Bemerkungen zur Semantik und Mechanisierung von Logik höherer Stufe

Christoph Benzmüller

Universität des Saarlandes, Saarbrücken

Deduktionstreffen, Augsburg, 8. Oktober 2003

Logik erster Stufe

+ Semi-Entscheidbarkeit des Folgerungsbegriffs
+ entscheidbare Unterfragmente
+ entscheidbare, unitäre Unifikation
+ Unifikation als Unterprozess, Termindexing
+ gute Automatisierbarkeit
+ geeignete Semantik
+ Techniken zur Analyse von Kalkülen
- Ausdrucksschwäche, unnatürliche Kodierungen

Logik höherer Stufe

+ Ausdruckstärke, natürliche Formalisierungen
- Unentscheidbarkeit des Folgerungsbegriffs
- Unentscheidbarkeit der Unifikation
- Unifikation nicht mehr nur reiner Unterprozess
- wenig gut untersuchte Kalküle
- Automatisierung komplex und schwierig
- wenig gut untersuchte Semantik(en)
- wenig geeignete Beweistechniken

Motivation

Ist die Situation wirklich so aussichtslos?

Ist es gerechtfertigt, dass sich die Deduktionsgemeinde so stark auf die Mechanisierung der ersten Stufe (und ihrer Unterfragmente) konzentriert?

Müssen wir unsere Anwender (welche?) notwendigerweise an unnatürliche Kodierungen gewöhnen?

Übersicht zum Vortrag

- Logik höherer Stufe (klassische Typtheorie) basierend auf Church's einfach getypten λ-Kalkül
- Landschaft von Semantiken (Modellklassen) für klassische Logik höherer Stufe
- Beweistechnik: Abstrakte Konsistenzmethode
- Kalküle
- Kommentar zu Trend: eingeschränkte Erweiterungen der ersten Stufe in Richtung höherer Stufe

HOL: Klassische Logik höherer Stufe

- **Typen:** (i) $\{i, o\} \in \mathcal{T}$ (ii) $\alpha, \beta \in \mathcal{T} \rightsquigarrow \alpha \to \beta \in \mathcal{T}$
- **Die Sprache** HOL:
  - (i) Abzählbare getypte Variablen: $V_\alpha \subseteq$ HOL (Notation X_α)
  - (ii) Getypte Konstanten: $C_\alpha \subseteq$ HOL (Notation d_α)

    Gefordert: $\neg \in C_{o\to o}, \vee \in C_{o\to(o\to o)}, \Pi \in C_{(\alpha\to o)\to o}$
  - (iii) Applikationen: $\mathbf{A}_{\alpha\to\beta}, \mathbf{B}_\alpha \in$ HOL $\rightsquigarrow (\mathbf{A}\ \mathbf{B})_\beta \in$ HOL
  - (iii) Abstraktionen: $X_\alpha \in V_\alpha, \mathbf{A}_\beta \in$ HOL $\rightsquigarrow (\lambda X.\mathbf{A})_{\alpha\to\beta} \in$ HOL
- **Normalformen** (z.B. $\beta\eta$-Normalform / $\beta\eta$-Kopfnormalform):
  - (i) α-Konversion: $\lambda X_\gamma.\mathbf{A} \longleftrightarrow^\alpha \lambda Y_\gamma.\mathbf{A}[Y/X]$
  - (ii) λ-Konversion: $(\lambda X_\gamma.\mathbf{A})\ \mathbf{B}_\gamma \longrightarrow^\beta \mathbf{A}[\mathbf{B}/X]$

    (falls X nicht frei in $\mathbf{A}$) $\lambda X.\mathbf{A}\ X \longrightarrow^\eta \mathbf{A}$

Einige Anmerkungen

- Leibniz-Definition der Gleichheit

$$\doteq^{\alpha} \;:= (\lambda X_\alpha, Y_\alpha\text{▪}\, \forall P_{\alpha\to o}\text{▪}\, P\ X \Rightarrow P\ Y)$$

- Extensionalitätsaxiome

$$\forall F_{\alpha\to\beta}, G_{\alpha\to\beta}\text{▪}\, (\forall X_\beta\text{▪}\, F\ X \doteq G\ X) \Rightarrow F \doteq G$$

$$\forall A_o, B_o\text{▪}\, (A \equiv B) \Rightarrow (A \doteq B)$$

HOL: Semantik

Standardsemantik	Wähle	Erzwungen
Semantische Domänen	D_ι	$D_o = \{\bot, \top\}$, $D_{\alpha\to\beta} = \mathcal{F}(D_\alpha, D_\beta)$
Interpretation von Konst.	$I : (I_\alpha : C_\alpha \longrightarrow D_\alpha)_{\alpha\in\mathcal{T}}$	$I(\neg)$, $I(\vee)$, $I(\Pi)$ wie üblich
Variablenbelegung	$\varphi : (\varphi_\alpha : V_\alpha \longrightarrow D_\alpha)_{\alpha\in\mathcal{T}}$	
Interpretation von Termen I_φ : HOL $\longrightarrow D$ def. durch	$I_\varphi(X) = \varphi(X)$, $I_\varphi(c) = I(c)$, $I_\varphi(\mathbf{A}\ \mathbf{B}) = I_\varphi(A)@I_\varphi(B)$, $I_\varphi(\lambda X_\alpha.\mathbf{B}_\beta) = f \in D_{\alpha\to\beta}$, so dass $\forall a : f@a = I_{\varphi[a/X]}(\mathbf{B})$	

Henkinsemantik	Wähle	Erzwungen
Semantische Domänen	D_ι, $D_{\alpha\to\beta} \subseteq \mathcal{F}(D_\alpha, D_\beta)$	$D_o = \{\bot, \top\}$, Totalität von I_φ
Interpretation von Konst.	wie oben	wie oben
Variablenbelegung	wie oben	
Interpretation von Termen	wie oben	

Modell: $\mathcal{M} = (\mathcal{D} : \{D_\alpha\}, \mathcal{I} : \{I_\alpha\})$; Erfüllbarkeit und Gültigkeit wie üblich

Logik höherer Stufe: Probleme

Problem 1:

Es gibt keinen gut geeigneten semantischen Bezugsrahmen für Logik höherer Stufe.

