PSC 2024/25 (375AA, 9CFU)

Principles for Software Composition

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

http://didawiki.di.unipi.it/doku.php/magistraleinformatica/psc/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

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

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

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

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

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

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

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

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

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

Op is more concrete

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

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

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 $t_0 \equiv_{\text{den}} t_1$

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

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

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

Den is strictly more abstract

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

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 $\quad t \to n \quad \Leftrightarrow \quad \forall \rho. [\![t]\!] \rho = \lfloor n \rfloor$

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

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

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

assume $t_0 \equiv_{\mathrm{den}} t_1$ 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 $t_0 \equiv_{\mathrm{op}} t_1$

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

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

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

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

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

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

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

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

---

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.

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

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

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

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

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

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

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

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

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

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