Formale Methoden der Softwaretechnik
Vorlesung vom 23.05.11: Prädikatenlogik erster Stufe

Till Mossakowski & Christoph Lüth

Universität Bremen

Sommersemester 2011

Das Tagesmenü

- Logik mit Quantoren
- Von Aussagenlogik zur Prädikatenlogik
- Natürliches Schließen mit Quantoren
- Gleichheit und natürliche Zahlen in Logik 1. Stufe
- Die Notwendigkeit von Logik höherer Stufe

Fahrplan

- Aussagenlogik
- Prädikatenlogik
- Isabelle I: Grundlagen
  - Aussagenlogik und natürliches Schließen
  - Prädikatenlogik und Quantoren
  - Logik höherer Stufe
  - Definitionen und konservative Erweiterung
  - Automatische Beweisprozeduren
- Isabelle II: Anwendungen

Motivation Prädikatenlogik

- Beschränkte Ausdrucksmächtigkeit der Aussagenlogik:
  - Eine Zahl n ist eine Primzahl genau dann wenn sie nicht 1 ist und nur durch 1 und sich selbst teilbar ist.
  - Eine Zahl m ist durch eine Zahl n teilbar genau dann wenn es eine Zahl p gibt, so dass $m = n \cdot p$.
  - Nicht in Aussagenlogik formalisierbar.
- Ziel: Formalisierung von Aussagen wie
  - Alle Zahlen sind ein Produkt von Primfaktoren.
  - Es gibt keine größte Primzahl.

Erweiterung der Sprache

- Terme beschreiben die zu formalisierenden Objekte.
- Formeln sind logische Aussagen.
- Unser Alphabet:
  - Prädikatensymbole: $P_1, \ldots, P_n, =$ mit Arität $ar(P_i) \in \mathbb{N}$, $ar(=) = 2$
  - Funktionssymbole: $f_1, \ldots, f_m$ mit Arität $ar(t_i) \in \mathbb{N}$
  - Menge X von Variablen (abzählbar viele)
  - Konnektive: $\wedge, \longrightarrow, \mathit{false}, \forall$, abgeleitet: $\vee, \longleftrightarrow, \neg, \longleftrightarrow, \exists$

Terme

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

Formeln

- Menge $\mathcal{F}orm$ der Formeln gegeben durch:
  - $\mathit{false} \in \mathcal{F}orm$
  - Wenn $\phi \in \mathcal{F}orm$, dann $\neg\phi \in \mathcal{F}orm$
  - Wenn $\phi, \psi \in \mathcal{F}orm$, dann $\phi \wedge \psi \in \mathcal{F}orm$, $\phi \vee \psi \in \mathcal{F}orm$, $\phi \longrightarrow \psi \in \mathcal{F}orm$, $\phi \longleftrightarrow \psi \in \mathcal{F}orm$
  - Wenn $\phi \in \mathcal{F}orm, x \in X$, dann $\forall x.\phi \in \mathcal{F}orm, \exists x.\phi \in \mathcal{F}orm$
  - Prädikatensymbol p mit $ar(p) = m$ und $t_1, \ldots, t_m \in \mathcal{T}erm$, dann $p(t_1, \ldots, t_m) \in \mathcal{F}orm$
    - Sonderfall: $t_1, t_2 \in \mathcal{T}erm$, dann $t_1 = t_2 \in \mathcal{F}orm$

Freie und gebundene Variable

- Variablen in $t \in \mathcal{T}erm, p \in \mathcal{F}orm$ sind frei, gebunden, oder bindend.
  - x bindend in $\forall x.\phi$, $\exists x.\psi$
  - Für $\forall x.\phi$ und $\exists x.\phi$ ist x in Teilformel ϕ gebunden
  - Ansonsten ist x frei
- $FV(\phi)$: Menge der freien Variablen in ϕ
- Beispiel:

$$(q(x) \vee \exists x.\forall y.p(f(x), z) \wedge q(a)) \vee \forall r(x, z, g(x))$$

