Formale Modellierung
Vorlesung 7 vom 23.05.13: FOL mit Induktion und Rekursion

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

- Axiomatische Definition von Theorien ist gefährlich
- Prädikatenlogik mit mehreren Typen
- Konservative Erweiterungen als sicheres Theorie Definitionsprinzip
  - Typdefinitionen
  - Wohlfundierte rekursive Funktionen/Prädikate

Natürliches Schließen — Die Regeln

$$\frac{\phi \quad \psi}{\phi \wedge \psi}\ \wedge I$$

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

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

$$\frac{\phi \quad \phi \longrightarrow \psi}{\psi}\ \longrightarrow E$$

$$\frac{\bot}{\phi}\ \bot$$

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

Die fehlenden Schlußregeln

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

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

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

Natürliches Schließen mit Quantoren

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

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

Der Existenzquantor

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

$$\frac{\phi\left[\begin{smallmatrix} t \\ x \end{smallmatrix}\right]}{\exists x.\phi}\ \exists I\ \ (\dagger) \qquad\qquad \frac{\exists x.\phi \qquad \begin{array}{c}[\phi] \\ \vdots \\ \psi\end{array}}{\psi}\ \exists E\ \ (*)$$

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

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

Motivation

- Typen müssen nicht-leere Trägermengen haben

Motivation

- Typen müssen nicht-leere Trägermengen haben — Korrektheit
- Neue Typen axiomatisch zu spezifizieren gefährlich

Motivation

- Typen müssen nicht-leere Trägermengen haben — Korrektheit
- Neue Typen axiomatisch zu spezifizieren gefährlich
- Konservative Erweiterungen
  - Typdefinitionen sind konservative Erweiterungen
  - Terminierende totale rekursive Funktionen/Prädikate sind konservative Erweiterungen

Getypte Prädikatenlogik – Signatur

	Ungetypt	Getypt
Signatur Σ		
- Typen $\mathcal{T}$	–	$i, \mathbb{N}, \mathbb{Z}$
- Funktionssymbole $\mathcal{F}$	$f, ar(f) = n$	$f : \tau_1 \times \cdots \times \tau_n \to \tau_0,\ \tau_i \in \mathcal{T}$
- Prädikatssymbole $\mathcal{P}$	$P, ar(P) = n$	$P : \tau_1 \times \cdots \times \tau_n,\ \tau_i \in \mathcal{T}$
	$\dot{=}, ar(\dot{=}) = 2$	$\dot{=}_\tau : \tau \times \tau,\ \tau \in \mathcal{T}$
Variablen X	abz. unendlich	abz. unendlich X_τ für jedes $\tau \in \mathcal{T}$
		$x_i, x_{\mathbb{N}}, x_{\mathbb{Z}}, \ldots$

Getypte Prädikatenlogik – Terme & Formeln

	Ungetypt	Getypt
Terme $\mathcal{T}erm_\Sigma$		$\mathcal{T}erm_\Sigma{}^{\tau_1} \cup \cdots \cup \mathcal{T}erm_\Sigma{}^{(\tau_n)}$, $\tau \in \mathcal{T}$
- Variablen	$x \in \mathcal{T}erm_\Sigma$ $x \in X$	$x \in \mathcal{T}erm_\Sigma{}^{\tau}$, $x \in X_\tau$
- Funktionen	$f \in \mathcal{F}$ mit $ar(f) = n$ und $t_1, \ldots, t_n \in \mathcal{T}erm_\Sigma$, dann $f(t_1, \ldots, t_n) \in \mathcal{T}erm_\Sigma$	$f : \tau_1 \times \cdots \times \tau_n \to \tau_0 \in \mathcal{F}$ und $t_i \in \mathcal{T}erm_\Sigma^{\tau_i}, 1 \leq i \leq n$, dann $f(t_1, \ldots, t_n) \in \mathcal{T}erm_\Sigma^{\tau_0}$
Formeln $\mathcal{F}orm_\Sigma$		
- Atome	$P \in \mathcal{P}$ mit $ar(P) = n$ und $t_1, \ldots, t_n \in \mathcal{T}erm_\Sigma$, dann $P(t_1, \ldots, t_n) \in \mathcal{F}orm_\Sigma$	$P : \tau_1 \times \cdots \times \tau_n \in \mathcal{P}$ und $t_i \in \mathcal{T}erm_\Sigma^{\tau_i}, 1 \leq i \leq n$, dann $P(t_1, \ldots, t_n) \in \mathcal{F}orm_\Sigma$
- PL Konnective	$\neg\psi, \varphi \wedge \psi, \varphi \vee \psi, \varphi \longrightarrow \psi, \varphi \longleftrightarrow \psi \ldots$	
- Quantoren	$\forall x.\phi \in \mathcal{F}orm_\Sigma$, $x \in X$ $\exists x.\phi \in \mathcal{F}orm_\Sigma$, $x \in X$	$\forall x_\tau.\phi \in \mathcal{F}orm_\Sigma$ $\exists x_\tau.\phi \in \mathcal{F}orm_\Sigma$

