Semantics and Automation of Higher-Order Logic

– Some Remarks –

Christoph Benzmüller

Department of Computer Science, Saarland University

Workshop on Logic, Proofs and Programs

17–18 June 2004, Nancy, France

UNIVERSITÄT DES SAARLANDES

First-order Logic

+ semi-decidable
+ decidable fragments
+ decidable, unitary unification
+ unification subordinated, termindexing
+ relatively simple to automate
+ well understood suitable semantics
+ well developed proof theory, proof techniques
- restricted expressivity, non-natural encodings

Higher-Order Logic

+ expressive, natural encodings
+ first-order logic as a fragment
- not decidable
- unification not decidable and not unitary
- unification no longer subordinated process
- no/few well developed and well understood calculi
- automation complex and challenging
- no well developed notion(s) of semantics
- no well developed proof theory, proof techniques

Motivation for Talk

Is the situation really hopeless?

Is it justifiable that the deduction community concentrates so strongly mainly on the automation of first-order logic as they did in last decades?

Talk Outline

- Higher-order logic (HOL, classical type theory) based on Church's simply typed λ-calculus
- Landscape of model classes (semantics) for HOL
- Proof techniques: abstract consistency method
- Calculi for HOL
- Comment to a recent trend: restricted extensions of first-order reasoning in direction of higher-order reasoning

HOL: Classical Type Theory

- Types: (i) $\{\mathsf{i},\mathsf{o}\} \in \mathcal{T}$ (ii) $\alpha,\beta \in \mathcal{T} \quad \rightsquigarrow \quad \alpha \to \beta \in \mathcal{T}$
- The language HOL:
  - (i) Countable sets of typed variables: $\mathsf{V}_\alpha \subseteq \mathsf{HOL}$ (Notation X_α)
  - (ii) Typed constants: $\mathsf{C}_\alpha \subseteq \mathsf{HOL}$ (Notation d_α)
    Required: $\neg \in \mathsf{C}_{\mathsf{o}\to\mathsf{o}}, \vee \in \mathsf{C}_{\mathsf{o}\to(\mathsf{o}\to\mathsf{o})}, \Pi \in \mathsf{C}_{(\alpha\to\mathsf{o})\to\mathsf{o}}$
  - (iii) Application: $\mathsf{A}_{\alpha\to\beta}, \mathsf{B}_\alpha \in \mathsf{HOL} \quad \rightsquigarrow \quad (\mathsf{A}\ \mathsf{B})_\beta \in \mathsf{HOL}$
  - (iii) Abstraction: $\mathsf{X}_\alpha \in \mathsf{V}_\alpha, \mathsf{A}_\beta \in \mathsf{HOL} \quad \rightsquigarrow \quad (\lambda \mathsf{X}.\mathsf{A})_{\alpha\to\beta} \in \mathsf{HOL}$
- Normal forms (e.g. $\beta\eta$-normal form / $\beta\eta$-head normal form):
  - (i) α-conversion: $\lambda \mathsf{X}_\gamma.\mathsf{A} \longleftrightarrow^\alpha \lambda \mathsf{Y}_\gamma.\mathsf{A}[\mathsf{Y}/\mathsf{X}]$
  - (ii) β-conversion, η-conversion: $(\lambda \mathsf{X}_\gamma.\mathsf{A})\ \mathsf{B}_\gamma \longrightarrow^\beta \mathsf{A}[\mathsf{B}/\mathsf{X}]$
    (if X not free in A) $\lambda \mathsf{X}.\mathsf{A}\ \mathsf{X} \longrightarrow^\eta \mathsf{A}$

Equality and Extensionality

- Leibniz definition of equality

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

- Functional extensionality

  $EXT^{\doteq}_{\alpha\to\beta} := \forall F_{\alpha\to\beta} . \forall G_{\alpha\to\beta} (\forall X_\alpha . F\ X \doteq G\ X) \Rightarrow F \doteq G \quad \overset{CNF}{\rightsquigarrow}$

  $\mathcal{C}_1 : [p_{\beta\to o}\ (F\ s_\alpha)]^T \vee [P_{(\alpha\to\beta)\to o}\ F]^F \vee [P_{(\alpha\to\beta)\to o}\ G]^T,$

  $\mathcal{C}_2 : [p_{\beta\to o}\ (G\ s_\alpha)]^F \vee [P_{(\alpha\to\beta)\to o}\ F]^F \vee [P_{(\alpha\to\beta)\to o}\ G]^T$

- Boolean extensionality

  $EXT^{\doteq}_{o} := \forall A_o . \forall B_o . (A \Leftrightarrow B) \Leftrightarrow A \doteq^{o} B \quad \overset{CNF}{\rightsquigarrow}$

