



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

**PSC 2020/21** (375AA, 9CFU)

Principles for Software Composition

Roberto Bruni

<http://www.di.unipi.it/~bruni/>

15 - HOF: Consistency?

# HOFL

## Operational vs Denotational

# Differences

operational  $t \rightarrow c$

closed, typeable terms

no environment

not a congruence

canonical terms

denotational  $\llbracket t \rrbracket \rho$

typeable terms

environment

congruence

mathematical entities

$$\forall t, c. t \rightarrow c \stackrel{?}{\Leftrightarrow} \forall \rho. \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho$$

$$t \rightarrow c \Rightarrow \forall \rho. \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho$$

$$(\forall \rho. \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho) \not\Rightarrow t \rightarrow c$$

there is only one  
type for which the  
implication holds

# Inconsistency: example

$x : int$

$c_0 = \lambda x. x + 0$

$c_1 = \lambda x. x$

already in canonical forms

$$\llbracket c_0 \rrbracket \rho = \llbracket c_1 \rrbracket \rho$$

$$c_0 \not\rightarrow c_1$$

$$\llbracket c_0 \rrbracket \rho = \llbracket \lambda x. x + 0 \rrbracket \rho = \llbracket \lambda d. d \underline{+} \underline{0} \rrbracket \rho = \llbracket \lambda d. d \rrbracket \rho = \llbracket \lambda x. x \rrbracket \rho = \llbracket c_1 \rrbracket \rho$$

# Correctness

**TH.**

$$t \rightarrow c \Rightarrow \forall \rho. \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho$$

*proof.*

we proceed by rule induction

$$P(t \rightarrow c) \stackrel{\text{def}}{=} \forall \rho. \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho$$

$$\frac{}{c \rightarrow c}$$

$$P(c \rightarrow c) \stackrel{\text{def}}{=} \forall \rho. \llbracket c \rrbracket \rho = \llbracket c \rrbracket \rho \quad \text{obvious}$$

**TH.**

$$t \rightarrow c \Rightarrow \forall \rho. \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho$$

(continue)

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

assume

$$P(t_1 \rightarrow n_1) \stackrel{\text{def}}{=} \forall \rho. \llbracket t_1 \rrbracket \rho = \llbracket n_1 \rrbracket \rho = \lfloor n_1 \rfloor$$

$$P(t_2 \rightarrow n_2) \stackrel{\text{def}}{=} \forall \rho. \llbracket t_2 \rrbracket \rho = \llbracket n_2 \rrbracket \rho = \lfloor n_2 \rfloor$$

we prove  $P(t_1 \text{ op } t_2 \rightarrow n_1 \underline{\text{op}} n_2) \stackrel{\text{def}}{=} \forall \rho. \llbracket t_1 \text{ op } t_2 \rrbracket \rho = \llbracket n_1 \underline{\text{op}} n_2 \rrbracket \rho$

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

**TH.**

$$t \rightarrow c \Rightarrow \forall \rho. \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho$$

(continue)

$$t \rightarrow 0 \quad t_0 \rightarrow c_0$$

**if  $t$  then  $t_0$  else  $t_1 \rightarrow c_0$**

assume

$$P(t \rightarrow 0) \stackrel{\text{def}}{=} \forall \rho. \llbracket t \rrbracket \rho = \llbracket 0 \rrbracket \rho = \llbracket 0 \rrbracket$$

$$P(t_0 \rightarrow c_0) \stackrel{\text{def}}{=} \forall \rho. \llbracket t_0 \rrbracket \rho = \llbracket c_0 \rrbracket \rho$$

we prove  $P(\text{if } t \text{ then } t_0 \text{ else } t_1 \rightarrow c_0) \stackrel{\text{def}}{=} \forall \rho. \llbracket \text{if } t \text{ then } t_0 \text{ else } t_1 \rrbracket \rho = \llbracket c_0 \rrbracket \rho$

