Harper 2

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 $A \doteq A'$ and $M \doteq M' \in A$ then $M \doteq M' \in A'$

I will <u>assert</u> the existence of certain type systems (for lack of time)

Hypotheticals express functionality

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

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

$a : A \overset{Ne}{\gg} B$ means B is a family of el' types

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

similarly for $B \doteq B'$, $N \doteq N' \in B$

defined in terms of evaluation
all about behavior of programs
using "certain constructions"

presupposition $a : A >> B$ type

A type

↳ for: $a : A >> N \in B$

(computational, semantic)

eg) there exists a type system containing booleans

$Bool \doteq Bool$ i.e. Bool type

$M \doteq M' \in Bool$ iff either ($M \Downarrow true$ and $M' \Downarrow true$)
or ($M \Downarrow false$ and $M' \Downarrow false$)

Fact: If $a : Bool >> B$ type and $M_1 \in B[true/a]$
(need to prove) and $M_2 \in B[false/a]$ and $M \in Bool$
then $if(M_1; M_2)(M) \in B[M/a]$.

(cf. program analysis)

$if(M_1; M_2)(M) \mapsto if(M_1; M_2)(M')$
when $M \mapsto M'$
$if(M_1; M_2)(true) \mapsto M_1$
$if(M_1; M_2)(false) \mapsto M_2$

Pf. either $M \Downarrow$ true or $M \Downarrow$ false

(from $M \in$ Bool) and def of $\in$ Bool

$\therefore M \doteq$ true $\in$ Bool (by head expansion)

$\therefore M \doteq$ false $\in$ Bool (by head expansion)

$M_1 \in B[\text{true}/a]$

if $(M_1; M_2)(M) \doteq$ if $(M_1; M_2)$(true) $\doteq M_1 \in B[\text{true}/a) \doteq B[M/a]$ (by head expansion)

similarly for false

$\boxtimes$

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

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

3) ... $M \doteq$ if (true; false)$(M) \in$ Bool (universal property)

if a: Bool $\gg P \in B$

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

("Shannon expansion" (Binary decision diagram)

"pivot on M")

eg.) ∃ type system containing natural numbers

$Nat \doteq Nat$

$M \doteq M \in Nat$ is (least, ck) strongest such that either $M \Downarrow 0$, $M' \Downarrow 0$

or $M \Downarrow succ(N)$ $M' \Downarrow succ(N')$

$N \doteq N' \in Nat$

N's are computations

want only nat comps

hence "strongest"

which gives us an induction principle (not usual one)

ef. consider

$fix\ (a.\ succ(a)) \longmapsto succ(fix\ a.\ succ(a))$ val

ω (call this)

infinite succ's

ω inhabits the greatest soln to spec,

$\overline{0\ \text{val}}$ $\overline{\text{succ}(M)\ \text{val}}$ $\text{rec}(M_0; a,b.M_1)(M)$

ω inhabits "greatest" soln

if $n = n' \in \text{Nat}$

then $n \Downarrow 0$ $n' \Downarrow 0$

or $n \Downarrow \text{succ}(N)$

$n' \Downarrow \text{succ}(N')$

$N \doteq N' \in \text{Co-Nat}$

pick "strongest" so that $\omega \notin \text{Nat}$

$R = \overbrace{\text{rec}(M_0; a,b.M_1)(M) \mapsto \text{rec}(M_0; a,b.M_1)(M') \text{ if } M \mapsto M'}$

$R(0) \mapsto M_0$

$R(\text{succ}(M)) \longmapsto M_1[M, R(M) / a, b]$

↑ pred ↑ result of recursive call

Fact. Suppose $a : Nat \gg B$ type

$M_0 \in B[0/a]$

$a : Nat, b : B \gg M_1 \in B[succ(a)/a]$

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

Pf. 1) $M \Downarrow 0$ $M_0 \doteq 0 \in Nat$ $M_0 \in B[0/a] \doteq B[M/a]$

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

ie $R(M) \in B[M/a]$ ✓

2) $M \Downarrow succ(N)$ IH: $R(N) \in B[N/a]$

Ex. → finish the proof

(a lot like conditional)

representative examples of inductive types

(coinductive — greatest versions)

