Review of S(HOL)

11-3 C. Smolka 22.6.2005

Model ⟶ Axioms ⟶ Formal Proofs

Model		Axioms		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)

Induction enforces recursive structure

$0 : N$

$\sigma : N \to N$

$\sigma x \doteq \sigma y \to x \doteq y$ — injectivity

$\neg(\sigma x \doteq 0)$

$f0 \wedge (\forall x.\ fx \to f(\sigma x)) \to \forall f$ — induction

$+ : N \to N \to N$

$0 + y = y$

$\sigma x + y = \sigma(x+y)$

$* : N \to N \to N$

$0 * y = 0$

$\sigma x * y = x * y + y$

$$\boxed{\mathbb{B}, \mathbb{N} \models e \iff BI \cup PA \models e}$$

Semantic completeness

Modular Approach to HOL

$S(A)$ — pure equational logic (simply typed λ-calculus)

↓

$S(HB)$ — axiomatization of $0, 1, \neg, \wedge, \vee$

↓

$S(HOL)$ — axiomatization of $\forall, \exists, \doteq$

$HOL \vdash HB \cup QA$

- $\models$ and $\vdash$ are defined by S
- logic constants are axiomatized as ordinary constants

$\models_0$, $\vdash_0$, Conversion Proofs

$E \models^{A}_{0} s = t \overset{\text{def}}{\iff}$ For every interpretation satisfying A, every solution of E is a solution of $s = t$

Variables in E are fixed, variables in A are universally quantified

$E \vdash^{A}_{0} s = t \overset{\text{def}}{\iff}$ $\exists$ conversion proof $s = \dots = t$ where each step is

- a λ-conversion, or
- a conservative E-conversion, or
- an A-conversion

$E \vdash^{A}_{0} e \Rightarrow E \models^{A}_{0} e$ — soundness

Notation

$E \vdash^{A}_{0} F \overset{\text{def}}{\iff} \forall e \in F:\ E \vdash^{A}_{0} F$

$E \vdash^{A} e \overset{\text{def}}{\iff} \emptyset \vdash^{E \cup A}_{0} e$

- Analogous definitions for $\models$
- Omit E, A if $E = \emptyset$, $A = \emptyset$:
  $E \vdash_0 e$, $\vdash^{A}_{0} e$, $\vdash_0 e$
  $E \vdash e$, $\vdash^{A} e$, $\vdash e$
- Formula Convention: Omit $= \top$: $E \vdash^{A}_{0} s$

Structural Properties of $\vdash_0$, $\models_0$

Exp, Weak, Accu, Trans

Sub, Dual

β, Xi, Eta

only $\vdash_0$: Compactness, Semi-decidability

Expansivity, Weakening, Accumulation, Transitivity

Exp	$E \vdash^{A}_{0} E \cup A$
Weak	$E \vdash^{A}_{0} F \wedge E \subseteq E' \wedge A \subseteq A' \wedge F' \subseteq F \Rightarrow E' \vdash^{A'}_{0} F'$
Accu	$E \vdash^{A}_{0} F_1 \wedge E \vdash^{A}_{0} F_2 \Rightarrow E \vdash^{A}_{0} F_1 \cup F_2$
Trans	$E \vdash^{A}_{0} E' \wedge E' \vdash^{A}_{0} F \Rightarrow E \vdash^{A}_{0} F$
Trans'	$\vdash^{A}_{0} A' \wedge E \vdash^{A'}_{0} F \Rightarrow E \vdash^{A}_{0} F$

(Trans, Trans': proof non-trivial)

Stability under Substitution (SuS)

$$E \vdash^{A}_{\circ} F \Rightarrow \varphi\sigma E \vdash^{A}_{\circ} \varphi\sigma F$$

special case: $A \vdash F \Rightarrow A \vdash \varphi\sigma F$

Duality

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

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

$$A \text{ dual wrt } \hat{\ } \Rightarrow (E \vdash^{A}_{\circ} e \Leftrightarrow \hat{E} \vdash^{A}_{\circ} \hat{e})$$

