Formale Methoden der Softwaretechnik
Vorlesung vom 13.05.2011: Isabelle — eine Einführung

Till Mossakowski & Christoph Lüth

Universität Bremen

Sommersemester 2011

Inhalt

- Heute: Übersicht auf (über) Isabelle
- Danach: systematische Einführung

Isabelle

- Weit verbreiteter Theorembeweiser
- Generisch: mehr als eine Logik
- Interaktiv: Beweis wird durch den Benutzer konstruiert und von Isabelle geprüft
- Heimatseite: `http://isabelle.in.tum.de/`

Geschichte

- Entstanden in Cambridge, entwickelt in Cambridge und München

Larry Paulson  Tobias Nipkow 

- Teil der LCF-Familie
- Erste Version 1988, seit Ende der 1990er weit verbreitet

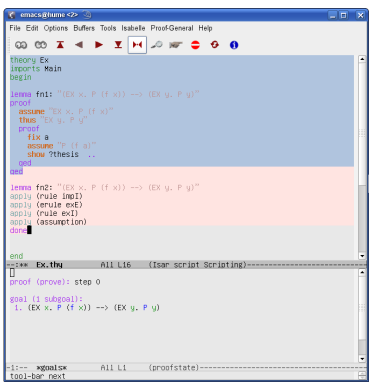
Architektur

- Implementiert in Standard ML (SML)
- Ca. 150 kloc Standard ML
- Ca. 200 kloc Beweisskripte
- Korrekt durch LCF-Design

Theorien

- Isabelle-Quellcode: Theorien
- Theorien bestehen aus
  - Definitionen
  - Behauptungen
  - Beweisen
- Isabelle liest Theorien und prüft sie
- Theorien sind hierarchisch strukturiert

Benutzung: ProofGeneral



Grundlagen von Isabelle

- Grundlage: getypter λ-Kalkül
- Unifikation und Matching
- Variablen, Formeln, Resolution

Formeln

- Formeln in Isabelle:

$$\frac{\phi_1, \ldots, \phi_n}{\psi} \qquad [\![\phi_1, \ldots, \phi_n]\!] \Longrightarrow \psi$$

  - $\phi_1, \ldots, \phi_n$ Formeln, ψ atomar
  - Theoreme: ableitbare Formeln
  - Ableitung von Formeln: Resolution, Instantiierung, Gleichheit
- Randbemerkung:
  - $\Longrightarrow$, $\bigwedge$, $\equiv$ formen Meta-Logik
  - Einbettung anderer Logiken möglich — generischer Theorembeweiser

Variablen

- Meta-Variablen: können unifiziert und beliebig instantiiert werden
- freie Variablen (fixed): beliebig aber fest
- Gebundene Variablen: Name beliebig (α-Äquivalenz)
- Meta-Quantoren: Isabelles Eigenvariablen

$$\frac{\bigwedge x.P(x)}{\forall x.P(x)}\ \mathit{alll} \qquad \texttt{!!x. P x ==> ALL x. P x}$$

  - Beliebig instantiierbar
  - Gültigkeit auf diese (Teil)-Formel begrenzt

Rückwärtsbeweis

- Ausgehend von Beweisziel ψ
- Beweiszustand ist $[\![\phi_1, \ldots, \phi_n]\!] \Longrightarrow \psi$
- $\phi_1, \ldots, \phi_n$: subgoals
- Beweisverfahren: Resolution, Termersetzung, Beweissuche
- Beweis endet wenn $n = 0$

HOL

- HOL: getypte Logik höherer Ordnung (nach Church und Gordon)
- " HOL = Funktionale Programmierung + Logik "
- In Isabelle:
  - Datentypdefinition
  - Funktionsdefinitionen
- Beispiel: einfache Listen selbstgemacht

Zusammenfassung

- Isabelle ist ein generischer, interaktiver Theorembeweiser
- HOL = FP + Logik
- Beweismethoden:
  - Regelkomposition
  - Induktion
  - Termersetzung
- Nächste Wochen: Systematische Einführung
  - Aussagenlogik $\rightsquigarrow$ Prädikatenlogik $\rightsquigarrow$ Logik höherer Stufe $\rightsquigarrow$ Isabelle/HOL
  - Danach: Programmverifikation mit Isabelle