  $\mathcal{C}_1 : [A]^F \vee [B]^F \vee [P\ A]^F \vee [P\ B]^T,\ \mathcal{C}_2 : [A]^T \vee [B]^T \vee [P\ A]^F \vee [P\ B]^T,\ \mathcal{C}_3 : [A]^F \vee [B]^T \vee [p\ A]^T,\ \mathcal{C}_4 : [A]^F \vee [B]^T \vee [p\ B]^F,\ \mathcal{C}_5 : [A]^T \vee [B]^F \vee [p\ A]^T,\ \mathcal{C}_6 : [A]^T \vee [B]^F \vee [p\ B]^F$

HOL: Semantics

Standard semantics	Choose	Required
Semantical domains	D_ι	$D_o = \{\bot, \top\}$, $D_{\alpha\to\beta} = \mathcal{F}(D_\alpha, D_\beta)$
Interpretation of const.	$I : (I_\alpha : C_\alpha \longrightarrow D_\alpha)_{\alpha\in\mathcal{T}}$	$I(\neg), I(\vee), I(\Pi)$ as usual
Variable assignment	$\varphi : (\varphi_\alpha : V_\alpha \longrightarrow D_\alpha)_{\alpha\in\mathcal{T}}$	
Interpretation of terms	$I_\varphi(X) = \varphi(X)$, $I_\varphi(c) = I(c)$, $I_\varphi(A\ B) = I_\varphi(A)@I_\varphi(B)$,	
I_φ : HOL $\longrightarrow$ D def. by	$I_\varphi(\lambda X_\alpha.B_\beta) = f \in D_{\alpha\to\beta}$, such that $\forall a : f@a = I_{\varphi[a/X]}(B)$	

Henkin semantics	Choose	Required
Semantical domains	D_ι, $D_{\alpha\to\beta} \subseteq \mathcal{F}(D_\alpha, D_\beta)$	$D_o = \{\bot, \top\}$, Totality of I_φ
Interpretation of const.	as above	as above
Variable assignment	as above	
Interpretation of terms	as above	

Model: $\mathcal{M} = (\mathcal{D} : \{D_\alpha\}, \mathcal{I} : \{I_\alpha\})$; satisfiability and validity defined as usual

Sidetrack: Logical Frameworks

Presentation by

Marc Wagner

Logical Frameworks

See extra slides

Exercise Sheet III

Please provide (a) the clause normal form (of the negated theorems) and (b) the resolution proofs for (Leibniz equality is defined as $\doteq^{\alpha} := (\lambda X_\alpha, Y_\alpha . \forall P_{\alpha\to o} . P\ X \Rightarrow P\ Y)$):

1. The trivial and non-trivial direction of the extensionality property for truth values: if a_o is equivalent to b_o, then a_o is Leibniz equal to b_o:
   (non-triv) $\forall A_o, B_o . (A \equiv B) \Rightarrow (A \doteq B)$ (triv) $\forall A_o, B_o . (A \equiv B) \Leftarrow (A \doteq B)$
2. Instances of the trivial and non-trivial direction of the functional extensionality axiom for type $\iota \to \iota$:
   (non-triv) $\forall M_{\iota\to\iota}, N_{\iota\to\iota} . (\forall X_\iota . (M_{\iota\to\iota} X) \doteq (N_{\iota\to\iota} X)) \Rightarrow M \doteq N$
   (triv) $\forall M_{\iota\to\iota}, N_{\iota\to\iota} . (\forall X_\iota . (M_{\iota\to\iota} X) \doteq (N_{\iota\to\iota} X)) \Leftarrow M \doteq N$
3. $\forall B_{\alpha\to o}, C_{\alpha\to o}, D_{\alpha\to o} . B \cap (C \cup D) = (B \cap C) \cup (B \cap D)$ with $\cap$ and $\cup$ being defined as: $\cup = \lambda A_{\alpha\to o}, B_{\alpha\to o}, X_\alpha . (A\ X) \vee (B\ X)$ and $\cap = \lambda A_{\alpha\to o}, B_{\alpha\to o}, X_\alpha . (A\ X) \wedge (B\ X)$

Deadline: Lecture at July, 1st

HOL: Problems

Problem 1:

There exists no well understood semantical reference framework that can guide the development of higher-order calculi.

