The following slides have been adapted from the material of the course

Principles for Software Composition

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

by

Roberto Bruni (University of Pisa, Italy)

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

Used with permission of the author

w.f. induction principle

a w.f. relation $\prec \subseteq A \times A$

$$\frac{\forall a \in A.\ (\ (\forall b \prec a.\ P(b)) \Rightarrow P(a)\ )}{\forall a \in A.\ P(a)}$$

Advantage: when proving $P(a)$ for a generic a,

we can exploit the assumption $\forall b \prec a.\ P(b)$!

Weak mathematical induction principle

$$\frac{P(0) \qquad \forall n \in \mathbb{N}.\ (\ P(n) \Rightarrow P(n+1)\ )}{\forall n \in \mathbb{N}.\ P(n)}$$

Weak: we can exploit $P(n)$,

for proving $P(n+1)$!

Strong mathematical induction

$$\frac{P(0) \qquad \forall n \in \mathbb{N}.\ (\ (P(0) \wedge \cdots \wedge P(n)) \Rightarrow P(n+1)\ )}{\forall n \in \mathbb{N}.\ P(n)}$$

Strong: we can exploit more hypotheses than $P(n)$, for proving $P(n+1)$!

Structural induction principle

$$\frac{\forall n \in \mathbb{N}.\ \forall f \in \Sigma_n.\ \forall t_1, ..., t_n \in T_\Sigma.\ (P(t_1) \wedge \cdots \wedge P(t_n)) \Rightarrow P(f(t_1, ..., t_n))}{\forall t \in T_\Sigma.\ P(t)}$$

Arithmetic expressions [IMP]

$$a ::= x \mid n \mid a \ \mathsf{op} \ a$$

$$x \in \mathsf{Ide} \qquad \mathsf{op} \in \{+, \times, -\}$$

$$n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : \mathsf{Ide} \to \mathbb{Z}\}$$

$$\frac{}{\langle x, \sigma\rangle \longrightarrow \sigma(x)} \qquad \frac{}{\langle n, \sigma\rangle \longrightarrow n} \qquad \frac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \ \mathsf{op} \ a_1, \sigma\rangle \longrightarrow n_0 \ op \ n_1}$$

Arithmetic expressions [IMP]

$$a ::= x \mid n \mid a \text{ op } a$$

$$x \in \text{Ide} \qquad \text{op} \in \{+, \times, -\}$$

$$n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : \text{Ide} \to \mathbb{Z}\}$$

$$\frac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)} \qquad \frac{}{\langle n, \sigma \rangle \longrightarrow n} \qquad \frac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow n_0 \; op \; n_1}$$

Termination: $P(a) \triangleq \forall \sigma \in \mathbb{M}.\ \exists m \in \mathbb{Z}.\ \langle a, \sigma \rangle \longrightarrow m$

$$\forall a.\ P(a)\ ?$$

Structural induction principle

$$\frac{\forall a_0, a_1.\ P(a_0) \wedge P(a_1) \Rightarrow P(a_0\ \mathsf{op}\ a_1)}{\forall a.\ P(a)} \qquad \forall x \in \mathsf{Ide}.\ P(x) \qquad \forall n \in \mathbb{Z}.\ P(n)$$

Termination: $P(a) \triangleq \forall \sigma \in \mathbb{M}.\ \exists m \in \mathbb{Z}.\ \langle a, \sigma \rangle \longrightarrow m$

$$\forall a.\ P(a)$$

Determinacy by structural induction

Arithmetic expressions [IMP]

$$a ::= x \mid n \mid a \text{ op } a$$

$$x \in \text{Ide} \qquad \text{op} \in \{+, \times, -\}$$

$$n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : \text{Ide} \to \mathbb{Z}\}$$

$$\frac{}{\langle x, \sigma\rangle \longrightarrow \sigma(x)} \qquad \frac{}{\langle n, \sigma\rangle \longrightarrow n} \qquad \frac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma\rangle \longrightarrow n_0 \; op \; n_1}$$

Determinacy:

$$P(a) \triangleq \forall \sigma \in \mathbb{M}.\ \forall m, m' \in \mathbb{Z}.\ \langle a, \sigma\rangle \longrightarrow m \wedge \langle a, \sigma\rangle \longrightarrow m' \Rightarrow m = m'$$

$$\forall a.\ P(a)\ ?$$

Structural induction principle

$$\frac{\forall a_0, a_1.\ P(a_0) \wedge P(a_1) \Rightarrow P(a_0\ \mathsf{op}\ a_1)}{\forall a.\ P(a)}$$

$\forall x \in \mathsf{Ide}.\ P(x)$ $\qquad$ $\forall n \in \mathbb{Z}.\ P(n)$

Determinacy:

$$P(a) \triangleq \forall \sigma \in \mathbb{M}.\ \forall m, m' \in \mathbb{Z}.\ \langle a, \sigma \rangle \longrightarrow m \wedge \langle a, \sigma \rangle \longrightarrow m' \Rightarrow m = m'$$

$$\forall a.\ P(a)\ ?$$

!!

