Formale Modellierung
Vorlesung 4 vom 04.05.15: Prädikatenlogik erster Stufe

Christoph Lüth

Universität Bremen

Sommersemester 2015

Fahrplan

- Teil I: Formale Logik
  - Einführung
  - Aussagenlogik (PL): Syntax und Semantik, Natürliches Schließen
  - Konsistenz & Vollständigkeit der Aussagenlogik
  - Prädikatenlogik (FOL): Syntax und Semantik
  - Konsistenz & Vollständigkeit von FOL
  - FOL mit induktiven Datentypen
  - FOL mit rekursiven Definitionen
  - Logik höherer Stufe (HOL): Syntax und Eigenschaften
  - Berechungsmodelle (Models of Computation)
  - Die Unvollständigkeitssätze von Gödel
- Teil II: Spezifikation und Verifikation

Das Tagesmenü

- Von Aussagenlogik zur Prädikatenlogik
- Logik mit Quantoren
- Semantik der Prädikatenlogik
- Natürliches Schließen mit Quantoren

Eine Beispielspezifikation

Das Flugbuchungssystem

Das Flugbuchungssystem soll eine Menge von Flügen verwalten, Anfragen beantworten und Buchungen vornehmen.

Ein Flug hat einen Startflughafen und ein Zielflughafen (durch ihr IATA-Kürzel repräsentiert), eine eindeutige Kennung, einen Starttermin, eine Ankunftsermin, sowie eine Anzahl von verfügbaren Plätzen.

Eine Flugbuchung für einen durch die Flugnummer und Starttermin identifizierten Flug soll eine Anzahl von Plätzen auf diesem Flug reservieren. Sind die verfügbaren Plätze für einen Flug erschöpft, können keine weiteren Buchungen vorgenommen werden.

Eine Anfrage besteht aus den Daten (Start, Ziel, Datum) für einen Flug, und liefert die Anzahl freier Plätze auf diesem Flug zurück.

Beschränkungen der Aussagenlogik

- Beschränkung der Aussagenlogik:
  - Die Menge unserer Atome ist unstrukturiert und flach.
  - Wir können nicht zwischen Logik (Meta-Ebene) und Objekt unterscheiden.
  - Wir können keine strukturellen Eigenschaften beschreiben.
  - Wir können keine Aussagen über Existenz von Objekten machen.
- Ziel: Formalisierung von Aussagen wie
  - "Ein Flug hat eine eindeutige Kennung."
  - "Alle Menschen sind sterblich. Sokrates ist ein Mensch. Also ist Sokrates sterblich."
  - "Alle Zahlen sind ein Produkt von Primfaktoren."

Prädikatenlogik: Erweiterung der Sprache

- Terme beschreiben die zu formalisierenden Objekte.
- Formeln sind logische Aussagen.
- Eine Signatur Σ beschreibt Prädikate und Funktionen:
  - Prädikatensymbole: $P_1, \ldots, P_n, \doteq$ mit Arität $ar(P_i) \in \mathbb{N}$, $ar(\doteq) = 2$
  - Funktionssymbole: $f_1, \ldots, f_m$ mit Arität $ar(t_i) \in \mathbb{N}$
- Menge X von Variablen (abzählbar viele)
- Konnektive: $\wedge, \longrightarrow, \bot, \forall$, abgeleitet: $\vee, \longleftrightarrow, \neg, \longleftrightarrow, \exists$
- Die Trennung zwischen Termen und Formeln ist der wesentliche Abstraktionsschritt in der Prädikatenlogik.