Substitution

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

$$
\begin{array}{rcl}
y\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right] & \stackrel{def}{=} & \begin{cases} s & x = y \\ y & x \neq y \end{cases} \\
f(t_1,\ldots,t_n)\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right] & \stackrel{def}{=} & f(t_1\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right],\ldots,t_n\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right]) \\
\mathit{false}\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right] & \stackrel{def}{=} & \mathit{false} \\
(\phi\wedge\psi)\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right] & \stackrel{def}{=} & \phi\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right]\wedge\psi\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right] \\
(\phi\longrightarrow\psi)\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right] & \stackrel{def}{=} & \phi\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right]\longrightarrow\psi\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right] \\
p(t_1,\ldots,t_n)\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right] & \stackrel{def}{=} & p(t_1\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right],\ldots,t_n\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right]) \\
(\forall y.\phi)\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right] & \stackrel{def}{=} & \begin{cases} \forall y.\phi & x = y \\ \forall y.(\phi\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right]) & x \neq y, y \notin FV(s) \\ \forall z.((\phi\left[\begin{smallmatrix}z\\y\end{smallmatrix}\right])\left[\begin{smallmatrix}s\\x\end{smallmatrix}\right]) & x \neq y, y \in FV(s) \\ & \text{mit } z \notin FV(s)\ (z \text{ frisch}) \end{cases}
\end{array}
$$

Natürliches Schließen mit Quantoren

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

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

Der Existenzquantor

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

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

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

Regeln für die Gleichheit

- Reflexivität, Symmetrie, Transitivität:

$$\frac{}{x = x}\ \text{refl} \qquad \frac{x = y}{y = x}\ \text{sym} \qquad \frac{x = y \quad y = z}{x = z}\ \text{trans}$$

- Kongruenz:

$$\frac{x_1 = y_1,\ldots,x_n = y_n}{f(x_1,\ldots,x_n) = f(y_1,\ldots,y_n)}\ \text{cong}$$

- Substitutivität:

$$\frac{x_1 = y_1,\ldots,x_m = y_m \quad P(x_1,\ldots,x_m)}{P(y_1,\ldots,y_m)}\ \text{subst}$$

Axiomatisierung der natürlichen Zahlen

- Operationen: $0, S, +, \cdot$ mit Arität $0, 1, 2, 2$
- Peano-Axiome (P1– P3):
  - Beschreiben natürliche Zahlen
  - Induktionsschema $P3$

  $P1$ $\forall x.\neg(x = 0)$
  $P2$ $\forall x.\forall y.\, S(x) = S(y) \longrightarrow x = y$
  $P3$ $\forall x.\forall y.\, \phi(0)\wedge(\forall x.\,\phi(x)\longrightarrow\phi(S(x)))\longrightarrow\forall x.\,\phi(x)$
- Presburger-Arithmetik (P1 – P5):
  - Konsistent und vollständig
  - Entscheidbar (Aufwand $2^{2^{cn}}$, n Länge der Aussage)

  $P4$ $\forall x.\, x + 0 = x$
  $P5$ $\forall x.\forall y.\, x + S(y) = S(x + y)$
- Peano-Arithmetik (P1 – P7):
  - Konsistent
  - Unvollständig, nicht entscheidbar

  $P6$ $\forall x.\, x \cdot 0 = 0$
  $P7$ $\forall x.\forall y.\, x \cdot S(y) = (x \cdot y) + x$

Zusammenfassung

- Prädikatenlogik: das natürliche Schließen mit Quantoren
  - Variablenbindungen — Umbenennungen bei Substitution
  - Eigenvariablenbedingung
- Gleichungslogik in natürlichem Schließen:
  - möglich, aber umständlich
- Entwicklung natürlicher Zahlen benötigt:
  - Zusätzliche Axiome,
  - Konzepte höherer Ordnung (Induktion!)
- Deshalb nächste Woche: Logik höherer Stufe