Formale Methoden der Softwaretechnik 1
Vorlesung vom 18.11.09:
Logik Höherer Stufe in Isabelle

Christoph Lüth, Lutz Schröder

Universität Bremen

Wintersemester 2009/10

Fahrplan

- Teil I: Grundlagen der Formalen Logik
- Teil II: Arbeiten mit Isabelle
  - Grundlagen von Isabelle
  - Logik höherer Ordnung in Isabelle
  - Isabelle/HOL
  - Beweise über funktionale Programme in Isabelle/HOL
  - Beweisen mit Isabelle: Simplifikation, Taktiken
- Teil III: Modellierung imperative Programme

Fahrplan

- Alles über Logik höherer Stufe (Higher-order Logic, HOL):
  - Typen und Terme
  - Die Basis-Axiome
  - Definierte Operatoren

Logik höherer Stufe

- Ziel: Formalisierung von Mathematik
  - "Logik für Erwachsene"
- Problem: Mögliche Inkonsistenz (Russel's Paradox)
- Lösung: Restriktion vs. Ausdrucksstärke
- Alternative Grundlagen:
  - Andere Typtheorien (Martin-Löf, Calculus of Constructions)
  - Ungetypte Mengenlehre (ZFC)
- HOL: guter Kompromiss, weit verbreitet.
  - Klassische Logik höherer Stufe nach Church
  - Schwächer als ZFC, stärker als Typtheorien

Warum Logik höherer Stufe?

- Aussagenlogik: keine Quantoren
- Logik 1. Stufe: Quantoren über Terme

$$\forall x\, y.\, x = y \longrightarrow y = x$$

- Logik 2. Stufe: Quantoren über Prädikaten und Funktionen

$$\forall P.(P\,0 \wedge \forall x.P\,x \longrightarrow P\,(S\,x)) \longrightarrow \forall x.P\,x$$

- Logik 3. Stufe: Quantoren über Argumenten von Prädikaten
- Logik höherer Stufe (HOL): alle endlichen Quantoren
  - Keine wesentlichen Vorteile von Logik 2. Ordnung

Vermeidung von Inkonsistenzen

- Russell's Paradox
  - $R = \{X \mid X \notin X\}$
  - Abhilfe: Typen
- Gödel's 2. Unvollständigkeitssatz:
  - Jede Logik, die ihre eigene Konsistenz beweist, ist inkonsistent.
- Unterscheidung zwischen Termen und Aussagen
  - Dadurch **in** HOL keine Aussage **über** HOL

Typen

- Typen $\mathcal{T}ype$ gegeben durch
  - Typkonstanten: $c \in \mathcal{C}_{\mathcal{T}ype}$ (Menge $\mathcal{C}_{\mathcal{T}ype}$ durch Signatur gegeben)
    - $Prop, Bool \in \mathcal{C}_{\mathcal{T}ype}$: *Prop* alle Terme, *Bool* alle Aussagen
  - Typvariablen: $\alpha \in \mathcal{V}_{\mathcal{T}ype}$ (Menge $\mathcal{V}_{\mathcal{T}ype}$ fest)
  - Funktionen: $s, t \in \mathcal{T}ype$ dann $s \Rightarrow t$ in $\mathcal{T}ype$
- Konvention: Funktionsraum nach rechts geklammert
  $\alpha \Rightarrow \beta \Rightarrow \gamma$ für $\alpha \Rightarrow (\beta \Rightarrow \gamma)$

Terme

- Terme $\mathcal{T}erm$ gegeben durch
  - Konstanten: $c \in \mathcal{C}$ (Menge $\mathcal{C}$ durch Signatur gegeben)
  - Variablen: $v \in \mathcal{V}$
  - Applikation: $s, t \in \mathcal{T}erm$ dann $s\,t \in \mathcal{T}erm$
  - Abstraktion: $x \in \mathcal{V}, t \in \mathcal{T}erm$ dann $\lambda x.\, t \in \mathcal{T}erm$
- Konventionen: Applikation links geklammert, mehrfache Abstraktion
  $\lambda x\, y\, z.\, f\, x\, y\, z$ für $\lambda x.\, \lambda y.\, \lambda z.\, ((f\, x)\, y)\, z$

Basis-Syntax

$= \quad :: \alpha \Rightarrow \alpha \Rightarrow \mathit{Bool}$
$\longrightarrow :: \mathit{Bool} \Rightarrow \mathit{Bool} \Rightarrow \mathit{Bool}$
$\iota \quad :: (\alpha \Rightarrow \mathit{Bool}) \Rightarrow \alpha$