Getypte Prädikatenlogik – ND Regeln

$$\frac{\phi}{\forall x_\tau.\phi}\ \forall I\ \ (*) \qquad\qquad \frac{\forall x_\tau.\phi}{\phi\left[\begin{smallmatrix} t \\ x \end{smallmatrix}\right]}\ \forall E\ \ (\dagger)$$

- (*) Eigenvariablenbedingung:
  x_τ nicht frei in offenen Vorbedingungen von ϕ (x_τ beliebig)

- ($\dagger$) $t \in \mathcal{T}erm^\tau_\Sigma$; Ggf. Umbenennung durch Substitution

Der Existenzquantor

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

$$\frac{\phi\left[\begin{smallmatrix} t \\ x \end{smallmatrix}\right]}{\exists x_\tau.\phi}\ \exists I\ \ (\dagger) \qquad\qquad \frac{\exists x_\tau.\phi \qquad \begin{array}{c}[\phi] \\ \vdots \\ \psi\end{array}}{\psi}\ \exists E\ \ (*)$$

- (*) Eigenvariablenbedingung:
  x_τ nicht frei in ψ, oder einer offenenen Vorbedingung außer ϕ
- ($\dagger$) $t \in \mathcal{T}erm^\tau_\Sigma$; Ggf. Umbenennung durch Substitution

Regeln für die Gleichheit

- Reflexivität, Symmetrie, Transitivität:

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

- Kongruenz:

$$\frac{x_1 =_{t_1} y_1, \ldots, x_n =_{t_n} y_n}{f(x_1, \ldots, x_n) =_t f(y_1, \ldots, y_n)}\ \text{cong}$$

- Substitutivität:

$$\frac{x_1 =_{t_1} y_1, \ldots, x_m =_{t_m} y_m \quad P(x_1, \ldots, x_m)}{P(y_1, \ldots, y_m)}\ \text{subst}$$

Basic Definitions

Definition 1 (Loose Spezifikationen)

Sei $\Sigma = (\mathcal{T}, \mathcal{F}, \mathcal{P})$ eine getypte Signature und $\Phi \in \mathcal{F}orm_\Sigma$. Dann ist $S = (\Sigma, \Phi)$ eine lose Spezifikation.
Die Theorie einer Spezifikation S ist $\mathrm{Th}(S) := \{\varphi \in \mathcal{F}orm_\Sigma | \Phi \vdash \varphi\}$.

Definition 2 (Konsistenz)

Eine lose Spezifikation S ist konsistent wenn $\bot$ nicht beweisbar in S: $\bot \notin \mathrm{Th}(S)$.

- Insbesondere müssen dann alle Typen nicht-leere Trägermengen haben

Spezifikations Erweiterungen

Definition 3 (Erweiterungen)

Eine Spezifikation $S' = (\Sigma', \Phi')$ ist eine Erweiterung einer Spezifikation $S = (\Sigma, \Phi)$ genau dann wenn

- $\Sigma \subseteq \Sigma'$
- $\Phi \subseteq \Phi'$

S' is eine konservative Erweiterung von S genau dann wenn

$$\mathsf{Th}(S) = \mathsf{Th}(S')_{|\Sigma}$$

wobei die $|\Sigma$ die Einschränkung auf Formeln aus $\mathcal{T}erm_{\Sigma}$ ist

Lemma 4

Jede konservative Erweiterung einer konsistenten Theorie ist konsistent.