Inductive case

$\forall a_0, a_1.\ P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \text{ op } a_1)$ Take generic a_0, a_1

We assume (inductive hypotheses)

$$P(a_i) \triangleq \forall \sigma, m_i, m_i'.\ \langle a_i, \sigma \rangle \longrightarrow m_i \wedge \langle a_i, \sigma \rangle \longrightarrow m_i' \Rightarrow m_i = m_i'$$

We want to prove

$$P(a_0 \text{ op } a_1) \triangleq \forall \sigma, m, m'.\ \langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m \wedge \langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m' \Rightarrow m = m'$$

Take generic σ, m, m' such that $\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m$ and $\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m'$

We want to prove $m = m'$

Inductive case (ctd)

Consider the goal $\langle a_0 \text{ op } a_1, \sigma\rangle \longrightarrow m$

Only the rule $\dfrac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma\rangle \longrightarrow n_0 \; op \; n_1}$ is applicable

hence $m = n_0 \; op \; n_1$ with $\langle a_0, \sigma\rangle \longrightarrow n_0$ and $\langle a_1, \sigma\rangle \longrightarrow n_1$

Similarly, since $\langle a_0 \text{ op } a_1, \sigma\rangle \longrightarrow m'$

it must be $m' = n'_0 \; op \; n'_1$ with $\langle a_0, \sigma\rangle \longrightarrow n'_0$ and $\langle a_1, \sigma\rangle \longrightarrow n'_1$

By inductive hypotheses, $n_0 = n'_0$ and $n_1 = n'_1$

and thus we conclude $m = n_0 \; op \; n_1 = n'_0 \; op \; n'_1 = m'$

The full language IMP

Boolean expressions

$$a \;::=\; x \;\mid\; n \;\mid\; a \;\mathsf{op}\; a$$
$$b \;::=\; v \;\mid\; a \;\mathsf{cmp}\; a \;\mid\; \neg b \;\mid\; b \;\mathsf{bop}\; b$$

$$\frac{}{\langle x, \sigma\rangle \longrightarrow \sigma(x)} \qquad \frac{}{\langle n, \sigma\rangle \longrightarrow n} \qquad \frac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \;\mathsf{op}\; a_1, \sigma\rangle \longrightarrow n_0 \;op\; n_1}$$

$$\frac{}{\langle v, \sigma\rangle \longrightarrow v} \qquad \frac{\langle b, \sigma\rangle \longrightarrow v}{\langle \neg b, \sigma\rangle \longrightarrow \neg v} \qquad \frac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \;\mathsf{cmp}\; a_1, \sigma\rangle \longrightarrow n_0 \;cmp\; n_1}$$

$$\frac{\langle b_0, \sigma\rangle \longrightarrow v_0 \quad \langle b_1, \sigma\rangle \longrightarrow v_1}{\langle b_0 \;\mathsf{bop}\; b_1, \sigma\rangle \longrightarrow v_0 \;bop\; v_1}$$

$$P(b) \stackrel{\triangle}{=} \forall \sigma \in \mathbb{M}.\ \exists v \in \mathbb{B}.\ \langle b, \sigma\rangle \longrightarrow v$$

A surprising base case

$\forall a_0, a_1.\ P(a_0 \text{ cmp } a_1)$ Take generic a_0, a_1

We want to prove $P(a_0 \text{ cmp } a_1) \triangleq \forall \sigma.\ \exists v.\ \langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow v$

Consider the goal $\langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow v$

By rule $\dfrac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow n_0\ cmp\ n_1}$ we have

$$\langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow v \nwarrow_{[v = n_0\ cmp\ n_1]} \langle a_0, \sigma \rangle \longrightarrow n_0, \langle a_1, \sigma \rangle \longrightarrow n_1$$

By termination of arithmetic expressions, such n_0, n_1 exist

And we are done (taking $v = n_0\ cmp\ n_1$)

The Language IMP: Commands

Commands of IMP

$$a ::= x \mid n \mid a + a \mid \cdots \qquad b ::= v \mid a \leq a \mid \cdots$$

$$c ::= \mathbf{skip} \mid x := a \mid c\,;c \mid \mathbf{if}\ b\ \mathbf{then}\ c\ \mathbf{else}\ c \mid \mathbf{while}\ b\ \mathbf{do}\ c$$

$$S \triangleq \{\mathsf{Aexp}, \mathsf{Bexp}, \mathsf{Com}\}$$

$$\Sigma_{\epsilon,\mathsf{Aexp}} \triangleq \mathsf{Ide} \cup \mathbb{Z} \qquad \Sigma_{\mathsf{AexpAexp},\mathsf{Aexp}} \triangleq \{+, \times, -\}$$

$$\Sigma_{\epsilon,\mathsf{Bexp}} \triangleq \mathbb{B} \qquad \Sigma_{\mathsf{AexpAexp},\mathsf{Bexp}} \triangleq \{<, \leq, >, \geq, =, \neq\}$$

