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

14 - HOFL Denotational Semantics

Interpretation Domains

Interpretation Domains

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

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

to distinguish:
pair of divergent terms
from divergent pair

$$D_{\tau_1 \to \tau_2} \triangleq [D_{\tau_1} \to D_{\tau_2}]_\perp$$

to distinguish:
takes arg and diverge
from divergence without taking arg

Example

$$D_{int*int} \triangleq (\mathbb{Z}_\perp \times \mathbb{Z}_\perp)_\perp$$

$\mathbf{rec}\ p.\ p$	$(\mathbf{rec}\ x.\ x, \mathbf{rec}\ y.\ y)$
$\perp_{D_{int*int}}$	$(\perp_{D_{int}}, \perp_{D_{int}})$

Example

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

$\mathbf{rec}\ f.\ f$	$\lambda x.\ \mathbf{rec}\ y.\ y$
$\perp_{D_{int \to int}}$	$\lambda d.\ \perp_{D_{int}}$

Interpretation Domains

$$D_{int} \triangleq \mathbb{Z}_\perp \qquad D_{\tau_1 * \tau_2} \triangleq (D_{\tau_1} \times D_{\tau_2})_\perp \qquad D_{\tau_1 \to \tau_2} \triangleq [D_{\tau_1} \to D_{\tau_2}]_\perp$$

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

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

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

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

Interpretation Function

$t : \tau$ $\quad\quad$ $[\![t]\!]\rho \in D_\tau$

environment $\quad \rho : Var \to \bigcup_{\tau \in \mathcal{T}} D_\tau$

type consistent assignment of values to variables $\quad x : \tau \Rightarrow \rho(x) \in D_\tau$

we define the interpretation function by structural recursion

Denotational Semantics

Constants

$$\underbrace{[\![\underbrace{n}_{int}]\!]\rho}_{D_{int} = \mathbb{Z}_\perp} \triangleq \underbrace{\lfloor \underbrace{n}_{\mathbb{Z}} \rfloor}_{\mathbb{Z}_\perp}$$

Variables

$$\underbrace{[\![\underbrace{x}_{\tau}]\!]\rho}_{D_\tau} \triangleq \underbrace{\rho(x)}_{D_\tau} \qquad x : \tau \Rightarrow \rho(x) \in D_\tau$$

Arithmetic ops

to prove: $\underline{\mathsf{op}}_\perp$ is monotone and continuous

$$\mathsf{op} \in \{+, - \times\}$$

$$\llbracket \underbrace{\underbrace{\underbrace{t_1}_{int} \ \mathsf{op} \ \underbrace{t_2}_{int}}_{int} \rrbracket \rho}_{D_{int} = \mathbb{Z}_\perp} \triangleq \underbrace{\underbrace{\llbracket \underbrace{t_1}_{int} \rrbracket \rho}_{D_{int} = \mathbb{Z}_\perp} \ \underline{\mathsf{op}}_\perp \ \underbrace{\llbracket \underbrace{t_2}_{int} \rrbracket \rho}_{D_{int} = \mathbb{Z}_\perp}}_{D_{int} = \mathbb{Z}_\perp}$$

$$\underline{\mathsf{op}}_\perp : \mathbb{Z}_\perp \times \mathbb{Z}_\perp \to \mathbb{Z}_\perp$$

$$v_1 \ \underline{\mathsf{op}}_\perp \ v_2 \triangleq \begin{cases} \lfloor n_1 \ \underline{\mathsf{op}} \ n_2 \rfloor & \text{if } v_1 = \lfloor n_1 \rfloor \text{ and } v_2 = \lfloor n_2 \rfloor \\ \perp_{\mathbb{Z}_\perp} & \text{otherwise } (v_1 = \perp_{\mathbb{Z}_\perp} \text{ or } v_2 = \perp_{\mathbb{Z}_\perp}) \end{cases}$$

