MPRI

PRFSYS

Benjamin Werner

Higher-Order Logic

30 Sept. 2025

Motivations / Introduction

(on the blackboard)

note to self: start with definitional / propositional equality

$$T := \iota \mid o \mid T \to T$$

$$t ::= x^T \mid t\,t \mid \lambda x^T.t$$

$$\vdash x^T : T \qquad \frac{\vdash t : A \to B \quad \vdash u : A}{\vdash t\,u : B} \qquad \frac{\vdash t : B}{\vdash \lambda x^A.t : A \to B}$$

One rule per form:

- $x^A : B \Rightarrow A = B$
- $t\,u : B \Rightarrow \exists A.\ t : A \to B$ and $u:A$
- $\lambda x^A.t : C \Rightarrow \exists B.\ C = A \to B,\ t : B$

Two simple properties of simply typed λ-calculus

- Subject reduction: if $t : A$ and $t \rhd_\beta t'$ then $t' : A$
- Strong normalization: if $t : A$, there is no infinite sequence
  $t \rhd_\beta t_1 \rhd_\beta t_2 \rhd_\beta t_3 \rhd_\beta t_4 \ldots$

Alternative inductive definition: SN is the smallest set of terms such that:
$(\forall u,\ t \rhd_\beta u \Rightarrow u \in SN) \Rightarrow t \in SN$

Proof: in part 2

A very simple model

For each atomic type α, take a set $U(\alpha)$

Define : $|\alpha| \equiv U(\alpha)$

$$|A \rightarrow B| \equiv |B|^{|A|} \quad \text{(total set-theoretical functions)}$$

Given $\mathcal{I}$ s.t. $\mathcal{I}(x^A) \in |A|$ we define for every $t : B$, $|t|_{\mathcal{I}} \in |B|$

- $|x^B|_{\mathcal{I}} \equiv \mathcal{I}(x^B)$
- $|(t\ u)|_{\mathcal{I}} \equiv |t|_{\mathcal{I}}(|u|_{\mathcal{I}})$
- $|\lambda x^A . t|_{\mathcal{I}} \equiv \gamma \in |A| \mapsto |t|_{\mathcal{I};\, x^A \leftarrow \gamma}$

Is this linked to normalization ?

A very simple model (2)

If we add the possibility for non-terminating functions :

$Y_A : ((A \to A) \to (A \to A)) \to (A \to A)$ s.t. $Y_A\, F \; \rhd \; F\,(Y_A\, F)$

$F : (A \to A) \to (A \to A)$

$YF : (A \to A)$

$F\,(Y\,F) : (A \to A)$

corresponds to let rec f (x:A) = … (f t)… (f u)…

What happens with the model ?

$|Y_A|$ is not (totally) defined

Normal terms in simply typed calculus

Normal λ-terms: x , $\lambda x.n$, $\lambda x_1.\lambda x_2.n \ldots$

$(x\ n_1\ n_2\ \ldots\ n_m)$

in the end : $\lambda x_1.\lambda x_2.\ \ldots\ \lambda x_k.\ (x\ n_1\ n_2\ \ldots\ n_m)$

Consider the following signature :

$0 : \iota$, $S : \iota \to \iota$, $+\ \times : \iota \to \iota \to \iota$ what terms $f : \iota \to \iota$ can we construct ?

$S \quad (+\ n) \quad (\times\ n)$

$\lambda x^{\iota}.\ n$

$\lambda x^{\iota}.\ 0$

$(S\ n)$

$(+\ n_1\ n_2)$ only polynomials (with constant exponents)

$(\times\ n_1\ n_2)$

x^{ι}

Higher-Oder Logic

Aka : Simple Theory of Types   Church 1940

Two atomic types : ι (natural numbers) and o (propositions)

