MPP 2025/26 (0077A, 9CFU)

Models for Programming Paradigms

Roberto Bruni Filippo Bonchi
http://www.di.unipi.it/~bruni/

https://didawiki.di.unipi.it/doku.php/magistraleinformatica/mpp/start

15 - HOFL: Consistency?

HOFL
Operational vs Denotational

Differences

operational $t \to c$

closed, typeable terms

no environment

not a congruence

canonical terms

denotational $[\![t]\!]\,\rho$

typeable terms

environment

congruence

mathematical entities

$$\forall t, c. \quad t \to c \quad \overset{?}{\Leftrightarrow} \quad \forall \rho.\ [\![t]\!]\,\rho = [\![c]\!]\,\rho$$

$$t \to c \Rightarrow \forall \rho.\ [\![t]\!]\,\rho = [\![c]\!]\,\rho$$

$$(\forall \rho.\ [\![t]\!]\,\rho = [\![c]\!]\,\rho) \not\Rightarrow t \to c$$

there is only one type for which the implication holds

Inconsistency: example

$x : int$ $\qquad c_0 = \lambda x.\, x + 0$ $\qquad c_1 = \lambda x.\, x$

already in canonical forms

$[\![c_0]\!]\,\rho = [\![c_1]\!]\,\rho$ $\qquad c_0 \not\to c_1$

$$[\![c_0]\!]\,\rho = [\![\lambda x.\, x+0]\!]\,\rho = \lfloor \lambda d.\, d \underline{+}_{\perp} \lfloor 0 \rfloor \rfloor = \lfloor \lambda d.\, d \rfloor = [\![\lambda x.\, x]\!]\,\rho = [\![c_1]\!]\,\rho$$

Correctness

TH. $t \to c \Rightarrow \forall \rho.\ [\![t]\!]\rho = [\![c]\!]\rho$

proof. we proceed by rule induction

$$P(t \to c) \stackrel{\text{def}}{=} \forall \rho.\ [\![t]\!]\rho = [\![c]\!]\rho$$

$$\frac{}{c \to c}$$

$$P(c \to c) \stackrel{\text{def}}{=} \forall \rho.\ [\![c]\!]\rho = [\![c]\!]\rho$$ obvious

TH. $t \to c \Rightarrow \forall \rho.\ [\![t]\!]\rho = [\![c]\!]\rho$ (continue)

$$\frac{t_1 \to n_1 \quad t_2 \to n_2}{t_1 \text{ op } t_2 \to n_1 \underline{\text{op}}\ n_2}$$

assume

$$P(t_1 \to n_1) \stackrel{\text{def}}{=} \forall \rho.\ [\![t_1]\!]\rho = [\![n_1]\!]\rho = \lfloor n_1 \rfloor$$

$$P(t_2 \to n_2) \stackrel{\text{def}}{=} \forall \rho.\ [\![t_2]\!]\rho = [\![n_2]\!]\rho = \lfloor n_2 \rfloor$$

we prove $P(t_1 \text{ op } t_2 \to n_1 \underline{\text{op}}\ n_2) \stackrel{\text{def}}{=} \forall \rho.\ [\![t_1 \text{ op } t_2]\!]\rho = \left[\!\!\left[n_1 \underline{\text{op}}\ n_2 \right]\!\!\right]\rho$

$$\begin{aligned}
[\![t_1 \text{ op } t_2]\!]\rho &= [\![t_1]\!]\rho\ \underline{\text{op}}_\perp\ [\![t_2]\!]\rho && \text{(by definition of } [\![\cdot]\!]) \\
&= \lfloor n_1 \rfloor\ \underline{\text{op}}_\perp\ \lfloor n_2 \rfloor && \text{(by inductive hypotheses)} \\
&= \lfloor n_1 \underline{\text{op}}\ n_2 \rfloor && \text{(by definition of } \underline{\text{op}}_\perp) \\
&= \left[\!\!\left[n_1 \underline{\text{op}}\ n_2 \right]\!\!\right]\rho && \text{(by definition of } [\![\cdot]\!])
\end{aligned}$$