called *strict* extension

Conditionals

to prove: Cond_τ is monotone and continuous

$$\underbrace{[\![\mathbf{if}\ \underbrace{\underbrace{t}_{int}\ \mathbf{then}\ \underbrace{t_1}_{\tau}\ \mathbf{else}\ \underbrace{t_2}_{\tau}}_{\tau}]\!]\rho}_{D_\tau} \triangleq \underbrace{\mathsf{Cond}_\tau(\ \underbrace{[\![\underbrace{t}_{int}]\!]\rho}_{D_{int}=\mathbb{Z}_\perp}\ ,\ \underbrace{[\![\underbrace{t_1}_{\tau}]\!]\rho}_{D_\tau}\ ,\ \underbrace{[\![\underbrace{t_2}_{\tau}]\!]\rho}_{D_\tau}\ )}_{D_\tau}$$

$$\mathsf{Cond}_\tau : \mathbb{Z}_\perp \times D_\tau \times D_\tau \to D_\tau$$

$$\mathsf{Cond}_\tau(v, d_1, d_2) \triangleq \begin{cases} \perp_{D_\tau} & \text{if } v = \perp_{\mathbb{Z}_\perp} \\ d_1 & \text{if } v = \lfloor 0 \rfloor \\ d_2 & \text{otherwise } (v = \lfloor n \rfloor \text{ with } n \neq 0) \end{cases}$$

Pairing

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

$$\underbrace{[\![\underbrace{(\underbrace{t_1}_{\tau_1} \ , \ \underbrace{t_2}_{\tau_2})}_{\tau_1 * \tau_2}]\!] \rho}_{D_{\tau_1 * \tau_2} = (D_{\tau_1} \times D_{\tau_2})_\perp} \triangleq \underbrace{\lfloor \ \underbrace{(\ \underbrace{[\![\underbrace{t_1}_{\tau_1}]\!] \rho}_{D_{\tau_1}} \ , \ \underbrace{[\![\underbrace{t_2}_{\tau_2}]\!] \rho}_{D_{\tau_2}} \ )}_{D_{\tau_1} \times D_{\tau_2}} \ \rfloor}_{D_{\tau_1 * \tau_2} = (D_{\tau_1} \times D_{\tau_2})_\perp}$$

Projections

Equivalently:

$$[\![\mathbf{fst}(\ t\ )]\!]\rho \triangleq \mathbf{let}\ d \Leftarrow [\![t]\!]\rho.\ \pi_1(d)$$

$$\underbrace{[\![\underbrace{\mathbf{fst}(\ \underbrace{t}_{\tau_1 * \tau_2}\ )}_{\tau_1}]\!]\rho}_{D_{\tau_1}} \triangleq \underbrace{\underbrace{\underbrace{\pi_1}_{D_{\tau_1} \times D_{\tau_2} \to D_{\tau_1}}^{*}}_{(D_{\tau_1} \times D_{\tau_2})_\perp \to D_{\tau_1}}\ (\ \underbrace{[\![\underbrace{t}_{\tau_1 * \tau_2}]\!]\rho}_{D_{\tau_1 * \tau_2} = (D_{\tau_1} \times D_{\tau_2})_\perp}\ )}_{D_{\tau_1}}$$

$$[\![\mathbf{snd}(\ t\ )]\!]\rho \triangleq \pi_2^*\ (\ [\![t]\!]\rho\ )$$

Abstraction

$$D_{\tau_1 \to \tau_2} \triangleq [D_{\tau_1} \to D_{\tau_2}]_\perp$$

$$\underbrace{[\![\underbrace{\lambda \underbrace{x}_{\tau_1}.\ \underbrace{t}_{\tau_2}}_{\tau_1 \to \tau_2}]\!]\rho}_{D_{\tau_1 \to \tau_2} = [D_{\tau_1} \to D_{\tau_2}]_\perp} \triangleq \underbrace{\lfloor\ \underbrace{\lambda \underbrace{d}_{D_{\tau_1}}.\ \underbrace{[\![\underbrace{t}_{\tau_2}]\!]\rho[{}^d/_x]}_{D_{\tau_2}}}_{[D_{\tau_1} \to D_{\tau_2}]}\ \rfloor}_{[D_{\tau_1} \to D_{\tau_2}]_\perp}$$