$$\Sigma_{\mathsf{Bexp},\mathsf{Bexp}} \triangleq \{\neg\} \qquad \Sigma_{\mathsf{BexpBexp},\mathsf{Bexp}} \triangleq \{\wedge, \vee\}$$

$$\Sigma_{\epsilon,\mathsf{Com}} \triangleq \{\mathbf{skip}\} \qquad \Sigma_{\mathsf{Aexp},\mathsf{Com}} \triangleq \{x := \mid x \in \mathsf{Ide}\}$$

$$\Sigma_{\mathsf{ComCom},\mathsf{Com}} \triangleq \{\ ;\ \} \qquad \Sigma_{\mathsf{BexpComCom},\mathsf{Com}} \triangleq \{\ \mathbf{if}\ \}$$

$$\Sigma_{\mathsf{BexpCom},\mathsf{Com}} \triangleq \{\ \mathbf{while}\ \}$$

Memories

$\mathbb{M} \triangleq \{\, \sigma : \mathsf{Ide} \to \mathbb{Z} \mid \sigma \text{ has finite support} \,\}$

$\{x \in \mathsf{Ide} \mid \sigma(x) \neq 0\}$ is finite

$(n_1/x_1, ..., n_k/x_k) : \mathsf{Ide} \to \mathbb{Z}$

all different

$$(n_1/x_1, ..., n_k/x_k)(x) \triangleq \begin{cases} n_i & \text{if } x = x_i \\ 0 & \text{otherwise} \end{cases}$$

$\sigma_0 \triangleq ()$ is the typical initial memory

Memory updates

$$\sigma[n/y](x) \triangleq \begin{cases} n & \text{if } x = y \\ \sigma(x) & \text{otherwise} \end{cases}$$

$\forall \sigma, m, n, y.\ \sigma[m/y][n/y] = \sigma[n/y]$

$$\sigma[m/y][n/y](x) \triangleq \begin{cases} n & \text{if } x = y \\ \sigma[m/y](x) = \sigma(x) & \text{otherwise} \end{cases}$$

$\forall \sigma, m, n, y, z.\ \ y \neq z \ \Rightarrow\ \sigma[n/y][m/z] = \sigma[m/z][n/y]$

we write $\sigma[n/y, m/z]$ in such cases

$(n_1/x_1, ..., n_k/x_k) = \sigma_0[n_1/x_1, ..., n_k/x_k]$

Semantics of commands

$$c ::= \textbf{skip} \mid x := a \mid c\,;c \mid \textbf{if } b \textbf{ then } c \textbf{ else } c \mid \textbf{while } b \textbf{ do } c$$

$$\frac{}{\langle \textbf{skip}, \sigma\rangle \longrightarrow \sigma} \qquad \frac{\langle a, \sigma\rangle \longrightarrow n}{\langle x := a, \sigma\rangle \longrightarrow \sigma[n/x]} \qquad \frac{\langle c_0, \sigma\rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma''\rangle \longrightarrow \sigma'}{\langle c_0\,; c_1, \sigma\rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma\rangle \longrightarrow \textbf{ff} \quad \langle c_1, \sigma\rangle \longrightarrow \sigma'}{\langle \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, \sigma\rangle \longrightarrow \sigma'} \qquad \frac{\langle b, \sigma\rangle \longrightarrow \textbf{tt} \quad \langle c_0, \sigma\rangle \longrightarrow \sigma'}{\langle \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, \sigma\rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma\rangle \longrightarrow \textbf{ff}}{\langle \textbf{while } b \textbf{ do } c, \sigma\rangle \longrightarrow \sigma} \qquad \frac{\langle b, \sigma\rangle \longrightarrow \textbf{tt} \quad \langle c, \sigma\rangle \longrightarrow \sigma'' \quad \langle \textbf{while } b \textbf{ do } c, \sigma''\rangle \longrightarrow \sigma'}{\langle \textbf{while } b \textbf{ do } c, \sigma\rangle \longrightarrow \sigma'}$$

Does termination hold for IMP?
What about determinancy?

Recursive definition!

one of the premises is as complex as the conclusion

$$\frac{\langle b, \sigma\rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma\rangle \longrightarrow \sigma'' \quad \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma'}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma'}$$

Semantics of commands

$$c ::= \textbf{skip} \mid x := a \mid c\,;c \mid \textbf{if } b \textbf{ then } c \textbf{ else } c \mid \textbf{while } b \textbf{ do } c$$

$$\frac{}{\langle \textbf{skip}, \sigma\rangle \longrightarrow \sigma} \qquad \frac{\langle a, \sigma\rangle \longrightarrow n}{\langle x := a, \sigma\rangle \longrightarrow \sigma[n/x]} \qquad \frac{\langle c_0, \sigma\rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma''\rangle \longrightarrow \sigma'}{\langle c_0\,; c_1, \sigma\rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma\rangle \longrightarrow \textbf{ff} \quad \langle c_1, \sigma\rangle \longrightarrow \sigma'}{\langle \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, \sigma\rangle \longrightarrow \sigma'} \qquad \frac{\langle b, \sigma\rangle \longrightarrow \textbf{tt} \quad \langle c_0, \sigma\rangle \longrightarrow \sigma'}{\langle \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, \sigma\rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma\rangle \longrightarrow \textbf{ff}}{\langle \textbf{while } b \textbf{ do } c, \sigma\rangle \longrightarrow \sigma} \qquad \frac{\langle b, \sigma\rangle \longrightarrow \textbf{tt} \quad \langle c, \sigma\rangle \longrightarrow \sigma'' \quad \langle \textbf{while } b \textbf{ do } c, \sigma''\rangle \longrightarrow \sigma'}{\langle \textbf{while } b \textbf{ do } c, \sigma\rangle \longrightarrow \sigma'}$$

