



PSC 2021/22 (375AA, 9CFU)

Principles for Software Composition

Roberto Bruni

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

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

08c - Immediate Consequences Operator

Recap

Kleene's theorem

$$p \triangleq f(p)$$

a recursive definition

is there such a p ?

is there a least p ?

if $f : D \rightarrow D$ continuous D CPO $_{\perp}$

then $p \triangleq \bigsqcup_{n \in \mathbb{N}} f^n(\perp_D)$

also written $fix(f)$

McCarthy 91 function

$$f = M f \quad (\mathbf{Pf}(\mathbb{N}, \mathbb{N}), \sqsubseteq) \quad \perp = \emptyset \quad \text{CPO}_\perp$$

$$M f n = \begin{cases} n - 10 & \text{if } n > 100 \\ f(f(n + 11)) & \text{if } n \leq 100 \text{ and } f(n + 11) \downarrow \\ \perp & \text{otherwise} \end{cases}$$

$$M \text{ monotone?} \quad f \sqsubseteq g \stackrel{?}{\Rightarrow} M(f) \sqsubseteq M(g)$$

$$M \text{ continuous?} \quad M \left(\bigsqcup_i f_i \right) \stackrel{?}{\sqsubseteq} \bigsqcup_i M(f_i)$$

McCarthy 91 function

$$M f n = \begin{cases} n - 10 & \text{if } n > 100 \\ f(f(n + 11)) & \text{if } n \leq 100 \text{ and } f(n + 11) \downarrow \\ \perp & \text{otherwise} \end{cases}$$

M monotone? 

we assume $f \sqsubseteq g$ and prove $M(f) \sqsubseteq M(g)$

take $(n, m) \in M(f)$ we prove $(n, m) \in M(g)$

if $n > 100$

$m = n - 10$ and $(n, n - 10) \in M(g)$

if $n \leq 100$

$m = f(f(n + 11))$

thus $\exists k. \{(n + 11, k), (k, m)\} \in f \subseteq g$
and $(n, m) \in M(g)$

McCarthy 91 function

$$M f n = \begin{cases} n - 10 & \text{if } n > 100 \\ f(f(n + 11)) & \text{if } n \leq 100 \text{ and } f(n + 11) \downarrow \\ \perp & \text{otherwise} \end{cases}$$

M continuous? 

let $f \triangleq \bigsqcup_i f_i$

$$M \left(\bigsqcup_i f_i \right) \stackrel{?}{\subseteq} \bigsqcup_i M(f_i)$$

take $(n, m) \in M(f)$

we prove $(n, m) \in \bigsqcup_i M(f_i)$

if $n > 100$ $m = n - 10$ and $(n, n - 10) \in M(f_1) \subseteq \bigsqcup_i M(f_i)$

if $n \leq 100$ $m = f(f(n + 11))$

thus $\exists k. \{(n + 11, k), (k, m)\} \in f$

thus $\exists j_1, j_2. (n + 11, k) \in f_{j_1}, (k, m) \in f_{j_2}$

let $j \triangleq \max\{j_1, j_2\}$ thus $\{(n + 11, k), (k, m)\} \in f_j$

and $(n, m) \in M(f_j) \subseteq \bigsqcup_i M(f_i)$

McCarthy 91 function

$$f = M f \quad (\mathbf{Pf}(\mathbb{N}, \mathbb{N}), \sqsubseteq) \quad \perp = \emptyset \quad \text{CPO}_{\perp}$$

$$M f n = \begin{cases} n - 10 & \text{if } n > 100 \\ f(f(n + 11)) & \text{if } n \leq 100 \text{ and } f(n + 11) \downarrow \\ \perp & \text{otherwise} \end{cases}$$

$$M^0(\emptyset) = \emptyset$$

$$M^1(\emptyset) = \{(n, n - 10) \mid n > 100\} = \{(101, 91), (102, 92), \dots\}$$

$$M^2(\emptyset) = \{(100, 91), (101, 91), (102, 92), \dots\}$$

$$M^3(\emptyset) = \{(99, 91), (100, 91), (101, 91), (102, 92), \dots\}$$

...