Application (lazy)

Equivalently:

$$[\![\; t \; t_0 \;]\!]\rho \triangleq (\lambda\varphi.\ \varphi([\![t_0]\!]\rho))^* \ ([\![t]\!]\rho)$$

$$\underbrace{[\![\; \underbrace{\underbrace{t}_{\tau_0 \to \tau}\ \underbrace{t_0}_{\tau_0}}_{\tau} \;]\!]\rho}_{D_\tau} \triangleq \underbrace{\mathbf{let}\ \underbrace{\varphi}_{V_{\tau_0\to\tau} = [D_{\tau_0} \to D_\tau]} \Leftarrow \underbrace{[\![\underbrace{t}_{\tau_0 \to \tau}]\!]\rho}_{D_{\tau_0\to\tau} = (V_{\tau_0\to\tau})_\perp}.\ \underbrace{\underbrace{\varphi}_{[D_{\tau_0} \to D_\tau]}(\underbrace{[\![\underbrace{t_0}_{\tau_0}]\!]\rho}_{D_{\tau_0}})}_{D_\tau}}_{D_\tau}$$

Recursion

$$\underbrace{[\![\underbrace{\mathbf{rec}\ \underbrace{x}_{\tau}.\ \underbrace{t}_{\tau}}_{\tau}]\!]\rho}_{D_\tau} \triangleq \underbrace{[\![\underbrace{t}_{\tau}]\!]\rho\left[{}^{\underbrace{[\![\mathbf{rec}\ x.\ t]\!]\rho}_{D_\tau}}/_{\underbrace{x}_{\tau}}\right]}_{D_\tau}$$

Recursion

$$\underbrace{[\![\underbrace{\mathbf{rec}\ \underbrace{x}_{\tau}.\ \underbrace{t}_{\tau}}_{\tau}]\!]\rho}_{D_\tau} \triangleq \underbrace{\underbrace{\mathit{fix}}_{[[D_\tau \to D_\tau] \to D_\tau]}\ \underbrace{\lambda \underbrace{d}_{D_\tau}.\ \underbrace{[\![\underbrace{t}_{\tau}]\!]\rho[{}^{\underbrace{d}_{D_\tau}}/{}_{\underbrace{x}_{\tau}}]}_{D_\tau}}_{[D_\tau \to D_\tau]}}_{D_\tau}$$

Recap

$$[\![n]\!]\rho \triangleq \lfloor n \rfloor$$

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

$$[\![t_1 \ \mathsf{op}\ t_2]\!]\rho \triangleq [\![t_1]\!]\rho \ \underline{\mathsf{op}}_\perp \ [\![t_2]\!]\rho$$

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

$$[\![(t_1\ ,\ t_2)]\!]\rho \triangleq \lfloor\ (\ [\![t_1]\!]\rho\ ,\ [\![t_2]\!]\rho\ )\ \rfloor$$

$$[\![\mathbf{fst}(\ t\ )]\!]\rho \triangleq \pi_1^*\ (\ [\![t]\!]\rho\ )$$

$$[\![\mathbf{snd}(\ t\ )]\!]\rho \triangleq \pi_2^*\ (\ [\![t]\!]\rho\ )$$

$$[\![\lambda x.\ t]\!]\rho \triangleq \lfloor\ \lambda d.\ [\![t]\!]\rho[^d/_x]\ \rfloor$$

$$[\![\ t\ t_0\ ]\!]\rho \triangleq \mathbf{let}\ \varphi \Leftarrow [\![t]\!]\rho.\ \varphi([\![t_0]\!]\rho)$$