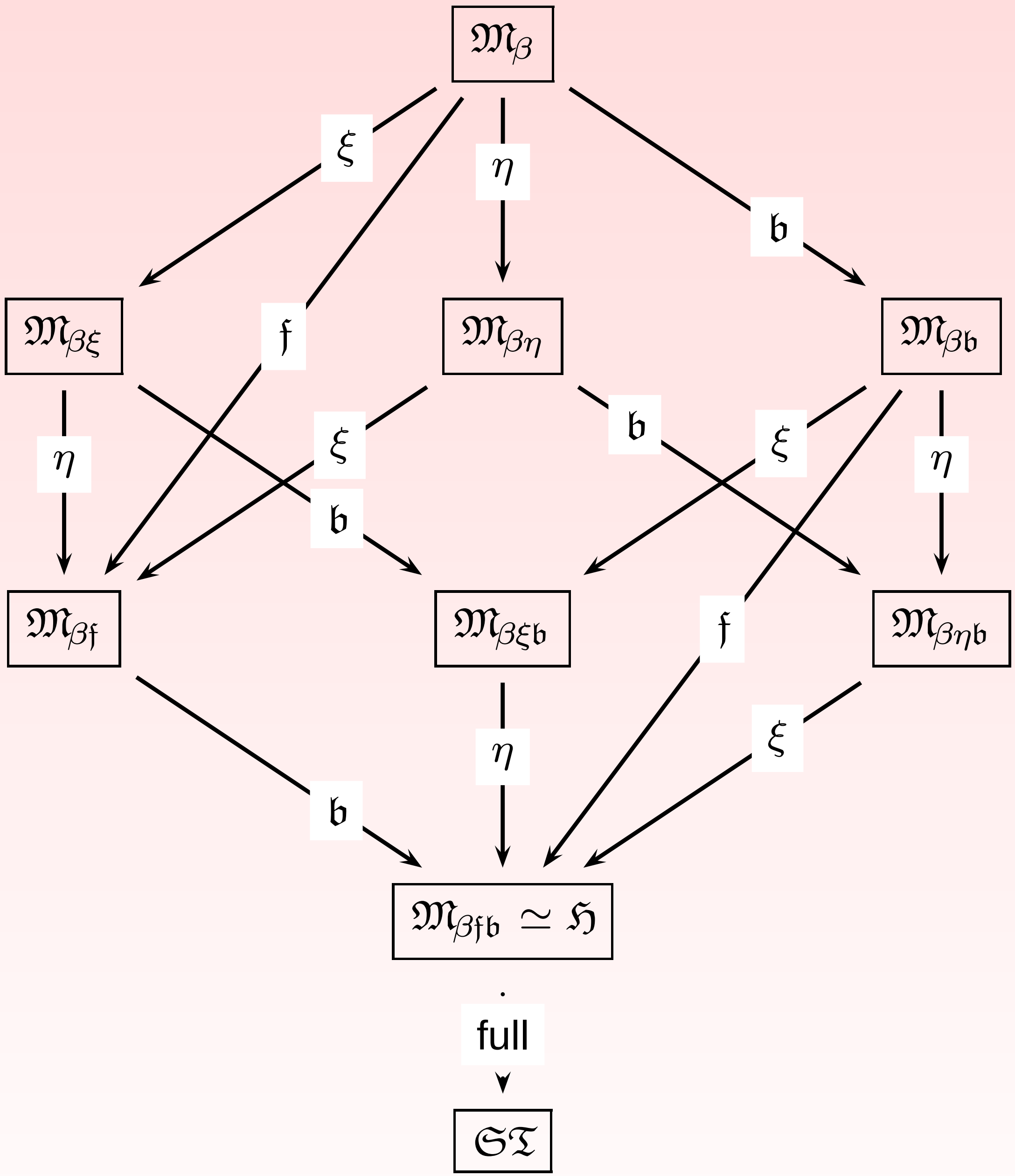
Wirklich?

Semantiken für HOL

Situation bis vor kurzem:

- Standardsemantik
  - volle Funktionsuniversen
  - keine vollständigen Kalküle
  - funktionale und Boole'sche Extensionalität gelten
- Henkinsemantik [Henkin-50]
  - partielle Funktionsuniversen, Denotatpflicht
  - vollständige Kalküle
  - funktionale und Boole'sche Extensionalität gelten
- . . . Lücke . . .
- Andrews v-Complexes [Andrews-71]
  - funktionale und Boole'sche Extensionalität gelten nicht

Semantiken für HOL



1995 — 2003: Entwicklung einer Landschaft von Semantiken für die Logik höherer Stufe
[Kohlhase-Diss-94]
[Benzmüller-Diss-99]
[Brown-Diss-??]
[BenzmüllerBrownKohlhase-JSL]

$\mathfrak{b}$: Boole'sche Extensionalität

$\mathfrak{f}$: Funktionale Extensionalität

η: Modelle respektieren η-Konversion

ξ: Denotationen von $\lambda X.\, \mathbf{M}$ und $\lambda X.\, \mathbf{N}$ sind identisch, falls Denotationen von $\mathbf{M}$ und $\mathbf{N}$ es sind für jede Belegung von von X.