$\neg \quad :: \mathit{Bool} \Rightarrow \mathit{Bool}$
$\mathit{true} :: \mathit{Bool}$
$\mathit{false} :: \mathit{Bool}$
$\mathit{if} \quad :: \mathit{Bool} \Rightarrow \alpha \Rightarrow \alpha \Rightarrow \alpha$
$\forall \quad :: (\alpha \Rightarrow \mathit{Bool}) \Rightarrow \mathit{Bool}$
$\exists \quad :: (\alpha \Rightarrow \mathit{Bool}) \Rightarrow \mathit{Bool}$
$\wedge \quad :: \mathit{Bool} \Rightarrow \mathit{Bool} \Rightarrow \mathit{Bool}$
$\vee \quad :: \mathit{Bool} \Rightarrow \mathit{Bool} \Rightarrow \mathit{Bool}$

- Einbettung (wird weggelassen)
  $\mathit{trueprop} :: \mathit{Bool} \Rightarrow \mathit{Prop}$
- Basis-Operatoren: $=, \longrightarrow, \iota$
- Syntaktische Konventionen:
  - Bindende Operatoren: $\forall$, $\exists$, ι
    $\forall x.P \equiv \forall(\lambda x.P)$
  - Infix-Operatoren: $\wedge, \vee, \longrightarrow, =$
  - Mixfix-Operator:
    $\mathit{if}\ b\ \mathit{then}\ p\ \mathit{else}\ q \equiv \mathit{if}\ b\ p\ q$

Basis-Axiome I: Gleichheit

- Reflexivität:
$$\frac{}{t = t}\ \text{refl}$$
- Substitutivität:
$$\frac{s = t \quad P(s)}{P(t)}\ \text{subst}$$
- Extensionalität:
$$\frac{\forall x.fx = gx}{(\lambda x.fx) = (\lambda x.gx)}\ \text{ext}$$
- Einführungsregel:
$$\frac{}{(P \longrightarrow Q) \longrightarrow (Q \longrightarrow P) \longrightarrow (P = Q)}\ \text{iff}$$

Basis-Axiome II: Implikation und Auswahl

- Einführungsregel Implikation:
$$\frac{\begin{array}{c}[P] \\ \vdots \\ Q\end{array}}{P \longrightarrow Q}\ \text{impl}$$
- Eliminationsregel Implikation:
$$\frac{P \longrightarrow Q \quad P}{Q}\ \text{mp}$$
- Eliminationsregel Auswahloperator:
$$\frac{}{(\iota x.x = a) = a}\ \text{the\_eq}$$
- HOL ist klassisch:
$$\frac{}{(P = \mathit{true}) \vee (P = \mathit{false})}\ \text{true\_or\_false}$$

Die Basis-Axiome (Isabelle-Syntax)

refl : $t = t$
subst : $[\![s = t; P(s)]\!] \Longrightarrow P(t)$
ext : $[\![\bigwedge x.fx = gx]\!] \Longrightarrow (\lambda x.fx) = (\lambda x.gx)$
impl : $[\![P \Longrightarrow Q]\!] \Longrightarrow P \longrightarrow Q$
mp : $[\![P \longrightarrow Q; P]\!] \Longrightarrow Q$
iff : $(P \longrightarrow Q) \longrightarrow (Q \longrightarrow P) \longrightarrow (P = Q)$
the_eq : $(\iota x.x = a) = a$
true_or_false : $(P = \mathit{true}) \vee (P = \mathit{false})$

Abgeleitete Operatoren

$$\begin{aligned}
\mathit{true} &\equiv (\lambda x.x) = (\lambda x.x) \\
\forall P &\equiv (P = \lambda x.\mathit{true}) \\
\exists P &\equiv \forall Q.(\forall x.Px \longrightarrow Q) \longrightarrow Q \\
\mathit{false} &\equiv \forall P.P \\
\neg P &\equiv P \longrightarrow \mathit{false} \\
P \wedge Q &\equiv \forall R.(P \longrightarrow Q \longrightarrow R) \longrightarrow R \\
P \vee Q &\equiv \forall R.(P \longrightarrow R) \longrightarrow (Q \longrightarrow R) \longrightarrow R \\
\mathit{if}\ P\ \mathit{then}\ x\ \mathit{else}\ y &\equiv \iota z.(P = \mathit{true} \longrightarrow z = x) \wedge (P = \mathit{false} \longrightarrow z = y)
\end{aligned}$$

Erweiterungen

- Weitere Operatoren
- Weitere Typen: natürliche Zahlen, Datentypen
- Axiomatisch (vgl. Peano/Presburger in FOL)
  - Mögliche Inkonsistenzen
- Konserverative Erweiterung
  - Logik konsistentzerhaltend erweitern

Zusammenfassung

Logik höherer Stufe (HOL):

- Syntax basiert auf dem einfach getypten λ-Kalkül
- Drei Basis-Operatoren, acht Basis-Axiome
- Rest folgt durch konservative Erweiterung — nächstes Mal