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

Example

$$f \stackrel{\text{def}}{=} \lambda x : int \,.\, 3$$

$$[\![\lambda x.\ t]\!]\rho \triangleq \lfloor\ \lambda d.\ [\![t]\!]\rho[^d/_x]\ \rfloor \qquad\qquad [\![n]\!]\rho \triangleq \lfloor n \rfloor$$

$$[\![f]\!]\rho = [\![\lambda x.\ 3]\!]\rho = \lfloor \lambda d.\ [\![3]\!]\rho[^d/_x] \rfloor = \lfloor \lambda d.\ \lfloor 3 \rfloor \rfloor$$

Example

$$g \stackrel{\text{def}}{=} \lambda x : int.\ \textbf{if}\ x\ \textbf{then}\ 3\ \textbf{else}\ 3$$

$$[\![\lambda x.\ t]\!]\rho \triangleq \lfloor\ \lambda d.\ [\![t]\!]\rho[^d/_x]\ \rfloor$$

$$\begin{aligned}
[\![g]\!]\rho &= [\![\lambda x.\ \textbf{if}\ x\ \textbf{then}\ 3\ \textbf{else}\ 3]\!]\rho \\
&= \lfloor \lambda d.\ [\![\textbf{if}\ x\ \textbf{then}\ 3\ \textbf{else}\ 3]\!]\rho[^d/_x] \rfloor \\
&= \lfloor \lambda d.\ Cond(d, \lfloor 3 \rfloor, \lfloor 3 \rfloor) \rfloor \\
&= \lfloor \lambda d.\ \textbf{let}\ x \Leftarrow d.\ \lfloor 3 \rfloor \rfloor
\end{aligned}$$

$$[\![f]\!]\rho \neq [\![g]\!]\rho$$

$$\lfloor \lambda d.\ \lfloor 3 \rfloor \rfloor$$

Example

$$h \stackrel{\text{def}}{=} \mathbf{rec}\, y : int \to int\,.\ \lambda x : int\,.\ 3$$

$$\begin{aligned}
[\![h]\!]\rho &= [\![\mathbf{rec}\ y.\ \lambda x.\ 3]\!]\rho \\
&= \text{fix}\ \lambda d_y.\ [\![\lambda x.\ 3]\!]\rho[^{d_y}/_y] \\
&= \text{fix}\ \lambda d_y.\ \lfloor \lambda d_x.\ [\![3]\!]\rho[^{d_y}/_y, ^{d_x}/_x] \rfloor \\
&= \text{fix}\ \lambda d_y.\ \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor
\end{aligned}$$

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

$$[\![\lambda x.\ t]\!]\rho \triangleq \lfloor\ \lambda d.\ [\![t]\!]\rho[^d/_x]\ \rfloor$$

$$\Gamma_h = \lambda d_y.\ \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor$$

$$\begin{aligned}
d_0 &= \Gamma_h^0(\bot_{[\mathbb{Z}_\bot \to \mathbb{Z}_\bot]_\bot}) = \bot_{[\mathbb{Z}_\bot \to \mathbb{Z}_\bot]_\bot} \\
d_1 &= \Gamma_h(d_0) = (\lambda d_y.\ \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor)\bot = \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor \\
d_2 &= \Gamma_h(d_1) = (\lambda d_y.\ \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor)\lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor = \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor = d_1
\end{aligned}$$