Terme

- Menge $\mathcal{T}erm_\Sigma$ der Terme (zur Signatur Σ) gegeben durch:
  - Variablen: $X \subseteq \mathcal{T}erm_\Sigma$
  - Funktionssymbol $f \in \Sigma$ mit $ar(f) = n$ und $t_1, \ldots, t_n \in \mathcal{T}erm_\Sigma$, dann $f(t_1, \ldots, t_n) \in \mathcal{T}erm_\Sigma$
  - Sonderfall: $n = 0$, dann ist f eine Konstante, $f \in \mathcal{T}erm_\Sigma$

Formeln

- Menge $\mathcal{F}orm_\Sigma$ der Formeln (zur Signatur Σ) gegeben durch:
  - $\bot \in \mathcal{F}orm_\Sigma$
  - Wenn $\phi \in \mathcal{F}orm_\Sigma$, dann $\neg\phi \in \mathcal{F}orm_\Sigma$
  - Wenn $\phi, \psi \in \mathcal{F}orm_\Sigma$, dann $\phi \wedge \psi \in \mathcal{F}orm_\Sigma, \quad \phi \vee \psi \in \mathcal{F}orm_\Sigma,$
    $\phi \longrightarrow \psi \in \mathcal{F}orm_\Sigma, \quad \phi \longleftrightarrow \psi \in \mathcal{F}orm_\Sigma$

Formeln

- Menge $\mathcal{F}orm_\Sigma$ der Formeln (zur Signatur Σ) gegeben durch:
  - $\bot \in \mathcal{F}orm_\Sigma$
  - Wenn $\phi \in \mathcal{F}orm_\Sigma$, dann $\neg\phi \in \mathcal{F}orm_\Sigma$
  - Wenn $\phi, \psi \in \mathcal{F}orm_\Sigma$, dann $\phi \wedge \psi \in \mathcal{F}orm_\Sigma, \quad \phi \vee \psi \in \mathcal{F}orm_\Sigma,$ $\phi \longrightarrow \psi \in \mathcal{F}orm_\Sigma, \quad \phi \longleftrightarrow \psi \in \mathcal{F}orm_\Sigma$
  - Wenn $\phi \in \mathcal{F}orm_\Sigma, x \in X$, dann $\forall x.\phi \in \mathcal{F}orm_\Sigma, \exists x.\phi \in \mathcal{F}orm_\Sigma$
  - Prädikatensymbol $p \in \Sigma$ mit $ar(p) = m$ und $t_1, \ldots, t_m \in \mathcal{T}erm_\Sigma$, dann $p(t_1, \ldots, t_m) \in \mathcal{F}orm_\Sigma$
    - Sonderfall: $t_1, t_2 \in \mathcal{T}erm_\Sigma$, dann $t_1 \doteq t_2 \in \mathcal{F}orm_\Sigma$

Freie und gebundene Variable

Definition (Freie und gebundene Variablen)

Variablen in $t \in \mathcal{T}erm, p \in \mathcal{F}orm$ sind frei, gebunden, oder bindend:

(i) x bindend in $\forall x.\phi$, $\exists x.\psi$

(ii) Für $\forall x.\phi$ und $\exists x.\phi$ ist x in Teilformel ϕ gebunden

(iii) Ansonsten ist x frei

- $FV(\phi)$: Menge der freien Variablen in ϕ
- Beispiel:
$$(q(x) \vee \exists x.\forall y.p(f(x), z) \wedge q(a)) \vee \forall r(x, z, g(x))$$
- Formel (Term) s geschlossen, wenn $FV(s) = \emptyset$
- Abschluss einer Formel: $Cl(\phi) = \forall z_1 \dots z_k.\phi$ für $FV(\phi) = \{z_1, \dots, z_k\}$

Semantik: Strukturen

Definition (Struktur $\mathfrak{A}$ zur Signatur Σ)

$\mathfrak{A} = (A, f, P)$ mit

(i) A nicht-leere Menge (Universum)

(ii) für $f \in \Sigma$ mit $ar(f) = n$, n-stellige Funktion $f_{\mathfrak{A}} : A^n \to A$

(iii) für $P \in \Sigma$ mit $ar(P) = n$, n-stellige Relation $P_{\mathfrak{A}} \subseteq A^n$