Semantiken: Anwendungen

Henkinsemantik

- Mathematik

Verzicht auf Boole'sche Extensionalität

- Linguistik, intensionale Kontexte
- "Ich glaube, das ich den Morgenstern sehe"
  versus
  "Ich glaube, das ich den Abendstern sehe"

Verzicht auf Funktionale Extensionalität

- Programmiersprachen, Analyse von Programmen
- $\lambda X_{list}.\ X$ versus $\lambda X_{list}.\ (reverse\ (reverse\ X))$

Logik höherer Stufe: Probleme

Problem 2:

Es gibt keine starken Beweistechniken, die eine semantische Analyse von Kalkülen für Logik höherer Stufe unterstützen.

Wirklich?

Abstrakte Konsistenz

- Vollständigkeitsanalysen in Logik höherer Stufe sind ungleich schwerer als in Logik erster Stufe
- Direkte semantische Analyse ist sehr aufwendig
- Abstrakte Konsistenzmethode:
  Beweistechnik die Syntax und Semantik verbindet, ermöglicht z.B. Vollständigkeitsanalyse durch syntaktische Kriterien
  - Logik erster Stufe:
    [Hintikka-55, Smullyan-63, Smullyan-68]
  - Logik höherer Stufe:
    [Andrews-71] nur für υ-Komplexe

Abstrakte Konsistenz

$\nabla_c, \nabla_\beta, \nabla_\neg, \nabla_\vee, \nabla_\wedge, \nabla_\forall, \nabla_\exists, \nabla_{sat}$

$$\begin{tikzcd}
 & & \boxed{\mathfrak{M}_\beta} \arrow[dl, "\xi"'] \arrow[ddl, "\mathfrak{f}"] \arrow[d, "\eta"] \arrow[dr, "\mathfrak{b}"] & & \\
\nabla_\xi & \boxed{\mathfrak{M}_{\beta\xi}} \arrow[d, "\eta"] \arrow[dr, "\mathfrak{b}"] & \boxed{\mathfrak{M}_{\beta\eta}}\ \nabla_\eta \arrow[dl, "\xi"'] \arrow[dr, "\mathfrak{b}"] & \boxed{\mathfrak{M}_{\beta\mathfrak{b}}} \arrow[dl, "\xi"'] \arrow[ddl, "\mathfrak{f}"] \arrow[d, "\eta"] & \nabla_\mathfrak{b} \\
\nabla_\mathfrak{f} & \boxed{\mathfrak{M}_{\beta\mathfrak{f}}} \arrow[dr, "\mathfrak{b}"] & \boxed{\mathfrak{M}_{\beta\xi\mathfrak{b}}} \arrow[d, "\eta"] & \boxed{\mathfrak{M}_{\beta\eta\mathfrak{b}}} \arrow[dl, "\xi"'] & \\
 & & \boxed{\mathfrak{M}_{\beta\mathfrak{f}\mathfrak{b}} \simeq \mathfrak{H}} \arrow[d, dotted, "\text{full}"] & & \\
 & & \boxed{\mathfrak{ST}} & &
\end{tikzcd}$$

[Kohlhase-Diss-94]
[Benzmüller-Diss-99]
[Brown-Diss-??]
[BenzmüllerBrownKohlhase-JSL]

Abstrakte Konsistenz

Let Γ_Σ be a class of sets of HOL-sentences and $\Phi \in \Gamma_\Sigma$.

We define: ($\Phi * \mathbf{A}$ stands for $\Phi \cup \{\mathbf{A}\}$)

∇_c If $\mathbf{A}$ is atomic, then $\mathbf{A} \notin \Phi$ or $\neg\mathbf{A} \notin \Phi$.

$\nabla_\neg$ If $\neg\neg\mathbf{A} \in \Phi$, then $\Phi * \mathbf{A} \in \Gamma_\Sigma$.

∇_β If $\mathbf{A} \equiv_\beta \mathbf{B}$ and $\mathbf{A} \in \Phi$, then $\Phi * \mathbf{B} \in \Gamma_\Sigma$.

∇_η If $\mathbf{A} \equiv_{\beta\eta} \mathbf{B}$ and $\mathbf{A} \in \Phi$, then $\Phi * \mathbf{B} \in \Gamma_\Sigma$.

$\nabla_\vee$ If $\mathbf{A} \vee \mathbf{B} \in \Phi$, then $\Phi * \mathbf{A} \in \Gamma_\Sigma$ or $\Phi * \mathbf{B} \in \Gamma_\Sigma$.

$\nabla_\wedge$ If $\neg(\mathbf{A} \vee \mathbf{B}) \in \Phi$, then $\Phi * \neg\mathbf{A} * \neg\mathbf{B} \in \Gamma_\Sigma$.

$\nabla_\forall$ If $\Pi^\alpha\mathbf{F} \in \Phi$, then $\Phi * \mathbf{F}\mathbf{W} \in \Gamma_\Sigma$ for each $\mathbf{W} \in \mathit{cwff}_\alpha(\Sigma)$.

$\nabla_\exists$ If $\neg\Pi^\alpha\mathbf{F} \in \Phi$, then $\Phi * \neg(\mathbf{F}w) \in \Gamma_\Sigma$ for any parameter $w_\alpha \in \Sigma_\alpha$ which does not occur in any sentence of Φ.