$$\begin{aligned} \llbracket \text{if } t \text{ then } t_0 \text{ else } t_1 \rrbracket \rho &= \text{Cond}(\llbracket t \rrbracket \rho, \llbracket t_0 \rrbracket \rho, \llbracket t_1 \rrbracket \rho) && \text{(by def. of } \llbracket \cdot \rrbracket \text{)} \\ &= \text{Cond}(\llbracket 0 \rrbracket, \llbracket t_0 \rrbracket \rho, \llbracket t_1 \rrbracket \rho) && \text{(by ind. hyp.)} \\ &= \llbracket t_0 \rrbracket \rho && \text{(by def. of } \text{Cond}) \\ &= \llbracket c_0 \rrbracket \rho && \text{(by ind. hyp.)} \end{aligned}$$

ifn) analogous (omitted)

**TH.**

$$t \rightarrow c \Rightarrow \forall \rho. \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho$$

(continue)

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

**assume**

$$P(t \rightarrow (t_0, t_1)) \stackrel{\text{def}}{=} \forall \rho. \llbracket t \rrbracket \rho = \llbracket (t_0, t_1) \rrbracket \rho$$

$$P(t_0 \rightarrow c_0) \stackrel{\text{def}}{=} \forall \rho. \llbracket t_0 \rrbracket \rho = \llbracket c_0 \rrbracket \rho$$

**we prove**  $P(\mathbf{fst}(t) \rightarrow c_0) \stackrel{\text{def}}{=} \forall \rho. \llbracket \mathbf{fst}(t) \rrbracket \rho = \llbracket c_0 \rrbracket \rho$

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

snd) analogous (omitted)



**TH.**

$$t \rightarrow c \Rightarrow \forall \rho. \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho$$

(continue)

$$\frac{t_1 \rightarrow \lambda x. t'_1 \quad t'_1 [t_0/x] \rightarrow c}{(t_1 t_0) \rightarrow c}$$

**assume**

$$P(t_1 \rightarrow \lambda x. t'_1) \stackrel{\text{def}}{=} \forall \rho. \llbracket t_1 \rrbracket \rho = \llbracket \lambda x. t'_1 \rrbracket \rho$$

$$P(t'_1 [t_0/x] \rightarrow c) \stackrel{\text{def}}{=} \forall \rho. \llbracket t'_1 [t_0/x] \rrbracket \rho = \llbracket c \rrbracket \rho$$

**we prove**  $P((t_1 t_0) \rightarrow c) \stackrel{\text{def}}{=} \forall \rho. \llbracket (t_1 t_0) \rrbracket \rho = \llbracket c \rrbracket \rho$

$$\llbracket (t_1 t_0) \rrbracket \rho = \mathbf{let} \ \varphi \Leftarrow \llbracket t_1 \rrbracket \rho. \ \varphi(\llbracket t_0 \rrbracket \rho) \quad (\text{by definition of } \llbracket \cdot \rrbracket)$$

$$= \mathbf{let} \ \varphi \Leftarrow \llbracket \lambda x. t'_1 \rrbracket \rho. \ \varphi(\llbracket t_0 \rrbracket \rho) \quad (\text{by ind. hypothesis})$$

$$= \mathbf{let} \ \varphi \Leftarrow [\lambda d. \llbracket t'_1 \rrbracket \rho [d/x]] . \ \varphi(\llbracket t_0 \rrbracket \rho) \quad (\text{by definition of } \llbracket \cdot \rrbracket)$$

$$= (\lambda d. \llbracket t'_1 \rrbracket \rho [d/x]) (\llbracket t_0 \rrbracket \rho) \quad (\text{by de-lifting})$$

$$= \llbracket t'_1 \rrbracket \rho [\llbracket t_0 \rrbracket \rho / x] \quad (\text{by application})$$

$$= \llbracket t'_1 [t_0/x] \rrbracket \rho \quad (\text{by Subst. Lemma})$$

$$= \llbracket c \rrbracket \rho \quad (\text{by ind. hypothesis})$$

**TH.**

$$t \rightarrow c \Rightarrow \forall \rho. \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho$$

