Formale Modellierung

Vorlesung 7 vom 02.06.14: Prädikatenlogik mit induktiven Datentypen

Serge Autexier & Christoph Lüth

Universität Bremen

Sommersemester 2014

Fahrplan

- Teil I: Formale Logik
  - Einführung
  - Aussagenlogik: Syntax und Semantik, Natürliches Schließen
  - Konsistenz & Vollständigkeit der Aussagenlogik
  - Prädikatenlogik (FOL): Syntax und Semantik
  - Konsistenz & Vollständigkeit von FOL
  - Beschreibungslogiken
  - FOL mit induktiven Datentypen
  - FOL mit Induktion und Rekursion
  - Die Unvollständigkeitssätze von Gödel
- Teil II: Spezifikation und Verifikation

Das Tagesmenü

- Standard und Nichtstandardmodelle
- Kann man nichtstandard modell ausschliessen?
- Beweis von Eigenschaften von Funktionen mit FOL-ND
  - Induktive Datentypen mit einfacher, struktureller Induktion
  - Wohlfundierte Induktion und rekursive Funktionen

Beweisen mit Natürlichen Zahlen

- Axiome der Natürlichen Zahlen $\mathbb{N}$

$$\forall x.\, \mathsf{s}(x) \neq 0 \tag{N1}$$
$$\forall x.\forall y.\, \mathsf{s}(x) = \mathsf{s}(y) \longrightarrow x = y \tag{N2}$$
$$\forall x. 0 + x = x \tag{A1}$$
$$\forall x.\forall y.\, \mathsf{s}(x) + y = \mathsf{s}(x + y) \tag{A2}$$

- Beweise in ND

$$(\mathrm{N1})(\mathrm{N2})(\mathrm{A1})(\mathrm{A2}) \vdash \forall x.\, \mathsf{s}(0) + x = \mathsf{s}(x)$$

Natürliches Schließen — Die Regeln

$$\frac{\phi \quad \psi}{\phi \wedge \psi}\wedge I \qquad \frac{\phi \wedge \psi}{\phi}\wedge E_L \qquad \frac{\phi \wedge \psi}{\psi}\wedge E_R$$

$$\frac{\begin{matrix}[\phi]\\ \vdots \\ \psi\end{matrix}}{\phi \longrightarrow \psi}\longrightarrow I \qquad \frac{\phi \quad \phi \longrightarrow \psi}{\psi}\longrightarrow E$$

$$\frac{\bot}{\phi}\bot \qquad \frac{\begin{matrix}[\phi \longrightarrow \bot]\\ \vdots \\ \bot\end{matrix}}{\phi}\text{raa}$$

Die fehlenden Schlußregeln

$$\frac{\begin{matrix}[\phi]\\ \vdots \\ \bot\end{matrix}}{\neg\phi}\neg I \qquad \frac{\phi \quad \neg\phi}{\bot}\neg E$$

$$\frac{\phi}{\phi \vee \psi}\vee I_L \qquad \frac{\psi}{\phi \vee \psi}\vee I_R \qquad \frac{\phi \vee \psi \quad \begin{matrix}[\phi]\\ \vdots \\ \sigma\end{matrix} \quad \begin{matrix}[\psi]\\ \vdots \\ \sigma\end{matrix}}{\sigma}\vee E$$

$$\frac{\phi \longrightarrow \psi \quad \psi \longrightarrow \phi}{\phi \longleftrightarrow \psi}\longleftrightarrow I \qquad \frac{\phi \quad \phi \longleftrightarrow \psi}{\psi}\longleftrightarrow E_L \qquad \frac{\psi \quad \phi \longleftrightarrow \psi}{\phi}\longleftrightarrow E_R$$

Natürliches Schließen mit Quantoren

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

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

Der Existenzquantor

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

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

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

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

- Substitutivität:

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

Beweise in ND

$$(\text{N1})(\text{N2})(\text{A1})(\text{A2}) \vdash \forall x. \succ (0) + x = \mathsf{s}(x)$$

In Isabelle.

Wie sehen unsere Zahlen eigtl. aus?

- Angefangen mit "0" und "s"
- Axiome $N1$ und $N2$

Modelle

- Füge hinzu:

$$\forall x. x \neq 0 \longrightarrow \exists y. x = \mathsf{s}(y) \qquad (\text{N3})$$

- Füge weiter hinzu:

$$\forall x. x \neq \underbrace{\mathsf{s} \ldots \mathsf{s}}_{n}(x) \qquad (\text{K}_n)$$

- "Mehrere" Kopien von $\mathbb{N}$ weg, Zyklen weg... $\mathbb{Z}$ bleibt.
- $\mathbb{N}$ is das Standardmodell. Alle anderen Strukturen $\mathbb{N} + \mathbb{Z}$, $\mathbb{N} + \mathbb{Z} + \mathbb{Z}$, ... die mehr als nur $\mathbb{N}$ enthalten sind Nichtstandardmodelle