Determinacy:

$$P(c) \triangleq \forall \sigma, \sigma_1, \sigma_2.\ \langle c, \sigma\rangle \longrightarrow \sigma_1 \wedge \langle c, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2 \qquad \forall c.\ P(c)\ ?$$

Structural induction principle

$$\frac{\begin{array}{c}\forall x, a.\ P(x := a) \qquad\qquad P(\mathbf{skip}) \\ \forall c_0, c_1.\ P(c_0) \wedge P(c_1) \Rightarrow P(c_0\,;c_1) \\ \forall b, c_0, c_1.\ P(c_0) \wedge P(c_1) \Rightarrow P(\mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1) \\ \forall b, c.\ P(c) \Rightarrow P(\mathbf{while}\ b\ \mathbf{do}\ c)\end{array}}{\forall c \in \mathsf{Com}.\ P(c)}$$

Base case

$\forall x, a.\ P(x := a)$

Take generic $x \in \mathsf{Ide}, a \in \mathsf{Aexp}$

We want to prove

$$P(x := a) \triangleq \forall \sigma, \sigma_1, \sigma_2.\ \langle x := a, \sigma\rangle \longrightarrow \sigma_1 \wedge \langle x := a, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

Take generic $\sigma, \sigma_1, \sigma_2$ s.t. $\langle x := a, \sigma\rangle \longrightarrow \sigma_1$ and $\langle x := a, \sigma\rangle \longrightarrow \sigma_2$

We want to prove $\sigma_1 = \sigma_2$

Consider the goal $\langle x := a, \sigma\rangle \longrightarrow \sigma_1$

Only the rule $\dfrac{\langle a, \sigma\rangle \longrightarrow n}{\langle x := a, \sigma\rangle \longrightarrow \sigma[n/x]}$ is applicable, hence $\sigma_1 = \sigma[n/x]$ with $\langle a, \sigma\rangle \longrightarrow n$

Similarly, since $\langle x := a, \sigma\rangle \longrightarrow \sigma_2$ it must be $\sigma_2 = \sigma[m/x]$ with $\langle a, \sigma\rangle \longrightarrow m$

by determinacy of Aexp we have $n = m$ and thus $\sigma_1 = \sigma_2$

Inductive case

$\forall c_0, c_1.\ P(c_0) \wedge P(c_1) \Rightarrow P(c_0\,;c_1)$ Take generic c_0, c_1

We assume (inductive hypotheses)

$$P(c_i) \triangleq \forall \sigma, \sigma_1, \sigma_2.\ \langle c_i, \sigma\rangle \longrightarrow \sigma_1 \wedge \langle c_i, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

We want to prove

$$P(c_0\,;c_1) \triangleq \forall \sigma, \sigma_1, \sigma_2.\ \langle c_0\,;c_1, \sigma\rangle \longrightarrow \sigma_1 \wedge \langle c_0\,;c_1, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

Take generic $\sigma, \sigma_1, \sigma_2$ such that $\langle c_0\,;c_1, \sigma\rangle \longrightarrow \sigma_1$ and $\langle c_0\,;c_1, \sigma\rangle \longrightarrow \sigma_2$

We want to prove $\sigma_1 = \sigma_2$

Inductive case (ctd)

Consider the goal $\langle c_0 \,;\, c_1, \sigma\rangle \longrightarrow \sigma_1$

Only the rule $\dfrac{\langle c_0, \sigma\rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma''\rangle \longrightarrow \sigma'}{\langle c_0 \,;\, c_1, \sigma\rangle \longrightarrow \sigma'}$ is applicable

hence $\sigma_1 = \sigma_1'$ with $\langle c_0, \sigma\rangle \longrightarrow \sigma_1''$ and $\langle c_1, \sigma_1''\rangle \longrightarrow \sigma_1'$

Similarly, since $\langle c_0 \,;\, c_1, \sigma\rangle \longrightarrow \sigma_2$

it must be $\sigma_2 = \sigma_2'$ with $\langle c_0, \sigma\rangle \longrightarrow \sigma_2''$ and $\langle c_1, \sigma_2''\rangle \longrightarrow \sigma_2'$

By inductive hypothesis $P(c_0)$, we have $\sigma_1'' = \sigma_2''$

and thus $\langle c_1, \sigma_2''\rangle \longrightarrow \sigma_1'$ and $\langle c_1, \sigma_2''\rangle \longrightarrow \sigma_2'$