TH. $t \to c \Rightarrow \forall\rho.\ [\![t]\!]\,\rho = [\![c]\!]\,\rho$ (continue)

$$\frac{t \to 0 \quad t_0 \to c_0}{\textbf{if}\ t\ \textbf{then}\ t_0\ \textbf{else}\ t_1 \to c_0}$$

assume

$$P(t \to 0) \stackrel{\text{def}}{=} \forall\rho.\ [\![t]\!]\,\rho = [\![0]\!]\,\rho = \lfloor 0 \rfloor$$

$$P(t_0 \to c_0) \stackrel{\text{def}}{=} \forall\rho.\ [\![t_0]\!]\,\rho = [\![c_0]\!]\,\rho$$

we prove $P(\textbf{if}\ t\ \textbf{then}\ t_0\ \textbf{else}\ t_1 \to c_0) \stackrel{\text{def}}{=} \forall\rho.\ [\![\textbf{if}\ t\ \textbf{then}\ t_0\ \textbf{else}\ t_1]\!]\,\rho = [\![c_0]\!]\,\rho$

$$\begin{aligned}
[\![\textbf{if}\ t\ \textbf{then}\ t_0\ \textbf{else}\ t_1]\!]\,\rho &= Cond([\![t]\!]\,\rho, [\![t_0]\!]\,\rho, [\![t_1]\!]\,\rho) && \text{(by def. of } [\![\cdot]\!]) \\
&= Cond(\lfloor 0 \rfloor, [\![t_0]\!]\,\rho, [\![t_1]\!]\,\rho) && \text{(by ind. hyp.)} \\
&= [\![t_0]\!]\,\rho && \text{(by def. of } Cond) \\
&= [\![c_0]\!]\,\rho && \text{(by ind. hyp.)}
\end{aligned}$$

ifn) analogous (omitted)

TH. $t \to c \Rightarrow \forall \rho.\ [\![t]\!]\rho = [\![c]\!]\rho$ (continue)

$$\frac{t \to (t_0, t_1) \quad t_0 \to c_0}{\mathbf{fst}(t) \to c_0}$$

assume

$$P(t \to (t_0, t_1)) \stackrel{\text{def}}{=} \forall \rho.\ [\![t]\!]\rho = [\![(t_0, t_1)]\!]\rho$$

$$P(t_0 \to c_0) \stackrel{\text{def}}{=} \forall \rho.\ [\![t_0]\!]\rho = [\![c_0]\!]\rho$$

we prove $P(\mathbf{fst}(t) \to c_0) \stackrel{\text{def}}{=} \forall \rho.\ [\![\mathbf{fst}(t)]\!]\rho = [\![c_0]\!]\rho$

$$\begin{aligned}
[\![\mathbf{fst}(t)]\!]\rho &= \pi_1^*([\![t]\!]\rho) && \text{(by def. of } [\![\cdot]\!]) \\
&= \pi_1^*([\![(t_0, t_1)]\!]\rho) && \text{(by ind. hyp.)} \\
&= \pi_1^*(\lfloor([\![t_0]\!]\rho, [\![t_1]\!]\rho)\rfloor) && \text{(by def. of } [\![\cdot]\!]) \\
&= \pi_1([\![t_0]\!]\rho, [\![t_1]\!]\rho) && \text{(by def. of lifting)} \\
&= [\![t_0]\!]\rho && \text{(by def. of } \pi_1) \\
&= [\![c_0]\!]\rho && \text{(by ind. hyp.)}
\end{aligned}$$

snd) analogous (omitted)

TH. $t \to c \Rightarrow \forall \rho.\ [\![t]\!]\rho = [\![c]\!]\rho$ (continue)

$$\frac{t_1 \to \lambda x.\, t_1' \qquad t_1'[^{t_0}/_x] \to c}{(t_1\ t_0) \to c}$$

assume

$P(t_1 \to \lambda x.\, t_1') \stackrel{\text{def}}{=} \forall \rho.\ [\![t_1]\!]\rho = [\![\lambda x.\, t_1']\!]\rho$