$\nabla_\mathfrak{b}$ If $\neg(\mathbf{A} \doteq^o \mathbf{B}) \in \Phi$, then $\Phi * \mathbf{A} * \neg\mathbf{B} \in \Gamma_\Sigma$ or $\Phi * \neg\mathbf{A} * \mathbf{B} \in \Gamma_\Sigma$.

∇_ξ If $\neg(\lambda X_\alpha.\, \mathbf{M} \doteq^{\alpha\to\beta} \lambda X_\alpha.\, \mathbf{N}) \in \Phi$, then $\Phi * \neg([w/X]\mathbf{M} \doteq^\beta [w/X]\mathbf{N}) \in \Gamma_\Sigma$ for any parameter $w_\alpha \in \Sigma_\alpha$ which does not occur in any sentence of Φ.

$\nabla_\mathfrak{f}$ If $\neg(\mathbf{G} \doteq^{\alpha\to\beta} \mathbf{H}) \in \Phi$, then $\Phi * \neg(\mathbf{G}w \doteq^\beta \mathbf{H}w) \in \Gamma_\Sigma$ for any parameter $w_\alpha \in \Sigma_\alpha$ which does not occur in any sentence of Φ.

∇_{sat} Either $\Phi * \mathbf{A} \in \Gamma_\Sigma$ or $\Phi * \neg\mathbf{A} \in \Gamma_\Sigma$.

Abstrakte Konsistenz

Definition (Abstrakte Konsistenzklasse für Henkinsemantik)

Sei Γ_Σ eine Teilmengenabgeschlossene Klasse von Mengen von HOL-Propositionen. Γ_Σ muss $\nabla_c, \nabla_\neg, \nabla_\beta, \nabla_\vee, \nabla_\wedge, \nabla_\forall, \nabla_\exists$, $\nabla_\mathfrak{f}, \nabla_\mathfrak{b}$ erfüllen.

Theorem (Modellexistenzsatz für Henkinsemantik)

Falls eine Menge Φ von HOL-Propositionen Element einer abstrakten Konsistenzklasse für Henkinsemantik ist, dann existiert ein Henkinmodell für Φ

Technik (Henkinvollständigkeit für Kalkül K)

- Zeige: Klasse der Mengen K-konsistenter (d.h. in K nicht wiederlegbarer) HOL-Propositionen ist Abstrakte Konsistenzklasse für Henkinsemantik.
- Einfaches Korollar: Henkinvollständigkeit von K

Interaktionsorientierte Kalküle

Korrekte und Vollständige Kalküle für Landschaft von Semantiken

- ND: [BenzmüllerBrownKohlhase-JSL]
  Korrektheit und Vollständigkeit wird mittels abstrakter Konsistenzmethode auf nur 1 Seite gezeigt
- Sequenzen: Arbeit noch nicht veröffentlicht

ND Kalküle: Vollständigkeit

Auszug aus Vollständigkeitsbeweis ...

∇_β: Let $\mathbf{A} \in \Phi$ and $\Phi * \mathbf{A}{\downarrow_\beta}$ be $\mathfrak{NK}_*$-inconsistent. That is, $\Phi * \mathbf{A}{\downarrow_\beta} \Vdash \mathbf{F}_o$. By $\mathfrak{NK}(\neg I)$, we know $\Phi \Vdash \neg\, \mathbf{A}{\downarrow_\beta}$. Since $\mathbf{A} \in \Phi$, we know $\Phi \Vdash \mathbf{A}{\downarrow_\beta}$ by $\mathfrak{NK}(Hyp)$ and $\mathfrak{NK}(\beta)$. So, by $\mathfrak{NK}(\neg E)$ we know $\Phi \Vdash \mathbf{F}_o$ and Φ is $\mathfrak{NK}_*$-inconsistent.

$\nabla_\mathfrak{b}$: We argue by contradiction. Assume that $\neg \mathbf{A} \doteq^o \mathbf{B} \in \Phi$ but both $\Phi * \neg \mathbf{A} * \mathbf{B} \notin \Gamma_\Sigma^*$ and $\Phi * \mathbf{A} * \neg \mathbf{B} \notin \Gamma_\Sigma^*$. So both are $\mathfrak{NK}_*$-inconsistent and we have $\Phi * \mathbf{A} \Vdash \mathbf{B}$ and $\Phi * \mathbf{B} \Vdash \mathbf{A}$ by $\mathfrak{NK}(Contr)$. By $\mathfrak{NK}(\mathfrak{b})$, we have $\Phi \Vdash (\mathbf{A} \doteq^o \mathbf{B})$. Since $\neg(\mathbf{A} \doteq^o \mathbf{B}) \in \Phi$, Φ is $\mathfrak{NK}_*$-inconsistent.

∇_{sat}: Let $\Phi * \mathbf{A}$ and $\Phi * \neg \mathbf{A}$ be $\mathfrak{NK}_*$-inconsistent. We show that Φ is $\mathfrak{NK}_*$-inconsistent. Using $\mathfrak{NK}(\neg I)$, we know $\Phi \Vdash \neg \mathbf{A}$ and $\Phi \Vdash \neg\neg \mathbf{A}$. By $\mathfrak{NK}(\neg E)$, we have $\Phi \Vdash \mathbf{F}_o$.

Saturation und Cut

Saturationsbedingung ist problematisch für maschinenorientierte Kalküle:

- erfordert Beweistechniken, die ebenso stark sein müssen wie die der Cut-Elimination
- deshalb alternative Bedingungen entwickelt basierend auf Ideen der Kalküle in [Benzmüller-Diss-99]; noch nicht veröffentlicht

Logik höherer Stufe: Probleme

Problem 3:

Die wichtigsten Herausforderungen bei der Automatisierung von Logik höherer Stufe

- Gleichheit und Extensionalität
- Instanziierung von Mengenvariablen

sind nur schwer in den Griff zu bekommen.

