Axioms of OS_{do}

(Const) $$\frac{}{\eta, k \Downarrow k}$$

(Var) $$\frac{}{\eta, x \Downarrow \eta(x)}$$

(Abstr) $$\frac{}{\eta, \text{fun } x \to e \Downarrow \langle \text{fun } x \to e, \eta \rangle}$$

(Rec) $$\frac{}{\eta, \text{rec } f = e \Downarrow \langle e, \eta' \rangle}$$

where $\eta' = \eta[f \to \langle e, \eta' \rangle]$

Rules of inference

(δ)

$$\frac{\eta, e_1 \Downarrow v_1 \qquad \eta, e_2 \Downarrow v_2 \qquad v_1 \oplus v_2 = v}{\eta \vdash e_1 \oplus e_2 \Downarrow v}$$

(app)

$$\frac{\eta, e_1 \Downarrow \langle \text{fun } x \to e, \eta' \rangle \qquad \eta, e_2 \Downarrow v \qquad \eta'[x \to v], e \Downarrow v'}{\eta, e_1\, e_2 \Downarrow v}$$

Example of OS_{clo}

$$\underbrace{(\text{fun } g \to g\ (g\ 5))}_{e}\ \underbrace{(\text{fun } a \to a+1)}_{e'}$$

$x : g$

$e : g\ (g\ 5)$

$\eta' : \emptyset$

$$\text{App}\ \dfrac{\text{Abstr}\ \dfrac{}{\emptyset, e \Downarrow \langle e, \emptyset \rangle} \qquad \text{Abstr}\ \dfrac{}{\emptyset, e' \Downarrow \langle e', \emptyset \rangle} \qquad \text{App}\ \dfrac{}{\emptyset[g \mapsto \langle e', \emptyset \rangle],\ g\ (g\ 5) \Downarrow 7}}{\underbrace{\emptyset}_{\eta},\ \underbrace{e}_{e_1}\ \underbrace{e'}_{e_2} \Downarrow \underbrace{7}_{v'}}$$

$$e' = \text{fun } a \to a+1$$

$$\dfrac{}{\phi[a\to 6],\ 1 \Downarrow 1}\ \text{Const}$$

$$\dfrac{}{\phi[a\to 6],\ a \Downarrow 6}\ \text{Var}$$

$$\dfrac{\phi[a\to 6],\ a \Downarrow 6 \qquad \phi[a\to 6],\ 1 \Downarrow 1}{\phi[a\to 6],\ a+1 \Downarrow 7}\ +$$

$x : a$

$e : a+1$

$$\dfrac{}{\phi[g \to \langle e', \phi\rangle],\ g \Downarrow \langle \underbrace{e'}_{\lambda}, \underbrace{\phi}_{\eta'} \rangle}\ \text{Var}$$

$$\textcircled{A}\quad \dfrac{}{\phi[g\to \ldots](g\ 5) \Downarrow \underbrace{6}_{v}}\ \text{App}$$

$$\dfrac{\phi[g \to \langle e', \phi\rangle],\ g \Downarrow \langle e', \phi\rangle \qquad \phi[g\to \ldots](g\ 5) \Downarrow 6 \qquad \phi[a\to 6],\ a+1 \Downarrow 7}{\underbrace{\phi[g \to \langle e', \phi\rangle]}_{\eta},\ \underbrace{g}_{e_1}\ \underbrace{(g\ 5)}_{e_2} \Downarrow \underbrace{7}_{v'}}\ \text{App}$$

$e' = \text{fun } a \to a+1$

$x:\ a$
$e:\ a+1$

$$
A \quad
\dfrac{
\dfrac{}{\eta_1, g \Downarrow \langle e', \emptyset \rangle}\,\text{Var}
\qquad
\dfrac{}{\eta_1, 5 \Downarrow 5}\,\text{Const}
\qquad
\dfrac{
\dfrac{}{\emptyset[a \to 5], a \Downarrow 5}\,\text{Var}
\quad
\dfrac{}{\emptyset[a \to 5], 1 \Downarrow 1}\,\text{Const}
}{\emptyset[a \to 5], a+1 \Downarrow 6}\,\delta
}{
\underbrace{\emptyset[g \to \langle e', \emptyset \rangle]}_{\eta_1},\ g\ 5 \Downarrow 6
}\,\text{App}
$$

η' v

(Var) $$\frac{\Gamma(x) = \sigma \quad , \quad \tau \leq \sigma}{\Gamma \vdash x : \tau}$$

(Abstr) $$\frac{\Gamma[x : \tau] \vdash e : \tau'}{\Gamma \vdash \text{fun } x \to e : \tau \to \tau'}$$

(App) $$\frac{\Gamma \vdash e_1 : \tau \to \tau' \qquad \Gamma \vdash e_2 : \tau}{\Gamma \vdash e_1\, e_2 : \tau'}$$

T_{ocaml}

(Tuple)
$$\frac{\Gamma \vdash e_1 : \tau_1 \qquad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash (e_1, e_2) : \tau_1 * \tau_2}$$

(let)
$$\frac{\Gamma \vdash e : \tau \qquad \Gamma[x : GEN_\Gamma(\tau)] \vdash e' : \tau'}{\Gamma \vdash \text{let } x = e \text{ in } e' : \tau'}$$