$P(t_1'[^{t_0}/_x] \to c) \stackrel{\text{def}}{=} \forall \rho.\ [\![t_1'[^{t_0}/_x]]\!]\rho = [\![c]\!]\rho$

we prove $P((t_1\ t_0) \to c) \stackrel{\text{def}}{=} \forall \rho.\ [\![(t_1\ t_0)]\!]\rho = [\![c]\!]\rho$

$$\begin{aligned}
[\![(t_1\ t_0)]\!]\rho &= \textbf{let}\ \varphi \Leftarrow [\![t_1]\!]\rho.\ \varphi([\![t_0]\!]\rho) && \text{(by definition of } [\![\cdot]\!]) \\
&= \textbf{let}\ \varphi \Leftarrow [\![\lambda x.\, t_1']\!]\rho.\ \varphi([\![t_0]\!]\rho) && \text{(by ind. hypothesis)} \\
&= \textbf{let}\ \varphi \Leftarrow \lfloor \lambda d.\ [\![t_1']\!]\rho[^d/_x] \rfloor.\ \varphi([\![t_0]\!]\rho) && \text{(by definition of } [\![\cdot]\!]) \\
&= (\lambda d.\ [\![t_1']\!]\rho[^d/_x])\ ([\![t_0]\!]\rho) && \text{(by de-lifting)} \\
&= [\![t_1']\!]\rho[^{[\![t_0]\!]\rho}/_x] && \text{(by application)} \\
&= [\![t_1'[^{t_0}/_x]]\!]\rho && \text{(by Subst. Lemma)} \\
&= [\![c]\!]\rho && \text{(by ind. hypothesis)}
\end{aligned}$$

TH. $t \to c \Rightarrow \forall \rho.\ [\![t]\!]\,\rho = [\![c]\!]\,\rho$ (continue)

$$\frac{t[^{\mathbf{rec}\ x.\ t}/_x] \to c}{\mathbf{rec}\ x.\ t \to c}$$

assume

$$P(t[^{\mathbf{rec}\ x.\ t}/_x] \to c) \stackrel{\text{def}}{=} \forall \rho.\ [\![t[^{\mathbf{rec}\ x.\ t}/_x]]\!]\,\rho = [\![c]\!]\,\rho$$

we prove $P(\mathbf{rec}\ x.\ t \to c) \stackrel{\text{def}}{=} \forall \rho.\ [\![\mathbf{rec}\ x.\ t]\!]\,\rho = [\![c]\!]\,\rho$

$$\begin{aligned}
[\![\mathbf{rec}\ x.\ t]\!]\,\rho &= [\![t]\!]\,\rho[^{[\![\mathbf{rec}\ x.\ t]\!]\rho}/_x] && \text{(by definition)}\\
&= [\![t[^{\mathbf{rec}\ x.\ t}/_x]]\!]\,\rho && \text{(by the Substitution Lemma)}\\
&= [\![c]\!]\,\rho && \text{(by inductive hypothesis)}
\end{aligned}$$

HOFL convergence
Operational vs Denotational

Operational convergence

$t : \tau$ closed

$$t\downarrow \quad \Leftrightarrow \quad \exists c \in C_\tau .\, t \longrightarrow c$$

$$t\uparrow \quad \Leftrightarrow \quad \neg\; t\downarrow$$

Examples

$$\mathbf{rec}\ x.\ x \ \uparrow$$

$$\lambda y.\ \mathbf{rec}\ x.\ x \ \downarrow$$

$$(\lambda y.\ \mathbf{rec}\ x.\ x)\ 0 \ \uparrow$$

$$\mathbf{if}\ 0\ \mathbf{then}\ 1\ \mathbf{else}\ \mathbf{rec}\ x.\ x \ \downarrow$$

Denotational converg.

$t : \tau$ closed

$$t \Downarrow \quad \Leftrightarrow \quad \forall \rho \in Env, \exists v \in V_\tau. \ [\![t]\!]\rho = \lfloor v \rfloor$$

$$t \Uparrow \quad \Leftrightarrow \quad \neg \ t \Downarrow$$

Examples

$$[\![\mathbf{rec}\ x.\ x]\!]\rho \ \Uparrow$$

$$[\![\lambda y.\ \mathbf{rec}\ x.\ x]\!]\rho \ \Downarrow$$

$$[\![(\lambda y.\ \mathbf{rec}\ x.\ x)\ 0]\!]\rho \ \Uparrow$$

$$[\![\mathbf{if}\ 0\ \mathbf{then}\ 1\ \mathbf{else}\ \mathbf{rec}\ x.\ x]\!]\rho \ \Downarrow$$

Consistency on converg.

TH. $t : \tau$ closed $\quad t\downarrow \;\Rightarrow\; t\Downarrow$

proof.

