PSC 2023/24 (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

<table>
<thead>
<tr>
<th>Operational</th>
<th>Denotational</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t \rightarrow c$</td>
<td>$\llbracket t \rrbracket \rho$</td>
</tr>
<tr>
<td>closed, typeable</td>
<td>typeable</td>
</tr>
<tr>
<td>terms</td>
<td>terms</td>
</tr>
<tr>
<td>no environment</td>
<td>environment</td>
</tr>
<tr>
<td>not a congruence</td>
<td>congruence</td>
</tr>
<tr>
<td>canonical terms</td>
<td>mathematical</td>
</tr>
</tbody>
</table>

$\forall t, c. \ t \rightarrow c \iff \forall \rho. \ [t] \rho = [c] \rho$

$\forall \rho. \ [t] \rho = [c] \rho \implies t \rightarrow c$

$(\forall \rho. \ [t] \rho = [c] \rho) \nmid t \rightarrow c$

There is only one type for which the implication holds.
Inconsistency: example

\[ x : int \quad c_0 = \lambda x. x + 0 \quad c_1 = \lambda x. x \]

already in canonical forms

\[
[ c_0 ] \rho = [ c_1 ] \rho \quad \quad c_0 \not\sim c_1
\]

\[
[ c_0 ] \rho = [ \lambda x. x + 0 ] \rho = [ \lambda d. d + \bot 0 ] = [ \lambda d. d ] = [ \lambda x. x ] \rho = [ c_1 ] \rho
\]
**Correctness**

### TH.

\[ t \to c \Rightarrow \forall \rho. \ [t] \rho = [c] \rho \]

**proof.** we proceed by rule induction

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

\[
P(c \to c) \overset{\text{def}}{=} \forall \rho. \ [c] \rho = [c] \rho \quad \text{obvious}
\]
We have and we want to prove

In the case of the conditional construct we have two rules to consider. For

\[ t \rightarrow c \Rightarrow \forall \rho. \ [t] \rho = [c] \rho \] 

(continue)

\[
\frac{t_1 \rightarrow n_1 \quad t_2 \rightarrow n_2}{t_1 \text{ op } t_2 \rightarrow n_1 \text{ op } n_2}
\]

assume

\[ P(t_1 \rightarrow n_1) \overset{\text{def}}{=} \forall \rho. \ [t_1] \rho = [n_1] \rho = [n_1] \]

\[ P(t_2 \rightarrow n_2) \overset{\text{def}}{=} \forall \rho. \ [t_2] \rho = [n_2] \rho = [n_2] \]

we prove

\[ P(t_1 \text{ op } t_2 \rightarrow n_1 \text{ op } n_2) \overset{\text{def}}{=} \forall \rho. \ [t_1 \text{ op } t_2] \rho = [n_1 \text{ op } n_2] \rho \]

\[
[t_1 \text{ op } t_2] \rho = [t_1] \rho \text{ op } [t_2] \rho \quad (\text{by definition of } [\cdot])
\]

\[ = [n_1] \text{ op } [n_2] \quad (\text{by inductive hypotheses})
\]

\[ = [n_1 \text{ op } n_2] \quad (\text{by definition of } \text{ op } \downarrow)
\]

\[ = [n_1 \text{ op } n_2] \rho \quad (\text{by definition of } [\cdot])
\]
We assume the inductive hypotheses:

and we want to prove

In the case of the conditional construct we have two rules to consider. For

\[ t \rightarrow 0 \quad t_0 \rightarrow c_0 \]

if \( t \) then \( t_0 \) else \( t_1 \rightarrow c_0 \)

we prove \( P(\text{if } t \text{ then } t_0 \text{ else } t_1 \rightarrow c_0) \equiv \forall \rho. \ [\text{if } t \text{ then } t_0 \text{ else } t_1] \rho = [c_0] \rho \)

\[
[\text{if } t \text{ then } t_0 \text{ else } t_1] \rho = \text{Cond}([t] \rho, [t_0] \rho, [t_1] \rho) \quad \text{(by def. of } [\cdot] \text{)}
\]

\[
= \text{Cond}([0], [t_0] \rho, [t_1] \rho) \quad \text{(by ind. hyp.)}
\]