By inductive hypothesis $P(c_1)$, we then have $\sigma_1' = \sigma_2'$

and thus we conclude $\sigma_1 = \sigma_1' = \sigma_2' = \sigma_2$

Inductive case

$\forall b, c.\ P(c) \Rightarrow P(\mathbf{while}\ b\ \mathbf{do}\ c)$ Take generic b, c

We assume (inductive hypothesis)

$$P(c) \triangleq \forall \sigma, \sigma_1, \sigma_2.\ \langle c, \sigma\rangle \longrightarrow \sigma_1 \wedge \langle c, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

We want to prove

$$P(\mathbf{while}\ b\ \mathbf{do}\ c) \triangleq \forall \sigma, \sigma_1, \sigma_2.\ \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma_1 \wedge \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

Take $\sigma, \sigma_1, \sigma_2$ such that $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma_1$ and $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2$

We want to prove $\sigma_1 = \sigma_2$

By determinacy of boolean expressions, there are two cases

$\langle b, \sigma\rangle \longrightarrow \mathbf{ff}$ $\langle b, \sigma\rangle \longrightarrow \mathbf{tt}$

Inductive case (ctd)

if $\langle b, \sigma \rangle \longrightarrow \mathbf{ff}$

Consider the goal $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma \rangle \longrightarrow \sigma_1$

Only the rule $\dfrac{\langle b, \sigma \rangle \longrightarrow \mathbf{ff}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma \rangle \longrightarrow \sigma}$ is applicable hence $\sigma_1 = \sigma$

Similarly, since $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma \rangle \longrightarrow \sigma_2$ it must be $\sigma_2 = \sigma$

and thus we conclude $\sigma_1 = \sigma = \sigma_2$

Inductive case (ctd)

if $\langle b, \sigma\rangle \longrightarrow \mathbf{tt}$

Consider the goal $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma_1$

Only the rule $\dfrac{\langle b,\sigma\rangle \longrightarrow \mathbf{tt} \quad \langle c,\sigma\rangle \longrightarrow \sigma'' \quad \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma'}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma'}$ is applicable

hence $\sigma_1 = \sigma_1'$ with $\langle c, \sigma\rangle \longrightarrow \sigma_1''$ and $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma_1''\rangle \longrightarrow \sigma_1'$

Similarly, since $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2$

it must be $\sigma_2 = \sigma_2'$ with $\langle c, \sigma\rangle \longrightarrow \sigma_2''$ and $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma_2''\rangle \longrightarrow \sigma_2'$

By inductive hypothesis $P(c)$, we have $\sigma_1'' = \sigma_2''$

thus $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma_2''\rangle \longrightarrow \sigma_1'$ and $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma_2''\rangle \longrightarrow \sigma_2'$

but there is no inductive hypothesis $P(\mathbf{while}\ b\ \mathbf{do}\ c)$!

Recursive definition!

one of the premises is as complex as the conclusion

$$\frac{\langle b, \sigma\rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma\rangle \longrightarrow \sigma'' \quad \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma'}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma'}$$

to close the proof of determinacy
we need a more convenient induction principle:

Rule induction

Induction on derivations

Derivations

Given a logical system *R*, a derivation in *R*, is written

$$d \Vdash_R y$$

where

- either $d = (\frac{}{y}) \in R$ is an axiom of R;
- or $d = \left(\frac{d_1,\ldots,d_n}{y}\right)$ for some derivations $d_1 \Vdash_R x_1, \ldots, d_n \Vdash_R x_n$ such that $(\frac{x_1,\ldots,x_n}{y}) \in R$ is an inference rule of R.

$$D_R \triangleq \{d \mid d \Vdash_R y\}$$

Immediate subderivation

Take $A = D_R$

$$\prec = \left\{ \left(d_i, \frac{d_1, ..., d_n}{y} \right) \;\middle|\; d_1 \Vdash_R x_1, ..., d_n \Vdash_R x_n, \left(\frac{x_1, ..., x_n}{y} \right) \in R \right\}$$

(immediate subderivation relation)

Example

$$R = \left\{ \frac{}{\mathsf{N} \longrightarrow n}, \frac{\mathsf{E}_0 \longrightarrow n_0 \quad \mathsf{E}_1 \longrightarrow n_1}{\mathsf{E}_0 \oplus \mathsf{E}_1 \longrightarrow n_0 + n_1}, \frac{\mathsf{E}_0 \longrightarrow n_0 \quad \mathsf{E}_1 \longrightarrow n_1}{\mathsf{E}_0 \otimes \mathsf{E}_1 \longrightarrow n_0 \cdot n_1} \right\}$$

$$\frac{}{2 \longrightarrow 2} \quad \prec \quad \frac{\dfrac{}{1 \longrightarrow 1} \quad \dfrac{}{2 \longrightarrow 2}}{(1 \oplus 2) \longrightarrow 3} \quad \prec \quad \frac{\dfrac{\dfrac{}{1 \longrightarrow 1} \quad \dfrac{}{2 \longrightarrow 2}}{(1 \oplus 2) \longrightarrow 3} \quad \dfrac{\dfrac{}{3 \longrightarrow 3} \quad \dfrac{}{4 \longrightarrow 4}}{(3 \oplus 4) \longrightarrow 7}}{(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow 21}$$

Lemma

$D_R, \prec$ is w.f.