$t\downarrow$	$\Rightarrow$	$t \to c$	by def (for some c)
	$\Rightarrow$	$\forall\rho.\ [\![t]\!]\,\rho = [\![c]\!]\,\rho$	by correctness
	$\Rightarrow$	$\forall\rho.\ [\![t]\!]\,\rho \neq \bot$	canonical $[\![c]\!]\,\rho \neq \bot$
	$\Rightarrow$	$t\Downarrow$	by def

TH. $t : \tau$ closed $\quad t\Downarrow \;\Rightarrow\; t\downarrow$

the proof is not part of the program of the course
(structural induction would not work)

HOFL equivalence
Operational vs Denotational

HOFL equivalences

$t_0, t_1 : \tau$ closed

$$t_0 \equiv_{\mathrm{op}} t_1 \quad \text{iff} \quad \forall c.\ t_0 \to c \ \Leftrightarrow t_1 \to c$$

$$t_0 \equiv_{\mathrm{den}} t_1 \quad \text{iff} \quad \forall \rho.\ [\![t_0]\!]\rho = [\![t_1]\!]\rho$$

Op is more concrete

TH. $\equiv_{\mathrm{op}} \subseteq \equiv_{\mathrm{den}}$

proof. take $t_0, t_1 : \tau$ closed, such that $t_0 \equiv_{\mathrm{op}} t_1$

either $\exists c.\ t_0 \to c \ \wedge\ t_1 \to c$ or $t_0 \uparrow \wedge\ t_1 \uparrow$

if $\exists c.\ t_0 \to c \ \wedge\ t_1 \to c$

by correctness $\forall \rho.\ [\![t_0]\!] \rho = [\![c]\!] \rho = [\![t_1]\!] \rho$ thus $t_0 \equiv_{\mathrm{den}} t_1$

if $t_0 \uparrow \wedge\ t_1 \uparrow$

by agreement on convergence $t_0 \Uparrow \wedge\ t_1 \Uparrow$

i.e. $\forall \rho.\ [\![t_0]\!] \rho = \bot_{D_\tau} = [\![t_1]\!] \rho$ thus $t_0 \equiv_{\mathrm{den}} t_1$

Den is strictly more abstract

TH. $\equiv_{\mathrm{den}} \not\subseteq \equiv_{\mathrm{op}}$

proof.

see previous counterexample

$x : int$ $\qquad c_0 = \lambda x.\, x + 0$ $\qquad c_1 = \lambda x.\, x$

Consistency on int

TH. $t : int$ closed $\qquad t \to n \quad \Leftrightarrow \quad \forall \rho. [\![t]\!] \rho = \lfloor n \rfloor$

proof.

$\Rightarrow)$ if $t \to n$ then $[\![t]\!] \rho = [\![n]\!] \rho = \lfloor n \rfloor$

$\Leftarrow)$ if $[\![t]\!] \rho = \lfloor n \rfloor$ it means $t \Downarrow$

by agreement on convergence $t \downarrow$

thus $t \to m$ for some m

but then by correctness $[\![t]\!] \rho = [\![m]\!] \rho = \lfloor m \rfloor$

and it must be $m = n$

Equivalence on int

TH. $t_0, t_1 : int \quad t_0 \equiv_{\text{op}} t_1 \;\Leftrightarrow\; t_0 \equiv_{\text{den}} t_1$

proof. we know $t_0 \equiv_{\text{op}} t_1 \;\Rightarrow\; t_0 \equiv_{\text{den}} t_1$

we prove $t_0 \equiv_{\text{den}} t_1 \;\Rightarrow\; t_0 \equiv_{\text{op}} t_1$

assume $t_0 \equiv_{\text{den}} t_1$ either $\forall \rho.\; [\![t_0]\!]\rho = \bot_{\mathbb{Z}_\bot} = [\![t_1]\!]\rho$

or $\forall \rho.\; [\![t_0]\!]\rho = \lfloor n \rfloor = [\![t_1]\!]\rho$ for some n

if $\forall \rho.\; [\![t_0]\!]\rho = \bot_{\mathbb{Z}_\bot} = [\![t_1]\!]\rho$ then $t_0 \Uparrow, t_1 \Uparrow$

by agreement on convergence $t_0 \uparrow, t_1 \uparrow$ thus $t_0 \equiv_{\text{op}} t_1$

if $\forall \rho.\; [\![t_0]\!]\rho = \lfloor n \rfloor = [\![t_1]\!]\rho$ then $t_0 \to n \;,\; t_1 \to n$