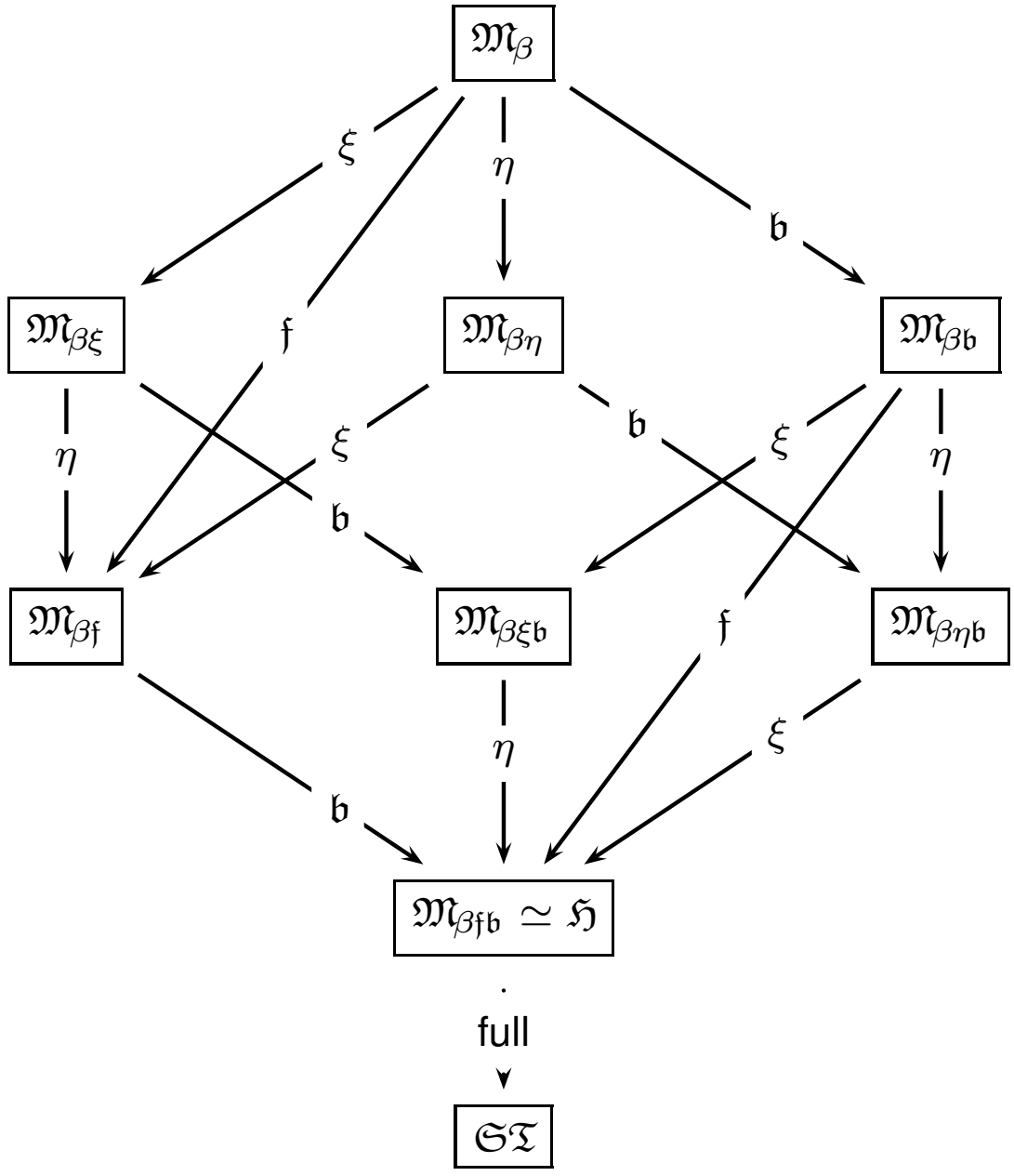
Really?

Semantics for HOL

Situation until recently:

- Standard semantics
  - full function universes
  - no complete calculi
  - functional and Boolean extensionality
- Henkin semantics [Henkin-50]
  - partial function universes, “Denotatpflicht”
  - complete calculi
  - functional and Boolean extensionality
- . . . Gap . . .
- Andrews’ v-complexes [Andrews-71]
  - no functional and Boolean extensionality

Semantics for HOL



1995 — 2004: Development of a landscape of model classes for HOL
[Kohlhase-PhD-94]
[Benzmüller-PhD-99]
[Brown-PhD-04]
[BenzmüllerBrownKohlhase-JSL04]

$\mathfrak{b}$: Boolean extensionality

$\mathfrak{f}$: Functional extensionality

η: Models that respect η-conversion

ξ: Denotations of λX.M and λX.N are identical, if denotations of M and N are for each assignment of X.