- Für $a \in A$, Konstante $\overline{a} \in \mathcal{T}erm_{\Sigma}$
- Damit Auswertung von geschlossenen Termen: $[\![\cdot]\!]_{\mathfrak{A}} : \mathcal{T}erm_{\Sigma} \to A$

$$[\![\overline{a}]\!]_{\mathfrak{A}} = a$$
$$[\![f(t_1, \ldots, t_n]\!]_{\mathfrak{A}} = f_{\mathfrak{A}}([\![t_1]\!]_{\mathfrak{A}}, \ldots, [\![t_n]\!]_{\mathfrak{A}})$$

Semantische Gültigkeit

- Auswertung von Formeln: $[\![\cdot]\!]_{\mathfrak{A}} : \mathcal{F}orm_\Sigma \to \{0, 1\}$

$$
\begin{aligned}
[\![\bot]\!]_{\mathfrak{A}} &= 0 & [\![\neg\phi]\!]_{\mathfrak{A}} &= 1 - [\![\phi]\!]_{\mathfrak{A}} \\
[\![\phi \wedge \psi]\!]_{\mathfrak{A}} &= \min([\![\phi]\!]_{\mathfrak{A}}, [\![\psi]\!]_{\mathfrak{A}}) & [\![\phi \vee \psi]\!]_{\mathfrak{A}} &= \max([\![\phi]\!]_{\mathfrak{A}}, [\![\psi]\!]_{\mathfrak{A}})
\end{aligned}
$$

$$
\begin{aligned}
[\![\phi \longrightarrow \psi]\!]_{\mathfrak{A}} &= \max(1 - [\![\phi]\!]_{\mathfrak{A}}, [\![\psi]\!]_{\mathfrak{A}}) \\
[\![\phi \longleftrightarrow \psi]\!]_{\mathfrak{A}} &= 1 - |[\![\phi]\!]_{\mathfrak{A}} - [\![\psi]\!]_{\mathfrak{A}}|
\end{aligned}
$$

$$
\begin{aligned}
[\![P(t_1, \ldots, t_n)]\!]_{\mathfrak{A}} &= \begin{cases} 1 & \langle [\![t_1]\!]_{\mathfrak{A}}, \ldots, [\![t_n]\!]_{\mathfrak{A}} \rangle \in P_{\mathfrak{A}} \\ 0 & \text{sonst} \end{cases} \\
[\![t_1 \doteq t_2]\!]_{\mathfrak{A}} &= \begin{cases} 1 & [\![t_1]\!]_{\mathfrak{A}} = [\![t_2]\!]_{\mathfrak{A}} \\ 0 & \text{sonst} \end{cases} \\
[\![\forall x. \phi]\!]_{\mathfrak{A}} &= \min(\{[\![\phi\left[\tfrac{\overline{a}}{x}\right]]\!]_{\mathfrak{A}} \mid a \in A\}) \\
[\![\exists x. \phi]\!]_{\mathfrak{A}} &= \max(\{[\![\phi\left[\tfrac{\overline{a}}{x}\right]]\!]_{\mathfrak{A}} \mid a \in A\})
\end{aligned}
$$

- Damit semantische Gültigkeit (Wahrheit):

$$\mathfrak{A} \models \phi \text{ gdw. } [\![Cl(\phi)]\!]_{\mathfrak{A}} = 1, \models \phi \text{ gdw. } \mathfrak{A} \models \phi \text{ für alle } \mathfrak{A}$$

Syntaktische Gültigkeit: Natürliches Schließen

- Die alten Regeln blieben ($\longrightarrow I, \longrightarrow E, \wedge I, \wedge E_L, \wedge E_R, \mathrm{raa}, \bot, \ldots$)
  - Mutatis mutandis: $\mathcal{F}orm_\Sigma$ statt $\mathcal{P}rop$
- Dazu benötigen wir Regeln für die Quantoren.
- Zu behandelnde Probleme:
  - Substitution
  - Bindung