thus $t_0 \equiv_{\text{op}} t_1$

HOFL
Unlifted Semantics

Unlifted Domains

lifted domains

$$D_\tau \triangleq (V_\tau)_\perp$$

$$V_{int} \triangleq \mathbb{Z}$$

$$V_{\tau_1 * \tau_2} \triangleq D_{\tau_1} \times D_{\tau_2} = (V_{\tau_1})_\perp \times (V_{\tau_2})_\perp$$

$$V_{\tau_1 \to \tau_2} \triangleq [D_{\tau_1} \to D_{\tau_2}] = [(V_{\tau_1})_\perp \to (V_{\tau_2})_\perp]$$

unlifted domains

$$U_{int} \triangleq \mathbb{Z}_\perp$$

$$U_{\tau_1 * \tau_2} \triangleq U_{\tau_1} \times U_{\tau_2}$$

$$U_{\tau_1 \to \tau_2} \triangleq [U_{\tau_1} \to U_{\tau_2}]$$

Unlifted Semantics

as before

$$(\!|n|\!)\rho \triangleq \lfloor n \rfloor$$

$$(\!|x|\!)\rho \triangleq \rho(x)$$

$$(\!|t_1 \ \mathsf{op}\ t_2|\!)\rho \triangleq (\!|t_1|\!)\rho \ \underline{\mathsf{op}}_{\bot}\ (\!|t_2|\!)\rho$$

$$(\!|\mathbf{if}\ t\ \mathbf{then}\ t_1\ \mathbf{else}\ t_2|\!)\rho \triangleq \mathsf{Cond}_{\tau}(\ (\!|t|\!)\rho\ ,\ (\!|t_1|\!)\rho\ ,\ (\!|t_2|\!)\rho\ )$$

$$(\!|\mathbf{rec}\ x.\ t|\!)\rho \triangleq \mathit{fix}\ \lambda d.\ (\!|t|\!)\rho[^d/_x]$$

---

without lifting

$$(\!|(t_1\ ,\ t_2)|\!)\rho \triangleq (\ (\!|t_1|\!)\rho\ ,\ (\!|t_2|\!)\rho\ )$$

$$(\!|\mathbf{fst}(\ t\ )|\!)\rho \triangleq \pi_1\ (\ (\!|t|\!)\rho\ )$$
$$(\!|\mathbf{snd}(\ t\ )|\!)\rho \triangleq \pi_2\ (\ (\!|t|\!)\rho\ )$$

$$(\!|\lambda x.\ t|\!)\rho \triangleq \lambda d.\ (\!|t|\!)\rho[^d/_x]$$

$$(\!|\ t\ t_0\ |\!)\rho \triangleq (\ (\!|t|\!)\rho\ )\ (\ (\!|t_0|\!)\rho\ )$$

Inconsistency on converg.

$t_1 \triangleq \textbf{rec}\ x.\ x \quad : int \to int$ $\qquad$ $t_2 \triangleq \lambda y.\ \textbf{rec}\ z.\ z \quad : int \to int$

$x : int \to int$ $\qquad$ $y, z : int$

$$D_{int \to int} = [\mathbb{Z}_\perp \to \mathbb{Z}_\perp]_\perp$$

$[\![t_1]\!]\rho = \perp_{[\mathbb{Z}_\perp \to \mathbb{Z}_\perp]_\perp}$ $\qquad$ $[\![t_2]\!]\rho = \lfloor \perp_{[\mathbb{Z}_\perp \to \mathbb{Z}_\perp]} \rfloor$

$t_1 \Uparrow$ $\qquad$ $t_2 \Downarrow$

$t_1 \uparrow$ $\qquad$ $t_2 \downarrow \qquad t_2 \to t_2$

$$U_{int \to int} = [\mathbb{Z}_\perp \to \mathbb{Z}_\perp]$$

$(\!| t_1 |\!)\rho = \perp_{[\mathbb{Z}_\perp \to \mathbb{Z}_\perp]}$ $\qquad$ $(\!| t_2 |\!)\rho = \perp_{[\mathbb{Z}_\perp \to \mathbb{Z}_\perp]} = \lambda d.\ \perp_{\mathbb{Z}_\perp}$

$t_1 \Uparrow_{\text{unlifted}}$ $\qquad$ $t_2 \Uparrow_{\text{unlifted}}$

$t_2 \downarrow \not\Rightarrow t_2 \Downarrow_{\text{unlifted}}$

Exercises
HOFL denotational semantics

Ex. Test for convergence

(Test for convergence) We would like to modify the denotational semantics of HOFL assigning to the construct

$$\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1$$

- the semantics of t_1 if the semantics of t is $\bot_{\mathbb{Z}_\bot}$, and
- the semantics of t_0 otherwise.

