Fixed point property of $[\![\mathbf{while}\ B\ \mathbf{do}\ C]\!]$

$$[\![\mathbf{while}\ B\ \mathbf{do}\ C]\!] = f_{[\![B]\!],[\![C]\!]}([\![\mathbf{while}\ B\ \mathbf{do}\ C]\!])$$

where, for each $b : State \to \{true, false\}$ and $c : State \rightharpoonup State$, we define

$$f_{b,c} : (State \rightharpoonup State) \to (State \rightharpoonup State)$$

as

$$f_{b,c} = \lambda w \in (State \rightharpoonup State).\, \lambda s \in State.\, \mathit{if}\, \big(b(s), w(c(s)), s\big).$$

- Why does $w = f_{[\![B]\!],[\![C]\!]}(w)$ have a solution?
- What if it has several solutions—which one do we take to be $[\![\mathbf{while}\ B\ \mathbf{do}\ C]\!]$?

Approximating $[\![\textbf{while } B \textbf{ do } C]\!]$: State $\to$ State

$w_0 \sqsubseteq [\![\text{while } B \text{ do } C]\!]$

$\| \text{def}$

$\bot$ empty partial function

$f_{[\![B]\!],[\![C]\!]}(w_0)(s) \sqsubseteq [\![\text{while } B \text{ do } C]\!]$

$= \mathrm{if}([\![B]\!](s), w_0([\![C]\!]s), s)$

$= \mathrm{if}([\![B]\!](s), \uparrow, s)$

$$\omega_{n+1} \stackrel{\text{def}}{=} f_{[\![B]\!],[\![C]\!]}(\omega_n)$$

$$\omega_2 = f_{[\![B]\!],[\![C]\!]}(\omega_1)$$

$$\omega_2(s) = \mathit{if}([\![B]\!]s, \omega_1([\![C]\!]s), s)$$

$$= \mathit{if}([\![B]\!]s, \mathit{if}([\![B]\!]([\![C]\!]s), \uparrow, [\![C]\!]s), s)$$

$$w_n \sqsubseteq [\![\underline{\text{while}}\ B\ \underline{\text{do}}\ C]\!]$$

$$w_0 \sqsubseteq w_1 \sqsubseteq \cdots \sqsubseteq w_n \sqsubseteq w_{n+1} \sqsubseteq \cdots$$

$\underline{\text{join}}$ $\quad \bigsqcup_n w_n = [\![\underline{\text{while}}\ B\ \underline{\text{do}}\ C]\!]$

the union of the graphs of the w_n's.

$\boxed{?}$

$$f_{[\![B]\!],[\![C]\!]}\Big(\bigsqcup_n \omega_n\Big) = \bigsqcup_n \omega_n \quad ?$$

Approximating $[\![\mathbf{while}\ B\ \mathbf{do}\ C]\!]$

$$f_{[\![B]\!],[\![C]\!]}{}^{n}(\bot)$$

$$= \lambda s \in State. \begin{cases} [\![C]\!]^k(s) & \text{if } \exists\, 0 \leq k < n.\, [\![B]\!]([\![C]\!]^k(s)) = \mathit{false} \\ & \text{and } \forall\, 0 \leq i < k.\, [\![B]\!]([\![C]\!]^i(s)) = \mathit{true} \\ \uparrow & \text{if } \forall\, 0 \leq i < n.\, [\![B]\!]([\![C]\!]^i(s)) = \mathit{true} \end{cases}$$

$$D \stackrel{\text{def}}{=} (State \rightharpoonup State)$$

- **Partial order $\sqsubseteq$ on D:**

  $w \sqsubseteq w'$ iff for all $s \in State$, if w is defined at s then so is w' and moreover $w(s) = w'(s)$.

  iff the graph of w is included in the graph of w'.

- **Least element $\bot \in D$ w.r.t. $\sqsubseteq$:**

  $\bot$ = totally undefined partial function

  = partial function with empty graph

  (satisfies $\bot \sqsubseteq w$, for all $w \in D$).

Topic 2

Least Fixed Points

Thesis

All domains of computation are partial orders with a least element.

approximation order

bottom element

Thesis

All domains of computation are partial orders with a least element.

All computable functions are monotonic.

$f : D \to E$

$x \sqsubseteq y$ in D $\implies$ $f(x) \sqsubseteq f(y)$ in E

Partially ordered sets

A binary relation $\sqsubseteq$ on a set D is a partial order iff it is

reflexive: $\forall d \in D.\ d \sqsubseteq d$

transitive: $\forall d, d', d'' \in D.\ d \sqsubseteq d' \sqsubseteq d'' \Rightarrow d \sqsubseteq d''$

anti-symmetric: $\forall d, d' \in D.\ d \sqsubseteq d' \sqsubseteq d \Rightarrow d = d'$.

Such a pair $(D, \sqsubseteq)$ is called a partially ordered set, or poset.

$$\frac{}{x \sqsubseteq x}$$

$$\frac{x \sqsubseteq y \qquad y \sqsubseteq z}{x \sqsubseteq z}$$

$$\frac{x \sqsubseteq y \qquad y \sqsubseteq x}{x = y}$$

Domain of partial functions, $X \rightharpoonup Y$

$f \sqsubseteq g : X \rightharpoonup Y$

$\Leftrightarrow$ def iff $\mathrm{graph}(f) \subseteq \mathrm{graph}(g)$.

