# Formale Modellierung
# Vorlesung 7 vom 01.06.15: FOL mit Induktion und Rekursion

Christoph Lüth

Universität Bremen

Sommersemester 2015

# Fahrplan

- Teil I: Formale Logik
  - Einführung
  - Aussagenlogik (PL): Syntax und Semantik, Natürliches Schließen
  - Konsistenz & Vollständigkeit der Aussagenlogik
  - Prädikatenlogik (FOL): Syntax und Semantik
  - Konsistenz & Vollständigkeit von FOL
  - FOL mit induktiven Datentypen
  - FOL mit rekursiven Definitionen
  - Logik höherer Stufe (HOL): Syntax und Eigenschaften
  - Berechungsmodelle (Models of Computation)
  - Die Unvollständigkeitssätze von Gödel
- Teil II: Spezifikation und Verifikation

# Das Tagesmenü

- Beweis von Eigenschaften von Funktionen mit FOL-ND
  - Rekursive Funktionen und wohlfundierte Induktion
- Terminierende Funktionen und abgeleitete Induktionsschemata
- Axiomatische Definition von Theorien ist gefährlich

# Beweis der Eigenschaften von Funktion

- 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

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

# Mehr Information

- Besser zum beweisen wäre wenn man gleich hätte

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

# Mehr Information

- Besser zum beweisen wäre wenn man gleich hätte

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

- Vergleiche:

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

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

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

# Mehr Information

- Besser zum beweisen wäre wenn man gleich hätte

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

- Vergleiche:

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

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

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

- Generiere Induktionschema aus rekursiven Funktionsdefinitionen

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

# 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
-

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

# 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
-

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

# Zulässige Induktionsschema

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

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

  $P_i \wedge P_j \longleftrightarrow \bot, \forall i \neq j$
  - 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

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

# 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.

$$
\begin{aligned}
f(99) &= f(f(110)) \\
&= f(100) \\
&= f(f(111)) \\
&= f(101) \\
&= 91
\end{aligned}
\qquad
\begin{aligned}
f(87) &= f(f(98)) \\
&= f(f(f(109))) \\
&= f(f(99)) \\
&= f(f(f(110))) \\
&= f(f(100)) \\
&= f(f(f(111))) \\
&= f(f(101)) \\
&= f(91) \\
&= f(f(102)) \\
&= f(92) \\
&= f(f(103)) \\
&= f(93) \\
&\quad \ldots\text{. etc } \ldots \\
&= f(99) \\
&\quad (\text{siehe links}) \\
&= 91
\end{aligned}
$$

# Zusammenfassung

- 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)
- Axiomatisierung "von Hand" fehleranfällig
  - Kernkonzept in Isabelle: konservative Erweiterung
  - Dazu nötig: Rekursion und Induktion als abgeleitetes Prinzip