Induktionsschema

- Induktionsschema für Natürliche Zahlen:

$$P(0) \wedge (\forall x. P(x) \longrightarrow P(\mathsf{s}(x))) \longrightarrow \forall x. P(x) \qquad (\text{ISNat})$$

- $P(\$)$ Formelschema: \$ ausgezeichnetes, neues Symbol ("Variable") und

$$P(t) := P(\$)\begin{bmatrix} t \\ \$ \end{bmatrix}$$

- Abgeleitete ND Regeln:

$$\frac{P(0) \quad \forall x. P(x) \longrightarrow P(\mathsf{s}(x))}{\forall x. P(x)}\ ISNat \qquad \frac{P(0) \quad \begin{array}{c}[P(c)] \\ \vdots \\ P(\mathsf{s}(c))\end{array}}{\forall x. P(x)}\ IS^c,\ c \text{ Eigenvariable}$$

Hilft das Induktionsschema zum Beweisen?

- Es gelten:

$$(\text{N1}), (\text{N2}), (\text{ISNat}) \vdash (\text{N3})$$
$$(\text{N1}), (\text{N2}), (\text{ISNat}) \vdash (\text{K}_n)$$

- Beweise in ND

$$(\text{N1})(\text{N2})(\text{A1})(\text{A2})(\text{ISNat}) \vdash \forall x. 0 + x = x$$
... und auch
$$(\text{N1})(\text{N2})(\text{A1})(\text{A2})(\text{ISNat}) \vdash \forall x. \forall y. x + \mathsf{s}(y) = \mathsf{s}(x + y)$$
... und auch
$$(\text{N1})(\text{N2})(\text{A1})(\text{A2})(\text{ISNat}) \vdash \forall x. \forall y. x + y = y + x$$

- Definiere

$$(\text{N1})(\text{N2})(\text{A1})(\text{A2})(\text{ISNat}) \quad =: \quad (\text{Presburger})$$

Und was ist mit den Modellen?

- Ist $\mathbb{Z}$ jetzt weg?
- Sei $PA^\infty := (\text{N1}), (\text{N2}), (\text{ISNat})+$ neues Symbol ∞ und Axiome

$$\infty \neq 0, \infty \neq \mathsf{s}(0), \infty \neq \mathsf{s}(\mathsf{s}(0)), \ldots$$

- Jede endliche Teilmenge von PA^∞ hat Modell

Theorem 1 (Kompaktheit)
Γ hat ein Modell gdw. jede endliche Teilmenge $\Delta \subseteq \Gamma$ hat ein Modell

- Also hat PA^∞ Modell, das aber größer ist als $\mathbb{N}$
- Es kann keine Axiomenmenge geben für $\mathbb{N}$ geben, die nicht auch noch Nichtstandartmodelle hat

Allgemein

- Alle natürlichen Zahlen sind konstruiert aus 0 und s:

$$\mathbb{N} := 0 \mid \mathsf{s}(\mathbb{N})$$

$$P(0) \wedge (\forall x_{\mathbb{N}}. P(x) \longrightarrow P(\mathsf{s}(x))) \longrightarrow \forall x_{\mathbb{N}}. P(x) \qquad (\text{ISNat})$$

- Alle natürlichen Listen über Zahlen sind konstruiert aus Nil und cons:

$$\mathbb{LIST} := \text{Nil} \mid \text{cons}(\mathbb{N}, \mathbb{LIST})$$

$$P(\text{Nil}) \wedge (\forall x_{\mathbb{LIST}}. P(x) \longrightarrow \forall n_{\mathbb{N}}. P(\text{cons}(n, x))) \longrightarrow \forall x_{\mathbb{LIST}}. P(x) \qquad (\text{ISList})$$

Allgemein

- Alle Binärbäume über Zahlen sind konstruiert aus Leaf und Node:

$$\mathbb{TREE} := \mathsf{Leaf}(\mathbb{N}) \mid \mathsf{Node}(\mathbb{TREE}, \mathbb{TREE})$$

$$\begin{aligned} &\forall n_{\mathbb{N}}.P(\mathsf{Leaf}(n)) \wedge \\ &(\forall x_{\mathbb{TREE}}.\forall y_{\mathbb{TREE}}.(P(x) \wedge P(y)) \longrightarrow P(\mathsf{Node}(x, y))) \\ &\longrightarrow \forall x_{\mathbb{TREE}}.P(x) \end{aligned} \tag{ISTree}$$

- Und allgemein für frei erzeugte Datentypen.

Zusammenfassung

- Jede Axiomenmenge zur Formalisierung der Natürlichen Zahlen hat Nichtstandardmodelle
- Induktionsschema für erzeugte Datentypen
- Strukturelle Induktionsschema
  - Einfach, aber zum Beweisen zu rigide