HOL Semantics: Applications

Henkin semantics

- Mathematics

Without Boolean extensionality

- Linguistics, intensional contexts
- "I believe, I see the morning star"
  versus
  "I believe, I see the evening star"

Without auf functional extensionality

- Programming languages, program analysis
- $\lambda X_{\text{list}}.X$ versus $\lambda X_{\text{list}}.(\text{reverse}\ (\text{reverse}\ X))$

HOL: Problems

Problem 2:

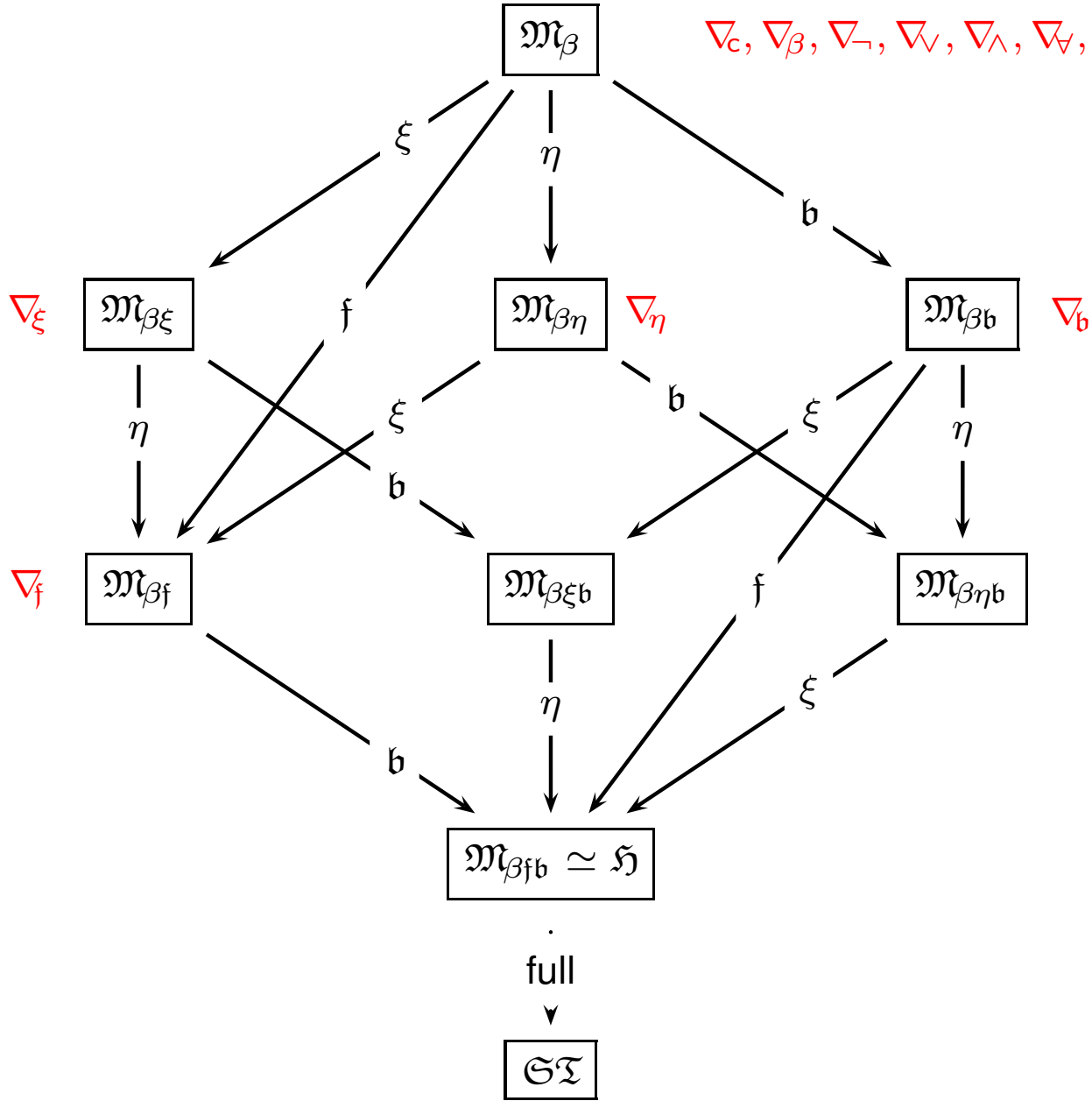
There exists no well suitable proof techniques that can support the analysis of calculi.

Really?