Is it possible? If not, why?

Ex. Test for convergence

$$[\![\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1]\!]\rho \triangleq \mathsf{Cond}^{\perp}_{\tau}(\ [\![t]\!]\rho\ ,\ [\![t_0]\!]\rho\ ,\ [\![t_1]\!]\rho\ )$$

$$\mathsf{Cond}^{\perp}_{\tau}(v, d_0, d_1) \triangleq \begin{cases} d_0 & \text{if } v = \lfloor n \rfloor \text{ for some } n \\ d_1 & \text{otherwise} \end{cases}$$

Any problem?

$\mathsf{Cond}^{\perp}_{\tau}$ is not monotone on *v* !

Counterexample $\perp_{\mathbb{Z}_\perp} \sqsubseteq_{\mathbb{Z}_\perp} \lfloor 1 \rfloor$ Take $d_1 \not\sqsubseteq_{D_\tau} d_0$

$$(\perp_{\mathbb{Z}_\perp}, d_0, d_1) \sqsubseteq_{\mathbb{Z}_\perp \times D_\tau \times D_\tau} (\lfloor 1 \rfloor, d_0, d_1)$$

$$\mathsf{Cond}^{\perp}_{\tau}(\perp_{\mathbb{Z}_\perp}, d_0, d_1) = d_1 \not\sqsubseteq_{D_\tau} d_0 = \mathsf{Cond}^{\perp}_{\tau}(\lfloor 1 \rfloor, d_0, d_1)$$

Ex. Test for convergence

For example take $d_0 = \lfloor 0 \rfloor$ $\quad d_1 = \lfloor 1 \rfloor$

$$[\![\textbf{if rec } x.\ x \textbf{ then } 0 \textbf{ else } 1]\!]\rho = \lfloor 1 \rfloor$$

$$\not\sqsubseteq_{\mathbb{Z}_\perp}$$

$$[\![\textbf{if } 1 \textbf{ then } 0 \textbf{ else } 1]\!]\rho = \lfloor 0 \rfloor$$

as a consequence

$$t \triangleq \lambda x.\ \textbf{if } x \textbf{ then } 0 \textbf{ else } 1 \ :\ int \to int$$

has no possible semantics in $D_{int \to int} = [\mathbb{Z}_\perp \to \mathbb{Z}_\perp]_\perp$

because $[\![t]\!]\rho$ is not continuous (not monotone)

Ex. Strict conditional

(Strict conditional) Modify the operational semantics of HOFL by taking the following rules for conditionals:

$$\frac{t \to 0 \quad t_0 \to c_0 \quad t_1 \to c_1}{\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \;\to\; c_0} \qquad \frac{t \to n \quad n \neq 0 \quad t_0 \to c_0 \;\; t_1 \to c_1}{\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \;\to\; c_1}.$$

Without changing the denotational semantics, prove that:

1. for any term t and canonical form c, we have $t \to c \;\Rightarrow\; \forall \rho.\; [\![t]\!]\,\rho = [\![c]\!]\,\rho$;
2. in general $t{\Downarrow} \not\Rightarrow t{\downarrow}$ (exhibit a counterexample).

Ex. Strict conditional 1

$$\frac{t \to 0 \quad t_0 \to c_0 \quad t_1 \to c_1}{\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \;\to\; c_0} \qquad \frac{t \to n \quad n \neq 0 \quad t_0 \to c_0 \;\; t_1 \to c_1}{\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \;\to\; c_1}.$$

$$t \to c \;\Rightarrow\; \forall \rho.\; [\![t]\!]\,\rho = [\![c]\!]\,\rho$$

$$P(t \to c) \triangleq \forall \rho.\; [\![t]\!]\rho = [\![c]\!]\rho$$

we extend the proof of correctness (by rule induction) to consider the new rules

Ex. Strict conditional 1

$$P(t \to c) \triangleq \forall \rho.\ [\![t]\!]\rho = [\![c]\!]\rho$$

$$\frac{t \to 0 \quad t_0 \to c_0 \quad t_1 \to c_1}{\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \quad \to \quad c_0}$$