$$M^{11}(\emptyset) = \{(91, 91), (92, 91), \dots, (101, 91), (102, 92), \dots\}$$

$$M^{12}(\emptyset) = \{(80, 91), (81, 91), \dots, (101, 91), (102, 92), \dots\}$$

...

$$M^{20}(\emptyset) = \{(0, 91), (1, 91), \dots, (101, 91), (102, 92), \dots\}$$

fixpoint reached! (total function)

Alternative perspective

$$f = M f \quad (\mathbf{Pf}(\mathbb{N}, \mathbb{N}), \sqsubseteq) \quad \perp = \emptyset \quad \text{CPO}_\perp$$

$$M f n = \begin{cases} n - 10 & \text{if } n > 100 \\ f(f(n + 11)) & \text{if } n \leq 100 \text{ and } f(n + 11) \downarrow \\ \perp & \text{otherwise} \end{cases}$$

formulas: $(n, m) \in f$

or just (n, m) for brevity

$$R_M \triangleq \left\{ \frac{}{(n, n - 10)} \quad n > 100 \quad , \quad \frac{(n + 11, k) \quad (k, m)}{(n, m)} \quad n \leq 100 \right\}$$

$$f(n) = m \quad \Leftrightarrow \quad (n, m) \in I_{R_M}$$

(set of theorems of R_M)

Immediate Consequences Operator (ICO)

Immediate Consequences Operator

F a set of formulas $(\wp(F), \subseteq) \text{ CPO}_\perp$

R a logical system
(with some restrictions) $\hat{R} : \wp(F) \rightarrow \wp(F) \text{ ICO}$

$$\hat{R}(S) \triangleq \left\{ y \mid \exists \frac{x_1 \dots x_n}{y} \in R. \{x_1, \dots, x_n\} \subseteq S \right\}$$

\hat{R} applies the rules to the facts in S in all possible ways

$\hat{R}(S)$: all conclusions we can draw in one step
from hypotheses on S

We prove the least fixpoint of \hat{R} is I_R
(set of theorems of R)

Example

Strings of balanced parentheses

$$F = \{s \in \mathcal{L} \mid s \in \{(,)\}^*\}$$

$$R = \left\{ \frac{\epsilon \in \mathcal{L}}{\epsilon \in \mathcal{L}}, \frac{s \in \mathcal{L}}{(s) \in \mathcal{L}}, \frac{s_1 \in \mathcal{L} \quad s_2 \in \mathcal{L}}{s_1 s_2 \in \mathcal{L}} \right\}$$

$$S = \emptyset$$

$$\hat{R}(S) = \{ \epsilon \in \mathcal{L} \}$$

$$\hat{R}(S) \triangleq \left\{ y \mid \exists \frac{x_1 \dots x_n}{y} \in R. \{x_1, \dots, x_n\} \subseteq S \right\}$$



Exercise

Strings of balanced parentheses

$$F = \{s \in \mathcal{L} \mid s \in \{(,)\}^*\}$$

$$R = \left\{ \frac{}{\epsilon \in \mathcal{L}}, \frac{s \in \mathcal{L}}{(s) \in \mathcal{L}}, \frac{s_1 \in \mathcal{L} \quad s_2 \in \mathcal{L}}{s_1 s_2 \in \mathcal{L}} \right\}$$

$$S = \{ \epsilon \in \mathcal{L} \}$$

$$\hat{R}(S) = ? \{ \epsilon \in \mathcal{L}, () \in \mathcal{L} \}$$

$$\hat{R}(S) \triangleq \left\{ y \mid \exists \frac{x_1 \dots x_n}{y} \in R. \{x_1, \dots, x_n\} \subseteq S \right\}$$