Abstract Consistency

- Completeness proofs in HOL much harder than in FOL
- Direct semantical arguments are too complicate
- Abstract consistency proof method
  - strong proof technique which combines syntax and semantics (model existence theorem)
  - supports completeness analysis based on pure syntactical criteria
  - FOL: [Hintikka-55, Smullyan-63, Smullyan-68]
  - HOL: [Andrews-71] only for v-complexes

Abstract Consistency



[Kohlhase-PhD-94]
[Benzmüller-PhD-99]
[Brown-PhD-04]
[BenzmüllerBrownKohlhase-JSL04]

Abstract Consistency

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 $\Phi * \mathbf{FW} \in \Gamma_\Sigma$ for each $\mathbf{W} \in cwff_\alpha(\Sigma)$.

$\nabla_\exists$ 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.

∇_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.

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

Abstract Consistency

Definition (Abstract consistency class for Henkin semantics):

. . . a subset closed class Γ_Σ of sets of HOL propositions which fulfills: $\nabla_c, \nabla_\neg, \nabla_\beta, \nabla_\vee, \nabla_\wedge, \nabla_\forall, \nabla_\exists, \nabla_f, \nabla_b, \nabla_{sat}$.

Theorem (Model existence theorem for Henkin semantics)

If a set Φ of HOL propositions is member of an abstract consistency class for Henkin semantics, then there exists a Henkin model for Φ.

Proof technique (Henkin completeness of (refutation-)calculus K)

- Show: class of sets of k-consistent (i.e. in K not refutable) HOL propositions is member of an abstract consistency class for Henkin semantics.
- Simple corollary: Henkin completeness of K

Interaction-Oriented Calculi

Correct and complete calculi for landscape of model classes

- ND calculi: [BenzmüllerBrownKohlhase-JSL04]
  Completeness is shown via abstract consistency method on one single page.
- Sequent calculi: [BenzmüllerBrownKohlhase-Draft03]
  [Brown-PhD-04]

ND Calculi: Completeness

Excerpt from completeness proof . . .

∇_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 and Cut

Saturation condition ∇_{sat} is a challenge for machine-oriented calculi:

- as hard as cut-elimination
- therefore development of alternative, weaker conditions in [BenzmüllerBrownKohlhase-Draft03] which are motivated by ideas developed in [Benzmüller-PhD-99]

Logik höherer Stufe: Probleme

Problem 3:

The two crucial challenges for automation of HOL

- treatment of equality and extensionality
- instantiation of set variables

are too hard to control successfully.

Really?

Extensional Resolution

Extensional Resolution
[BenzmüllerKohlhase-CADE-98] [Benzmüller-Diss-99]

- In HOL resolution [Andrews71, Huet72, Huet73]: blind search with extensionality axioms
- Huet's constrained resolution approach [Huet72,Huet73]: delayed pre-unification
- New: goal directed extensionality treatment; requires interleaving of proof search, pre-unification, and clause normalization

Extensional Resolution

- Notation for clauses: $C \vee [A]^F \vee [B]^T$
  Analogy to superposition: $C \vee A = F \vee B = T$
- No primitive equality; only Leibniz equality
- Unification constraints employ special symbol $=$ and they have negative polarity (no resolution or factorization on them allowed)
  Example: $C \vee [X = A]^F \vee [p\ A = F\ X]^F$

Extensional Resolution

Clause normalization

$$\frac{C \vee [A \vee B]^T}{C \vee [A]^T \vee [B]^T}\ \vee^T \qquad \frac{C \vee [A \vee B]^F}{C \vee [A]^F}\ \vee_l^F \qquad \frac{C \vee [A \vee B]^F}{C \vee [B]^F}\ \vee_r^F$$

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

$$\frac{C \vee [\Pi^\alpha A]^T \quad X_\alpha \text{ new variable}}{C \vee [A\ X]^T}\ \Pi^T$$

$$\frac{C \vee [\Pi^\alpha A]^F \quad sk_\alpha \text{ Skolem term}}{C \vee [A\ sk_\alpha]^F}\ \Pi^F$$

This rules may be combined into a single rule Cnf.

Extensional Resolution

Resolution rules

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

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

$$\frac{[\mathsf{Q}_{\gamma}\overline{\mathsf{U}^{\mathsf{k}}}]^{\alpha} \vee \mathsf{C} \quad \mathsf{P} \in \mathcal{GB}_{\gamma}^{\{\neg,\vee\} \cup \{\Pi^{\beta} \mid \beta \in \mathcal{T}^{\mathsf{k}}\}}}{[\mathsf{Q}_{\gamma}\overline{\mathsf{U}^{\mathsf{k}}}]^{\alpha} \vee \mathsf{C} \vee [\mathsf{Q} = \mathsf{P}]^{\mathsf{F}}}\ \mathsf{Prim}^{\mathsf{k}}$$