assume

$$P(t \to 0) \triangleq \forall \rho.\ [\![t]\!]\rho = [\![0]\!]\rho = \lfloor 0 \rfloor$$

$$P(t_0 \to c_0) \triangleq \forall \rho.\ [\![t_0]\!]\rho = [\![c_0]\!]\rho$$

$$P(t_1 \to c_1) \triangleq \forall \rho.\ [\![t_1]\!]\rho = [\![c_1]\!]\rho$$

we want to prove

$$P(\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \to c_0) \triangleq \forall \rho.\ [\![\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1]\!]\rho = [\![c_0]\!]\rho$$

$$[\![\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1]\!]\rho = \mathsf{Cond}_\tau([\![t]\!]\rho, [\![t_0]\!]\rho, [\![t_1]\!]\rho) \quad \text{by def}$$

$$= \mathsf{Cond}_\tau(\lfloor 0 \rfloor, [\![c_0]\!]\rho, [\![c_1]\!]\rho) \quad \text{by ind. hyp.}$$

$$= [\![c_0]\!]\rho \quad \text{by Cond}$$

Ex. Strict conditional 1

$$P(t \to c) \triangleq \forall \rho.\ [\![t]\!]\rho = [\![c]\!]\rho$$

$$\frac{t \to n \quad n \neq 0 \quad t_0 \to c_0 \quad t_1 \to c_1}{\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \ \to\ c_1}$$

assume $P(t \to n) \triangleq \forall \rho.\ [\![t]\!]\rho = [\![n]\!]\rho = \lfloor n \rfloor \quad n \neq 0$

$$P(t_0 \to c_0) \triangleq \forall \rho.\ [\![t_0]\!]\rho = [\![c_0]\!]\rho$$

$$P(t_1 \to c_1) \triangleq \forall \rho.\ [\![t_1]\!]\rho = [\![c_1]\!]\rho$$

we want to prove

$$P(\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \to c_1) \triangleq \forall \rho.\ [\![\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1]\!]\rho = [\![c_1]\!]\rho$$

$[\![\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1]\!]\rho = \mathsf{Cond}_\tau([\![t]\!]\rho, [\![t_0]\!]\rho, [\![t_1]\!]\rho)$ by def

$= \mathsf{Cond}_\tau(\lfloor n \rfloor, [\![c_0]\!]\rho, [\![c_1]\!]\rho)$ by ind. h.

$= [\![c_1]\!]\rho$ by Cond

Ex. Strict conditional 2

we want to find a term t such that $t \Downarrow$ $t \uparrow$

take $t \triangleq \mathbf{if}\ 0\ \mathbf{then}\ 1\ \mathbf{else}\ \mathbf{rec}\ x.\ x \ : \ int$

$$[\![t]\!]\rho = \mathsf{Cond}_{int}([\![0]\!]\rho, [\![1]\!]\rho, [\![\mathbf{rec}\ x.\ x]\!]\rho)$$

$$= \mathsf{Cond}_{int}(\lfloor 0 \rfloor, \lfloor 1 \rfloor, \bot_{\mathbb{Z}_\bot}) \quad = \lfloor 1 \rfloor \qquad t \Downarrow$$

$$t \to c \ \nwarrow \ 0 \to 0\ ,\ 1 \to c\ ,\ \mathbf{rec}\ x.\ x \to c_1$$

$$\nwarrow^*_{c=1} \ \mathbf{rec}\ x.\ x \to c_1$$

$$\nwarrow \ x[^{\mathbf{rec}\ x.\ x}/_x] \to c_1$$

$$= \mathbf{rec}\ x.\ x \to c_1 \qquad t \uparrow$$

Ex. typing & semantics

Determine the type of the HOFL term

$$t \stackrel{\text{def}}{=} \mathbf{rec}\ f.\ (\ \lambda x.1\ ,\ \mathbf{fst}(f)\ 0\ )$$

Then, compute the (lazy) denotational semantics of t.