Let $height : D_R \to \mathbb{N}$ defined as:

$$height\left(\frac{}{y}\right) \triangleq 1 \quad \text{if } (\frac{}{y}) \in R$$

$$height\left(\frac{d_1,\ldots,d_n}{y}\right) \triangleq 1 + \max_{i\in[1,n]} height(d_i) \quad \text{if } d_1 \Vdash_R x_1, ..., d_n \Vdash_R x_n, (\frac{x_1,\ldots,x_n}{y}) \in R$$

By definition, if $d \prec d'$ then $height(d) < height(d')$

Any descending chain in $\prec$ induces a descending chain in $<$

Since $<$ is w.f., so is $\prec$

Induction on derivation principle

$$\frac{\forall \frac{x_1,\ldots,x_n}{y} \in R.\ \forall d_1 \Vdash_R x_1, \ldots, d_1 \Vdash_R x_n.\ (P(d_1) \wedge \cdots \wedge P(d_n)) \Rightarrow P(\frac{d_1,\ldots,d_n}{y})}{\forall d.\ P(d)}$$

Corollary

$D_R, \prec^+$ is w.f.

Because $\prec^+$ is the transitive closure of a w.f. relation

Example

$$R = \left\{ \frac{}{\mathsf{N} \longrightarrow n}, \frac{\mathsf{E}_0 \longrightarrow n_0 \quad \mathsf{E}_1 \longrightarrow n_1}{\mathsf{E}_0 \oplus \mathsf{E}_1 \longrightarrow n_0 + n_1}, \frac{\mathsf{E}_0 \longrightarrow n_0 \quad \mathsf{E}_1 \longrightarrow n_1}{\mathsf{E}_0 \otimes \mathsf{E}_1 \longrightarrow n_0 \cdot n_1} \right\}$$

$$\frac{}{2 \longrightarrow 2} \quad \prec^+ \quad \frac{\dfrac{\dfrac{}{1 \longrightarrow 1} \quad \dfrac{}{2 \longrightarrow 2}}{(1 \oplus 2) \longrightarrow 3} \quad \dfrac{\dfrac{}{3 \longrightarrow 3} \quad \dfrac{}{4 \longrightarrow 4}}{(3 \oplus 4) \longrightarrow 7}}{(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow 21}$$

Rule induction

Rule induction principle

we assume derivations exist
and that we can build a larger one
but don't need to mention this fact

$$\frac{\forall \frac{x_1,\ldots,x_n}{y} \in R.\ (\{x_1, \ldots, x_n\} \subseteq I_R \wedge P(x_1) \wedge \cdots \wedge P(x_n)) \Rightarrow P(y)}{\forall x \in I_R.\ P(x)}$$

$$I_R \triangleq \{y \mid \Vdash_R y\}$$

Rule induction simplified

assuming that premises are theorems
may be not even necessary

$$\frac{\forall \frac{x_1,\ldots,x_n}{y} \in R.\ (P(x_1) \wedge \cdots \wedge P(x_n)) \Rightarrow P(y)}{\forall x \in I_R.\ P(x)}$$

Induction schemes

properties of numbers $P(n)$ mathematical induction

two proof obligations: $P(0)$ and $P(n) \Rightarrow P(n+1)$

properties of terms $P(t)$ structural induction

one proof obligation for each function symbol

properties of formulas $\mathrm{P(F)}$ rule induction

one proof obligation for each inference rule

Determinacy: two views

properties of terms $P(t)$ structural induction

$$P(c) \stackrel{\triangle}{=} \forall \sigma, \sigma_1, \sigma_2.\ \langle c, \sigma \rangle \longrightarrow \sigma_1 \wedge \langle c, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

properties of formulas $\mathrm{P}(\mathrm{F})$ rule induction

$$P(\langle c, \sigma \rangle \longrightarrow \sigma_1) \stackrel{\triangle}{=} \forall \sigma_2.\ \langle c, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

Determinacy of commands

$$c ::= \mathbf{skip} \mid x := a \mid c\,;c \mid \mathbf{if}\ b\ \mathbf{then}\ c\ \mathbf{else}\ c \mid \mathbf{while}\ b\ \mathbf{do}\ c$$

$$\frac{}{\langle \mathbf{skip}, \sigma\rangle \longrightarrow \sigma} \qquad \frac{\langle a, \sigma\rangle \longrightarrow n}{\langle x := a, \sigma\rangle \longrightarrow \sigma[n/x]} \qquad \frac{\langle c_0, \sigma\rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma''\rangle \longrightarrow \sigma'}{\langle c_0\,; c_1, \sigma\rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma\rangle \longrightarrow \mathbf{ff} \quad \langle c_1, \sigma\rangle \longrightarrow \sigma'}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \longrightarrow \sigma'} \qquad \frac{\langle b, \sigma\rangle \longrightarrow \mathbf{tt} \quad \langle c_0, \sigma\rangle \longrightarrow \sigma'}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma\rangle \longrightarrow \mathbf{ff}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma} \qquad \frac{\langle b, \sigma\rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma\rangle \longrightarrow \sigma'' \quad \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma'}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma'}$$

$$P(\langle c, \sigma\rangle \longrightarrow \sigma_1) \stackrel{\triangle}{=} \forall \sigma_2.\ \langle c, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2 \qquad \forall c, \sigma, \sigma_1.\ P(\langle c, \sigma\rangle \longrightarrow \sigma_1)\ ?$$

