Higher Order Equational Logic

Gert Smolka

June 23, 2005

Higher Order Logic

- Elegant Model of mathematical reasoning
- Used in proof assistants
- Frege, Russel, Church 1940, Henkin
- Textbook by P. Andrews 2002
  not suitable as quick start

This Talk: Modular Reconstruction of HOL

- Our logic: Simply typed λ-calculus (Church 1940)
  pure equational logic
- Logical constants are axiomatized $(0, 1, \neg, \wedge, \vee, \forall, \exists, \doteq)$
  Hence they can be analyzed within a logic

  $S \rightarrow S(BA) \rightarrow S(HB) \rightarrow S(HOL)$
- Great for manual proofs
- Can simulate Hilbert and Gentzen proofs

Model	$\longrightarrow$	Axioms	$\longrightarrow$	Formal Proofs
validity		semantic entailment		deductive entailment
$\mathcal{D} \models e$	$\Leftarrow$	$A \models e$	$\Leftarrow$	$A \vdash e$
e valid in $\mathcal{D}$		e follows from axioms A satisfied by $\mathcal{D}$		$\exists$ formal proof of e from A

- Example: $\mathbb{N}$ and Peano Axioms
- Formal proofs are machine-verifiable

Peano Axioms (PA)

$0 : N$
$s : N \to N$

$sx \doteq sy \to x \doteq y$ — injectivity
$\neg(sx \doteq 0)$
$f0 \wedge (\forall x.\ fx \to f(sx)) \to \forall f$ — induction

Induction mirrors recursive structure

$+ : N \to N \to N$
$0 + y = y$
$sx + y = s(x+y)$

$* : N \to N \to N$
$0 * y = 0$
$sx * y = x * y + y$

$\mathbb{B}, \mathbb{N} \models e \iff BI \cup PA \models e$ — Semantic completeness

$\mathbb{B}, \mathbb{N} \models e$ not semi-decidable — Gödel 1931

Simply Typed λ-Calculus (S)

Syntax

Constants	C, c
Variables	x
Terms	$t = c \mid x \mid \lambda x.t \mid t\,t$
Types	$T = C \mid T \to T$

- variables and constants are equipped with types
- $\tau(\lambda x.t) = \tau x \to \tau t$
- $\tau(st) = T$ if $\tau s = \tau t \to T$

Semantic Entailment

Equation $s = t$ where s and t have the same type

e — equation
A, E, F — set of equations

$E \models^{A}_{0} F \overset{\text{def}}{\iff} \forall$ interpretation satisfying A: every solution of E is a solution of F

- free variables of E are fixed — Deduction Theorem
- free variables of A are universally quantified — Generalisation

Notations

- E and A are omitted if empty
- $E \mathrel{\dashv\models}^{A}_{\circ} F \overset{def}{\iff} E \models^{A}_{\circ} F \wedge F \models^{A}_{\circ} E$
- $E \models^{A} F \overset{def}{\iff} \models^{A \cup E} F$ no fixed variables

$\beta \qquad \models (\lambda x.s)t = s[x:=t]$

$\eta \qquad \models \lambda x.sx = s \qquad \text{if } x \notin FVs$

Conversion Proofs

$E \vdash^{A}_{\circ} s = t \overset{def}{\iff} \exists\ s \underbrace{= \cdots =}_{\text{conversions}} t$

A conversion is a subterm replacement wrt either

- β or η
- an equation of E where λ-capture is disallowed
- a substitution instance of an equation of A where λ-capture is allowed

Properties of $\vdash_\circ$

Soundness	$E \vdash^{A}_{\circ} F \Rightarrow E \models^{A}_{\circ} F$
Exp	$E \vdash^{A}_{\circ} E \cup A$
Mon	$E \vdash^{A}_{\circ} F \wedge E \subseteq E' \wedge A \subseteq A' \Rightarrow E' \vdash^{A'} F$
Trans	$E \vdash^{A}_{\circ} E' ,\ E' \vdash^{A}_{\circ} F \Rightarrow E \vdash^{A}_{\circ} F$
SuS	$E \vdash^{A}_{\circ} F \Rightarrow \sigma E \vdash^{A}_{\circ} \sigma F$

Compactness

Semi-decidability

Duality

Given: type preserving function $\hat{\ } \in VC \to VC$
such that $\forall c \in VC: \hat{c} = c$

A dual wrt $\hat{\ }$ $\overset{def}{\iff}$ $A \vdash \hat{A}$

$$\boxed{A \text{ dual wrt } \hat{\ } \Rightarrow \left(E \vdash^{A}_{\circ}\, e \iff \hat{E} \vdash^{A}_{\circ}\, \hat{e} \right)}$$

Completeness Result

$$\boxed{\begin{array}{l}\text{No higher order constants; } A \text{ first order} \\ \text{Then:} \quad A \models e \iff A \vdash e\end{array}}$$

[Kaminski / S 2005]

Builds on H. Friedman 1975, R. Statman 1985

Open Problem

Can we reformulate completeness of first order predicate logic in S?