Exercise

Strings of balanced parentheses

$$F = \{s \in \mathcal{L} \mid s \in \{(,)\}^*\}$$

$$R = \left\{ \frac{}{\epsilon \in \mathcal{L}}, \frac{s \in \mathcal{L}}{(s) \in \mathcal{L}}, \frac{s_1 \in \mathcal{L} \quad s_2 \in \mathcal{L}}{s_1 s_2 \in \mathcal{L}} \right\}$$

$$S = \{ () \in \mathcal{L} \}$$

$$\hat{R}(S) = ? \{ \epsilon \in \mathcal{L}, (()) \in \mathcal{L}, ()() \in \mathcal{L} \}$$

$$\hat{R}(S) \triangleq \left\{ y \mid \exists \frac{x_1 \dots x_n}{y} \in R. \{x_1, \dots, x_n\} \subseteq S \right\}$$



Exercise

Strings of balanced parentheses

$$F = \{s \in \mathcal{L} \mid s \in \{(,)\}^*\}$$

$$R = \left\{ \frac{\epsilon \in \mathcal{L}}{\epsilon \in \mathcal{L}}, \frac{s \in \mathcal{L}}{(s) \in \mathcal{L}}, \frac{s_1 \in \mathcal{L} \quad s_2 \in \mathcal{L}}{s_1 s_2 \in \mathcal{L}} \right\}$$

$$S = \{)(\in \mathcal{L} \}$$

$$\hat{R}(S) = ? \{ \epsilon \in \mathcal{L}, ()() \in \mathcal{L},)()(\in \mathcal{L} \}$$

$$\hat{R}(S) \triangleq \left\{ y \mid \exists \frac{x_1 \dots x_n}{y} \in R. \{x_1, \dots, x_n\} \subseteq S \right\}$$

Example

Strings of balanced parentheses

$$F = \{s \in \mathcal{L} \mid s \in \{(,)\}^*\}$$

$$R = \left\{ \frac{\epsilon \in \mathcal{L}}{\epsilon \in \mathcal{L}}, \frac{s \in \mathcal{L}}{(s) \in \mathcal{L}}, \frac{s_1 \in \mathcal{L} \quad s_2 \in \mathcal{L}}{s_1 s_2 \in \mathcal{L}} \right\}$$

$$S = \{)(\in \mathcal{L}, () \in \mathcal{L} \}$$

$$\widehat{R}(S) = \{ \epsilon \in \mathcal{L}, ()() \in \mathcal{L}, (()) \in \mathcal{L},)()(\in \mathcal{L},)(() \in \mathcal{L}, (()) \in \mathcal{L} \}$$

$$\widehat{R}(S) \triangleq \left\{ y \mid \exists \frac{x_1 \dots x_n}{y} \in R. \{x_1, \dots, x_n\} \subseteq S \right\}$$

Example

$\mathbf{Pf}(\mathbb{N}, \mathbb{N})$

$$F = \{(n, m) \mid n, m \in \mathbb{N}\}$$

$$R = \left\{ \frac{\quad}{(0, 0)}, \frac{\quad}{(1, 1)}, \frac{(n, h) \quad (n+1, k)}{(n+2, h+k)} \right\}$$

$$S = \emptyset$$

$$\widehat{R}(S) = \{(0, 0), (1, 1)\}$$

$$\widehat{R}(S) \triangleq \left\{ y \mid \exists \frac{x_1 \dots x_n}{y} \in R. \{x_1, \dots, x_n\} \subseteq S \right\}$$



Exercise

Pf(\mathbb{N}, \mathbb{N})

$$F = \{(n, m) \mid n, m \in \mathbb{N}\}$$

$$R = \left\{ \frac{(0, 0)}{(0, 0)}, \frac{(1, 1)}{(1, 1)}, \frac{(n, h) \quad (n+1, k)}{(n+2, h+k)} \right\}$$

$$S = \{(2, 1)\}$$

$$\widehat{R}(S) = ? \{(0, 0), (1, 1)\}$$

$$\widehat{R}(S) \triangleq \left\{ y \mid \exists \frac{x_1 \dots x_n}{y} \in R. \{x_1, \dots, x_n\} \subseteq S \right\}$$