Wirklich?

Extensionale Resolution

1995 — 1999: Extensionale Resolution höherer Stufe
[BenzmüllerKohlhase-CADE-98] [Benzmüller-Diss-99]

- In Resolution höherer Stufe [Andrews71, Huet73] blinde Suche mit Extensionalitätsaxiomen
- Huet: Nachgelagerte Prä-Unifi kation + Extensionalitätsaxiome
- Nun zielgerichteter Ansatz: Verzahnung von Beweissuche, (Prä-)Unifi kation, und Normalisierung

Extensionale Resolution

- Notation für Klauseln: $\mathbf{C} \vee [\mathbf{A}]^F \vee [\mathbf{B}]^T$

  Analogie zu Superposition: $\mathbf{C} \vee \mathbf{A} = F \vee \mathbf{B} = T$

- Keine primitive Gleichheit; nur Leibnizdefinition

- Unifikations-Constraints verwenden spezielles Symbol $=$ und haben negative Polarität (keine Resolution oder Faktorisierung auf diesen erlaubt)

  Beispiel: $\mathbf{C} \vee [X = \mathbf{A}]^F \vee [p\ \mathbf{A} = F\ \mathbf{X}]^F$

Extensionalitätsaxiome im Suchraum sind keine praktikable Lösung: ergäbe unendlich viele Axiome (Axiomenschema) mit flexiblen Literalen (d.h. Mengenvariablen an Kopfposition)

Extensionale Resolution

Klauselnormalisierung

$$\frac{\mathbf{C} \lor [\mathbf{A} \lor \mathbf{B}]^T}{\mathbf{C} \lor [\mathbf{A}]^T \lor [\mathbf{B}]^T} \lor^T \qquad \frac{\mathbf{C} \lor [\mathbf{A} \lor \mathbf{B}]^F}{\mathbf{C} \lor [\mathbf{A}]^F} \lor_l^F \qquad \frac{\mathbf{C} \lor [\mathbf{A} \lor \mathbf{B}]^F}{\mathbf{C} \lor [\mathbf{B}]^F} \lor_r^F$$

$$\frac{\mathbf{C} \lor [\neg \mathbf{A}]^T}{\mathbf{C} \lor [\mathbf{A}]^F} \neg^T \qquad \frac{\mathbf{C} \lor [\neg \mathbf{A}]^F}{\mathbf{C} \lor [\mathbf{A}]^T} \neg^F$$

$$\frac{\mathbf{C} \lor [\Pi^\alpha \mathbf{A}]^T \quad X_\alpha \text{ neue Variable}}{\mathbf{C} \lor [\mathbf{A}\ X]^T} \Pi^T$$

$$\frac{\mathbf{C} \lor [\Pi^\alpha \mathbf{A}]^F \quad \mathsf{sk}_\alpha \text{ Skolem-Term}}{\mathbf{C} \lor [\mathbf{A}\ \mathsf{sk}_\alpha]^F} \Pi^F$$

Diese Regeln können kombiniert werden zu Regel: $\mathbf{CNF}$

Extensionale Resolution

Resolutionsregeln

$$\frac{[\mathbf{N}]^\alpha \lor C \quad [\mathbf{M}]^\beta \lor D \quad \alpha \neq \beta}{C \lor D \lor [\mathbf{N} = \mathbf{M}]^F}\ Res$$

$$\frac{[\mathbf{N}]^\alpha \lor [\mathbf{M}]^\alpha \lor C \quad \alpha \in \{T, F\}}{[\mathbf{N}]^\alpha \lor C \lor [\mathbf{N} = \mathbf{M}]^F}\ Fac$$

$$\frac{[Q_\gamma \overline{\mathbf{U}^k}]^\alpha \lor C \quad \mathbf{P} \in \mathcal{AB}_\gamma^{\{\neg,\lor\} \cup \{\Pi^\beta | \beta \in \mathcal{T}^k\}}}{[Q_\gamma \overline{\mathbf{U}^k}]^\alpha \lor C \lor [Q = \mathbf{P}]^F}\ Prim^k$$

Extensionale Resolution

Unifi kationsregeln

$$\frac{C \vee [\mathbf{M}_{\alpha\to\beta} = \mathbf{N}_{\alpha\to\beta}]^F \quad s_\alpha \text{ Skolem-Term}}{C \vee [\mathbf{M}\ s = \mathbf{N}\ s]^F}\ Func$$

$$\frac{C \vee [h\overline{\mathbf{U}^n} = h\overline{\mathbf{V}^n}]^F}{C \vee [\mathbf{U}^1 = \mathbf{V}^1]^F \vee \ldots \vee [\mathbf{U}^n = \mathbf{V}^n]^F}\ Dec \qquad \frac{C \vee [\mathbf{A} = \mathbf{A}]^F}{C}\ Triv$$

$$\frac{C \vee [F_\gamma\overline{\mathbf{U}^n} = h\overline{\mathbf{V}}]^F \quad \mathbf{G} \in \mathcal{AB}^h_\gamma}{C \vee [F = \mathbf{G}]^F \vee [F\overline{\mathbf{U}} = h\overline{\mathbf{V}}]^F}\ Flex/Rigid$$

$$\frac{C \vee E \quad E \text{ gelöst für } C}{\mathbf{CNF}(\text{subst}_E(C))}\ Subst$$