(Quantifiers are higher order constants)

Higher Order Boolean Logic

S(HB)

Constants $0, 1 : \mathbb{B}$; $\neg : \mathbb{B} \to \mathbb{B}$; $\wedge, \vee : \mathbb{B} \to \mathbb{B} \to \mathbb{B}$

Notations

$$\bar{s} \overset{\text{def}}{=} \neg s$$

$$s \to t \overset{\text{def}}{=} \bar{s} \vee t$$

$$s \leftrightarrow t \overset{\text{def}}{=} (s \wedge t) \vee (\bar{s} \wedge \bar{t})$$

Formula Convention: s for $s = 1$

Axioms

$HB \overset{\text{def}}{=} BA \cup \{BCA\}$ Boolean Axioms

BCA $\quad f0 \wedge f1 \to fx$ higher order

Key Properties

Semantic Completeness $\mathbb{B} \models e \iff HB \models e$ fails for BA

Decidability $\{e \mid \mathbb{B} \models e\}$ decidable

Duality for $0 \leftrightsquigarrow 1$, $\wedge \leftrightsquigarrow \vee$

Deductive completeness (first order) $\mathbb{B} \models e \iff BA \vdash e$

Deductive incompleteness (higher order)* $\exists e : \mathbb{B} \models e \wedge HB \nvdash e$

Agreement External Internal

* Conjecture

Agreement of External and Internal Operations

And $\quad x, y \vdash^{BA}_{0} x \wedge y$

Equi $\quad x = y \vdash^{BA}_{0} x \leftrightarrow y$

Ded $\quad s \vdash^{A}_{0} t \iff A \vdash s = t \quad$ if $A \vdash HB$

Provides for implicational proofs (Hilbert, sequent, ND)

Implicational Proofs $\emptyset \vdash^{A}_{0} \cdots \vdash^{A}_{0} s$

- Can derive inference rules, e.g. $\quad (A \vdash HB)$

  MP $\quad x \to y, x \vdash^{A}_{0} y$

  W $\quad x \to y \vdash^{A}_{0} x \wedge x' \to y \vee y'$

- Proofs in Hilbert, sequent, and ND style are possible
- Can mix in conversion

$$\boxed{\begin{array}{l} A \vdash s \to t \iff s \vdash^{A}_{0} \cdots \vdash^{A}_{0} t \\ A \vdash s = t \iff s \vdash^{A}_{0} \cdots \vdash^{A}_{0} t \text{ and } t \vdash^{A}_{0} \cdots \vdash^{A}_{0} s \end{array}}$$

Quantifiers and Identities

S(HOL)

Constants $\forall_T, \exists_T : (T \to B) \to B$

Notations

$\forall x.s \overset{\text{def}}{=} \forall_T(\lambda x.s)$ where $x : T$

$\exists x.s \overset{\text{def}}{=} \exists_T(\lambda x.s)$

$s \doteq t \overset{\text{def}}{=} \forall f.\ fs \to ft$ Leibniz

Axioms

$\forall x.1 = 1$ $\exists x.0 = 0$

$\forall f = \forall f \wedge fx$ $\exists f = \exists f \vee fx$

$BQ \overset{\text{def}}{=} HB$ + quantifier axioms

Properties of S(BQ)

Duality for $0 \leftrightsquigarrow 1,\ \wedge \leftrightsquigarrow \vee,\ \forall \leftrightsquigarrow \exists$

Replacement $BQ \vdash x \doteq y \wedge fx = x \doteq y \wedge fy$ Rep

Agreement

$s \overset{BQ}{\vdash\!\dashv} \forall x.s$ Gen

$x \doteq y \overset{BQ}{\vdash\!\dashv}_0 x \leftrightarrow y$ BIA

$x = y \overset{BQ}{\vdash\!\dashv}_0 x \doteq y$ Ref

Extentionality

Ext $\forall x.\ fx \doteq gx = f \doteq g$

$BQ \models Ext$

$BQ \nvdash Ext$ Henkin?

provides for replacement with capture:

$Ext \overset{BQ}{\vdash\!\dashv} (\forall x.\ s \doteq t) = (\lambda x.s) \doteq (\lambda x.t)$

Open Problems

1. $BQ \vdash s \doteq t \;\Rightarrow\; BQ \vdash s = t$?

2. $x \doteq y \;\overset{BQ,\,Ext}{\models}\; x = y$?

Cantor's Theorem

$$\boxed{\text{Set } \mathcal{X} : \neg \exists \text{ surjective } f \in \mathcal{X} \to \mathcal{P}\mathcal{X}}$$

$$\mathcal{P}\mathcal{X} \doteq \mathcal{X} \to \mathbb{B}$$

Proof of Cantor's Theorem

$$\overline{\exists f\, \forall g\, \exists x.\ fx \doteq g}$$

$= \quad \forall f\, \exists g\, \forall x.\ \overline{fx \doteq g} \qquad dM$

$\dashv \quad \overline{fx \doteq \lambda y.\ \overline{fyy}} \qquad Gen,\ \exists I\ \ g = \lambda y.\ \overline{fyy},\ Gen$

$= \quad \overline{\forall y.\ fxy \doteq (\lambda y.\ \overline{fyy})\, y} \qquad Ext$

$\dashv \quad \overline{fxx \Leftrightarrow \overline{fxx}} \qquad dM,\ \exists I\ \ y = x,\ \beta,\ BIA$

$= \quad \neg \qquad BA$

Summary

Modular reconstruction of HOL

S — strong completeness result?

$\downarrow$

$S(AB)$ — deductive completeness?

$\downarrow$

$S(HOL)$ — agreement $=$ and $\doteq$?