\[
= [t_0] \rho \quad \text{(by def. of Cond)}
\]

\[
= [c_0] \rho \quad \text{(by ind. hyp.)}
\]

ifn) analogous (omitted)
assume

\[ P(t \rightarrow (t_0, t_1)) \overset{\text{def}}{=} \forall \rho. \ [t] \rho = [ (t_0, t_1) ] \rho \]

\[ P(t_0 \rightarrow c_0) \overset{\text{def}}{=} \forall \rho. \ [t_0] \rho = [c_0] \rho \]

we prove \[ P(\text{fst}(t) \rightarrow c_0) \overset{\text{def}}{=} \forall \rho. \ [\text{fst}(t)] \rho = [c_0] \rho \]

\[
[\text{fst}(t)] \rho = \pi_1^*([t] \rho) \quad \text{(by def. of \([\cdot]\))}
= \pi_1^*([ (t_0, t_1) ] \rho) \quad \text{(by ind. hyp.)}
= \pi_1^*([ [t_0] \rho, [t_1] \rho ]) \quad \text{(by def. of \([\cdot]\))}
= \pi_1([t_0] \rho, [t_1] \rho) \quad \text{(by def. of lifting)}
= [t_0] \rho \quad \text{(by def. of \(\pi_1\))}
= [c_0] \rho \quad \text{(by ind. hyp.)}
\]

snd) analogous (omitted)
\[ t \to c \Rightarrow \forall \rho. \ [t] \rho = [c] \rho \]

\[ t_1 \to \lambda x. t'_1 \quad t'_1[^{t_0} / x] \to c \]

\[ \frac{(t_1 \ t_0) \to c}{(t_1 \ t_0) \to c} \]

**Th.**

\[ P(t_1 \to \lambda x. t'_1) \overset{\text{def}}{=} \forall \rho. \ [t_1] \rho = [\lambda x. t'_1] \rho \]

\[ P(t'_1[^{t_0} / x] \to c) \overset{\text{def}}{=} \forall \rho. \ [t'_1[^{t_0} / x]] \rho = [c] \rho \]

we prove

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

\[ [(t_1 \ t_0)] \rho = \begin{array}{l}
\text{let } \varphi \leftarrow [t_1] \rho, \varphi([t_0] \rho) \\
\text{let } \varphi \leftarrow [\lambda x. t'_1] \rho, \varphi([t_0] \rho) \\
\text{let } \varphi \leftarrow [\lambda d. \ [t'_1] \rho[^{d / x}] \cdot \varphi([t_0] \rho) \\
(\lambda d. \ [t'_1] \rho[^{d / x}]) ([t_0] \rho) \\
[t'_1] \rho[^{[t_0] \rho / x}] \\
[t'_1[^{t_0} / x]] \rho \\
[c] \rho
\end{array} \]

(by definition of \([\cdot]\))

(by ind. hypothesis)

(by definition of \([\cdot]\))

(by de-lifting)

(by application)

(by Subst. Lemma)

(by ind. hypothesis)
\[ t \rightarrow c \Rightarrow \forall \rho. \ [t] \rho = [c] \rho \]  

(continue)

We define the following predicate:

\[ \text{if} \]

Definition 10.1

Now we define the concept of convergence (i.e., termination) for the operational and

, then we say that

(Operational convergence).

\[ r = t^K(\text{by definition of}) \]

\[ t = t^K(\text{by the Substitution Lemma}) \]

\[ = [t] \rho \]

(by inductive hypothesis)

\[ = [c] \rho \]

(by inductive hypothesis)
HOFL convergence
Operational vs Denotational
We define the following predicate:

\[ t : \tau \text{ closed} \]

\[ t \Downarrow \iff \exists c \in C_\tau. t \rightarrow c \]

\[ t \Uparrow \iff \neg t \Downarrow \]

**Examples**

\[ \text{rec } x. x \uparrow \]

\[ \lambda y. \text{rec } x. x \downarrow \]

\[ (\lambda y. \text{rec } x. x) \, 0 \uparrow \]

\[ \text{if } 0 \text{ then } 1 \text{ else rec } x. x \downarrow \]
Denotational converg.

