Formale Modellierung
Vorlesung 6 vom 13.05.13: Prädikatenlogik mit induktiven Datentypen

Serge Autexier & Christoph Lüth

Universität Bremen

Sommersemester 2013

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
  - FOL mit induktiven Datentypen
  - FOL mit Induktion und Rekursion
  - Die Gödel-Theoreme
  - Weitere Datentypen: Mengen, Multimengen, Punkte
- Teil II: Spezifikation und Verifikation
- Teil III: Schluß

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 $\mathbb{N}$

$$\forall x.\, \mathsf{s}(x) \neq 0 \tag{N1}$$

$$\forall x.\forall y.\, \mathsf{s}(x) = \mathsf{s}(y) \longrightarrow x = y \tag{N2}$$

$$\forall x. x + 0 = x \tag{A1}$$

$$\forall x.\forall y. x + \mathsf{s}(y) = \mathsf{s}(x + y) \tag{A2}$$

- Beweise in ND

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

Natürliches Schließen — Die Regeln

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

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

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

Die fehlenden Schlußregeln

$$\cfrac{\begin{array}{c}[\phi]\\ \vdots\\ \bot\end{array}}{\neg\phi}\ \neg I \qquad\qquad \cfrac{\phi \quad \neg\phi}{\bot}\ \neg E$$

$$\cfrac{\phi}{\phi \vee \psi}\ \vee I_L \qquad \cfrac{\psi}{\phi \vee \psi}\ \vee I_R \qquad\qquad \cfrac{\phi \vee \psi \qquad \begin{array}{c}[\phi]\\ \vdots\\ \sigma\end{array} \qquad \begin{array}{c}[\psi]\\ \vdots\\ \sigma\end{array}}{\sigma}\ \vee E$$

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

Natürliches Schließen mit Quantoren

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

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

Der Existenzquantor

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

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

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

Wie sehen unsere Zahlen eigtl. aus?

- Angefangen mit “0” und “s”

- Axiome $N1$ und $N2$

Modelle

- Füge hinzu:

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

- Füge weiter hinzu:

$$\forall x. x \neq \underbrace{\mathsf{s} \ldots \mathsf{s}}_{n}(x) \tag{K_n}$$

- "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:

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

Hilft das Induktionsschema zum Beweisen?

- Es gelten:

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

- Beweise in ND

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

... und auch

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

... und auch

$$(\mathrm{N1})(\mathrm{N2})(\mathrm{A1})(\mathrm{A2})(\mathrm{ISNat}) \vdash \forall x.\forall y.x + y = y + x$$

- Definiere

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

Und was ist mit den Modellen?

- Ist $\mathbb{Z}$ jetzt weg?

Und was ist mit den Modellen?

- Ist $\mathbb{Z}$ jetzt weg?
- Sei $PA^\infty := (\mathsf{N1}), (\mathsf{N2}), (\mathsf{ISNat})+$ 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

Und was ist mit den Modellen?

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

$$\infty \neq 0, \infty \neq s(0), \infty \neq s(s(0)), \ldots$$

- Jede endliche Teilmenge von PA^∞ hat Modell

Theorem 1 (Kompaktheit)

Γ hat ein Modell gdw. jede endliche Teilmenge $\Delta \Subset \Gamma$ 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:

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

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

Allgemein

- Alle natürlichen Zahlen sind konstruiert aus 0 und s:

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

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

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

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

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

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.

Mehr Beweise

- Definiere $\leq$ und half:

$$\forall x. 0 \leq x \tag{L1}$$
$$\forall x. \forall y. x \leq y \longrightarrow \mathsf{s}(x) \leq \mathsf{s}(y) \tag{L2}$$

$$\mathsf{half}(0) = 0 \tag{H1}$$
$$\mathsf{half}(\mathsf{s}(0)) = 0 \tag{H2}$$
$$\forall x. \mathsf{half}(\mathsf{s}(\mathsf{s}(x))) = \mathsf{s}(\mathsf{half}(x)) \tag{H3}$$

- Beweise

$$(\text{Presburger})(\text{L1})(\text{L2})(\text{H1})(\text{H2})(\text{H3}) \vdash \forall x. \mathsf{half}(x) \leq x$$

Wohlfundierte Induktion

- Wohlfundiertes Induktionsschema

$$(\forall y.(\forall x.x < y \wedge P(x)) \Rightarrow P(y)) \longrightarrow \forall x.P(x)$$

- $<$ wohlfundierte Relation:

$$\forall X \subseteq \mathbb{N}.X \neq \emptyset \longrightarrow \exists x \in X.\forall y \in X.\neg(y < x)$$

Beweis mit wohlfundierter Induktion

- $<$-Relation

$$\forall x.0 < \mathsf{s}(x) \qquad\qquad \forall x, y.x < y \longrightarrow \mathsf{s}(x) < \mathsf{s}(y)$$

- Beweise $<$ ist wohlfundiert
-

$$\frac{\begin{array}{c}\left[\ \forall x.x < c \wedge P(x)\ \right] \\ \vdots \\ P(c)\end{array}}{\forall x.P(x) \leq x}$$