(continue)

$$\frac{t[\mathbf{rec} \ x. t / x] \rightarrow c}{\mathbf{rec} \ x. t \rightarrow c}$$

assume

$$P(t[\mathbf{rec} \ x. t / x] \rightarrow c) \stackrel{\text{def}}{=} \forall \rho. \llbracket t[\mathbf{rec} \ x. t / x] \rrbracket \rho = \llbracket c \rrbracket \rho$$

we prove  $P(\mathbf{rec} \ x. t \rightarrow c) \stackrel{\text{def}}{=} \forall \rho. \llbracket \mathbf{rec} \ x. t \rrbracket \rho = \llbracket c \rrbracket \rho$

$$\llbracket \mathbf{rec} \ x. t \rrbracket \rho = \llbracket t \rrbracket \rho [\llbracket \mathbf{rec} \ x. t \rrbracket \rho / x]$$

(by definition)

$$= \llbracket t[\mathbf{rec} \ x. t / x] \rrbracket \rho$$

(by the Substitution Lemma)

$$= \llbracket c \rrbracket \rho$$

(by inductive hypothesis)

# HOFL convergence

## Operational vs Denotational

# Operational convergence

$t : \tau$  closed

$t \downarrow \iff \exists c \in C_\tau. t \longrightarrow c$

$t \uparrow \iff \neg t \downarrow$

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

$$t \Downarrow \iff \forall \rho \in Env, \exists v \in V_\tau. \llbracket t \rrbracket \rho = [v]$$

$$t \Uparrow \iff \neg t \Downarrow$$

## Examples

$$\llbracket \mathbf{rec} \ x. \ x \rrbracket \rho \ \Uparrow$$

$$\llbracket \lambda y. \ \mathbf{rec} \ x. \ x \rrbracket \rho \ \Downarrow$$

$$\llbracket (\lambda y. \ \mathbf{rec} \ x. \ x) \ 0 \rrbracket \rho \ \Uparrow$$

$$\llbracket \mathbf{if} \ 0 \ \mathbf{then} \ 1 \ \mathbf{else} \ \mathbf{rec} \ x. \ x \rrbracket \rho \ \Downarrow$$

# Consistency on converg.

**TH.**  $t : \tau$  closed  $t \downarrow \Rightarrow t \Downarrow$

*proof.*  $t \downarrow \Rightarrow t \rightarrow c$  by def (for some  $c$ )  
 $\Rightarrow \forall \rho. \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho$  by correctness  
 $\Rightarrow \forall \rho. \llbracket t \rrbracket \rho \neq \perp$  canonical  $\llbracket c \rrbracket \rho \neq \perp$   
 $\Rightarrow t \Downarrow$  by def

**TH.**  $t : \tau$  closed  $t \Downarrow \Rightarrow t \downarrow$

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

# HOFL equivalence

## Operational vs Denotational

# HOFPL equivalences

$t_0, t_1 : \tau$  closed

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

$t_0 \equiv_{\text{den}} t_1$  iff  $\forall \rho. \llbracket t_0 \rrbracket \rho = \llbracket t_1 \rrbracket \rho$



# 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  $\exists c. t_0 \rightarrow c \wedge t_1 \rightarrow c$  or  $t_0 \uparrow \wedge t_1 \uparrow$

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

by correctness  $\forall \rho. \llbracket t_0 \rrbracket \rho = \llbracket c \rrbracket \rho = \llbracket t_1 \rrbracket \rho$  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.  $\forall \rho. \llbracket t_0 \rrbracket \rho = \perp_{D_\tau} = \llbracket t_1 \rrbracket \rho$  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

$x : int$

$c_0 = \lambda x. x + 0$

$c_1 = \lambda x. x$

# Consistency on int

**TH.**  $t : \text{int}$  closed  $t \rightarrow n \iff \forall \rho. \llbracket t \rrbracket \rho = \lfloor n \rfloor$

*proof.*

$\Rightarrow$ ) if  $t \rightarrow n$  then  $\llbracket t \rrbracket \rho = \llbracket n \rrbracket \rho = \lfloor n \rfloor$