Example

$$h \stackrel{\text{def}}{=} \mathbf{rec}\, y : int \to int.\ \lambda x : int.\ 3$$

$$\begin{aligned}
[\![h]\!]\rho &= [\![\mathbf{rec}\ y.\ \lambda x.\ 3]\!]\rho \\
&= \text{fix}\ \lambda d_y.\ [\![\lambda x.\ 3]\!]\rho[{}^{d_y}/_y] \\
&= \text{fix}\ \lambda d_y.\ \lfloor \lambda d_x.\ [\![3]\!]\rho[{}^{d_y}/_y, {}^{d_x}/_x] \rfloor \\
&= \text{fix}\ \lambda d_y.\ \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor
\end{aligned}$$

$$\Gamma_h = \lambda d_y.\ \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor$$

$$d_0 = \Gamma_h^0(\bot_{[\mathbb{Z}_\bot \to \mathbb{Z}_\bot]_\bot}) = \bot_{[\mathbb{Z}_\bot \to \mathbb{Z}_\bot]_\bot}$$

$$d_1 = \Gamma_h(d_0) = (\lambda d_y.\ \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor)\bot = \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor$$

Maximal element in $[\mathbb{Z}_\bot \to \mathbb{Z}_\bot]_\bot$
we could already stop here

Example

$$h \stackrel{\text{def}}{=} \mathbf{rec}\, y : int \to int\,.\ \lambda x : int\,.\ 3$$

$$\begin{aligned}
[\![h]\!]\rho &= [\![\mathbf{rec}\ y.\ \lambda x.\ 3]\!]\rho \\
&= \text{fix}\ \lambda d_y.\ [\![\lambda x.\ 3]\!]\rho[{}^{d_y}/_{y}] \\
&= \text{fix}\ \lambda d_y.\ \lfloor \lambda d_x.\ [\![3]\!]\rho[{}^{d_y}/_{y}, {}^{d_x}/_{x}] \rfloor \\
&= \text{fix}\ \lambda d_y.\ \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor
\end{aligned}$$

$$[\![h]\!]\rho = \lfloor \lambda d_x.\ \lfloor 3 \rfloor \rfloor = [\![f]\!]\rho$$

Example

$$x : \tau$$

$$\begin{aligned}
[\![\textbf{rec } x.\ x]\!]\rho &= \mathit{fix}\ \lambda d_x.\ [\![x]\!]\rho[{}^{d_x}/_x] \\
&= \mathit{fix}\ \lambda d_x.\ d_x
\end{aligned}$$

$$\begin{aligned}
d_0 &= \bot_{D_\tau} \\
d_1 &= (\lambda d_x . d_x)\ d_0 = d_0 = \bot_{D_\tau}
\end{aligned}$$

$$[\![\textbf{rec } x.\ x]\!]\rho = \bot_{D_\tau}$$

$$x : int \to int \qquad [\![\textbf{rec } x.\ x]\!]\rho = \bot_{[\mathbb{Z}_\bot \to \mathbb{Z}_\bot]_\bot}$$

$$x : int * int \qquad [\![\textbf{rec } x.\ x]\!]\rho = \bot_{(\mathbb{Z}_\bot \times \mathbb{Z}_\bot)_\bot}$$

Example

$$y : \tau_1 \qquad z : \tau_2$$

$$
\begin{aligned}
[\![\lambda y.\ \mathbf{rec}\ z.\ z]\!]\rho &= \lfloor \lambda d_y.\ [\![\mathbf{rec}\ z.\ z]\!]\rho[{}^{d_y}/_y] \rfloor \\
&= \lfloor \lambda d_y.\ \bot_{D_{\tau_2}} \rfloor \\
&= \lfloor \bot_{[D_{\tau_1} \to D_{\tau_2}]} \rfloor \\
&= \lfloor \bot_{V_{\tau_1 \to \tau_2}} \rfloor \\
&\neq \bot_{D_{\tau_1 \to \tau_2}} \quad = \bot_{(V_{\tau_1 \to \tau_2})_\bot}
\end{aligned}
$$

$x : int \to int$ $\qquad [\![\mathbf{rec}\ x.\ x]\!]\rho = \bot_{[\mathbb{Z}_\bot \to \mathbb{Z}_\bot]_\bot}$ diverges

