Bob Harper (Lect 2) [2018/07/17] 1

A type system consists of

$A \doteq A'$ w/ (A type iff $A \doteq A$)
$M \doteq M' \in A$ w/ ($M \in A$ iff $M \doteq M \in A$)

✓ symmetric & transitive
✓ if $A \doteq A'$ & $M \doteq M' \in A$ then $M \doteq M' \in A'$.

"I will assert the existence of certain type systems (for lack of time)."

⟶ defined in terms of evaluation using "certain constructions".

- Hypotheticals express <u>functionality</u>

$a : A \gg B$ type means B is a family of types that depends functionally on $a : A$.

$M \doteq M' \in A$ implies $B[M/a] \doteq B[M'/a]$

$a : A \gg N \in B$ means B is a fam. of elements

$M \doteq M' \in A$ implies $N[M/a] \doteq N[M'/a] \in B[M/a] \doteq B[M'/a]$

Similarly for $B \doteq B'$, $N \doteq N' \in B$.

presupposing $a : A \gg B$ type, A type.

eg) $\exists$ a type system containing booleans.

$\text{Bool} \doteq \text{Bool}$ i.e. Bool type

$M \doteq M' \in \text{Bool}$ iff either $M \Downarrow \text{true}$ & $M' \Downarrow \text{true}$
or $M \Downarrow \text{false}$ & $M' \Downarrow \text{false}$

<u>Fact</u>: If $a : \text{Bool} \gg B$ type & $M_1 \in B[\text{true}/a]$ and $M_2 \in B[\text{false}/a]$ and $M \in \text{Bool}$ then $\text{if}(M_1, M_2)(M) \in B[M/a]$

Bob Harper (Lect 2) [2018/07/17] ②

Proof: either $M \Downarrow \text{true}$ or $M \Downarrow \text{false}$

$\therefore M \doteq \text{true} \in \text{Bool}$ by head exp. or $\therefore M \doteq \text{false} \in \text{Bool}$ by head exp.

$M_1 \in B[\text{true}/a]$ ✓

$\text{if}(M_1, M_2)(M) \doteq \text{if}(M_1, M_2)(\text{true}) \doteq M_1 \in B[\text{true}/a]$

$\doteq B[M/a]$ ✓

(similarly for false.)

Exercise: Under similar assumptions, check:

1) $\text{if}(M_1, M_2)(\text{true}) \doteq M_1 \in B[\text{true}/a]$

2) $\text{if}(M_1, M_2)(\text{false}) \doteq M_2 \in B[\text{false}/a]$

3) $M \doteq \text{if}(\text{true}; \text{false})(M) \in \text{Bool}$

Shannon expansion (BDD's)

if $a : \text{Bool} \gg P \in B$ then

$P[M/a] \doteq \text{if}(P[\text{true}/a], P[\text{false}/a])(M)$

eg) $\exists$ type system containing the nats.

$\text{Nat} \doteq \text{Nat}$

(so we have an induction principle.)

$M \doteq M' \in \text{Nat}$ is "strongest" such that

either $M \Downarrow 0,\ M' \Downarrow 0$

or $M \Downarrow \text{succ}(N),\ M' \Downarrow \text{succ}(N')$

w/ $N \doteq N' \in \text{Nat}$

cf. consider $\underline{\text{fix}}(a.\text{succ}(a)) \longmapsto \text{succ}(\underline{\text{fix}}\ a.\text{succ}(a))$

$= \omega$ val

(an infinite stack of successors)

ω inhabits the greatest soln to the specification s.t. if $M \doteq M' \in \text{Nat}$ then $M \Downarrow 0, M' \Downarrow 0$ or $M \Downarrow \text{succ}(N), M' \Downarrow \text{succ}(N')$,

$N \doteq N' \in \text{CoNat}$

$$\mathrm{rec}(M_0, a.b.M_1)(M) \longmapsto \mathrm{rec}(M_0, a,b\,M_1)(M')$$

if $M \longmapsto M'$ $\quad R(0) \longmapsto M_0$

$$R(\mathrm{succ}(M)) \longmapsto M_1[M, \underbrace{R(M)}_{\text{result of rec call}}/a,b]$$

Fact: Suppose $a{:}Nat \gg B$ type

$M_0 \in B[0/a] \qquad a{:}Nat,\ b{:}B \gg M_1 \in B[\mathrm{succ}(a)/a]$

Then $M \in Nat$ then $R(M) \in B[M/a]$

Proof: 1) $M \Downarrow 0 \qquad M \doteq 0 \in Nat$

$M_0 \in B[0/a] \doteq B[M/a]$

$R(M) \doteq R(0) \doteq M_0$

i.e. $R(M) \in B[M/a]$ ✓

2) $M \Downarrow \mathrm{succ}(N) \qquad$ I.H. $R(N) \in B[N/a]$

Exercise: finish the proof.
(it's a lot like the conditional)

Preparation for higher inductive types

Products

$$A_1 \times A_2 \doteq A_1' \times A_2' \quad \text{if } A_1 \doteq A_1' \ \& \ A_2 \doteq A_2'$$