Substitution

- $t\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right]$ ist Ersetzung von x durch s in t
- Definiert durch strukturelle Induktion:

$$
\begin{aligned}
y\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right] &\stackrel{def}{=} \begin{cases} s & x = y \\ y & x \neq y \end{cases} \\
f(t_1, \ldots, t_n)\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right] &\stackrel{def}{=} f(t_1\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right], \ldots, t_n\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right]) \\
\bot\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right] &\stackrel{def}{=} \bot \\
(\phi \wedge \psi)\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right] &\stackrel{def}{=} \phi\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right] \wedge \psi\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right] \\
(\phi \longrightarrow \psi)\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right] &\stackrel{def}{=} \phi\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right] \longrightarrow \psi\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right] \\
P(t_1, \ldots, t_n)\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right] &\stackrel{def}{=} P(t_1\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right], \ldots, t_n\left[\begin{smallmatrix} s \\ x \end{smallmatrix}\right])
\end{aligned}
$$

Substitution

- $t\left[{s \atop x}\right]$ ist Ersetzung von x durch s in t
- Definiert durch strukturelle Induktion:

$$
\begin{aligned}
y\left[{s \atop x}\right] &\overset{def}{=} \begin{cases} s & x = y \\ y & x \neq y \end{cases} \\
f(t_1, \ldots, t_n)\left[{s \atop x}\right] &\overset{def}{=} f(t_1\left[{s \atop x}\right], \ldots, t_n\left[{s \atop x}\right]) \\
\bot\left[{s \atop x}\right] &\overset{def}{=} \bot \\
(\phi \wedge \psi)\left[{s \atop x}\right] &\overset{def}{=} \phi\left[{s \atop x}\right] \wedge \psi\left[{s \atop x}\right] \\
(\phi \longrightarrow \psi)\left[{s \atop x}\right] &\overset{def}{=} \phi\left[{s \atop x}\right] \longrightarrow \psi\left[{s \atop x}\right] \\
P(t_1, \ldots, t_n)\left[{s \atop x}\right] &\overset{def}{=} P(t_1\left[{s \atop x}\right], \ldots, t_n\left[{s \atop x}\right]) \\
(\forall y.\phi)\left[{s \atop x}\right] &\overset{def}{=} \begin{cases} \forall y.\phi & x = y \\ \forall y.(\phi\left[{s \atop x}\right]) & x \neq y, y \notin FV(s) \\ \forall z.((\phi\left[{z \atop y}\right])\left[{s \atop x}\right]) & x \neq y, y \in FV(s) \\ & \quad \text{mit } z \notin FV(s) \cup FV(\phi) \\ & \quad (z \text{ frisch}) \end{cases}
\end{aligned}
$$

Natürliches Schließen mit Quantoren

$$\frac{\phi}{\forall x.\phi}\ \forall I \quad (*) \qquad\qquad \frac{\forall x.\phi}{\phi\left[{t \atop x}\right]}\ \forall E \quad (\dagger)$$

- (*) Eigenvariablenbedingung:
  x nicht frei in offenen Vorbedingungen von ϕ (x beliebig)
- ($\dagger$) Ggf. Umbenennung durch Substitution
- Gegenbeispiele für verletzte Seitenbedingungen

Der Existenzquantor

$$\exists x.\phi \stackrel{def}{=} \neg\forall x.\neg\phi$$

$$\frac{\phi\left[{t \atop x}\right]}{\exists x.\phi}\ \exists I\quad(\dagger) \qquad\qquad \frac{\exists x.\phi \qquad \begin{array}{c}[\phi]\\ \vdots \\ \psi\end{array}}{\psi}\ \exists E\quad(*)$$

- (*) Eigenvariablenbedingung:
  x nicht frei in ψ, oder einer offenenen Vorbedingung außer ϕ
- (†) Ggf. Umbenennung durch Substitution

Zusammenfassung

- Prädikatenlogik: Erweiterung der Aussagenlogik um
  - Konstanten- und Prädikatensymbole
  - Gleichheit
  - Quantoren
- Semantik der Prädikatenlogik: Strukturen
  - Bilden Operationen und Prädikate der Logik ab
- Das natürliche Schließen mit Quantoren
  - Variablenbindungen — Umbenennungen bei Substitution
  - Eigenvariablenbedingung
- Das nächste Mal: FOL at work, FOL in Isabelle
- Nächste VL: Vollständigkeit