\( t : \tau \) closed

\[ t \downarrow \iff \forall \rho \in Env, \exists v \in V_\tau. [t] \rho = [v] \]

\[ t \uparrow \iff \neg t \downarrow \]

Examples

\[ [\text{rec } x. x] \rho \uparrow \]

\[ [\lambda y. \text{rec } x. x] \rho \downarrow \]

\[ [(\lambda y. \text{rec } x. x) \ 0] \rho \uparrow \]

\[ [\text{if } 0 \text{ then } 1 \text{ else rec } x. x] \rho \downarrow \]
We define the following predicate:

If $t \triangleright$ then we say that $t$ converges operationally if the term can be evaluated to a canonical form.

Now we define the concept of convergence (i.e., termination) for the operational and structural induction; instead it is necessary to introduce a particular logical relation $\triangleright$, see Theorem 9.6 and thus it is different from (Denotational convergence).

Let us focus on the case of Remark 10.1.

Also the opposite implication $\triangleright \Rightarrow \triangleright$.

We aim to prove that the two semantics agree at least on the notion of convergence. A term $t$ converges denotationally if the term can be evaluated to a canonical form $\triangleright$. Here $t$ is a lifted value, i.e., that $t$ holds (for any closed and typable term $t$ of HOFL).

Theorem 10.3.

Proof. $t \triangleright \Rightarrow t \rightarrow c.$ by def (for some $c$)

$\Rightarrow \forall \rho. \left[ t \right] \rho = \left[ c \right] \rho$ by correctness

$\Rightarrow \forall \rho. \left[ t \right] \rho \neq \perp$ canonical $\left[ c \right] \rho \neq \perp$

$\Rightarrow t \triangleright$ by def

Remark 10.1

We give some insights on the reason why this is so.

the proof is not part of the program of the course (structural induction would not work)
HOFL equivalence
Operational vs Denotational
HOFL equivalences

\[ t_0, t_1 : \tau \quad \text{closed} \]

\[ t_0 \equiv_{\text{op}} t_1 \quad \text{iff} \quad \forall c. \ t_0 \to c \iff t_1 \to c \]

\[ t_0 \equiv_{\text{den}} t_1 \quad \text{iff} \quad \forall \rho. \ [t_0] \rho = [t_1] \rho \]
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 \( \exists c. \ t_0 \rightarrow c \land t_1 \rightarrow c \) or \( t_0 \uparrow \land t_1 \uparrow \)

if \( \exists c. \ t_0 \rightarrow c \land t_1 \rightarrow c \)

by correctness \( \forall \rho. \ [t_0]_\rho = [c]_\rho = [t_1]_\rho \) thus \( t_0 \equiv_{\text{den}} t_1 \)

if \( t_0 \uparrow \land t_1 \uparrow \)

by agreement on convergence \( t_0 \uparrow \land t_1 \uparrow \)

i.e. \( \forall \rho. \ [t_0]_\rho = \bot_{D_\tau} = [t_1]_\rho \) thus \( t_0 \equiv_{\text{den}} t_1 \)
Den is strictly more abstract

\[ \equiv_{\text{den}} \not\subset \equiv_{\text{op}} \]

\text{proof.}

see previous counterexample

\[ x : \text{int} \quad c_0 = \lambda x. x + 0 \quad c_1 = \lambda x. x \]
Consistency on int

**TH.** \( t : \text{int} \) closed \( t \rightarrow n \iff \forall \rho. [t] \rho = [n] \)

**proof.**

\[ \Rightarrow \) if \( t \rightarrow n \) then \( [t] \rho = [n] \rho = [n] \)

\[ \Leftarrow \) if \( [t] \rho = [n] \) it means \( t \Downarrow \)

by agreement on convergence \( t \Downarrow \)

thus \( t \rightarrow m \) for some \( m \)

but then by correctness \( [t] \rho = [m] \rho = [m] \)

and it must be \( m = n \)
**Equivalence on int**

**TH.** \( t_0, t_1 : \text{int} \)  \( t_0 \equiv_{\text{op}} t_1 \iff t_0 \equiv_{\text{den}} t_1 \)

**proof.** we know \( t_0 \equiv_{\text{op}} t_1 \implies t_0 \equiv_{\text{den}} t_1 \)

we prove \( t_0 \equiv_{\text{den}} t_1 \implies t_0 \equiv_{\text{op}} t_1 \)