$\Leftarrow$ ) if  $\llbracket t \rrbracket \rho = \lfloor n \rfloor$  it means  $t \Downarrow$

by agreement on convergence  $t \Downarrow$

thus  $t \rightarrow m$  for some  $m$

but then by correctness  $\llbracket t \rrbracket \rho = \llbracket m \rrbracket \rho = \lfloor m \rfloor$

and it must be  $m = n$

# Equivalence on int

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

*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  $\forall \rho. \llbracket t_0 \rrbracket \rho = \perp_{\mathbb{Z}_\perp} = \llbracket t_1 \rrbracket \rho$

or  $\forall \rho. \llbracket t_0 \rrbracket \rho = \llbracket n \rrbracket = \llbracket t_1 \rrbracket \rho$  for some  $n$

if  $\forall \rho. \llbracket t_0 \rrbracket \rho = \perp_{\mathbb{Z}_\perp} = \llbracket t_1 \rrbracket \rho$  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  $\forall \rho. \llbracket t_0 \rrbracket \rho = \llbracket n \rrbracket = \llbracket t_1 \rrbracket \rho$  then  $t_0 \rightarrow n, t_1 \rightarrow n$

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

# HOFL

## Unlifted Semantics

# Unlifted Domains

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

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

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

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

unlifted domains

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

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

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

# Unlifted Semantics

as before

$$\llbracket n \rrbracket \rho \triangleq \lfloor n \rfloor$$

$$\llbracket x \rrbracket \rho \triangleq \rho(x)$$

$$\llbracket t_1 \text{ op } t_2 \rrbracket \rho \triangleq \llbracket t_1 \rrbracket \rho \text{ op}_{\perp} \llbracket t_2 \rrbracket \rho$$

$$\llbracket \text{if } t \text{ then } t_1 \text{ else } t_2 \rrbracket \rho \triangleq \text{Cond}_{\tau} ( \llbracket t \rrbracket \rho , \llbracket t_1 \rrbracket \rho , \llbracket t_2 \rrbracket \rho )$$

$$\llbracket \text{rec } x. t \rrbracket \rho \triangleq \text{fix } \lambda d. \llbracket t \rrbracket \rho^{[d/x]}$$

---

without lifting

$$\llbracket (t_1 , t_2) \rrbracket \rho \triangleq ( \llbracket t_1 \rrbracket \rho , \llbracket t_2 \rrbracket \rho )$$

$$\llbracket \text{fst}( t ) \rrbracket \rho \triangleq \pi_1 ( \llbracket t \rrbracket \rho )$$

$$\llbracket \text{snd}( t ) \rrbracket \rho \triangleq \pi_2 ( \llbracket t \rrbracket \rho )$$

$$\llbracket \lambda x. t \rrbracket \rho \triangleq \lambda d. \llbracket t \rrbracket \rho^{[d/x]}$$

$$\llbracket t \ t_0 \rrbracket \rho \triangleq ( \llbracket t \rrbracket \rho ) ( \llbracket t_0 \rrbracket \rho )$$

# Inconsistency on converg.

$$t_1 \triangleq \mathbf{rec} \ x. \ x \ : \ int \rightarrow \ int$$

$x : int \rightarrow int$

$$t_2 \triangleq \lambda y. \mathbf{rec} \ z. \ z \ : \ int \rightarrow \ int$$

$y, z : int$

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

$$[[t_1]]\rho = \perp_{[\mathbb{Z}_\perp \rightarrow \mathbb{Z}_\perp]_\perp}$$

$$[[t_2]]\rho = \lfloor \perp_{[\mathbb{Z}_\perp \rightarrow \mathbb{Z}_\perp]} \rfloor$$

$$t_1 \uparrow$$

$$t_2 \Downarrow$$

$$t_1 \uparrow$$

$$t_2 \downarrow \quad t_2 \rightarrow t_2$$

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

$$(|t_1|)\rho = \perp_{[\mathbb{Z}_\perp \rightarrow \mathbb{Z}_\perp]}$$

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

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

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

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