$$[\![\underline{\text{while}}\ B\ \underline{\text{do}}\ C]\!] : \text{State} \rightarrow \text{State}$$

Desiderata:

$$[\![\underline{\text{while}}\ B\ \underline{\text{do}}\ C]\!](s) = \text{if}\big([\![B]\!](s),\ [\![\underline{\text{while}}\ B\ \underline{\text{do}}\ C]\!]([\![C]\!]s),\ s\big)$$

$$[\![\underline{\text{while}}\ B\ \underline{\text{do}}\ C]\!] = \lambda s.\ \text{if}\big([\![B]\!](s),\ [\![\underline{\text{while}}\ B\ \underline{\text{do}}\ C]\!]([\![C]\!]s),\ s\big)$$

$[\![\underline{\text{while}}\ B\ \underline{\text{do}}\ C]\!] : State \to State$

is a state transformer $w : State \to State$ satisfying

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

In other words:

$$[\![\underline{\text{while}}\ B\ \underline{\text{do}}\ C]\!] = \underline{\text{fix}}\big(\underbrace{\lambda w.\lambda s.\ \underline{\text{if}}\left([\![B]\!](s),\ w([\![C]\!]s),\ s\right)}_{(State \to State) \longrightarrow (State \to State)}\big)$$

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

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

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

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

as

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

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

NB: $[\![\text{while true do skip}]\!] = \bot : State \to State$

The empty partial function

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

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

$$w_1 = f_{[\![B]\!],[\![C]\!]}(w_0) = f_{[\![B]\!],[\![C]\!]}(\bot)$$

$$= \lambda s.\ \text{if}\left([\![B]\!](s), \bot([\![C]\!]s), s\right)$$

$$= \lambda s.\ \begin{cases} \uparrow & \text{if } [\![B]\!](s) = true \\ s & \text{if } [\![B]\!](s) = false \end{cases}$$

$$w_2 = f_{[\![B]\!],[\![C]\!]}(w_1)$$

$$= \lambda s.\ \mathrm{if}\left([\![B]\!](s),\ w_1([\![C]\!]s),\ s\right)$$

$$= \lambda s.\ \mathrm{if}\left([\![B]\!](s),\ \mathrm{if}\left([\![B]\!]([\![C]\!]s),\ \uparrow,\ [\![C]\!]s\right),s\right)$$

$$= \lambda s.\ \begin{cases} \uparrow & \text{, if } [\![B]\!](s) = [\![B]\!]([\![C]\!]s) = \mathrm{true} \\ [\![C]\!](s) & \text{, if } [\![B]\!](s) = \mathrm{true} \wedge [\![B]\!]([\![C]\!]s) = \mathrm{false} \\ s & \text{, if } [\![B]\!](s) = \mathrm{false} \end{cases}$$

$$w_{n+1} \overset{\mathrm{def}}{=} f_{[\![B]\!],[\![C]\!]}(w_n)$$

$$\underline{fix}(f_{[\![B]\!],[\![C]\!]}) = \bigsqcup_{n \in \mathbb{N}} w_n \qquad w_0 \stackrel{def}{=} \bot$$

"limit" $\quad w_{n+1} = f_{[\![B]\!],[\![C]\!]}(w_n)$

for state transformers is given by the union of the graphs of w_n

$$f_{[\![B]\!],[\![C]\!]}\left(\bigsqcup_n w_n\right) = \bigsqcup_n w_n$$

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

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

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

the domain of state transformers.

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

information order.

- **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'.

bottom element

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

$\perp$ = totally undefined partial function

= partial function with empty graph

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

<u>NB</u>: $f_{[\![B]\!],[\![C]\!]} : (State \to State) \to (State \to State)$

Has the property: (monotonicity)

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

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

$$f_{[\![B]\!],[\![C]\!]}(w') = \lambda s.\, if([\![B]\!](s), w'([\![C]\!]s), s)$$

Topic 2

Least Fixed Points

Thesis

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

All computable functions are monotonic.

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.

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

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

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

partial functions from X to Y

Domain of partial functions, $X \rightharpoonup Y$

$$f \sqsubseteq g \iff \underline{\mathrm{graph}}(f) \subseteq \underline{\mathrm{graph}}(g)$$

$$\iff \forall x \in \underline{\mathrm{dom}}(f) .\; x \in \underline{\mathrm{dom}}(g) \wedge f(x) = g(x)$$

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

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

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

$(\mathbb{Z}, \leq)$

Least Elements

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

An element $d \in S$ is the $\boxed{\textit{least} \text{ element}}$ of S if it satisfies

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

Suppose d_1 is least in S
Suppose d_2 is least in S $\Rightarrow$ $d_1 = d_2$

- Note that because $\sqsubseteq$ is anti-symmetric, S has at most one least element.

- Note also that a poset may not have least element.

fix(f) is a fixed point

Pre-fixed points

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

An element $d \in D$ is a 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

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

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

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

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

$$\dfrac{\dfrac{}{f(\underline{fix}(f)) \sqsubseteq \underline{fix}(f)}\,(lfp1) \qquad \dfrac{?}{\underline{fix}(f) \sqsubseteq f(\underline{fix}(f))}}{\underline{fix}(f) = f(\underline{fix}(f))}\ \text{f monotone}$$