Typdefinition

- Spezifiziere nicht-leere Teilmenge eines gegebenen Typs r
- Deklariere neuen Typ t mit Trägermenge isomorph zu Werten in spezifizierter Teilmenge
- Isomorphie wird durch inverse Funktionen $\mathrm{Abs}_t : r \to t, \mathrm{Rep}_t : t \to r$ axiomatisch Beschrieben

Typdefinitionen sind Erweiterungen

Definition 5 (Typdefinitionen)

Sei $S = ((\mathcal{T}, \mathcal{F}, \mathcal{P}), \Phi)$ eine Spezifikation, $r \in \mathcal{T}$ und $P \in \mathcal{F}orm_{\Sigma}$ mit genau einer freien Variable vom Typ r. Dann ist eine Erweiterung $S' = ((\mathcal{T}', \mathcal{F}', \mathcal{P}'), \Phi')$ eine Typdefinition für einen Typ $t \notin \mathcal{T}$ gdw.

- $\mathcal{T}' = \mathcal{T} \cup \{t\}$
- $\mathcal{F}' = \mathcal{F} \cup \{\mathsf{Abs}_t : r \to t, \mathsf{Rep}_t : t \to r\}$
- $\mathcal{P}' = \mathcal{P} \cup \{=_t : t \times t\}$
- $\Phi' = \Phi \cup \{\ \forall x_t.\, \mathsf{Abs}_t(\mathsf{Rep}_t(x)) =_t x,$
  $\forall x_r.P(x_r) \longrightarrow \mathsf{Rep}_t(\mathsf{Abs}_t(x)) =_r x\}$
- Man kann beweisen $S \vdash \exists x_r.P(x)$ (bzw. es gilt $\exists x_r.P(x) \in \mathsf{Th}(S)$)

Teminierende, totale Funktionen

- Spezifiziere Funktionen/Prädikate die beweisbar total, eindeutig und terminierend sind
- Theorie-Erweiterungen um beweisbar total, eindeutig und terminierende Funktionen/Prädikate sind konservative Erweiterungen
- Syntaktische Kriterien für eindeutige und totale Deklarationen
- Beweisverfahren für terminierende Funktionen

Frei Erzeugte Typen

Definition 6 (Frei Erzeugte Typen)

Sei $S = ((\mathcal{T}, \mathcal{F}, \mathcal{P}), \Phi)$ eine Spezifikation, $t \in \mathcal{T}$ and $c_i : \tau_1^i \times \tau_{n_i}^i \to t \in \mathcal{F}, 1 \leq i \leq k$. Dann ist t frei erzeugt in S durch Konstruktoren $c_1, \ldots, c_k$ gdw.

- $S \vdash \forall x_t . \bigvee_{i=1\ldots k} \exists y^1_{\tau_1^i}, \ldots y^{n_k}_{\tau^i_{n_i}} . x = c_i(y^1, \ldots, y^{n_i})$
- $S \vdash \forall y^1_{\tau_1^i}, \ldots y^{n_i}_{\tau^i_{n_i}} . \forall z^1_{\tau_1^i}, \ldots z^{n_i}_{\tau^i_{n_i}} . c_i(y^1, \ldots, y^{n_i}) = c_i(z^1, \ldots, z^{n_i}) \longrightarrow ((y^1 = z^1 \wedge \cdots \wedge y^{n_i} = y^{n_i}))$ für alle c_i
- $S \vdash \forall y^1_{\tau_1^i}, \ldots y^{n_i}_{\tau^i_{n_i}} . \forall z^1_{\tau_1^j}, \ldots z^{n_j}_{\tau^j_{n_j}} . c_i(y^1, \ldots, y^{n_i}) = c_j(z^1, \ldots, z^{n_j})$ für alle $i \neq j$