Extensionale Resolution

Extensionalitätsregeln

$$\frac{C \vee [\mathbf{M}_o = \mathbf{N}_o]^F}{\mathbf{CNF}(C \vee [\mathbf{M}_o \equiv \mathbf{N}_o]^F)}\ Equiv$$

$$\frac{C \vee [\mathbf{M}_\alpha = \mathbf{N}_\alpha]^F \quad \alpha \in \{o, \iota\}}{\mathbf{CNF}(C \vee [\forall P_{\alpha \to o}\text{.}\ P M \Rightarrow P N]^F)}\ Leib$$

Extensionale Resolution

$$\forall B_{\alpha\to o}, C_{\alpha\to o}, D_{\alpha\to o}.\ B \cup (C \cap D) = (B \cup C) \cap (B \cup D)$$

Die Aussage wird negiert (Widerlegungsansatz) und die Defi nitionen
$\cup = \lambda A_{\alpha\to o}, B_{\alpha\to o}, X_{\alpha}.\ (A\ X) \vee (B\ X)$ $\qquad$ $\cap = \lambda A_{\alpha\to o}, B_{\alpha\to o}, X_{\alpha}.\ (A\ X) \wedge (B\ X)$
expandiert. Dann erfolgt Klauselnormalisierung zu Unifi kationsconstraint

$$C_1 : [\lambda X_{\alpha}.\ (b\ X) \vee ((c\ X) \wedge (d\ X)) = \lambda X_{\alpha}.\ ((b\ X) \vee (c\ X)) \wedge ((b\ X) \vee (d\ X)))]^F$$

Zielgerichtete funktionale und Boole'sche Extensionalitätsbehandlung

$$C_2 : [(b\ x) \vee ((c\ x) \wedge (d\ x)) \Leftrightarrow ((b\ x) \vee (c\ x)) \wedge ((b\ x) \vee (d\ x)))]^F$$

Klauselnormalisierung ergibt dann eine rein propositionale, d.h. entscheidbare, Menge von Klauseln und nur diese Klauseln befi nden sich nun noch im Suchraum von LEO. Insgesamt werden lediglich 33 Klauseln erzeugt und auf einem 2,5GHz schnellen PC werden 820ms für den Wiederlegungsbeweis benötigt.

Ähnlicher Beweis ergibt sich auch bei eingebetteten Propositionen

$$\forall P_{(\alpha\to o)\to o}, B_{\alpha\to o}, C_{\alpha\to o}, D_{\alpha\to o}.\ P(B \cup (C \cap D)) \Rightarrow P((B \cup C) \cap (B \cup D))$$

Extensionale Resolution

$$\forall P_{o\to o} \centerdot (P\ a_o) \wedge (P\ b_o) \Rightarrow (P\ (a_o \wedge b_o))$$

Negation und Normalisierung

$$\mathcal{C}_1 : [p\ a]^T \qquad \mathcal{C}_2 : [p\ b]^T \qquad \mathcal{C}_3 : [p\ (a \wedge b)]^F$$

Resolution zwischen $\mathcal{C}_1$ und $\mathcal{C}_3$ and zwischen $\mathcal{C}_2$ und $\mathcal{C}_3$

$$\mathcal{C}_4 : [p\ a = p\ (a \wedge b)]^F \qquad \mathcal{C}_5 : [p\ b = p\ (a \wedge b)]^F$$

Dekomposition

$$\mathcal{C}_6 : [a = (a \wedge b)]^F \qquad \mathcal{C}_7 : [b = (a \wedge b)]^F$$

Simultaner rekursiver Beweiseraufruf mit Regel Equiv und $\mathbf{CNF}$

$$\mathcal{C}_8 : [a]^F \vee [b]^F \qquad \mathcal{C}_9 : [a]^T \vee [b]^T \qquad \mathcal{C}_{10} : [a]^T \qquad \mathcal{C}_{11} : [b]^T$$

Extensionale Resolution

Weitere kleine Beispiele, die Henkinvollstänigkeit testen:

$$\forall F_{o\to o}\blacksquare\ (F \doteq \lambda X_o\blacksquare\ X_o)\vee(F \doteq \lambda X_o\blacksquare\ \neg X_o)\vee(F \doteq \lambda X_o\blacksquare\ \bot)\vee(F \doteq \lambda X_o\blacksquare\ \top)$$

$$\forall H_{o\to o}\blacksquare\ H\ \bot \doteq H\ (H\ \top \doteq H\ \bot)$$

Mengenbeispiele; insbesondere mit Potenzmengen

$\ldots$

Extensionale Paramodulation

1995 — 1999: Extensionale RUE-Resolution höherer Stufe
[Benzmüller-CADE-99] [Benzmüller-Diss-99]

- Notation wie bisher; neu ist logisches Symbol $=$ für primitive Gleichheit
- Identifi kation von Unifi kationsconstraints und negierten Gleichungen
- Alle Regeln für Extensionale Resolution behalten Gültigkeit; Resolution und Faktorisierung nicht erlaubt auf Unifi kationsconstraints
- Weitere Regeln für $=$ benötigt

Extensionale Paramodulation

Paramodulations Regeln

$$\frac{[\mathbf{A}[\mathbf{T}_\beta]]^\alpha \vee C \quad [\mathbf{L} =^\beta \mathbf{R}]^T \vee D}{[\mathbf{A}[\mathbf{R}]]^\alpha \vee C \vee D \vee [\mathbf{T} =^\beta \mathbf{L}]^F}\ Para$$

Positive Extensionalitätsregeln

$$\frac{\mathbf{C} \vee [\mathbf{M}_o = \mathbf{N}_o]^T}{C \vee [\mathbf{M}_o \Leftrightarrow \mathbf{N}_o]^T}\ Equiv'$$

$$\frac{C \vee [\mathbf{M}_{\alpha\to\beta} = \mathbf{N}_{\alpha\to\beta}]^T \quad X \text{ neue freie Variable}}{C \vee [\mathbf{M}\ X = \mathbf{N}\ X]^T}\ Func'$$

Differenzreduzierung

1995 — 1999: Extensionale RUE-Resolution höherer Stufe
[Benzmüller-Diss-99]

1998 — 2003: Differenzreduzierender Matrixkalkül
[Brown-Diss-??]