$y : int, z : int$ $\qquad [\![\lambda y.\ \mathbf{rec}\ z.\ z]\!]\rho = \lfloor \bot_{[\mathbb{Z}_\bot \to \mathbb{Z}_\bot]} \rfloor$ waits arg and diverges

Exercise

$$x : int * int \ , \ \ y : int \ , \ \ z : int$$

$$[\![\ \mathbf{rec} \ x. \ x \ ]\!]\rho \quad \stackrel{?}{=} \quad [\![\ (\ \mathbf{rec} \ y. \ y \ , \ \mathbf{rec} \ z. \ z \ ) \ ]\!]\rho$$

diverges

a pair
of diverging computations

$$\perp_{D_{int*int}}$$

$$\lfloor(\perp_{D_{int}}, \perp_{D_{int}})\rfloor$$

Lazy vs Eager

Eager Application

returns $\perp$ when $[\![t]\!]\rho = \perp$

lazy $\quad [\![\ t\ t_0\ ]\!]\rho \triangleq \mathbf{let}\ \varphi \Leftarrow [\![t]\!]\rho.\ \varphi([\![t_0]\!]\rho)$

eager $\quad [\![\ t\ t_0\ ]\!]\rho \triangleq \mathbf{let}\ \varphi \Leftarrow [\![t]\!]\rho.\ \mathbf{let}\ d \Leftarrow [\![t_0]\!]\rho.\ \varphi(\lfloor d \rfloor)$

returns $\perp$ when $[\![t]\!]\rho = \perp$ or $[\![t_0]\!]\rho = \perp$

Well-given definitions

Well-definedness

We must guarantee that all functions we have used are monotone and continuous,
so that Kleene's fix point theory is applicable

$\pi_1 \;\; \pi_2 \;\; (\cdot)^* \;\; apply \;\; \mathit{fix}$ already considered
$\mathbf{let}$

$\underline{\mathsf{op}}_\perp \quad \mathsf{Cond}_\tau \quad \lambda$ to be checked

TH. $\underline{\mathsf{op}}_\perp$ is monotone and continuous

$$\underline{\mathsf{op}}_\perp : \mathbb{Z}_\perp \times \mathbb{Z}_\perp \to \mathbb{Z}_\perp$$

$$v_1 \ \underline{\mathsf{op}}_\perp \ v_2 \triangleq \begin{cases} \lfloor n_1 \ \underline{\mathsf{op}} \ n_2 \rfloor & \text{if } v_1 = \lfloor n_1 \rfloor \text{ and } v_2 = \lfloor n_2 \rfloor \\ \perp_{\mathbb{Z}_\perp} & \text{otherwise } (v_1 = \perp_{\mathbb{Z}_\perp} \text{ or } v_2 = \perp_{\mathbb{Z}_\perp}) \end{cases}$$

We omit monotonicity check

Since the domain has only finite chains, it is also continuous

TH. Cond_τ is monotone and continuous

$$\mathsf{Cond}_\tau : \mathbb{Z}_\perp \times D_\tau \times D_\tau \to D_\tau$$

$$\mathsf{Cond}_\tau(v, d_1, d_2) \triangleq \begin{cases} \perp_{D_\tau} & \text{if } v = \perp_{\mathbb{Z}_\perp} \\ d_1 & \text{if } v = \lfloor 0 \rfloor \\ d_2 & \text{otherwise } (v = \lfloor n \rfloor \text{ with } n \neq 0) \end{cases}$$

We omit monotonicity check

We prove continuity on each parameter separately

The first parameter is in $\mathbb{Z}_\perp$

only finite chains are possible, hence continuity is guaranteed

We prove continuity over the second parameter (next slides)

For the third parameter the proof is analogous and omitted

(continue)