∃ type system w/ these properties:

Products

$A_1 \times A_2 \doteq A_1' \times A_2'$ iff $A_1 \doteq A_1'$, $A_2 \doteq A_2'$

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

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

$M_1 \doteq M_1' \in A_1$

$M_2 \doteq M_2' \in A_2$

Fact.

under appropriate circumstances A_1 type, A_2 type

if $M \in A_1 \times A_2$

then $M \cdot 1 \in A_1$

and $M \cdot 2 \in A_2$

where $\dfrac{M \mapsto M'}{M \cdot i \mapsto M' \cdot i}$ $\qquad \dfrac{}{\langle M_1, M_2 \rangle \cdot i \mapsto M_i}\ i \in 1,2$

know $M \Downarrow \langle M_1, M_2 \rangle$ $\qquad M \cdot 1 \overset{*}{\longmapsto} \langle M_1, M_2 \rangle \cdot 1 \mapsto M_1 \in A_1$

with $M_1 \in A_1$

Fact (a little odd)

If A_1, ~~A_2~~ types

$M_1 \in A_1$

then $\langle M_1, M_2 \rangle \cdot 1 \doteq M_1 \in A_1$

note: no requirement on M_2

$M_1 \doteq M_1 \in A_1$

↕ steps to

$\langle M_1, M_2 \rangle \cdot 1$

Purpose of formal type system:

enforce protocol

Functions

$A_1 \to A_2 \doteq A_1' \to A_2'$ iff $A_1 \doteq A_1'$ and $A_2 \doteq A_2'$

$M \doteq M' \in A_1 \to A_2$ iff $M \Downarrow \lambda a.\, M_2$ $M' \Downarrow \lambda a.\, M_2'$

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

~~Fact.~~

$$\frac{}{\lambda a.M \text{ val}} \qquad \frac{M \mapsto M'}{ap(M, M_1) \longmapsto ap(M', M_1)}$$

in a total setup (no divergence, don't have to look at argument)

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

Fact. If $M_4 \in A_1 \to A_2$ and $M_1 \in A_1$
then $ap(M, M_1) \in A_2$

Pf. (exercise)

Fact. If $M, M' \in A_1 \to A_2$ and
and $a : A_1 >> ap(M, a) \doteq ap(M', a) \in A_2$
then $M \doteq M' \in A_1 \to A_2$ "function extensionality"

Pf exercise

This rule is valid

$$\frac{\Gamma \vdash M : A_1 \to A_2 \qquad \Gamma \vdash M_1 : A_1}{\Gamma \vdash ap(M, M_1) : A_2}$$

syntax or protocol

Observe: what is the quantifier complexity of judgement $M \doteq M' \in Nat \to Nat$

$\forall \; M_1 \doteq M_1' \in Nat$

$\exists \; P_1 \doteq P_1' \in Nat$

$ap(M, M_1) \doteq ap(M', M_1') \in Nat$

$\Downarrow$

$P_1 \doteq P_1'$

syntax

$$\frac{\cdots}{\Gamma \vdash M \equiv M' : Nat \to Nat}$$

meaning $\exists$ derivation that ends with

but $\exists$ does not capture $\forall$

cannot axiomatize equality in $Nat \to Nat$

Dependent products

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

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

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

iff $M \Downarrow \langle M_1, M_2 \rangle$ $\quad M' \Downarrow \langle M_1', M_2' \rangle$

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

(M_1 determines; eval to Type)

Dependent Functions

$$a_1:A_1 \to A_2 \doteq a:A_1' \to A_2' \text{ iff } A_1 \doteq A_1'$$

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

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

iff $M \Downarrow \lambda a.M_2$ $\quad M' \Downarrow \lambda a.M_2'$

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

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 $M \in a:A_1 \to A_2$

and $M_1 \in A_1$

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

(Exercises)

have Bool
Nat
$a:A_1 \times A_2$ Σ
$a:A_1 \to A_2$ Π

inherently computational in nature

[Ex Prove if $(17; true)(M) \in if(Nat; Bool)(M)$ for $M \in Bool$]

next time equality, identity types

propositions as types principle