Reasoning with Derivations

$\Downarrow \subseteq S \times State \times State$

Program, initial state, final state.

$(S, \sigma, \sigma') \in \Downarrow \iff S, \sigma \Downarrow \sigma'$

$$\frac{}{skip, \sigma \Downarrow \sigma} \qquad \frac{}{x \leftarrow e, \sigma \Downarrow \sigma[x \mapsto [\![e]\!]_A(\sigma)]}$$

$$\frac{S_1, \sigma_1 \Downarrow \sigma_2 \quad S_2, \sigma_2 \Downarrow \sigma_3}{S_1; S_2, \sigma_1 \Downarrow \sigma_3} \qquad \frac{S_1, \sigma_1 \Downarrow \sigma_2}{\text{if } e \text{ then } S_1 \text{ else } S_2, \sigma_1 \Downarrow \sigma_2}\ [\![e]\!]_B(\sigma) = T$$

$$\frac{S_2, \sigma_1 \Downarrow \sigma_2}{\text{if } e \text{ then } S_1 \text{ else } S_2, \sigma_1 \Downarrow \sigma_2}\ [\![e]\!]_B(\sigma) = \bot \qquad \frac{}{\text{while } e \text{ do } S, \sigma \Downarrow \sigma}\ [\![e]\!]_B(\sigma) = \bot$$

$$\frac{S, \sigma_1 \Downarrow \sigma_2 \quad \text{while } e \text{ do } S, \sigma_2 \Downarrow \sigma_3}{\text{while } e \text{ do } S, \sigma_1 \Downarrow \sigma_3}\ [\![e]\!]_B(\sigma_1) = T$$

Termination

while true do skip, $[\,] \Downarrow \sigma$

$$\frac{\dfrac{}{skip, [\,] \Downarrow [\,]} \quad \dfrac{\dfrac{\vdots}{skip, [\,] \Downarrow [\,]} \quad \text{while true do skip}, [\,] \Downarrow \sigma}{\text{while true do skip}, [\,] \Downarrow \sigma}}{\text{while true do skip}, [\,] \Downarrow \sigma}$$

No derivation

A program $S \in Stmt$ terminates in a state $\sigma \in State$ if $\exists \sigma' \in State.\ S, \sigma \Downarrow \sigma'$

Example Program

$$L \begin{cases} z \leftarrow 1; \\ \text{while } 0 \le x \text{ do} \\ \quad z \leftarrow z * y; \\ \quad x \leftarrow x - 1 \end{cases} E$$

y^{x+1} when $x \ge 0$

$\forall \sigma_I \in State.\ \exists \sigma_F \in State.\ \underbrace{E, \sigma_I \Downarrow \sigma_F}$

We must provide a recipe for a derivation

$$\frac{\dfrac{}{z \leftarrow 1, \sigma_I \Downarrow \sigma_I[z \mapsto 1]} \quad \overset{?}{L, \sigma_I[z \mapsto 1] \Downarrow \sigma_F}}{z \leftarrow 1; L, \sigma_I \Downarrow \sigma_F}$$

$\forall \sigma_I \exists \sigma'.\ L, \sigma \Downarrow \sigma'$ where $\sigma(x) \ge 0$

(Induction Principle. $\forall x \in X.\ P(x)$ — Inductively defined set.)

$\forall n \in \mathbb{N}.\ \forall \sigma.$ if $\sigma(x) = n$ then $\exists \sigma'.\ L, \sigma \Downarrow \sigma'$

* (Base Case)

Suppose $\sigma(x) = 0$

One iteration

$$\frac{\dfrac{\vdots}{z \leftarrow x * y;\ x \leftarrow x - 1, \sigma \Downarrow \sigma[z \to \sigma(x) \cdot \sigma(y),\ x \mapsto \sigma(x) - 1]} \quad \overbrace{L, \sigma[z \to \sigma(x) \cdot \sigma(y),\ x \mapsto \sigma(x) - 1] \Downarrow \sigma'}^{\sigma'}}{\text{while } 0 \le x \text{ do } z \leftarrow x * y;\ x \leftarrow x - 1, \sigma \Downarrow \sigma'}$$

* (Inductive Case)

Suppose $\sigma(x) = n + 1$

assm. $\underbrace{\forall \sigma.\ \text{if } \sigma(x) = n \text{ then } \exists \sigma',\ L, \sigma \Downarrow \sigma'}_{\text{Induction Hypothesis}}$

$$\frac{\dfrac{\vdots}{z \leftarrow z * y;\ x \leftarrow x - 1, \sigma \Downarrow \sigma'} \quad L, \sigma' \Downarrow\ ?}{L, \sigma \Downarrow\ ?}$$

$[z \mapsto \sigma(z) \cdot \sigma(y),\ x \mapsto \underbrace{\sigma(x) - 1}_{n}]$

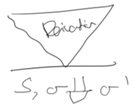
by I.H. $L, \sigma' \Downarrow \sigma_F$

$\therefore\ L, \sigma \Downarrow \sigma_F$

Inversion Principle

$\implies S, \sigma \Downarrow \sigma'$

$S, \sigma \Downarrow \sigma' \implies$



What form the derivation has?

Semantic Equivalence

S_1 and S_2 are semantically equivalent if $\forall \sigma, \sigma' \in State$

$S_1, \sigma \Downarrow \sigma' \iff S_2, \sigma \Downarrow \sigma'$

if e then S else S — Semantically equivalent to S

* $S, \sigma \Downarrow \sigma'$ then if e then S else $S, \sigma \Downarrow \sigma'$

- If $[\![e]\!]_B(\sigma) = T$,

$$\frac{S, \sigma \Downarrow \sigma'}{\text{if } e \text{ then } S \text{ else } S, \sigma \Downarrow \sigma'}$$

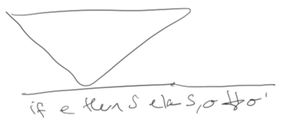
follow by assumption.

- If $[\![e]\!]_B(\sigma) = \bot$

$$\frac{S, \sigma \Downarrow \sigma'}{\text{if } e \text{ then } S \text{ else } S, \sigma \Downarrow \sigma'}$$

True if both $[\![e]\!]_B(\sigma) = T$ or $[\![e]\!]_B(\sigma) = \bot$

* if e then S else $S, \sigma \Downarrow \sigma'$ then $S, \sigma \Downarrow \sigma'$



Either:

$$\frac{S, \sigma \Downarrow \sigma'}{\text{if } e \text{ then } S \text{ else } S, \sigma \Downarrow \sigma'}\ [\![e]\!]_B(\sigma) = T$$

Or:

$$\frac{S, \sigma \Downarrow \sigma'}{\text{if } e \text{ then } S \text{ else } S, \sigma \Downarrow \sigma'}\ [\![e]\!]_B(\sigma) = \bot$$

i.e. if e then S else $S, \sigma \Downarrow \sigma'$

$\implies [\![e]\!]_B(\sigma) = T$ and $S, \sigma \Downarrow \sigma'$

or $[\![e]\!]_B(\sigma) = \bot$ and $S, \sigma \Downarrow \sigma'$

in either case $S, \sigma \Downarrow \sigma'$ as required.