- Regeln für Extensionale Resolution
- Positive Extensionalitätsregeln
- Neu: Resolution und Faktorisierung erlaubt auf Unifi kationsconstraints

Eigenschaften der Kalküle

Korrektheit und Vollständigkeit

- Korrektheit der Kalküle für Henkin-Semantik
- Vollständigkeit für Henkin-Semantik bisher nur modulo zusätzlicher (unendlich verzweigender) FlexFlex-Regel

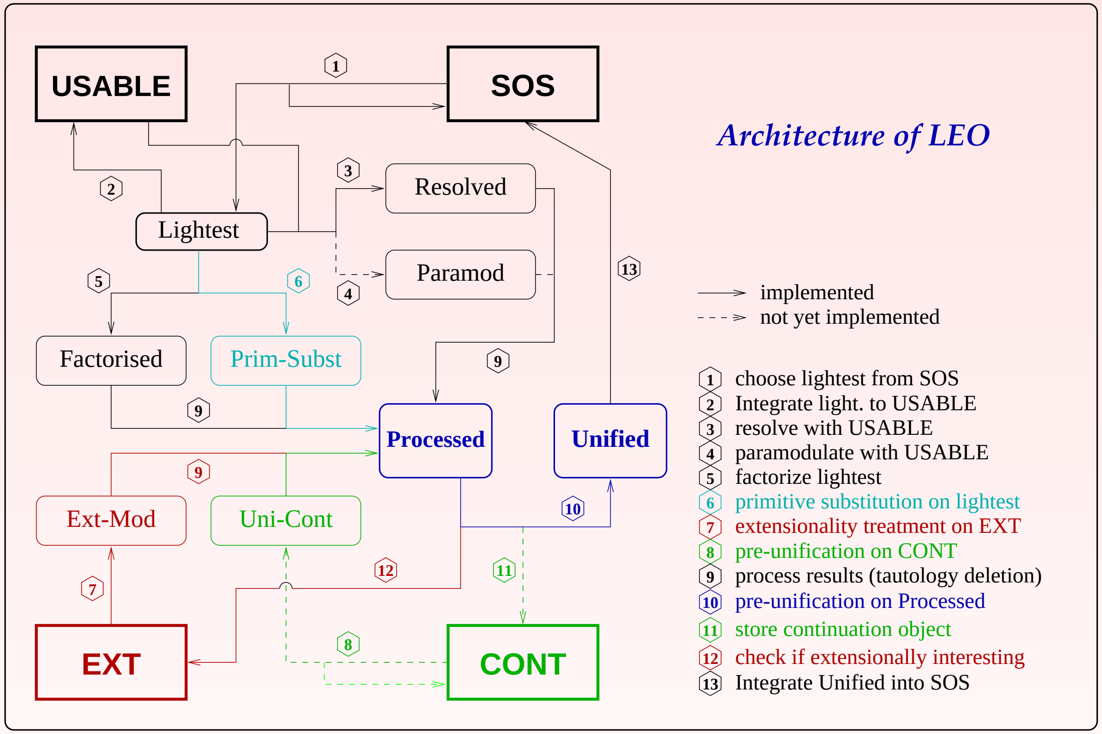
$$\frac{\mathbf{C} \vee [F_{\overline{\gamma^n} \to \alpha}\, \overline{\mathbf{U}^n} = H_{\overline{\delta^m} \to \alpha}\, \overline{\mathbf{V}^m}]^F \quad \mathbf{G} \in \mathcal{AB}^h_{\overline{\gamma^n} \to \alpha} \text{ für ein } h_\tau \in \mathcal{C}_\tau}{\mathbf{C} \vee [F\, \overline{\mathbf{U}^n} = H\, \overline{\mathbf{V}^m}]^F \vee [F = \mathbf{G}]^F}\ FlexFlex$$

Herausforderungen

- Vollständigkeit ohne FlexFlex-Regel
- Einschränkbarkeit der Beweiseraufrufe aus Unifi kation mit den Regeln Equiv und Leib auf Basistypen
- Adaption für andere Semantiken
- ...

Beweiser LEO

- [BenzmüllerKohlhase-CADE-98]
- Erweiterte Set-Of-Support-Architektur
- Vorschlag: Verteilte Architektur?



Instanziierung von Mengenvariablen

1998-2003: [Brown02-CADE, Brown-Diss]
zielgerichteter Ansatz für die Instanziierung von Mengenvariablen (Primitive Substitution)

- ersetzt bisherige á priori Ratestrategie (*choose-and-check*)
- nun á posteriori Methode beruhend auf Sammlung von Constraints und Wechselbeziehung zwischen Constraintstore und Beweissuche
- Interessanter Zusammenhang / Analogie:
  - á priori Methode $\Leftrightarrow$ explizite Induktion
  - á posteri Methode $\Leftrightarrow$ implizite Induktion

Logik höherer Stufe: Probleme

Ein derzeitiger Trend:

Eingeschränkte Erweiterungen von Verfahren der ersten Stufe in Richtung höherer Stufe; z.B.: “Superposition with Equivalence Reasoning” [GanzingerStuber-CADE-03]

Wie Sinnvoll?