$\mathsf{Cond}_\tau : \mathbb{Z}_\perp \times D_\tau \times D_\tau \to D_\tau$

$$\mathsf{Cond}_\tau(v, d_1, d_2) \triangleq \begin{cases} \perp_{D_\tau} & \text{if } v = \perp_{\mathbb{Z}_\perp} \\ d_1 & \text{if } v = \lfloor 0 \rfloor \\ d_2 & \text{otherwise } (v = \lfloor n \rfloor \text{ with } n \neq 0) \end{cases}$$

Continuity over the second parameter

take $v \in \mathbb{Z}_\perp, d \in D_\tau, \{d_i\}_{i \in \mathbb{N}} \subseteq D_\tau$

we want to prove $\mathsf{Cond}_\tau \left(v, \bigsqcup_{i \in \mathbb{N}} d_i, d \right) = \bigsqcup_{i \in \mathbb{N}} \mathsf{Cond}_\tau(v, d_i, d)$

we proceed by case analysis on v:

- $\perp_{\mathbb{Z}_\perp}$
- $\lfloor 0 \rfloor$
- $\lfloor n \rfloor \;,\; n \neq 0$

(continue)

$$\mathsf{Cond}_\tau : \mathbb{Z}_\perp \times D_\tau \times D_\tau \to D_\tau$$

$$\mathsf{Cond}_\tau(v, d_1, d_2) \triangleq \begin{cases} \perp_{D_\tau} & \text{if } v = \perp_{\mathbb{Z}_\perp} \\ d_1 & \text{if } v = \lfloor 0 \rfloor \\ d_2 & \text{otherwise } (v = \lfloor n \rfloor \text{ with } n \neq 0) \end{cases}$$

$v = \perp_{\mathbb{Z}_\perp}$

$$\mathsf{Cond}_\tau \left(\perp_{\mathbb{Z}_\perp}, \bigsqcup_{i \in \mathbb{N}} d_i, d \right) = \perp_{D_\tau} = \bigsqcup_{i \in \mathbb{N}} \perp_{D_\tau} = \bigsqcup_{i \in \mathbb{N}} \mathsf{Cond}_\tau(\perp_{\mathbb{Z}_\perp}, d_i, d)$$

(continue)

$$\mathsf{Cond}_\tau : \mathbb{Z}_\perp \times D_\tau \times D_\tau \to D_\tau$$

$$\mathsf{Cond}_\tau(v, d_1, d_2) \triangleq \begin{cases} \perp_{D_\tau} & \text{if } v = \perp_{\mathbb{Z}_\perp} \\ d_1 & \text{if } v = \lfloor 0 \rfloor \\ d_2 & \text{otherwise } (v = \lfloor n \rfloor \text{ with } n \neq 0) \end{cases}$$

$v = \lfloor 0 \rfloor$

$$\mathsf{Cond}_\tau \left(\lfloor 0 \rfloor, \bigsqcup_{i \in \mathbb{N}} d_i, d \right) = \bigsqcup_{i \in \mathbb{N}} d_i = \bigsqcup_{i \in \mathbb{N}} \mathsf{Cond}_\tau(\lfloor 0 \rfloor, d_i, d)$$

(continue)

$$\mathsf{Cond}_\tau : \mathbb{Z}_\perp \times D_\tau \times D_\tau \to D_\tau$$

$$\mathsf{Cond}_\tau(v, d_1, d_2) \triangleq \begin{cases} \perp_{D_\tau} & \text{if } v = \perp_{\mathbb{Z}_\perp} \\ d_1 & \text{if } v = \lfloor 0 \rfloor \\ d_2 & \text{otherwise } (v = \lfloor n \rfloor \text{ with } n \neq 0) \end{cases}$$

$v = \lfloor n \rfloor \ , \ n \neq 0$

$$\mathsf{Cond}_\tau\left(\lfloor n \rfloor, \bigsqcup_{i \in \mathbb{N}} d_i, d\right) = d = \bigsqcup_{i \in \mathbb{N}} d = \bigsqcup_{i \in \mathbb{N}} \mathsf{Cond}_\tau(\lfloor n \rfloor, d_i, d)$$