$M \doteq M' \in A_1 \times A_2$ iff $M \Downarrow \langle M_1, M_2 \rangle$ $\quad M_1 \doteq M_1' \in A_1$

$M' \Downarrow \langle M_1', M_2' \rangle$ $\quad M_2 \doteq M_2' \in A_2$

(assume these are values)

Fact: Suppose A_1 type, A_2 type. if $M \in A_1 \times A_2$ then $M.1 \in A_1$ and $M.2 \in A_2$

where $\dfrac{M \longmapsto M'}{M.i \longmapsto M'.i}$ $\qquad \dfrac{}{\langle M_1, M_2 \rangle . i \longmapsto M_i}$ $(i = 1, 2)$

Know $M \Downarrow \langle M_1, M_2 \rangle$ with $M_1 \in A_1$

$$M.1 \longmapsto^* \langle M_1, M_2 \rangle . 1 \longmapsto M_1 \in A_1$$

Fact If A_1 type, $M_1 \in A_1$ then $\langle M_1, M_2 \rangle . 1 \doteq M_1 \in A_1$

(no requirements on M_2!)

$$\underset{\langle M_1, M_2 \rangle . 1}{\underset{\uparrow}{M_1}} \doteq M_1 \in A_1$$

Functions

$$A_1 \longrightarrow A_2 \doteq A_1' \rightarrow A_2' \quad \text{iff } A_1 \doteq A_1' \ \& \ A_2 \doteq A_2'$$

$M \doteq M' \in A_1 \rightarrow A_2$ iff $M \Downarrow \lambda a. M_2$ $\quad M' \Downarrow \lambda a. M_2'$

$a : A_1 \gg M_2 \doteq M_2' \in A_2$

$$\dfrac{}{\lambda a. M \ \mathsf{val}}$$

$$\dfrac{M \longmapsto M'}{ap(M, M_1) \longmapsto ap(M', M_1)}$$

$$\dfrac{}{ap(\lambda a. M_2, M_1) \longmapsto M_2[M_1/a]}$$

Fact 1: If $M \in A_1 \to A_2$ and $M_1 \in A_1$ then $ap(M, M_1) \in A_2$

Proof: EXERCISE!

Fact 2 If $M, M' \in A_1 \to A_2$ and $a : A_1 \gg ap(M, a) \doteq ap(M', a) \in A_2$
then $M \doteq M' \in A_1 \to A_2$

"function extensionality".

Proof: EXERCISE!

Fact 1 says that the following rule is valid:

$$\frac{\Gamma \vdash M : A_1 \to A_2 \qquad \Gamma : M_1 : A_1}{\Gamma \vdash ap(M, M_1) : A_2} \qquad \frac{}{ap(\lambda a . M_2, M_1) \longmapsto M_2[M_1/a]}.$$

Observe: what is the quantifier complexity of

$M \doteq M' \in Nat \to Nat$? $\quad \forall \exists \longleftrightarrow \Pi^0_2$

"$\forall M_1 = M_1' \in Nat \quad \exists P_1 \doteq P_1' \in Nat$

$$\underset{\substack{\Downarrow \\ P_1}}{ap(M, M_1)} \doteq \underset{\substack{\Downarrow \\ P_1'}}{ap(M', M_1')} \in Nat$$

Dependent Products

$a : A_1 \times A_2 \doteq a : A_1' \times A_2'$ iff $A_1 \doteq A_1'$

$a : A_1 \gg A_2 \doteq A_2'$.

$M \doteq M' \in a : A_1 \times A_2$ iff

$M \Downarrow \langle M_1, M_2 \rangle \qquad M' \Downarrow \langle M_1', M_2' \rangle$

$M_1 \doteq M_1' \in A_1 \qquad M_2 \doteq M_2' \in A_2[M_1/a]$

$\doteq A_2[M_1'/a]$.

A_1 — $A_2[M_1]$, $A_2[M_2]$, ?

Dependent Functions

$a : A_1 \to A_2 \doteq a : A_1' \to A_2'$ iff $A_1 \doteq A_1'$

$a : A_1 \gg A_2 \doteq A_2'$

$M \doteq M' \in a : A_1 \to A_2$ iff

$M \Downarrow \lambda a.\, M_2 \qquad M' \Downarrow \lambda a.\, M_2'$

$a : a_1 \gg M_2 \doteq M_2' \in A_2(a)$

if $M_1 \doteq M_1' \in A_1$ then

$M_2[M_1/a] \doteq M_2[M_1'/a] \in A_2[M_1/a]$

$\doteq A_2[M_1'/a]$.

Fact:

1) If $M \in a : A_1 \times A_2$ then

$fst(M) \in A_1$ and $snd(M) \in A_2[fst(M)/a]$

2) if $M \in a : A_1 \to A_2$ & $M_1 \in A_1$ then

$ap(M, M_1) \in A_2[M_1/a]$.

$(\Sigma\, a : A_1 . A_2) \quad (\Pi\, a : A_1 , A_2)$

Exercises

Bool, Not, $a : A_1 \times A_2$, $a : A_1 \to A_2$

(inherently computational)