Bob Harper
Carnegie Mellon University

July 17, 2018

1 Recap

1.1 A type system consists of

$$A \doteq A' \text{ with } (A \text{ type } \iff A \doteq A)$$
$$M \doteq M' \in A \text{ with } (M \in A \iff M \doteq M \in A)$$

- Symmetric and transitive
- If $A \doteq A'$ and $M \doteq M' \in A$ then $M \doteq M' \in A'$

We will assert the existence of certian type systems (for lack of time).

1.2 Hypotheticals express functionality

- $a : A >> B$ type means B is a family that depends functionally on $a : A$ of type $M \doteq M' \in A \implies B[M/a] \doteq B[M'/a]$
- $a : A >> N \in B$ means B is a family 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 $B \doteq B', N \doteq N' \in B$

This presupposes $a : A; A$ type $>> B$ type

2 Defining a type system

2.1 There exists a type system containing booleans

Bool $\doteq$ Bool or 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 $M_1 \in B[\text{true}/a]$ and $M_2 \in B[\text{false}/a]$ and $M \in$ Bool
Then: if$(M_1, M_2)(M) \in B[M/a]$
Proof:

Either $M \Downarrow \text{true}$ or $M \Downarrow \text{false}$
By head espansion: $M \doteq \text{true} \in \text{Bool}$ or $M \doteq \text{false} \in \text{Bool}$

$$\frac{M \mapsto M'}{\text{if } (M_1; M_2)(M) \mapsto \text{if } (M_1; M_2)(M')}$$
$$\text{if } (M_1; M_2)(\text{true}) \mapsto M_1$$
$$\text{if } (M_1; M_2)(\text{false}) \mapsto M_2$$

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

Exercises:

1. $\ldots$ if $(M_1; M_2)(\text{true}) \doteq M_1 \in B[\text{true}/a]$
2. $\ldots$ if $(M_1; M_2)(\text{false}) \doteq M_2 \in B[\text{false}/a]$
3. $\ldots M \doteq$ if $(M_1; M_2)(M) \in \text{Bool}$
   $\ldots$ if $a : \text{Bool}$

Example: $\exists$ a type system containing the natural numbers
$\overline{\text{Nat} \doteq \text{Nat}}$
$M \doteq M' \in \text{Nat}$ is the strongest s.t. either

- $M \Downarrow 0$ and $M' \Downarrow 0$
- $M \Downarrow succ(N)$ and $M' \Downarrow succ(N')$ with $N \doteq N' \in \text{Nat}$

Valuations:

$$\overline{0 \text{ val}}$$
$$\overline{succ(M) \text{ val}}$$
$$rec(M_0; a, b.M_1)(M) \mapsto rec(M_0; a, b.M_1)(M') \text{ if } M \mapsto M'$$
$$R(0) \mapsto M_0$$
$$R(succ(M)) \mapsto M_1[M, R(M)/a, b]$$

Consider $fix(a, succ(a)) \mapsto succ(fix(a.succ(a)))$ val $\leftarrow \omega$
ω inhabits the greatest solution to specification:
i.e.: $M \doteq M' \in \text{Nat}$ then $M \Downarrow 0; M' \Downarrow 0$ or $M \Downarrow succ(N); M' \Downarrow succ(N'); N \doteq N' \in \text{CoNat}$
Fact:
Suppose $a : \text{Nat} >> B$ type
$M_0 \in B[0/a]$
$a : \text{Nat}, b : B >> M_1 \in B[succ(a)/a]$
Then: $M \in \text{Nat}$ then $R(M) \in B[M/a]$
Proof:

1. $M \Downarrow 0; M \doteq 0 \in \text{Nat}; M_0 \in B[0/a] \doteq B[M/a]$
   $R(M) \doteq R(0) \doteq M_0$
   i.e.: $R(M) \in B[M/a]$

2. $M \Downarrow succ(N)$ I.H.: $R(N) \in B[N/a]$
   Finish the proof...

2.2 Products

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

$$\begin{aligned} M \doteq M' \in A_1 \times A_2 \iff & M \Downarrow < M_1; M_2 >; M_1 \doteq M_1' \in A_1 \\ & M' \Downarrow < M_1'; M_2' >; M_2 \doteq M_2' \in A_2 \end{aligned}$$

Fact: Suppose A_1 type and A_2 type
If $M \in A_1 \times A_2$
Then $M \bullet l \in A_1$ and $M \bullet r \in A_2$
Where:

$$\frac{M \mapsto M'}{M \bullet l \mapsto M' \bullet l}$$

$$\frac{}{< M_1; M_2 > \bullet l \mapsto M_1}$$

2.3 Functions

$$A_1 \to A_2 \doteq A_1' \to A_2' \iff A_1 \doteq A_1' \text{ and } A_2 \doteq A_2'$$

$$\begin{aligned} M \doteq M' \in A_1 \to A_2 \iff & M \Downarrow \lambda a.M_2; M' \Downarrow \lambda a.M_2' \\ & a : A_1 >> M_2 \doteq M_2' \in A_2 \end{aligned}$$

Valuations:

$$\frac{}{\lambda a.M \text{ val}}$$

$$\frac{M \mapsto M'}{ap(M; M_1) \mapsto ap(M'; M_1}$$

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

Fact:
If $M \in A_1 \to A_2$ and $M_1 \in A_1$ then $ap(M; M_1) \in A_2$
Fact:
If $(M; M_1) \in A_1 \to A_2$ and $a : A_1 >> ap(M; a) \doteq ap(M'; a) \in A_2$
Then $M \doteq M' \in A_1 \to A_2$

2.4 Dependent Products

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

$$\begin{aligned} M \doteq M' \in a : A_1 \times A_2 \iff & M \Downarrow < M_1; M_2 >; M' \Downarrow < M_1'; M_2' > \\ & M_1 \doteq M_1' \in A_1 \\ & M_2 \doteq M_2' \in A_2[M_1/a] \doteq A_2[M_1'/a] \end{aligned}$$

2.5 Dependent Functions

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

$$\begin{aligned} M \doteq M' \in a : A_1 \to A_2 \iff & M \Downarrow \lambda a.M_2; M' \Downarrow \lambda a.M_2' \\ & a : A_1 >> M_2 \doteq M_2' \in A_2(a) \end{aligned}$$

<u>Fact</u>:

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