

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
 - ▶ Berechnungsmodelle (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:

$$\forall x. 0 \leq x \quad (L1)$$

$$\forall x. \forall y. x \leq y \rightarrow s(x) \leq s(y) \quad (L2)$$

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

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

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

- ▶ Beweise

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

Mehr Information

- ▶ Besser zum beweisen wäre wenn man gleich hätte

$$\frac{\begin{array}{c} [\text{half}(c) \leq c] \\ \vdots \\ \text{half}(0) \leq 0 \quad \text{half}(s(0)) \leq s(0) \quad \text{half}(s(s(c))) \leq s(s(c)) \end{array}}{\forall x. \text{half}(x) \leq x}$$

- ▶ Vergleiche:
 - $\text{half}(0) = 0 \quad (H1)$
 - $\text{half}(s(0)) = 0 \quad (H2)$
 - $\forall x. \text{half}(s(s(x))) = s(\text{half}(x)) \quad (H3)$

- ▶ Generiere Induktionsschema aus rekursiven Funktionsdefinitionen

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

Wohlfundierte Induktion

- ▶ Wohlfundiertes Induktionsschema

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

- ▶ $<$ wohlfundierte Relation:

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

Beweis mit wohlfundierter Induktion

- ▶ $<$ -Relation

$$\forall x. 0 < s(x) \quad \forall x, y. x < y \rightarrow s(x) < s(y)$$

- ▶ Beweise $<$ ist wohlfundiert

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

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

Zulässige Induktionsschema

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

$$P_0 \rightarrow f(x_1, \dots, x_n) = t_0$$

$$\vdots$$

$$P_n \rightarrow f(x_1, \dots, x_n) = t_n$$

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

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

$$P_i \rightarrow (x_1, \dots, x_n) > (t_1, \dots, t_n)$$

Grenzen

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

- ▶ 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.

9 [11]

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

10 [11]

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

11 [11]