$\perp \stackrel{\text{def}}{=} \emptyset : X \rightharpoonup Y$.

Domain of partial functions, $X \rightharpoonup Y$

Underlying set: all partial functions, f, with domain of definition $dom(f) \subseteq X$ and taking values in Y.

Partial order:

$$
\begin{array}{lll}
f \sqsubseteq g & \text{iff} & dom(f) \subseteq dom(g) \text{ and} \\
& & \forall x \in dom(f).\ f(x) = g(x) \\
& \text{iff} & graph(f) \subseteq graph(g)
\end{array}
$$

Monotonicity

- A function $f : D \to E$ between posets is monotone iff

$$\forall d, d' \in D.\ d \sqsubseteq d' \Rightarrow f(d) \sqsubseteq f(d').$$

$$\frac{x \sqsubseteq y}{f(x) \sqsubseteq f(y)} \quad (f \text{ monotone})$$

$$f_{[\![B]\!],[\![C]\!]} : (\underline{State} \to \underline{State}) \to (\underline{State} \to \underline{State})$$

$\|$ is monotone.

$$\underline{\lambda w. \lambda s.} \ \underline{\text{if}}([\![B]\!](s), w([\![C]\!]s), s)$$

$$w \sqsubseteq w' \ \underset{\underline{RTP}}{\Longrightarrow} \ f_{[\![B]\!],[\![C]\!]}(w) \sqsubseteq f_{[\![B]\!],[\![C]\!]}(w')$$

(1) $\underline{dom}(f_{[\![B]\!],[\![C]\!]}(w)) \subseteq \underline{dom}(f_{[\![B]\!],[\![C]\!]}(w'))$

$s \in$

$$f_{[\![B]\!],[\![C]\!]}(w)(s) \downarrow$$

$$\parallel$$

$$f([\![B]\!](s), w([\![C]\!](s)), s) \qquad w \sqsubseteq w'$$

(i) $[\![B]\!](s) = \text{true}$

$$\Rightarrow f_{[\![B]\!],[\![C]\!]}(w)(s) = w([\![C]\!]s)$$

$$\Rightarrow w'([\![C]\!]s)\downarrow \text{ and } w'([\![C]\!]s) = w([\![C]\!]s)$$

$$\Rightarrow f_{[\![B]\!],[\![C]\!]}(w')(s)\downarrow$$

Least Elements

Suppose that D is a poset and that S is a subset of D.

An element $d \in S$ is the *least* element of S if it satisfies

$$\forall x \in S.\, d \sqsubseteq x \ .$$

d_0 is the least element of S. $\Rightarrow$ $d_0 \sqsubseteq d_1$
d_1 is the least element of S. $\Rightarrow$ $d_1 \sqsubseteq d_0$
$\Rightarrow d_0 = d_1$

- Note that because $\sqsubseteq$ is anti-symmetric, S has at most one least element.
- Note also that a poset may not have least element.

Pre-fixed points

Let D be a poset and $f : D \to D$ be a function.

An element $d \in D$ is a $\boxed{\text{pre-fixed point of } f}$ if it satisfies $f(d) \sqsubseteq d$.

The *least pre-fixed point* of f, if it exists, will be written

$$\boxed{\mathit{fix}(f)}$$

⇝ computationally meaningful

It is thus (uniquely) specified by the two properties:

$$f(\mathit{fix}(f)) \sqsubseteq \mathit{fix}(f) \qquad \text{(lfp1)}$$

$$\forall d \in D.\ f(d) \sqsubseteq d \ \Rightarrow\ \mathit{fix}(f) \sqsubseteq d. \qquad \text{(lfp2)}$$

Proof principle

1.

$$\frac{}{f(\mathit{fix}(f)) \sqsubseteq \mathit{fix}(f)}$$

2. Let D be a poset and let $f : D \to D$ be a function with a least pre-fixed point $\mathit{fix}(f) \in D$.

   For all $x \in D$, to prove that $\mathit{fix}(f) \sqsubseteq x$ it is enough to establish that $f(x) \sqsubseteq x$.

$$\frac{f(x) \sqsubseteq x}{\mathit{fix}(f) \sqsubseteq x}$$

$f : D \to D$ monotone D poset

$\underline{fix}(f) \Rightarrow f(\underline{fix}(f)) = \underline{fix}(f)$

Least pre-fixed points are fixed points

If it exists, the least pre-fixed point of a mononote function on a partial order is necessarily a fixed point.

$$\frac{f(x) \sqsubseteq x}{\mathrm{fix}(f) \sqsubseteq x}$$

$$\dfrac{\overline{f(\mathrm{fix}\, f) \sqsubseteq \mathrm{fix}(f)}}{f(\boxed{f(\mathrm{fix}\, f)}) \sqsubseteq \boxed{f(\mathrm{fix}\, f)}}\ (f\ \mathrm{mon})$$

$$\dfrac{\overline{f(\mathrm{fix}\, f) \sqsubseteq \mathrm{fix}(f)} \qquad \dfrac{f(\boxed{f(\mathrm{fix}\, f)}) \sqsubseteq \boxed{f(\mathrm{fix}\, f)}}{\mathrm{fix}(f) \sqsubseteq \boxed{f(\mathrm{fix}\, f)}}}{f(\mathrm{fix}(f)) = \mathrm{fix}(f)}$$

Thesis*

All domains of computation are complete partial orders with a least element.

All computable functions are continuous.