Constants : $0 : \iota$, $S : \iota \to \iota$, $+ \times : \iota \to \iota \to \iota$

$$\Rightarrow : o \to o \to o$$

$$\forall_T : (T \to o) \to o$$

Propositions are objects

$$[]\ \mathrm{wf} \qquad \frac{\Gamma\ \mathrm{wf} \qquad \vdash A : o}{\Gamma ; A\ \ \mathrm{wf}} \qquad \mathrm{Ax}\ \frac{\Gamma\ \mathrm{wf}}{\Gamma \vdash A}\ \text{if } A \in \Gamma$$

Higher-Oder Logic : rules

$$\text{Ax}\ \frac{\Gamma\ \text{wf}}{\Gamma \vdash A}\ \text{if } A \in \Gamma$$

$$\frac{\Gamma ; A \vdash B}{\Gamma \vdash A \Rightarrow B}$$

$(\Rightarrow A\ B)$

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall_T\ x^T.\ A}\ \text{if } x \notin FV(\Gamma)$$

$(\forall_T\ \lambda\ x^T.\ A)$

$$\frac{\Gamma \vdash \forall_T\ A \qquad \vdash t : T}{\Gamma \vdash (A\ t)}$$

$$\frac{\Gamma \vdash A \qquad \vdash A' : o}{\Gamma \vdash A'}\ \text{if } A =_\beta A'$$

$\boxed{\text{If } \Gamma \vdash A, \text{ then } \Gamma\ \text{wf and } \vdash A : o}$

HOL : defining connectives

$\bot \;\equiv\; \forall X^o.\, X^o$

$\lambda A^o.\, \lambda B^o.\, \forall X^o.\, (A^o \Rightarrow B^o \Rightarrow X^o) \Rightarrow X^o$

$\lambda A^o.\, \lambda B^o.\, \forall X^o.\, (A^o \Rightarrow X^o) \Rightarrow (B^o \Rightarrow X^o) \Rightarrow X^o$

These are inductive definitions
elim rules "for free". We need to prove the intro rules

$= \quad \equiv \quad \lambda x^T.\, \lambda y^T.\, \forall P^{T\to o}.\, (P\, x^T) \Rightarrow (P\, y^T)$

Existential

$$\exists_T \quad \equiv \quad \lambda\, P^{T \to o}.\ \forall\, X^o\ .\ (\forall\, x^T.\ (P\ x^T) \Rightarrow X^o) \Rightarrow X^o$$

Inductive properties

$= \quad \equiv \quad \lambda\, x^{T}.\ \lambda\, y^{T}.\ \forall\, P^{T\to o}.\ (P\ x^{T}) \Rightarrow (P\ y^{T})$

What about :

$=' \quad \equiv \quad \lambda\, x^{T}.\ \lambda\, y^{T}.\ \forall\, R^{T\to T\to o}.\ (\forall\, z^{T}.\ R\ z^{T}\ z^{T}) \Rightarrow (R\ x^{T}\ y^{T})$

Inductive properties

How do we talk about x^y ?
Think of a function as a relation

$$(\mathrm{Exp}\ n\ 0\ 1)$$
$$(\mathrm{Exp}\ n\ m\ r) \Rightarrow (\mathrm{Exp}\ n\ (S\ m)\ (n \times r))$$

$$\begin{aligned}
\mathrm{Exp} \;\equiv\; \lambda n.\ \lambda m.\ \lambda r.\ \ \forall R.\ & \\
& (R\ 0\ 1) \Rightarrow \\
& \quad (\forall\, b\ c\ .\ (R\ b\ c) \Rightarrow (R\ (S\ b)\ (n \times c))) \Rightarrow \\
& \quad\quad R\ m\ r
\end{aligned}$$

Naming functions: Hilbert operator

$\varepsilon(P)$ "The" object verifying P ("choice operator")

$$\frac{\vdash (P\ t)}{\vdash (P\ \varepsilon(P))}$$

Using $\mathcal{E}$ is not (really) intuitionistic (see Coq exercise)