P(f(x, y)))) = \mathbf{t} \iff$$

für alle J mit $J(v) = I(v)$ für $v \neq x$ gilt

$$\text{impl}(\text{Gerade}(J(x)), \text{Gerade}(J(x) + J(y))) = \mathbf{t} \iff$$

für alle $k \in \mathbb{N}$ gilt

$$\text{impl}(\text{Gerade}(k), \text{Gerade}(k+2)) = \mathbf{t}.$$

$$v_{\mathcal{M}}(F) = \mathbf{t}.$$

Gültigkeit und Erfüllbarkeit:

- 1) Eine Formel F aus PL heißt *gültig*, wenn jede Interpretation von F ein Modell ist.
- 2) Eine Formel heißt *erfüllbar*, wenn sie ein Modell besitzt.
- 3) Zwei Formeln F, G aus PL heißen *logisch äquivalent* ($F \sim G$), wenn für alle Interpretationen \mathcal{M} von $(F \wedge G)$ gilt: $v_{\mathcal{M}}(F) = v_{\mathcal{M}}(G)$.
- 4) Zwei Formeln F, G aus PL heißen *erfüllungsäquivalent*, wenn gilt: F ist genau dann erfüllbar, wenn G erfüllbar ist ($F \sim_e G$).

Beispiele:

- $(\forall x)(P(x, a) \vee \neg P(x, a)), (\forall x)(\forall y)P(x, y) \supset P(a, b)$ und $(\forall x)P(x) \supset (\exists y)P(y)$ sind gültige Formeln.
- $(\exists y)(P(y) \supset Q(y)), (\forall x)(P(x, a) \vee \neg P(a, x))$ sind erfüllbar, aber nicht gültig.
- $(\exists y)(P(y) \supset Q(y))$ und $\neg(\forall y)\neg(\neg P(y) \vee Q(y))$ sind logisch äquivalent.
- $(\exists y)(P(y) \supset Q(y))$ und $(\exists y)(Q(y) \supset P(y))$ sind nicht logisch äquivalent.
- $(\exists y)(P(y) \supset Q(y))$ und $P(a) \supset Q(a)$ sind erfüllungsäquivalent (beide sind erfüllbar), aber nicht logisch äquivalent.
- $(\forall x)P(x, a) \wedge \neg P(a, b)$ und $(\forall x)P(x, a) \wedge \neg P(b, a)$ sind nicht erfüllungsäquivalent.

PROPOSITION:

- 1) F ist genau dann gültig, wenn $\neg F$ unerfüllbar ist.
- 2) Sind F und $\neg F$ beide erfüllbar, so ist F nicht gültig.

- 3) $F \sim G$ gilt genau dann, wenn

$$(F \supset G) \wedge (G \supset F)$$

gültig ist.

- 4) $F \sim G$ impliziert $F \sim_e G$.

Unentscheidbarkeit der Prädikatenlogik:

- Im Gegensatz zur Aussagenlogik ist das Gültigkeitsproblem der Prädikatenlogik *algorithmisch unentscheidbar*. Das bedeutet, es existiert *kein* Algorithmus der, bei Eingabe einer beliebigen prädikatenlogischen Formel A , feststellt ob A gültig ist oder nicht.
- Dagegen existiert ein algorithmisches *Aufzählungsverfahren* für die gültigen Formeln in PL (im Gegensatz zur Menge aller PL Formeln, die über endlichen Bereichen gültig sind!).
- Die Axiomatisierung der Gültigkeit mittels LK liefert ein Verfahren zur *Bestätigung* der Gültigkeit gültiger Formeln.
- Es existiert aber *kein* Verfahren, das stets terminiert und die Ungültigkeit aller ungültigen PL-Formeln feststellen kann.