β: $\vDash (\lambda x.s)t = s[x:=t]$ — $\forall x,s,t$ structural property

Xi: $s=t \;\vDash\!\!\!\dashv\; \lambda x.s = \lambda x.t$

Eta: $sx = tx \;\vDash\!\!\!\dashv\; s = t$ if $x \notin FV(s,t)$

η: $\vDash \lambda x.fx = f$ — $\forall\, T \to T' \in Ty$ equational property

Structural Properties of HB

Dual wrt $0 \leftrightarrow 1$, $\wedge \leftrightarrow \vee$

And, Equi

Ded, BDual

And $x, y \overset{BA}{\vdash}_0 x \wedge y$

Equi $x = y \overset{BA}{\vdash}_0 x \Leftrightarrow y$

external = internal

Ded $s \overset{A}{\vdash}_0 t \iff A \vdash s = t$

$s \overset{A}{\vdash}_0 t \iff A \vdash s \to t$

if $A \vdash HB$ and $s, t : \mathbb{B}$

holds for $A \vdash BA$ if s, t first-order

BDual $s \overset{A}{\vdash}_0 t \iff \hat{t} \overset{A}{\vdash}_0 \hat{s}$ if $A \vdash BA \cup \hat{A}$

Equational Properties of HB

Equations e such that $HB \vdash e$

Boolean Laws BL

MP $x \wedge (x \to y) = x \wedge y$

GR $x \to y = x \Leftrightarrow (x \wedge y)$

$x \to y = y \Leftrightarrow (y \vee x)$

UoC $x \Leftrightarrow \bar{y} = \overline{(x \wedge y)} \wedge (x \vee y)$

The following equations are $\overset{BA}{\vdash}$-equivalent:

BRep $x \Leftrightarrow y \wedge fx = x \Leftrightarrow y \wedge fy$

BCA $f0 \wedge f1 \to fx$

BExp $fx = (\bar{x} \wedge f0) \vee (x \wedge f1)$

$HB \overset{def}{=} BA \cup \{BRep\}$

$\mathbb{B} \models e \iff HB \models e$

HB is semantically complete for $\mathbb{B}$ (BA is not)

Structural Properties of BQ

- Dual wrt $0 \leftrightarrow 1$, $\wedge \leftrightarrow \vee$, $\forall \leftrightarrow \exists$
- $BQ \vdash HB$
- Gen $s \overset{BQ}{\vdash} \forall x.s$ Generalisation

Notational Definition of $\dot{=}$

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

The following equations are deducible from BQ

Ref $x \dot{=} x$

Sym $x \dot{=} y = y \dot{=} x$

Trans $x \dot{=} y \wedge y \dot{=} z \to x \dot{=} z$

Rep $x \dot{=} y \wedge fx = x \dot{=} y \wedge fy$

BIA $x \dot{=} y = x \Leftrightarrow y$

Extensionality

Ext $\forall x.\ fx \dot{=} gx = f \dot{=} g$

$BQ \models Ext$ $BQ \not\vdash Ext$ — Henkin?

$BQ \cup \{Ext\} \vdash \widehat{Ext}$ — Adding Ext preserves duality

The following equations are deducible from $BQ \cup \{Ext\}$:

IXi $\forall x.\ s \dot{=} t = (\lambda x.s) = (\lambda x.t)$

∀D $\forall f = f \dot{=} \lambda x.1$

∃D $\exists f = \overline{f \dot{=} \lambda x.0}$

Axiom of Choice

AoC $\forall x \exists y.\ fxy = \exists g \forall x.\ fx(gy)$

$BQ \models AoC$ $BQ \not\vdash AoC$ — conjecture!

$BQ \cup \{AoC\} \vdash \widehat{AoC}$ — Adding AoC preserves duality