Exercise

Pf(\mathbb{N}, \mathbb{N})

$$F = \{(n, m) \mid n, m \in \mathbb{N}\}$$

$$R = \left\{ \overline{(0, 0)}, \overline{(1, 1)}, \overline{\frac{(n, h) \quad (n+1, k)}{(n+2, h+k)}} \right\}$$

$$S = \{ (5, 5), (6, 8) \}$$

$$\widehat{R}(S) = ? \{ (0, 0), (1, 1), (7, 13) \}$$

$$\widehat{R}(S) \triangleq \left\{ y \mid \exists \frac{x_1 \dots x_n}{y} \in R. \{x_1, \dots, x_n\} \subseteq S \right\}$$

ICO is monotone

TH. \hat{R} is monotone

proof.

Take $S_1 \subseteq S_2$

we want to prove $\hat{R}(S_1) \subseteq \hat{R}(S_2)$

take $y \in \hat{R}(S_1)$ we want to prove $y \in \hat{R}(S_2)$

\Downarrow

$\exists \frac{x_1 \dots x_n}{y} \in R$ with $\{x_1, \dots, x_n\} \subseteq S_1$

$\Downarrow S_1 \subseteq S_2$

$\{x_1, \dots, x_n\} \subseteq S_2$

\Downarrow

$y \in \hat{R}(S_2)$

ICO is continuous

TH. \hat{R} is continuous (under some hypotheses)

proof. Take $\{S_i\}_{i \in \mathbb{N}}$ a chain in $\wp(F)$

We want to prove $\bigcup_{i \in \mathbb{N}} \hat{R}(S_i) = \hat{R} \left(\bigcup_{i \in \mathbb{N}} S_i \right)$

$\bigcup_{i \in \mathbb{N}} \hat{R}(S_i) \subseteq \hat{R} \left(\bigcup_{i \in \mathbb{N}} S_i \right)$ because \hat{R} is monotone

$\bigcup_{i \in \mathbb{N}} \hat{R}(S_i) \supseteq \hat{R} \left(\bigcup_{i \in \mathbb{N}} S_i \right)$?

ICO is continuous (ctd)

$$\bigcup_{i \in \mathbb{N}} \hat{R}(S_i) \supseteq \hat{R}\left(\bigcup_{i \in \mathbb{N}} S_i\right)$$

Take $y \in \hat{R}\left(\bigcup_{i \in \mathbb{N}} S_i\right)$ we want to prove $y \in \bigcup_{i \in \mathbb{N}} \hat{R}(S_i)$

\Downarrow
 $\exists \frac{x_1 \dots x_n}{y} \in R$ with $\{x_1, \dots, x_n\} \subseteq \bigcup_{i \in \mathbb{N}} S_i$

thus $\forall j \in [1, n]. \exists k_j \in \mathbb{N}. x_j \in S_{k_j}$ take $k = \max\{k_1, \dots, k_n\}$

clearly $\{x_1, \dots, x_n\} \subseteq S_k$

thus $y \in \hat{R}(S_k) \subseteq \bigcup_{i \in \mathbb{N}} \hat{R}(S_i)$

possible iff each rule has finitely many premises

Provable theorems

I_R set of theorems in R

I_R^n theorems provable with a derivation of height at most n

$$I_R^0 = \emptyset$$

$$I_R^{n+1} = I_R^n \cup \widehat{R}(I_R^n)$$

↑
provable using one more inference step

↑
theorems provable with a derivation of height at most n

clearly $I_R = \bigcup_{n \in \mathbb{N}} I_R^n$

n-depth theorems

TH. Let $P(n) \triangleq I_R^n = \widehat{R}^n(\emptyset) \quad \forall n \in \mathbb{N}. P(n)$

proof.

