# MPRI

## 2-7-1

Benjamin Werner

## Higher-Order Logic

24 Sept. 2024

# Motivations / Introduction

(on the blackboard)

note to self: start with definitional / propositional equality

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

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

$$\vdash x^T : T$$

$$\frac{\vdash t : A \to B \quad \vdash u : A}{\vdash t\ u : B}$$

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

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: next week

# A very simple model

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

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

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

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

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

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: $x$ , $\lambda x.n$, $\lambda x_1.\lambda x_2.n$ …

$(x\ n_1\ n_2\ \ldots\ n_{\boldsymbol{m}})$

in the end : $\lambda x_1.\lambda x_2.\ \ldots\ \lambda x_{\boldsymbol{k}}.\ (x\ n_1\ n_2\ \ldots\ n_{\boldsymbol{m}})$

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 ?

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

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

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

$(S\ n)$

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

$(\times\ n_1\ n_2)$

$x^{\iota}$

# Higher-Oder Logic

Aka : Simple Theory of Types  Church 1940

Two atomic types :  $\iota$ (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

[] wf

$$\frac{\Gamma \text{ wf} \qquad \vdash A : o}{\Gamma \text{ ; } A \text{ wf}}$$

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

# Higher-Oder Logic : rules

$$\text{Ax}\ \frac{\Gamma\ \text{wf}}{\Gamma \vdash A}\ \text{if } A \in \Gamma \qquad \frac{\Gamma\ ;\ A\ \vdash B}{\Gamma\ \vdash A \Rightarrow B} \qquad \frac{\Gamma\ \vdash A \Rightarrow B \quad \Gamma\ \vdash A}{\Gamma\ \vdash B}$$

$(\Rightarrow A\ B)$

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

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

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

If $\Gamma \vdash A$, then $\Gamma$ wf and $\vdash A : o$

# HOL : defining connectives

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

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

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

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

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

# 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

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

(Exp n 0 1)
(Exp n m r) ⇒ (Exp n (S m) (n × r))

$$\text{Exp} \equiv \lambda\, n.\, \lambda\, m.\, \lambda\, r.\ (\forall\, R.\, (R\ 0\ 1) \Rightarrow (\forall\, b\ c\ .\ (R\ b\ c) \Rightarrow (R\ (S\ b)\ (n \times c)\ )) \Rightarrow R\ n\ m\ r$$

# Naming functions: Hilbert operator

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

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

Using $\varepsilon$ is not (really) intuitionistic (see Coq exercise)