Extensional Resolution

(Pre-)unification rules

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

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

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

$$\frac{C \vee E \quad E \text{ solved for } C}{\text{Cnf}(\text{subst}_E(C))}\ \text{Subst}$$

Extensional Resolution

Extensionality rules

$$\frac{C \vee [M_o = N_o]^F}{Cnf(C \vee [M_o \equiv N_o]^F)}\ \text{Equiv}$$

$$\frac{C \vee [M_\alpha = N_\alpha]^F \quad \alpha \in \{o, \iota\}}{Cnf(C \vee [\forall P_{\alpha \to o}.PM \Rightarrow PN]^F)}\ \text{Leib}$$

Extensional Resolution

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

Negation and definition expansion with

$\cup = \lambda A_{\alpha\to o}, B_{\alpha\to o}, X_{\alpha}.(A\ X) \vee (B\ X) \quad \cap = \lambda A_{\alpha\to o}, B_{\alpha\to o}, X_{\alpha}.(A\ X) \wedge (B\ X)$

leads to:

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

Goal directed functional and Boolean extensionality treatment:

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

Clause normalization results then in a pure propositional, i.e. decidable, set of clauses. Only these clauses are still in the search space of LEO(in total there are 33 clauses generated and LEO finds the proof on a 2,5GHz PC in 820ms).

Similar proof in case of embedded propositions:

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

Extensional Resolution

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

Negation and clause normalization

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

Resolution between $\mathcal{C}_1$ and $\mathcal{C}_3$ and between $\mathcal{C}_2$ and $\mathcal{C}_3$

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

Decomposition

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

Recursive call of proof process with rules Equiv and Cnf

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

Extensional Resolution

Further small examples which test Henkin completeness:

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

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

$$\ldots$$

Sidetrack: Lambda Cube

Presentation by

Matthias Berg

Lambda Cube

See extra slides

Sidetrack: New Foundations

Presentation by

Robert Grabowski

Quine's New Foundations

See extra slides

Extensional Paramodulation

1995 — 1999: Extensional RUE-Resolution
[Benzmüller-CADE-99] [Benzmüller-PhD-99]

- Notation as vefore; new is logical symbol $=$ for primitive equality
- Identification of unification constraints and negative equality literals
- All rules for extensional resolution still valid; resolution and factorization not allowed on unification constraints
- Some further rules required for $=$; see next slide

Extensional Paramodulation

Paramodulation rules

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

Positive extensionality rules

$$\frac{C \vee [M_o = N_o]^T}{C \vee [M_o \Leftrightarrow N_o]^T}\ \text{Equiv}'$$

$$\frac{C \vee [M_{\alpha\to\beta} = N_{\alpha\to\beta}]^T \quad X \text{ new free variable}}{C \vee [M\ X = N\ X]^T}\ \text{Func}'$$

Difference Reduction

Extensional RUE-resolution

[Benzmüller-PhD-99]

Difference reduction matrix calculus

[Brown-PhD-04]

- All rules for extensional resolution
- Positive extensionality rules, but no paramodulation rule
- New: Resolution and factorization allowed on unification constraints

Properties of Calculi

Soundness and Completeness

- Soundness of the calculi for Henkin Semantics
- Completeness for Henkin semantics only with additional (infinitely branching) FlexFlex rule