Base case

$$\frac{}{\langle \mathbf{skip}, \sigma \rangle \longrightarrow \sigma}$$

We want to prove

$$P(\langle \mathbf{skip}, \sigma \rangle \longrightarrow \sigma) \stackrel{\Delta}{=} \forall \sigma_2.\ \langle \mathbf{skip}, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma = \sigma_2$$

Take σ_2 s.t. $\langle \mathbf{skip}, \sigma \rangle \longrightarrow \sigma_2$

We want to prove $\sigma = \sigma_2$

Consider the goal $\langle \mathbf{skip}, \sigma \rangle \longrightarrow \sigma_2$

Only the rule $\dfrac{}{\langle \mathbf{skip}, \sigma \rangle \longrightarrow \sigma}$ is applicable, hence $\sigma_2 = \sigma$

Base case

$$\frac{\langle a,\sigma\rangle \longrightarrow n}{\langle x := a,\sigma\rangle \longrightarrow \sigma[n/x]}$$

We assume $\langle a,\sigma\rangle \longrightarrow n$

We want to prove

$$P(\langle x := a,\sigma\rangle \longrightarrow \sigma[n/x]) \stackrel{\triangle}{=} \forall \sigma_2.\ \langle x := a,\sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma[n/x] = \sigma_2$$

Take σ_2 s.t. $\langle x := a,\sigma\rangle \longrightarrow \sigma_2$

We want to prove $\sigma[n/x] = \sigma_2$

Consider the goal $\langle x := a,\sigma\rangle \longrightarrow \sigma_2$

Only the rule $\frac{\langle a,\sigma\rangle \longrightarrow n}{\langle x := a,\sigma\rangle \longrightarrow \sigma[n/x]}$ is applicable, hence $\sigma_2 = \sigma[m/x]$ with $\langle a,\sigma\rangle \longrightarrow m$

since we assumed $\langle a,\sigma\rangle \longrightarrow n$

by determinacy of Aexp we have $n = m$ and thus $\sigma_2 = \sigma[m/x] = \sigma[n/x]$

Inductive case

$$\frac{\langle c_0, \sigma\rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma''\rangle \longrightarrow \sigma'}{\langle c_0\,; c_1, \sigma\rangle \longrightarrow \sigma'}$$

We assume (inductive hypotheses)

$$P(\langle c_0, \sigma\rangle \longrightarrow \sigma'') \stackrel{\triangle}{=} \forall \sigma_2''.\ \langle c_0, \sigma\rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma''\rangle \longrightarrow \sigma') \stackrel{\triangle}{=} \forall \sigma_2'.\ \langle c_1, \sigma''\rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

We want to prove

$$P(\langle c_0\,; c_1, \sigma\rangle \longrightarrow \sigma') \stackrel{\triangle}{=} \forall \sigma_2.\ \langle c_0\,; c_1, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$$

Take σ_2 such that $\langle c_0\,; c_1, \sigma\rangle \longrightarrow \sigma_2$

We want to prove $\sigma' = \sigma_2$

Inductive case (ctd)

$$P(\langle c_0, \sigma\rangle \longrightarrow \sigma'') \stackrel{\Delta}{=} \forall \sigma_2''.\ \langle c_0, \sigma\rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$
$$P(\langle c_1, \sigma''\rangle \longrightarrow \sigma') \stackrel{\Delta}{=} \forall \sigma_2'.\ \langle c_1, \sigma''\rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

Consider the goal $\langle c_0\,;c_1, \sigma\rangle \longrightarrow \sigma_2$

Only the rule $\dfrac{\langle c_0, \sigma\rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma''\rangle \longrightarrow \sigma'}{\langle c_0\,;c_1, \sigma\rangle \longrightarrow \sigma'}$ is applicable

hence $\sigma_2 = \sigma_2'$ with $\langle c_0, \sigma\rangle \longrightarrow \sigma_2''$ and $\langle c_1, \sigma_2''\rangle \longrightarrow \sigma_2'$

By inductive hypothesis $P(\langle c_0, \sigma\rangle \longrightarrow \sigma'')$, we have $\sigma'' = \sigma_2''$

and thus $\langle c_1, \sigma''\rangle \longrightarrow \sigma_2'$

By inductive hypothesis $P(\langle c_1, \sigma'\rangle \longrightarrow \sigma')$, we then have $\sigma' = \sigma_2'$