Superposition mit Äquivalenzen

Superposition mit Equivalenzen

$$\frac{\bot = \top \vee \mathbf{C}}{\mathbf{C}} \ \bot\text{-Elim}$$

$$\frac{\alpha \vee \mathbf{C}}{\alpha_{1,2} \vee \mathbf{C}} \ \alpha\text{-Elim}$$

$$\frac{\beta \vee \mathbf{C}}{\beta_1 \vee \beta_2 \vee \mathbf{C}} \ \beta\text{-Elim}$$

$$\frac{\alpha \vee \mathbf{C}}{\gamma(z) \vee \mathbf{C}} \ \gamma\text{-Elim}$$ z freie Variable

$$\frac{\alpha \vee \mathbf{C}}{\delta(sk) \vee \mathbf{C}} \ \delta\text{-Elim}$$ sk Skolem-Term

$$\frac{(\mathbf{A} = \mathbf{B}) = \top \vee \mathbf{C}}{(\mathbf{A} = \mathbf{B}) \vee \mathbf{C}} \ =\text{-Elim}$$

Extensionale Resolution/Paramodulation

$\top$ und $\bot$ defi nierbar als $\exists X_o \mathbf{.}\ X \vee \neg X$ und $\neg\top$.

Diese Regeln korrespondieren zu den zuvor eingeführten Klauselnormalisierungsregeln bei Wahl der logischen Primitive $\neg, \vee, \forall$

Alle Literale sind immer mit Polarität annotiert; Regel nicht notwendig

Kein wesentlicher Unterschied hinsichtlich der Klauselnormalisierung;
Regeln können kombiniert werden zu Regel $\mathbf{CNF}$.

Superposition mit Äquivalenzen

$$\frac{l = r \vee \mathbf{C}}{l = \bot \vee r = \top \vee \mathbf{C}}$$ Pos-Equiv-Elim-1

korrespondiert zu Equiv'

$$\frac{l = r \vee \mathbf{C}}{l = \top \vee r = \bot \vee \mathbf{C}}$$ Pos-Equiv-Elim-2

korrespondiert zu Equiv'

$$\frac{(l = r) = \bot \vee \mathbf{C}}{l = \top \vee r = \bot \vee \mathbf{C}}$$ Neg-Equiv-Elim-1

korrespondiert zu Equiv

$$\frac{(l = r) = \bot \vee \mathbf{C}}{l = \bot \vee r = \top \vee \mathbf{C}}$$ Neg-Equiv-Elim-2

korrespondiert zu Equiv

$$\frac{(s = t) = \bot \vee \mathbf{C}}{\mathbf{C}\sigma}$$ Reflexivity-Res

korrespondiert zu Subst/Unifikation

$$\frac{(s[l'] = t) = \bot \vee \mathbf{C} \quad l = r \vee \mathbf{D}}{((s[r] = t) = \bot \vee \mathbf{C} \vee \mathbf{D})\sigma}$$ Neg-Superposition

korrespondiert zu Para (bzw. ableitbar)

$$\frac{s[l'] = t \vee \mathbf{C} \quad l = r \vee \mathbf{D}}{((s[r] = t) \vee \mathbf{C} \vee \mathbf{D})\sigma}$$ Pos-Superposition

korrespondiert zu Para

$$\frac{l = r \vee l' = r' \vee \mathbf{C}}{((r = r') = \bot \vee l' = r' \vee \mathbf{C})\sigma}$$ =-Factoring

subsumiert durch Faktorisierung + Unifikation

Superposition mit Äquivalenzen

Evaluation in [GanzingerStuber-CADE-03] durch Beispiele wie

$$\forall B_{\alpha\to o}, C_{\alpha\to o}, D_{\alpha\to o}.\ B \cup (C \cap D) = (B \cup C) \cap (B \cup D)$$

- in TPTP als *set171+3* enthalten
- nicht lösbar durch Vampire 5.0 (Gewinner des CASC Wettbewerbs 2002) oder E-Setheo csp02
- Saturate unter Verwendung der Superposition mit Äquivalenzen erzeugt 159 Klauseln bei der Beweissuche und benötigt 2.900ms auf einem 2Ghz Notebook für den Widerlegungsbeweis
- ZF-Axiome (z.B. auch Extensionalitätsaxiome) ständig im Suchraum
- keine Überführbarkeit in rein propositionales Problem

Zusammenfassung

- Verbesserte Grundlagen
  - Verschiedene Semantiken
  - Abstrakte Konsistenz als Beweismethode
  - Kalküle: ND, Sequenzen, Matrix, Resolution
  - zielgerichtete Extensionalitätsbehandlung
  - zielgerichtete Mengenvariablen-Instanziierung
- Viele interaktive Beweisassistenten basieren auf Logik höherer Stufe
- Aber: Starke Funding/Aktivitäten-Konzentration auf Erweiterungen von Systemen der ersten Stufe! Sinnvoll? Gerechtfertigt?

Bemerkung

- Superpositionsbeispiel illustriert mangelnde Präsenz und Kommunikation von Ansätzen zur Mechanisierung von Logik höherer Stufe

- Sinnvoller als eingeschränkte Erweiterungen von Verfahren der ersten Stufe:
  Konsequente Einbettung/Transformation von Verfahren der ersten Stufe in Systeme der höheren Stufe!
  Argument: Ausnutzen der Expressivität

- Ganz wichtig: CASC Wettbewerb ausbauen für höherer Stufe; isolierte Betrachtungen bei Vergleichsanalysen vermeiden!