TH. lambda abstraction is monotone and continuous

$t : \tau$ $\qquad\qquad \lambda d.\ [\![t]\!]\rho[^{d}/_{x}]$ is continuous

we focus on the stronger property

$\lambda \widetilde{d}.\ [\![t]\!]\rho[^{\widetilde{d}}/_{\widetilde{x}}]$ is continuous

the proof is by structural induction on t

(try on your own)

Corollary $t : \tau_0 \to \tau$ $\qquad\qquad \mathit{fix}\ \lambda d.\ [\![t]\!]\rho[^{d}/_{x}]$ is continuous

(the limit of continuous functions is continuous)

Main properties

Substitution lemma

$$x, t_0 : \tau_0 \qquad t : \tau \qquad \llbracket t[{}^{t_0}/_x] \rrbracket \rho = \llbracket t \rrbracket \rho[{}^{\llbracket t_0 \rrbracket \rho}/_x]$$

environment update

syntactic substitution

the proof is by structural induction on t

(try on your own)

Compositionality

The substitution lemma $[\![t[^{t_0}/_x]]\!]\rho = [\![t]\!]\rho[^{[\![t_0]\!]\rho}/_x]$ is important: as it guarantees the compositionality of the denotational semantics

TH. $\quad [\![t_1]\!]\rho = [\![t_2]\!]\rho \quad \Rightarrow \quad [\![t[^{t_1}/_x]]\!]\rho = [\![t[^{t_2}/_x]]\!]\rho$

proof. assume $[\![t_1]\!]\rho = [\![t_2]\!]\rho$

$$\underbrace{[\![t[^{t_1}/_x]]\!]\rho = [\![t]\!]\rho[^{[\![t_1]\!]\rho}/_x]}_{\text{subs lemma}} \underbrace{= [\![t]\!]\rho[^{[\![t_2]\!]\rho}/_x]}_{[\![t_1]\!]\rho = [\![t_2]\!]\rho} \underbrace{= [\![t[^{t_2}/_x]]\!]\rho}_{\text{subs lemma}}$$

Only free variables matter

TH. $t : \tau$

$\forall x \in \mathsf{fv}(t).\ \rho(x) = \rho'(x) \quad \Rightarrow \quad [\![t]\!]\rho = [\![t]\!]\rho'$

the proof is by structural induction on t

(try on your own)

Corollary t closed $\quad \Rightarrow \quad \forall \rho, \rho'.\ [\![t]\!]\rho = [\![t]\!]\rho'$

TH. Canonical terms are not bottom

$$c \in C_\tau \;\; \Rightarrow \;\; \forall \rho.\ [\![c]\!]\rho \neq \bot_{D_\tau}$$

proof. by rule induction on the rules for canonical terms

$$P(c \in C_\tau) \triangleq \forall \rho.\ [\![c]\!]\rho \neq \bot_{D_\tau}$$

$$\frac{}{n \in C_{int}} \qquad [\![n]\!]\rho = \lfloor n \rfloor \neq \bot_{D_{int}}$$

$$\frac{t_0 : \tau_0 \quad t_1 : \tau_1 \quad t_0, t_1 \text{ closed}}{(t_0, t_1) \in C_{\tau_0 * \tau_1}} \qquad [\![(t_0, t_1)]\!]\rho = \lfloor ([\![t_0]\!]\rho, [\![t_1]\!]\rho) \rfloor \neq \bot_{D_{\tau_0 * \tau_1}}$$

$$\frac{\lambda x.\, t : \tau_0 \to \tau_1 \quad \lambda x.\, t \text{ closed}}{\lambda x.\, t \in C_{\tau_0 \to \tau_1}} \qquad [\![\lambda x.\ t]\!]\rho = \lfloor \lambda d.\ [\![t]\!]\rho[^d/_x] \rfloor \neq \bot_{D_{\tau_0 \to \tau_1}}$$