Beweis mit wohlfundierter Induktion

- $<$-Relation

$$\forall x. 0 < \mathsf{s}(x) \qquad\qquad \forall x, y. x < y \longrightarrow \mathsf{s}(x) < \mathsf{s}(y)$$

- Beweise $<$ ist wohlfundiert

-

$$\dfrac{\begin{array}{c} c = 0 \vee \\ c = \mathsf{s}(0) \vee \\ \exists u. c = \mathsf{s}(\mathsf{s}(u)) \end{array} \quad \begin{array}{c} \left[\begin{array}{c} \forall x. x < c \\ \mathsf{half}(x) \leq x \\ c = 0 \end{array}\right] \\ \vdots \\ \mathsf{half}(c) \leq c \end{array} \quad \begin{array}{c} \left[\begin{array}{c} \forall x. x < c \\ \mathsf{half}(x) \leq x \\ c = \mathsf{s}(0) \end{array}\right] \\ \vdots \\ \mathsf{half}(c) \leq c \end{array} \quad \begin{array}{c} \left[\begin{array}{c} \forall x. x < c \\ \mathsf{half}(x) \leq x \\ \exists u. c = \mathsf{s}(\mathsf{s}(u)) \end{array}\right] \\ \vdots \\ \mathsf{half}(c) \leq c \end{array}}{\forall x. \mathsf{half}(x) \leq x}$$

Mehr Information

- Besser zum beweisen wäre wenn man gleich hätte

$$\dfrac{\mathsf{half}(0) \le 0 \quad \mathsf{half}(\mathsf{s}(0)) \le \mathsf{s}(0) \quad \begin{array}{c} \left[\ \mathsf{half}(c) \le c\ \right] \\ \vdots \\ \mathsf{half}(\mathsf{s}(\mathsf{s}(c))) \le \mathsf{s}(\mathsf{s}(c)) \end{array}}{\forall x.\, \mathsf{half}(x) \le x}$$

Mehr Information

- Besser zum beweisen wäre wenn man gleich hätte

$$\dfrac{\mathsf{half}(0) \leq 0 \quad \mathsf{half}(\mathsf{s}(0)) \leq \mathsf{s}(0) \quad \begin{array}{c} \left[\ \mathsf{half}(c) \leq c\ \right] \\ \vdots \\ \mathsf{half}(\mathsf{s}(\mathsf{s}(c))) \leq \mathsf{s}(\mathsf{s}(c)) \end{array}}{\forall x.\, \mathsf{half}(x) \leq x}$$

- Vergleiche:

$$\mathsf{half}(0) = 0 \tag{H1}$$

$$\mathsf{half}(\mathsf{s}(0)) = 0 \tag{H2}$$

$$\forall x.\, \mathsf{half}(\mathsf{s}(\mathsf{s}(x))) = \mathsf{s}(\mathsf{half}(x)) \tag{H3}$$

Mehr Information

- Besser zum beweisen wäre wenn man gleich hätte

$$\dfrac{\mathsf{half}(0) \leq 0 \quad \mathsf{half}(\mathsf{s}(0)) \leq \mathsf{s}(0) \quad \begin{matrix}[\ \mathsf{half}(c) \leq c\ ] \\ \vdots \\ \mathsf{half}(\mathsf{s}(\mathsf{s}(c))) \leq \mathsf{s}(\mathsf{s}(c))\end{matrix}}{\forall x.\, \mathsf{half}(x) \leq x}$$

- Vergleiche:

$$\mathsf{half}(0) = 0 \qquad \text{(H1)}$$
$$\mathsf{half}(\mathsf{s}(0)) = 0 \qquad \text{(H2)}$$
$$\forall x.\, \mathsf{half}(\mathsf{s}(\mathsf{s}(x))) = \mathsf{s}(\mathsf{half}(x)) \qquad \text{(H3)}$$

- Generiere Induktionschema aus rekursiven Funktionsdefinitionen

$$\dfrac{P(0) \quad P(\mathsf{s}(0)) \quad \begin{matrix}[\ P(c)\ ] \\ \vdots \\ P(\mathsf{s}(\mathsf{s}(c)))\end{matrix}}{\forall x. P(x)}$$

Weitere Beispiele

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

- Sortieren

$$\forall x.\, \mathrm{sort}(\mathrm{Nil}) = \mathrm{Nil}$$
$$\forall s, t. m = \min(\mathrm{cons}(n, l))$$
$$\longrightarrow \mathrm{sort}(\mathrm{cons}(n, l)) = \mathrm{cons}(m, \mathrm{sort}(\mathrm{cons}(n, l) - m))$$
$$\forall n.\, \min(\mathrm{cons}(n, \mathrm{Nil})) = n$$
$$\forall n, l.\, \min(\mathrm{cons}(m, l)) < n \longrightarrow \min(\mathrm{cons}(n, \mathrm{cons}(m, l))) = \min(\mathrm{cons}(m, l))$$
$$\forall n, l. \neg(\min(\mathrm{cons}(m, l)) < n) \longrightarrow \min(\mathrm{cons}(n, \mathrm{cons}(m, l))) = n$$

