Formale Methoden der Softwaretechnik 1
Vorlesung vom 02.11.09:
Prädikatenlogik erster Stufe

Christoph Lüth, Lutz Schröder

Universität Bremen

Wintersemester 2009/10

Das Tagesmenü

- Logik mit Quantoren
- Von Aussagenlogik zur Prädikatenlogik
- Natürliches Schließen mit Quantoren
- Die Notwendigkeit von Logik höherer Stufe

Fahrplan

- Teil I: Grundlagen der Formalen Logik
  - Einführung
  - Natürliches Schließen, Aussagenlogik
  - Prädikatenlogik 1. Stufe
  - Gleichungslogik und natürliche Zahlen
- Teil II: Arbeiten mit Isabelle
- Teil III: Modellierung imperative Programme

Prädikatenlogik

- Beschränkung 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 Aussagenlogk 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: $P_1, \ldots, P_n, \doteq$ 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: $\wedge, \longrightarrow, \mathit{false}, \forall$, 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 $t_1 \doteq t_2 \in \mathcal{F}orm$

Beispielaussagen

- Alle Zahlen sind gerade oder ungerade.
- Keine Zahl ist gerade und ungerade.
- Es gibt keine größte Primzahl.
- Für jede Primzahl gibt es eine, die größer ist.
- Eine Funktion f ist stetig an der Stelle x_0, gdw. es für jedes $\varepsilon > 0$ ein $\delta > 0$ gibt, so dass für alle x mit $|x - x_0| < \delta$ gilt $|f(x) - f(x_0)| < \epsilon$.

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

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

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

Natürliches Schließen mit Quantoren

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

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

Der Existenzquantor

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

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

- (*) 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
- Das natürliche Schließen mit Quantoren
  - Variablenbindungen — Umbenennungen bei Substitution
  - Eigenvariablenbedingung
- Das nächste Mal: Gleichungen und natürliche Zahlen