Ex. typing & semantics

$$t \triangleq \mathbf{rec}\ f.\ (\ \lambda x.\ 1\ ,\ (\mathbf{fst}(\ f\ )\ 0\ )\ )\quad : (int \to int) * int$$

$$f : (int \to \tau_1) * \tau_2 \qquad x : \tau \qquad 1 : int \qquad f : (int \to \tau_1) * \tau_2 \qquad 0 : int$$

$$\lambda x.\ 1 : \tau \to int \qquad \mathbf{fst}(f) : int \to \tau_1$$

$$\mathbf{fst}(f)\ 0 : \tau_1$$

$$(\lambda x.\ 1,\ (\mathbf{fst}(f)\ 0)) : (\tau \to int) * \tau_1$$

$$(int \to \tau_1) * \tau_2 = (\tau \to int) * \tau_1$$

$$\begin{cases} int = \tau \\ \tau_1 = int \\ \tau_2 = \tau_1 \end{cases}$$

$$\tau = \tau_1 = \tau_2 = int$$

Ex. typing & semantics

$$t \triangleq \mathbf{rec}\ f.\ (\ \lambda x.\ 1\ ,\ (\mathbf{fst}(\ f\ )\ 0\ )\ )\quad : (int \to int) * int$$

$$[\![t]\!]\rho = \mathit{fix}\ \lambda d_f.\ [\![(\lambda x.\ 1, \mathbf{fst}(f)\ 0)]\!]\rho[^{d_f}/_f]$$

$$= \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ [\![\lambda x.\ 1]\!]\rho[^{d_f}/_f]\ ,\ [\![\mathbf{fst}(f)\ 0]\!]\rho[^{d_f}/_f]\ )\ \rfloor$$

$$\rho' = \rho[^{d_f}/_f]$$

$$= \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ \lfloor\ \lambda d_x.\ [\![1]\!]\rho'[^{d_x}/_x]\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow [\![\mathbf{fst}(f)]\!]\rho'.\ \varphi([\![0]\!]\rho'))\ )\ \rfloor$$

$$= \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*([\![f]\!]\rho').\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$= \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*\ d_f.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

Ex. typing & semantics

$$[\![t]\!]\rho = \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*\ d_f.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$f_0 = \bot_{D_{(int \to int) * int}}$$

$$f_1 = \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*\ f_0.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$= \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ \bot_{D_{int}}\ )\ \rfloor$$

$$f_2 = \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*\ f_1.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$= \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$= \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\lambda d_x.\ \lfloor 1 \rfloor)\ \lfloor 0 \rfloor\ )\ \rfloor$$

$$= \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ \lfloor 1 \rfloor\ )\ \rfloor$$ maximal element!

Ex. typing & semantics

$$t \triangleq \mathbf{rec}\ f.\ (\ \lambda x.\ 1\ ,\ (\mathbf{fst}(\ f\ )\ 0\ )\ )\ \ : (int \to int) * int$$

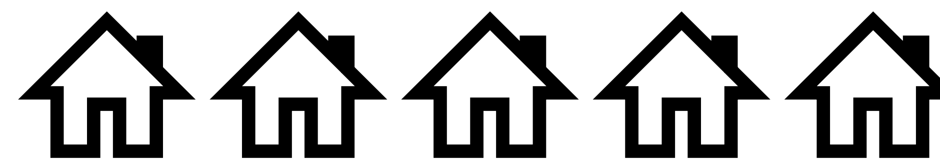
$$[\![t]\!]\rho = \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*\ d_f.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$[\![t]\!]\rho = \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ \lfloor 1 \rfloor\ )\ \rfloor$$

Mid-term badge

There are five adjacent houses on the same road.
Each house is painted on a different color.
In each house lives a person with a different nationality.
Every owner has his favorite drink, his favorite brand of cigarettes, and keeps pets of a particular kind.
No owners have the same pet, smoke the same kind of cigarette, or drink the same beverage.
Given the 15 clues below, the question is: **Who owns the... fish?**

1. The **Brit** lives in the **red** house.
2. The **Swede** keeps **dogs**.
3. The **Dane** drinks **tea**.
4. The **green** house is just to the left of the **white** one.
5. The owner of the **green** house drinks **coffee**.
6. The **Mall Pall** smoker keeps **birds**.
7. The owner of the **yellow** house smokes **Dunkill**
8. The man in the **center** house drinks **milk**.
9. The **Norwegian** lives in the **first** house.
10. The **Blenk** smoker has a neighbor who keeps **cats**.
11. The owner who smokes **Blue Monsters** drinks **bier**.
12. The man who keeps **horses** lives next to the **Dunkill** smoker.
13. The **German** smokes **Pringe**.
14. The **Norwegian** lives next to the **blue** house.
15. The **Blenk** smoker has a neighbor who drinks **water**.



Write a program to solve the riddle (using Prolog or Haskell)