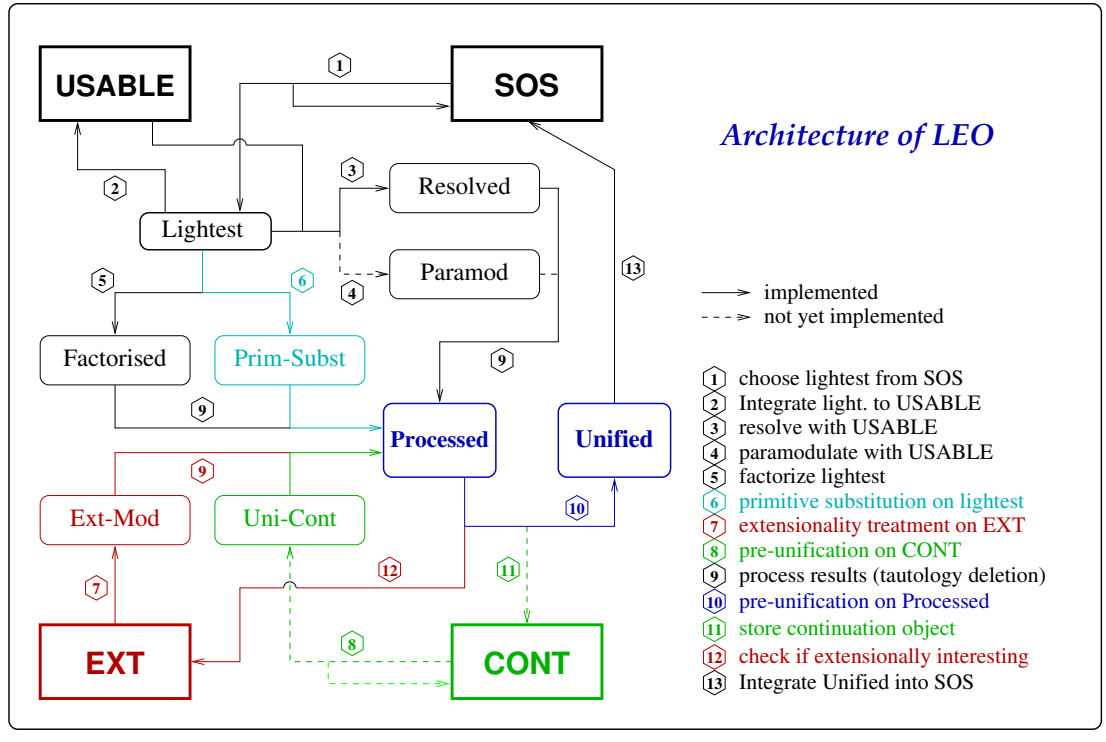
$$\frac{C \vee [F_{\overline{\gamma^n} \to \alpha}\ \overline{U^n} = H_{\overline{\delta^m} \to \alpha}\ \overline{V^m}]^F \quad G \in \mathcal{GB}^h_{\overline{\gamma^n} \to \alpha} \text{ for a } h_\tau \in \text{Consts}_\tau}{C \vee [F\ \overline{U^n} = H\ \overline{V^m}]^F \vee [F = G]^F}\ \text{FlexFlex}$$

Challenge

- Prove Henkin completeness without FlexFlex rule
- Restriction of the prover calls from within unification with rules Equiv and Leib to base types
- Development of powerful strategies and heuristics

Prover LEO

- [BenzmüllerKohlhase-CADE-98]
- Extended set-of-support-architecture



Instantiation of Set Variables

[Brown-CADE-02, Brown-PhD-04]
goal directed approach for instantiation of set variables

- Replaces the á priori guessing strategy of TPS and LEO
- Now á posteriori method based on accumulation of constraints and mutual information exchange between constraint store and proof search
- Interesting analogy:
  - á priori method $\Leftrightarrow$ explicit induction
  - á posteri method $\Leftrightarrow$ implicit induction

HOL: Problems

A recent trend:

Restricted extension of FOL approaches in direction of HOL: e.g., "Superposition with Equivalence Reasoning" [GanzingerStuber-CADE-03]

How reasonable?

Superposition with Equivalences

Superposition with Equivalences

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

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

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

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

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

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

Extensional Resolution/Paramodulation

$\top$ and $\bot$ definable as $\exists X_o.X \vee \neg X$ and $\neg\top$.

This rules correspond to the clause normalization rules introduced before (if we choose the logical connectives $\neg, \vee, \forall$).

All literals are annotated with polarities; rule not needed

No essential difference to clause normalization;
rules can be combined to a single rule Cnf.

Superposition with Equivalences

$\dfrac{l = r \vee C}{l = \bot \vee r = \top \vee C}$ Pos-Equiv-Elim-1	corresponds to Equiv'
$\dfrac{l = r \vee C}{l = \top \vee r = \bot \vee C}$ Pos-Equiv-Elim-2	corresponds to Equiv'
$\dfrac{(l = r) = \bot \vee C}{l = \top \vee r = \bot \vee C}$ Neg-Equiv-Elim-1	corresponds to Equiv
$\dfrac{(l = r) = \bot \vee C}{l = \bot \vee r = \top \vee C}$ Neg-Equiv-Elim-2	corresponds to Equiv
$\dfrac{(s = t) = \bot \vee C}{C\sigma}$ Reflexivity-Res	corresponds to Subst / unification
$\dfrac{(s[l'] = t) = \bot \vee C \quad l = r \vee D}{((s[r] = t) = \bot \vee C \vee D)\sigma}$ Neg-Superposition	corresponds to Para (is derivable)
$\dfrac{s[l'] = t \vee C \quad l = r \vee D}{((s[r] = t) \vee C \vee D)\sigma}$ Pos-Superposition	corresponds to Para
$\dfrac{l = r \vee l' = r' \vee C}{((r = r') = \bot \vee l' = r' \vee C)\sigma}$ =-Factoring	subsumed by factorization + unification