(letrec)
$$\frac{\Gamma[x : \tau] \vdash e : \tau \qquad \Gamma[x : GEN_\Gamma(\tau)] \vdash e' : \tau'}{\Gamma \vdash \text{let rec } x = e \text{ in } e' : \tau'}$$

Example of Tocaml

let h = fun x -> fun y -> y+1
in let g = fun a -> h true a
in g 3

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{\dfrac{}{\emptyset[\ldots] \vdash y : int}\,\text{Var} \qquad \dfrac{}{\emptyset[\ldots] \vdash 1 : int}\,\text{Const}}
            {\underbrace{\emptyset[x:\alpha,\ y:int]}_{\Gamma} \vdash y+1 : int}\,\delta
    }{
      \emptyset[x:\alpha] \vdash \text{fun } \overset{x}{y} \to \underbrace{y+1}_{e} : \underset{\tau}{int} \to \underset{\tau'}{int}
    }\,\text{Abs}
  }{
    \underset{\Gamma}{\emptyset} \vdash \text{fun } \underset{x}{x} \to \underbrace{\text{fun } y \to y+1}_{e} : \alpha \to \underbrace{int \to int}_{\tau'}
  }\,\text{Abs}
  \qquad
  \dfrac{
    \dfrac{A}{\Gamma_1 \vdash \text{fun } a \to \ldots : int \to int} \qquad \dfrac{B}{\Gamma_1[g:-] \vdash g\,3 : int}
  }{
    \underbrace{\emptyset[h : \forall\alpha.\ \alpha \to int \to int]}_{\Gamma_1} \vdash \text{let } g = \ldots : int
  }
}{
  \emptyset \vdash \text{let } h = \ldots \text{ in } g\,3 : int
}\,\text{let}
$$

A

$$\Gamma_1 = \emptyset[h : \forall\alpha.\,\alpha \to \text{int} \to \text{int}]$$

$$\text{Abs}\ \dfrac{\dfrac{\dfrac{\dfrac{\text{bool}\to\text{int}\to\text{int} \le \forall\alpha.\alpha\to\text{int}\to\text{int}}{\Gamma_2 \vdash h : \text{bool}\to\text{int}\to\text{int}}\,\text{Var} \qquad \dfrac{}{\Gamma_2 \vdash \text{true} : \text{bool}}\,\text{Const}}{\Gamma_2 \vdash h\ \text{true} : \text{int}\to\text{int}} \qquad \dfrac{}{\Gamma_2 \vdash a : \text{int}}\,\text{Var}}{\underbrace{\Gamma_1[a : \text{int}]}_{\Gamma_2} \vdash (h\ \text{true})\ a : \text{int}}\,\text{App}}{\underbrace{\Gamma_1}_{\Gamma} \vdash \text{fun}\ \underbrace{a}_{x} \to \underbrace{h\ \text{true}\ a}_{e} : \underbrace{\text{int}}_{\tau} \to \underbrace{\text{int}}_{\tau'}}$$

(B) $\Gamma_1 = \emptyset[h : \forall\alpha.\ \alpha \to \mathit{int} \to \mathit{int}]$

$$\dfrac{\dfrac{}{\Gamma_1[g : \dots] \vdash g : \underbrace{\mathit{int} \to \mathit{int}}_{\tau \to \tau'}}\ \text{Var} \qquad \dfrac{}{\Gamma_1[g : \dots] \vdash 3 : \underbrace{\mathit{int}}_{\tau}}\ \text{Const}}{\underbrace{\Gamma_1[g : \mathit{int} \to \mathit{int}]}_{\Gamma} \vdash \underbrace{g}_{e_1}\ \underbrace{3}_{e_2} : \underbrace{\mathit{int}}_{\tau'}}\ \text{App}$$

Inference rules of Hoare logic

$$\frac{}{P[e/x]\ \{x := e\}\ P}$$

$$\frac{P\ \&\ b\ \{S\}\ P}{P\ \{\text{while } (b)\ S\}\ P\ \&\ \neg b}$$

$$\frac{P\ \{S_1\}\ Q \quad Q\ \{S_2\}\ R}{P\ \{S_1; S_2\}\ R}$$

$$\frac{P \Rightarrow P' \quad P'\ \{S\}\ Q' \quad Q' \Rightarrow Q}{P\ \{S\}\ Q}$$

$$\frac{P\ \&\ b\ \{S_1\}\ Q \quad P\ \&\ \neg b\ \{S_2\}\ Q}{P\ \{\text{if } (b) \text{ then } S_1 \text{ else } S_2\}\ Q}$$

$\text{true}\ \{\ i := 0;\ \ l := l_0;$

$\quad \text{while}\ (l \neq [\,]\ \&\ a \neq \text{hd}\ l)\ \{$

$\qquad l := \text{tl}\ l;$

$\qquad i := i+1;$

$\quad \}\ \ \}\ \ l = [\,] \vee (l \neq [\,]\ \&\ a = \text{hd}(\text{tl}^i\, l_0))$

$\text{Inv}:\ \ l = \text{tl}^i(l_0)$

$\text{Want}\ \ \text{Inv}\ \&\ (l = [\,] \vee a = \text{hd}\ l)$

$\qquad \Rightarrow l = [\,] \vee (l \neq [\,]\ \&\ a = \text{hd}\ (\text{tl}^i\, l_0))$