Inductive case

$$\frac{\langle b, \sigma\rangle \longrightarrow \mathbf{ff} \quad \langle c_1, \sigma\rangle \longrightarrow \sigma'}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \longrightarrow \sigma'}$$

We assume

$\langle b, \sigma\rangle \longrightarrow \mathbf{ff}$

(inductive hypothesis)

$P(\langle c_1, \sigma\rangle \longrightarrow \sigma') \stackrel{\triangle}{=} \forall \sigma_2.\ \langle c_1, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$

We want to prove

$P(\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \longrightarrow \sigma') \stackrel{\triangle}{=} \forall \sigma_2.\ \langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$

Take σ_2 such that $\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \longrightarrow \sigma_2$

We want to prove $\sigma' = \sigma_2$

Inductive case (ctd)

$\langle b, \sigma\rangle \longrightarrow \mathbf{ff}$

$P(\langle c_1, \sigma\rangle \longrightarrow \sigma') \stackrel{\triangle}{=} \forall \sigma_2.\ \langle c_1, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$

Consider the goal $\langle \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, \sigma\rangle \longrightarrow \sigma_2$

By determinacy of Bexp

only the rule $\dfrac{\langle b, \sigma\rangle \longrightarrow \mathbf{ff} \quad \langle c_1, \sigma\rangle \longrightarrow \sigma'}{\langle \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, \sigma\rangle \longrightarrow \sigma'}$ is applicable

hence $\sigma_2 = \sigma_2'$ with $\langle c_1, \sigma\rangle \longrightarrow \sigma_2'$

By inductive hypothesis $P(\langle c_1, \sigma\rangle \longrightarrow \sigma')$, we then have $\sigma' = \sigma_2' = \sigma_2$

Inductive case

$$\frac{\langle b, \sigma\rangle \longrightarrow \mathbf{tt} \quad \langle c_0, \sigma\rangle \longrightarrow \sigma'}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \longrightarrow \sigma'}$$

Analogous to the previous case and thus omitted

Base case

$$\frac{\langle b, \sigma\rangle \longrightarrow \mathbf{ff}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma}$$

We assume

$\langle b, \sigma\rangle \longrightarrow \mathbf{ff}$

We want to prove

$P(\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma) \stackrel{\triangle}{=} \forall \sigma_2.\ \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma = \sigma_2$

Take σ_2 such that $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2$

We want to prove $\sigma = \sigma_2$

Inductive case (ctd)

$\langle b, \sigma \rangle \longrightarrow \mathbf{ff}$

Consider the goal $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma \rangle \longrightarrow \sigma_2$

By determinacy of Bexp

Only the rule $\dfrac{\langle b, \sigma \rangle \longrightarrow \mathbf{ff}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma \rangle \longrightarrow \sigma}$ is applicable hence $\sigma_2 = \sigma$

Inductive case

$$\frac{\langle b, \sigma\rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma\rangle \longrightarrow \sigma'' \quad \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma'}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma'}$$

We assume

$\langle b, \sigma\rangle \longrightarrow \mathbf{tt}$

(inductive hypotheses)

$P(\langle c, \sigma\rangle \longrightarrow \sigma'') \stackrel{\triangle}{=} \forall \sigma_2''.\ \langle c, \sigma\rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$

$P(\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma') \stackrel{\triangle}{=} \forall \sigma_2'.\ \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$

We want to prove

$P(\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma') \stackrel{\triangle}{=} \forall \sigma_2.\ \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$

Take σ_2 such that $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2$

We want to prove $\sigma' = \sigma_2$

Inductive case (ctd)

$\langle b, \sigma\rangle \longrightarrow \mathbf{tt}$

$P(\langle c, \sigma\rangle \longrightarrow \sigma'') \stackrel{\triangle}{=} \forall \sigma_2''.\ \langle c, \sigma\rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$

$P(\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma') \stackrel{\triangle}{=} \forall \sigma_2'.\ \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$

Consider the goal $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2$

By determinacy of Bexp

only the rule $\dfrac{\langle b, \sigma\rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma\rangle \longrightarrow \sigma'' \quad \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma'}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma'}$ is applicable

hence $\sigma_2 = \sigma_2'$ with $\langle c, \sigma\rangle \longrightarrow \sigma_2''$ and $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma_2''\rangle \longrightarrow \sigma_2'$

By inductive hypothesis $P(\langle c, \sigma\rangle \longrightarrow \sigma'')$, we have $\sigma'' = \sigma_2''$

thus $\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma_2'$

By inductive hypothesis $P(\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma')$

we conclude $\sigma' = \sigma_2' = \sigma_2$

Determinacy of commands

$$\forall c, \sigma, \sigma_1.\ P(\langle c, \sigma\rangle \longrightarrow \sigma_1)$$

$$P(\langle c, \sigma\rangle \longrightarrow \sigma_1) \stackrel{\Delta}{=} \forall \sigma_2.\ \langle c, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

Thank you for your attention!

Questions?