Superposition with Equivalences

Evaluation in [GanzingerStuber-CADE-03] via examples such as

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

- in TPTP as *set171+3*
- not provable with vampire 5.0 (CASC Winner 2002) or E-Setheo csp02
- Superposition with Equivalences in Saturate generates 159 clauses during proof search and needs 2.900ms on a 2Ghz Notebook for the proof
- ZF-Axiome (including extensionality are always) in search space
- no transformation in a pure propositional problem

Summary

- Improved foundations for automation of HOL
  - Landscape of model classes
  - Abstract consistency method
  - Calculi: ND, Sequent, Matrix, Resolution
  - Foundations for goal directed treatment of extensionality
  - Foundations for goal directed instantiation of set variables
- Many interactive proof assistants are based HOL
- But still: Strong concentration of funding and activities on improvement of FOL. Is this still justified?

Remark

- More useful as restricted extensions of FOL approaches: Embedding/Implementation of FOL approaches in HOL context?
- Very important: Extension of CASC competition and TPTP library in order to avoid isolated analysis of FOL approaches.

Church Numerals

One way to represent a natural number n is

$$\overline{n} = \lambda f_{\iota\to\iota}.\lambda y_\iota.(f^n\ y)$$

where f^n is an abbreviation for $\underbrace{(f\ (f\ (f \ldots (f}_{n-\text{times}}\ y))))$.

The successor function is then defined as

$$\overline{succ} = \lambda z_{(\iota\to\iota)\to(\iota\to\iota)}.(\lambda f_{\iota\to\iota}.\lambda y_\iota.f\ ((z\ f)\ y))$$

Church Numerals

Example: As an example, consider how the successor of 2 is computed:

$$
\begin{aligned}
\overline{\mathsf{succ}}\ \overline{2} &= \lambda z.(\lambda(f.\lambda y.f\ ((z\ f)\ y)))\ \overline{2} \\
&= \lambda f.\lambda y.(f\ ((\overline{2} f)\ y)) \\
&= \lambda f.\lambda y.(f\ (((\lambda f'.\lambda x'.f'^{2}\ x')\ f)\ y)) \\
&= \lambda f.\lambda y.(f\ ((\lambda x'.f^{2}\ x')\ y)) \\
&= \lambda f.\lambda y.(f\ (f^{2}\ y))) \\
&= \lambda f.\lambda y.(f^{3}\ y)
\end{aligned}
$$

Church Numerals

Addition on the numerals can be defined as:

$$\overline{+} = \lambda z_1.\lambda z_2.(\lambda x.\lambda y.((z_1\ x)\ ((z_2\ x)\ y)))$$

Exercise Sheet IV

1. Transform the following term in $\beta\eta$-normalform (maximal β-reduction and maximal η-expansion):
   - $((\overline{+}\ \overline{2})\ \overline{3})$, where $\overline{+}, \overline{2}, \overline{3}$ are the λ-terms as presented in the lecture on Church numerals.
2. Try to find λ-expressions (similar to $\overline{+}$ in the lecture) that encode multiplication $\overline{*}$, and exponentiation $\overline{\mathrm{exp}}$ for Church numerals such that
   - your first definition of $\overline{*}$ employs $\overline{+}$,
   - your second definition of $\overline{*}$ does not employ $\overline{+}$,
   - and your definition of $\overline{\mathrm{exp}}$ may be chosen arbitralily.

Exercise Sheet IV (contd.)

3. Unify the following terms with the higher order unification rules from the lecture (one solution for each term is sufficient). The types of the the occuring variable symbols H, Q, X, Y and the occuring constant symbols f, a, b are:
   $H_{((i\to i)\to i\to i)\to((i\to i)\to i\to i)\to((i\to i)\to i\to i)}, Q_{i\to i\to i}, f_{i\to i}, a_i, b_i, X_i, Y_i$.
   - $[((H\ \overline{2})\ \overline{3}) = \overline{6}]^F$
   - $[((H\ \overline{1})\ \overline{2}) = \overline{2}]^F$
   - $[((H\ \overline{2})\ \overline{3}) = \overline{6}]^F \vee [((H\overline{1})\ \overline{2}) = \overline{2}]^F$
   - $[((Q\ (f\ a))\ (f\ b)) = (f\ ((Q\ X)\ Y))]^F$
4. The surjective Cantor theorem can be encoded in HOL as follows

   $$\neg\exists G_{\iota\to\iota\to o}.\forall P_{\iota\to o}.\exists X_\iota.(G\ X) \doteq^{\iota\to o} P$$

   Give a proof of it in the extensional resolution calculus.