- Induktionsschema

$$\frac{P(\mathrm{Nil}) \qquad \begin{array}{l} \forall m, n. m = \min(\mathrm{cons}(n, l)) \wedge P(\mathrm{cons}(n, l) - m) \\ \longrightarrow P(\mathrm{cons}(n, l)) \end{array}}{\forall l. P(l)}$$

Weitere Beispiele

- Fibonacci:

$$\begin{aligned} \mathrm{fib}(0) &= 0 \\ \mathrm{fib}(\mathrm{s}(0)) &= s(0) \\ \forall n.\, \mathrm{fib}(s(s(n))) &= \mathrm{fib}(s(n)) + \mathrm{fib}(n) \end{aligned}$$

$$\dfrac{P(0) \quad P(\mathrm{s}(0)) \quad \begin{array}{c} \left[\; P(\mathrm{s}(c)), P(c) \;\right] \\ \vdots \\ P(c) \end{array}}{\forall x.P(x)}$$

Weitere Beispiele

- GGT:

$$
\begin{aligned}
&\forall y.\, \mathrm{ggt}(0, y) = y\\
&\forall x.\, \mathrm{ggt}(\mathrm{s}(x), 0) = \mathrm{s}(x)\\
&\forall x, y. x \leq y \longrightarrow \mathrm{ggt}(x, y) = \mathrm{ggt}(x, y - x)\\
&\forall x, y. \neg(x \leq y) \longrightarrow \mathrm{ggt}(x, y) = \mathrm{ggt}(x - y, y)
\end{aligned}
$$

$$
\frac{\forall y. P(0, y) \quad \forall x. P(\mathrm{s}(x), 0) \quad \begin{matrix} \begin{bmatrix} x \leq y \\ P(x, y - x) \end{bmatrix} \\ \vdots \\ P(x, y) \end{matrix} \quad \begin{matrix} \begin{bmatrix} \neg(x \leq y) \\ P(x - y, x) \end{bmatrix} \\ \vdots \\ P(x, y) \end{matrix}}{\forall x, y. P(x, y)}
$$

Zulässige Induktionsschema

- Wann darf man die Rekursionsstruktur verwenden?
- Definierte Funktion muß...
  - eindeutig definiert sein und ...

$$P_0 \longrightarrow f(x_1, \ldots, x_n) = t_0$$
$$\vdots$$
$$P_n \longrightarrow f(x_1, \ldots, x_n) = t_n$$

    $P_i \wedge P_j \longleftrightarrow \perp, \forall i \neq j$

  - terminierend
- Rekursive Definition nach wohlfundierter Relation garantiert Terminierung
  Für jeden atomaren, rekursiven Aufruf $f(t_1, \ldots, t_n)$ erzeuge Terminierungshypothese

$$P_i \longrightarrow (x_1, \ldots, x_n) > (t_1, \ldots, t_n)$$

Grenzen

$$\begin{aligned} \forall x. x < 101 &\longrightarrow f(x) = f(f(x+11)) \\ \forall x. \neg(x < 101) &\longrightarrow f(x) = x - 10 \end{aligned}$$

Grenzen

$$\forall x. x < 101 \longrightarrow f(x) = f(f(x + 11))$$
$$\forall x. \neg(x < 101) \longrightarrow f(x) = x - 10$$

- f terminiert immer
- f ist

$$f(x) := \begin{cases} x - 10 & \text{if } x > 100 \\ 91 & \text{if } x \leq 100 \end{cases}$$

- Definition der geeigneten wohlfundierten Relation extrem schwierig.

$$\begin{aligned} f(99) &= f(f(110)) \\ &= f(100) \\ &= f(f(111)) \\ &= f(101) \\ &= 91 \end{aligned}$$

$$\begin{aligned} f(87) &= f(f(98)) \\ &= f(f(f(109))) \\ &= f(f(99)) \\ &= f(f(f(110))) \\ &= f(f(100)) \\ &= f(f(f(111))) \\ &= f(f(101)) \\ &= f(91) \\ &= f(f(102)) \\ &= f(92) \\ &= f(f(103)) \\ &= f(93) \\ & \quad \text{.... Pattern continues} \\ &= f(99) \\ & \quad \text{(same as on the left)} \\ &= 91 \end{aligned}$$

Zusammenfassung

- Jede Axiomenmenge zur Formalisierung der Natürlichen Zahlen hat Nichtstandardmodelle
- Induktionsschema für erzeugte Datentypen
- Strukturelle Induktionsschema
  - Einfach, aber zum Beweisen zu rigide
- Wohlfundiertes Induktionsschema
  - Mächtig und flexibel, wenig Hilfestellung beim Beweisen
- Wohlfundierte Relation aus Rekursionsstruktur terminierender Funktionen
  - Angepasst an Beweisproblem und vorhandene Definitionsgleichungen
  - Terminierungsbeweis notwendig (einfache Fälle automatisierbar, i.A. unentscheidbar)