assume \( t_0 \equiv_{\text{den}} t_1 \) either \( \forall \rho. \ [t_0] \rho = \bot_{\mathbb{Z}_\perp} = [t_1] \rho \)

or \( \forall \rho. \ [t_0] \rho = [n] = [t_1] \rho \) for some \( n \)

if \( \forall \rho. \ [t_0] \rho = \bot_{\mathbb{Z}_\perp} = [t_1] \rho \) 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 \( \forall \rho. \ [t_0] \rho = [n] = [t_1] \rho \) then \( t_0 \rightarrow n \), \( t_1 \rightarrow n \)

thus \( t_0 \equiv_{\text{op}} t_1 \)
HOFL
Unlifted Semantics
# Unlifted Domains

\[ D_\tau \triangleq (V_\tau)_\bot \]

\[ V_{int} \triangleq \mathbb{Z} \]

\[ V_{\tau_1 \ast \tau_2} \triangleq D_{\tau_1} \times D_{\tau_2} = (V_{\tau_1})_\bot \times (V_{\tau_2})_\bot \]

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

## Unlifted Domains

\[ U_{int} \triangleq \mathbb{Z}_\bot \]

\[ U_{\tau_1 \ast \tau_2} \triangleq U_{\tau_1} \times U_{\tau_2} \]

\[ U_{\tau_1 \rightarrow \tau_2} \triangleq [U_{\tau_1} \rightarrow U_{\tau_2}] \]
Unlifted Semantics

as before

\[(n)\rho \triangleq \lfloor n \rfloor\]

\[(x)\rho \triangleq \rho(x)\]

\[(t_1 \text{ op } t_2)\rho \triangleq (t_1)\rho \text{ op}_\bot (t_2)\rho\]

\[(\text{if } t \text{ then } t_1 \text{ else } t_2)\rho \triangleq \text{Cond}_\tau( (t)\rho , (t_1)\rho , (t_2)\rho )\]

\[(\text{rec } x. t)\rho \triangleq \text{fix } \lambda d. (t)\rho[^d/x]\]

without lifting

\[(t_1 , t_2)\rho \triangleq ( (t_1)\rho , (t_2)\rho )\]

\[(\text{fst}( t ))\rho \triangleq \pi_1 ( (t)\rho )\]

\[(\text{snd}( t ))\rho \triangleq \pi_2 ( (t)\rho )\]

\[(\lambda x. t)\rho \triangleq \lambda d. (t)\rho[^d/x]\]

\[( t t_0 )\rho \triangleq ( (t)\rho ) ( (t_0)\rho )\]
Inconsistency on converg.

\[ t_1 \triangleq \text{rec } x. \ x : \text{int} \to \text{int} \quad t_2 \triangleq \lambda y. \ \text{rec } z. \ z : \text{int} \to \text{int} \]

\[ x : \text{int} \to \text{int} \quad y, z : \text{int} \]

\[
\begin{align*}
D_{\text{int} \to \text{int}} &= [\mathbb{Z}_\perp \to \mathbb{Z}_\perp]_\perp \\
[t_1] \rho &= \perp [\mathbb{Z}_\perp \to \mathbb{Z}_\perp]_\perp \\
t_1 &\uparrow \\
[t_2] \rho &= \perp [\mathbb{Z}_\perp \to \mathbb{Z}_\perp] \\
t_2 &\downarrow \\
t_1 &\uparrow \\
t_2 &\downarrow \\
t_2 &\to t_2
\end{align*}
\]

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

\[
\begin{align*}
(t_1) \rho &= \perp [\mathbb{Z}_\perp \to \mathbb{Z}_\perp] \\
t_1 &\uparrow \text{unlifted} \\
(t_2) \rho &= \perp [\mathbb{Z}_\perp \to \mathbb{Z}_\perp] = \lambda d. \ \perp \mathbb{Z}_\perp \\
t_2 &\uparrow \text{unlifted} \\
t_2 &\not\to t_2 \\
t_2 &\downarrow \text{unlifted}
\end{align*}
\]