by mathematical induction

$$P(0) \triangleq I_R^0 = \widehat{R}^0(\emptyset)$$

$$I_R^0 = \emptyset = \widehat{R}^0(\emptyset)$$

$$\forall n \in \mathbb{N}. P(n) \Rightarrow P(n+1)$$

take a generic n
we assume $P(n) \triangleq I_R^n = \widehat{R}^n(\emptyset)$

we want to prove $P(n+1) \triangleq I_R^{n+1} = \widehat{R}^{n+1}(\emptyset)$

$$I_R^{n+1} = I_R^n \cup \widehat{R}(I_R^n)$$

by def

$$= \widehat{R}^n(\emptyset) \cup \widehat{R}(\widehat{R}^n(\emptyset))$$

by inductive hypothesis

$$= \widehat{R}^n(\emptyset) \cup \widehat{R}^{n+1}(\emptyset)$$

by def

$$= \widehat{R}^{n+1}(\emptyset)$$

because $\widehat{R}^n(\emptyset) \subseteq \widehat{R}^{n+1}(\emptyset)$

ICO's fixpoint

TH. $fix(\hat{R}) = I_R$ (under some hypotheses)

**each rule must have
finitely many premises**

proof.

by Kleene's fixpoint theorem we know that $fix(\hat{R})$ exists

$$fix(\hat{R}) = \bigcup_{n \in \mathbb{N}} \hat{R}^n(\emptyset) \quad \text{by def}$$

$$= \bigcup_{n \in \mathbb{N}} I_R^n \quad \text{by previous result}$$

$$= I_R \quad \text{by def}$$

Example

Strings of balanced parentheses

$$F = \{s \in \mathcal{L} \mid s \in \{(,)\}^*\}$$

$$R = \left\{ \frac{}{\epsilon \in \mathcal{L}}, \frac{s \in \mathcal{L}}{(s) \in \mathcal{L}}, \frac{s_1 \in \mathcal{L} \quad s_2 \in \mathcal{L}}{s_1 s_2 \in \mathcal{L}} \right\}$$

$$\hat{R}^0(\emptyset) = \emptyset$$

$$\hat{R}^1(\emptyset) = \{ \epsilon \in \mathcal{L} \}$$

$$\hat{R}^2(\emptyset) = \{ \epsilon \in \mathcal{L}, () \in \mathcal{L} \}$$

$$\hat{R}^3(\emptyset) = \{ \epsilon \in \mathcal{L}, () \in \mathcal{L}, (() \in \mathcal{L}, ()() \in \mathcal{L} \}$$

$$\begin{aligned} \hat{R}^4(\emptyset) = \{ & \epsilon \in \mathcal{L}, () \in \mathcal{L}, (() \in \mathcal{L}, ()() \in \mathcal{L}, (((() \in \mathcal{L}, \\ & (()()) \in \mathcal{L}, ()(()) \in \mathcal{L}, (()()) \in \mathcal{L}, ()()() \in \mathcal{L}, \\ & (()())() \in \mathcal{L}, ()()() \in \mathcal{L}, (()()) \in \mathcal{L}, ()()()() \in \mathcal{L} \} \end{aligned}$$

Example

$\mathbf{Pf}(\mathbb{N}, \mathbb{N})$

$$F = \{(n, m) \mid n, m \in \mathbb{N}\}$$

$$R = \left\{ \overline{(0, 0)}, \overline{(1, 1)}, \overline{\begin{matrix} (n, h) & (n+1, k) \\ (n+2, h+k) \end{matrix}} \right\}$$

$$\widehat{R}^0(\emptyset) = \emptyset$$

$$\widehat{R}^1(\emptyset) = \{ (0, 0), (1, 1) \}$$

$$\widehat{R}^2(\emptyset) = \{ (0, 0), (1, 1), (2, 1) \}$$

$$\widehat{R}^3(\emptyset) = \{ (0, 0), (1, 1), (2, 1), (3, 2) \}$$

$$\widehat{R}^4(\emptyset) = \{ (0, 0), (1, 1), (2, 1), (3, 2), (4, 3) \}$$

$$\widehat{R}^5(\emptyset) = \{ (0, 0), (1, 1), (2, 1), (3, 2), (4, 3), (5, 5) \}$$

$$\widehat{R}^6(\emptyset) = \{ (0, 0), (1, 1), (2, 1), (3, 2), (4, 3), (5, 5), (6, 8) \}$$