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

Operationally

$$\text{while } B \text{ do } C \equiv \text{if } B \text{ then } (C;\ \text{while } B \text{ do } C) \text{ else skip.}$$

We should have:

$$[\![\text{while } B \text{ do } C]\!] = [\![\text{if } B \text{ then } (C;\ \text{while } B \text{ do } C) \text{ else skip}]\!]$$

So for all states s:

$$[\![\text{while } B \text{ do } C]\!]\, s$$
$$= [\![\text{if } B \text{ then } (C;\ \text{while } B \text{ do } s) \text{ else skip}]\!]\, s$$

$$= if\left([\![B]\!]s,\ [\![C;\ \text{while } B \text{ do } C]\!]s,\ [\![\text{skip}]\!]s\right)$$

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

So

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

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

Can we make this a definition? No, but this tells us that $[\![\text{while } B \text{ do } C]\!]$ is a fixed point; and we will use that fact.

For any function $h : A \to A$, a <u>fixed point</u> of h is (by definition) an element $a \in A$ such that

$$h(a) = a$$

<u>Claim</u>: $[\![\text{while } B \text{ do } C]\!]$ is a fixed point of the function $f_{[\![B]\!],[\![C]\!]}$:

from $(State \to State) \longrightarrow (State \to State)$

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

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

as

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

Now we can define

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

$= \underline{\text{fix}}\left(f_{[\![B]\!],[\![C]\!]} \right)$

$\boxed{?}$ Does this always exist?

$\boxed{?}$ If so, what is its operational meaning?

$\boxed{?}$ What is this $\underline{\text{fix}}$?

$\vdash$ in (States $\to$ States)

$fix\,(f_{[\![B]\!],[\![C]\!]})$ always exists.

In fact we can calculate it by approximation as follows

$\bot \in$ (States $\to$ States) — is the completely undefined function

Consider

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

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

$= \lambda s.\ if\,([\![B]\!]s, \uparrow, s)$

$$f_{[\![B]\!],[\![C]\!]}\left(f_{[\![B]\!],[\![C]\!]}(\bot)\right)$$

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

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

Then

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

is the approximation of the while loop up to n iterations

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

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

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

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

Furthermore

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

is a fixed point of $f_{[\![B]\!],[\![C]\!]}$

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

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

Define $\mathit{fix}(f_{[\![B]\!],[\![C]\!]}) = \bigcup_n f_{[\![B]\!],[\![C]\!]}{}^n(\perp)$

a special kind of partial order.

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

- **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.

Example:

(State → State)

Thesis

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

All computable functions are mononotic.

Example: $f_{[\![B]\!],[\![C]\!]} : (States \to States) \to (States \to States)$

is monotone:

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

$\sqsubseteq \subseteq D \times D$

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.

Example: for every pair of sets X and Y, the set of partial functions from X to Y is a partial order.

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

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

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

Domain of partial functions, $X \rightharpoonup Y$

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.

graph(f) = { (x, fx) | fx is defined }

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:

$$f \sqsubseteq g \quad \text{iff} \quad dom(f) \subseteq dom(g) \text{ and}$$
$$\forall x \in dom(f).\ f(x) = g(x)$$
$$\text{iff} \quad graph(f) \subseteq graph(g)$$

Example: $(\mathcal{P}(S), \subseteq)$ is a partial order, with least element $\emptyset$

Monotonicity

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

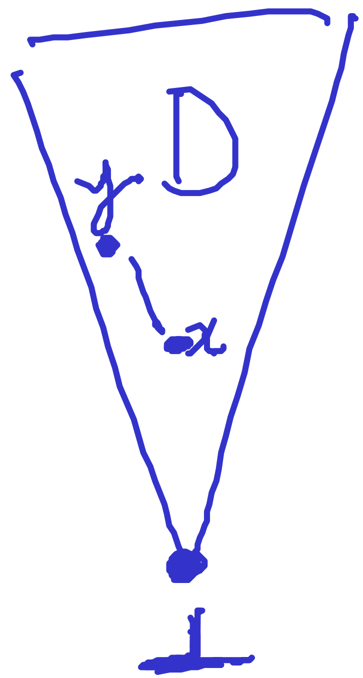
$$\forall d, d' \in D.\ d \sqsubseteq d' \Rightarrow f(d) \sqsubseteq f(d').$$

More input yields more output!

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

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

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

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

$\mathbb{B} \stackrel{\text{def}}{=} \{\text{true}, \text{false}\}$

Example: $(\mathbb{Z}, \leq)$, $(\mathbb{B}, =)$

true •   • false

It is good to generalise to pre fixed points.

Pre-fixed points

A pre fixed point of f is an element x s.t.

$f(x) \sqsubseteq x$

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

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

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

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

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

Proof principle

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 $f(x) \sqsubseteq x$.

Proof principle

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 $f(x) \sqsubseteq x$.

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

Proof principle

1. Claim: $\mathit{fix}(f) \sqsubseteq f(\mathit{fix}(f))$.

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

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 $f(x) \sqsubseteq x$.

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