Formale Modellierung
Vorlesung 6 vom 28.05.15: FOL mit induktiven Datentypen 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

- Modellierung natürlicher Zahlen als Beispiel für einen induktiven Datentyp
- Beweis durch Induktion und Gleichungen
- Modelle der natürlichen Zahlen

Die natürlichen Zahlen

- Der einfachste Datentyp
  - Aber hinreichend (Turing-mächtig)
- Wie in FOL formulieren?
  - Axiomatisch
- Was sind die Modelle?

Regeln für die Gleichheit

- Reflexivität, Symmetrie, Transitivität:

$$\frac{}{x \doteq x}\ \text{refl} \qquad \frac{x \doteq y}{y \doteq x}\ \text{sym} \qquad \frac{x \doteq y \quad y \doteq z}{x \doteq z}\ \text{trans}$$

- Kongruenz:

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

- Substitutivität:

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

Axiomatisierung der natürlichen Zahlen

- Axiome (erster Versuch):

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

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

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

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

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

- Beweise in ND

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

Modelle für Presburger-Arithmetik

- Angefangen mit “0” und “s”
- Axiome (N1), (N2)
- Füge hinzu: (N3) und

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

- “Mehrere” Kopien von $\mathbb{N}$ weg, Zyklen weg — $\mathbb{Z}$ bleibt.
- $\mathbb{N}$ is das Standardmodell.
- Alle anderen Strukturen $\mathbb{N} + \mathbb{Z}$, $\mathbb{N} + \mathbb{Z} + \mathbb{Z}$, … sind Nichtstandardmodelle.

Induktionsschema

- Axiome für die Multiplikation:

$$x \cdot 0 \doteq 0 \tag{M1}$$

$$x \cdot \mathsf{s}(y) \doteq x \cdot y + x \tag{M2}$$

- Induktionsschema:

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

- $P(\$)$ Formelschema
  - \$ ausgezeichnetes, neues Symbol ("Loch") und $P(t) \stackrel{def}{=} P(\$)\left[\begin{smallmatrix} t \\ \$ \end{smallmatrix}\right]$

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

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

...und auch

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

...und auch

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

Und was ist mit den Modellen?

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

Und was ist mit den Modellen?

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

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

Und was ist mit den Modellen?

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

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

Theorem (Kompaktheit)

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

Theorem (Löwenheim-Skolem Theorem)

Wenn FOL-Theorie T ein unendliches Modell M hat, dann hat es Modelle beliebiger Größe (Kardinalität).

- Also hat PA^∞ Modell, das aber größer ist als $\mathbb{N}$
- Es kann in FOL keine Axiomatiserung für $\mathbb{N}$ geben, die keine Nichtstandardmodelle hat

Axiomatisierungen der natürlichen Zahlen

- Presburger-Arithmetik
  - 5 Axiome: (N1)(N2)(A1)(A2)(ISNat)
  - Konsistent und vollständig
  - Entscheidbar (Aufwand $2^{2^{cn}}$, n Länge der Aussage)
  - Enthält Nichtstandardmodelle
- Peano-Arithmetik
  - 7 Axiome: (N1)(N2)(A1)(A2)(M1)(M2)(ISNat)
  - Konsistent, aber unvollständig (bzgl. Standard-Modellen)
  - Enthält Nichtstandardmodelle
  - Nicht entscheidbar

Zusammenfassung

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