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.

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 $m = n \cdot p$.

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**: $P_1, \dots, P_n, =$ mit **Arität** $ar(P_i) \in \mathbb{N}$, $ar(=) = 2$
 - ▶ **Funktionssymbole**: $f_1, \dots, f_m$ mit **Arität** $ar(t_i) \in \mathbb{N}$
 - ▶ Menge X von **Variablen** (abzählbar viele)
 - ▶ **Konnektive**: $\wedge, \longrightarrow, \text{false}, \forall, \text{abgeleitet: } \forall, \longleftrightarrow, \neg, \longleftrightarrow, \exists$

Terme

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

Formeln

- ▶ Menge $\mathcal{Form}$ der **Formeln** gegeben durch:
 - ▶ $false \in \mathcal{Form}$
 - ▶ Wenn $\phi \in \mathcal{Form}$, dann $\neg\phi \in \mathcal{Form}$
 - ▶ Wenn $\phi, \psi \in \mathcal{Form}$, dann $\phi \wedge \psi \in \mathcal{Form}$, $\phi \vee \psi \in \mathcal{Form}$,
 $\phi \longrightarrow \psi \in \mathcal{Form}$, $\phi \longleftrightarrow \psi \in \mathcal{Form}$

Formeln

- ▶ Menge *Form* der **Formeln** gegeben durch:
 - ▶ $false \in Form$
 - ▶ Wenn $\phi \in Form$, dann $\neg\phi \in Form$
 - ▶ Wenn $\phi, \psi \in Form$, dann $\phi \wedge \psi \in Form$, $\phi \vee \psi \in Form$,
 $\phi \longrightarrow \psi \in Form$, $\phi \longleftrightarrow \psi \in Form$
 - ▶ Wenn $\phi \in Form, x \in X$, dann $\forall x.\phi \in Form, \exists x.\phi \in Form$
 - ▶ Prädikatensymbol p mit $ar(p) = m$ und $t_1, \dots, t_m \in Term$, dann $p(t_1, \dots, t_m) \in Form$
 - ▶ Sonderfall: $t_1, t_2 \in Term$, dann $t_1 = t_2 \in Form$

Freie und gebundene Variable

- ▶ Variablen in $t \in \mathcal{Term}$, $p \in \mathcal{Form}$ 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**:

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

Natürliches Schließen mit Quantoren

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

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

Der Existenzquantor

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

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

- ▶ (*) **Eigenvariablenbedingung:**
x nicht frei in ψ , oder einer offenen Vorbedingung außer ϕ
- ▶ ($\dagger$) 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:

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

- ▶ Substitutivität:

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

Axiomatisierung der natürlichen Zahlen

- ▶ Operationen: $0, S, +, \cdot$ mit Arität $0, 1, 2, 2$
- ▶ **Peano-Axiome** (P1– P3):
 - ▶ Beschreiben natürliche Zahlen
 - ▶ **Induktionsschema** P3
$$P1 \quad \forall x. \neg(x = 0)$$
$$P2 \quad \forall x. \forall y. S(x) = S(y) \longrightarrow x = y$$
$$P3 \quad \forall x. \forall y. \phi(0) \wedge (\forall x. \phi(x) \longrightarrow \phi(S(x))) \longrightarrow \forall x. \phi(x)$$
- ▶ **Presburger-Arithmetik** (P1 – P5):
 - ▶ Konsistent und vollständig
 - ▶ Entscheidbar (Aufwand $2^{2^{cn}}$, n Länge der Aussage)
$$P4 \quad \forall x. x + 0 = x$$
$$P5 \quad \forall x. \forall y. x + S(y) = S(x + y)$$
- ▶ **Peano-Arithmetik** (P1 – P7):
 - ▶ Konsistent
 - ▶ Unvollständig, nicht entscheidbar
$$P6 \quad \forall x. x \cdot 0 = 0$$
$$P7 \quad \forall x. \forall y. x \cdot S(y) = (x \cdot y) + x$$

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