Kriterien für eindeutig und total

- Sei t Typ
- Definitionsgleichungen für Funktion f sind Menge von bedingten geschlossene Gleichungen der Form

$$\forall x_{1\tau_1} \ldots x_{n\tau_n} \ldots . P_0 \longrightarrow f(x_1, \ldots, x_n) = t_0$$
$$\vdots$$
$$\forall x_{1\tau_1} \ldots x_{n\tau_n} \ldots . P_n \longrightarrow f(x_1, \ldots, x_n) = t_n$$

  so daß beweisbar

  - $S \vdash \forall x_{1\tau_1} \ldots x_{n\tau_n} . P_i \wedge P_j \longleftrightarrow \bot, \forall i \neq j$
  - $S \vdash \forall x_{1\tau_1} \ldots x_{n\tau_n} . P_1 \vee \ldots \vee P_n$

Terminierungsbeweise – Idee

- Die natürlichen Zahlen sind frei erzeugt über 0 und s:
- Jedem Grundterm über $\mathbb{N}$ kann eine größe zugeordnet werden über die Anzahl der Konstruktoren.
- Zeige für rekursiv definierte Funktionen auf $\mathbb{N}$, dass die rekursiven Argument in rekursiven Funktionsaufrufen kleiner sind bezüglich der Ordnung auf den natürlichen Zahlen unter der entsprechenden Bedingung P_i.

Terminierung

- Beispiele:
  - half(x) eine Hypothese pro Rekursionsgleichung
  - fib(x): mehrere Hypothesen pro Rekursionsgleichung
  - gcd(x, y): lexicographische Ordnung
- Beweise alle Hypothesen im Kalkül. Terminierung gilt relativ zur Terminierung der anderen involvierten Funktionen und Prädikate.
- Analog für Prädikate auf $\mathbb{N}$ mit bedingten Äquivalenzen
- Allgemeine Typen: für frei erzeugte Datentypen kann Abbildung in natürliche Zahlen definiert werden, die die Anzahl der Konstruktoren zählt. Damit lässt sich das Terminierungsverfahren auf all frei erzeugten Datentypen erweitern

Erweiterung um Totale, Terminierende Funktionen is Konservativ

Definition 7 (Funktions- und Prädikatsdefinitionen)

Sei $S = ((\mathcal{T}, \mathcal{F}, \mathcal{P}), \Phi)$ eine Spezifikation, $f : \tau_1 \times \cdots \times \tau_n \to \tau_0 \notin \mathcal{F}$ ($\tau_i \in \mathcal{T}$) und $\Psi \in \mathcal{F}orm_{\Sigma \cup \{f\}}$. Dann ist eine Erweiterung $S' = ((\mathcal{T}, \mathcal{F}', \mathcal{P}), \Phi')$ eine Funktionsdefinition gdw.

- Ψ ist eine eindeutig und totale Definition für f
- f ist terminierend und alle in der Definition von f vorkommenden Funktionen und Prädikate sind terminierend
- $\Phi' = \Phi \cup \Psi$
- $\mathcal{F}' = \mathcal{F} \cup \{f : \tau_1 \times \cdots \times \tau_n \to \tau_0\}$

Analog für Prädikatsdefinitionen.

Lemma 8

Funktionsdefinitionen bzw. Prädikatsdefinitionen sind konservativ

Sicheres Spezifikationsprinzip

- Beginne mit Basistheorie mit $\mathbb{N}$ und wohlfundiertem Induktionsschemata für $\mathbb{N}$ (getypte Prädikatenlogik mit Typ $\mathbb{N}$ und Induktionsschemata!)
  - $\mathbb{N}$ hat beweisbar nicht-leere Trägermenge
- Erweitere nur konservativ um
  - totale, terminierende Funktionen und Prädikate
  - Typdefinitionen (ausgehend von $\mathbb{N}$)
    - Erbt Induktionsprinzip über Umweg über $\mathbb{N}$
- Erlaubt Definition von Konstruktoren für neue Typen
  - Terminierung: Abbildung der Termgröße auf $\mathbb{N}$ mittels geschachtelter Anwendung von Rep_t
  - Wenn freie Erzeugtheit des neuen Typs beweisbar, dann folgt Induktionsschema direkt auf dem neuen Typ
- Damit hat man garantiert immer konsistente Spezifikationen (= Modellierung).