

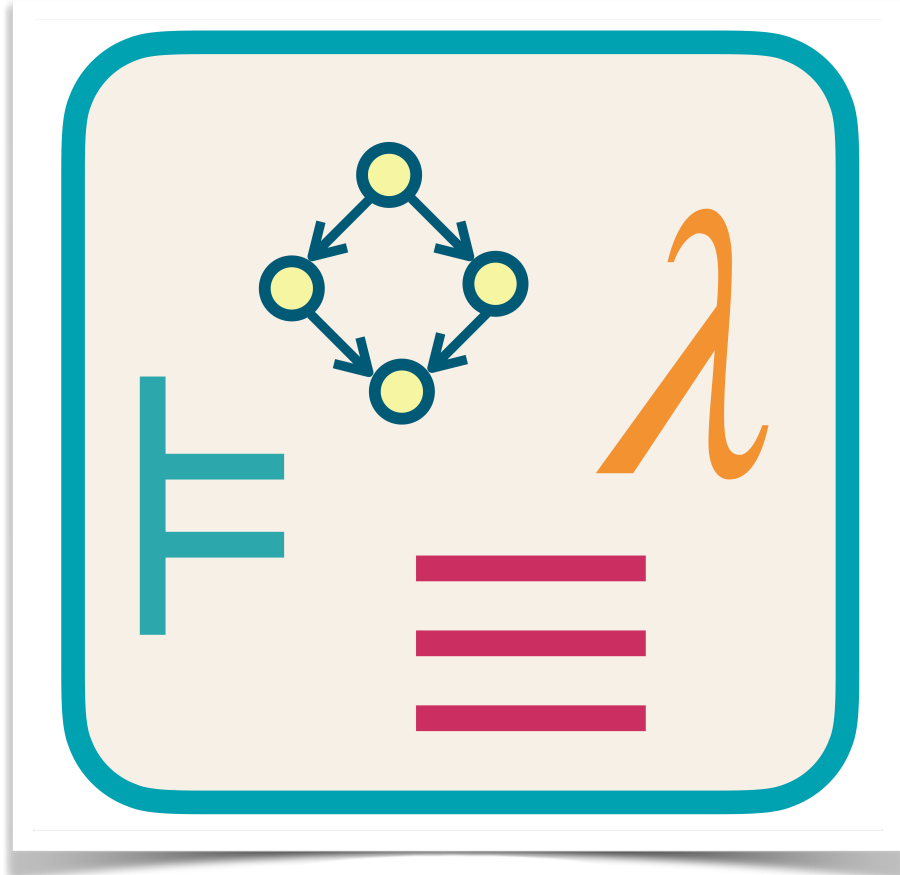
LPP 2026/27 (063AA, 9CFU)

Programming Languages

Fabio Gadducci

and Laboratory

Vincenzo Ciancia



05c - Rule Induction

Induction on derivations

Derivations

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

$$d \Vdash_R y$$

where

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

Derivations

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

$$d \Vdash_R y$$

where

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

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

Immediate subderivation

Take $A = D_R$

$$\prec = \left\{ \left(d_i, \frac{d_1, \dots, d_n}{y} \right) \mid d_1 \Vdash_R x_1, \dots, d_n \Vdash_R x_n, \left(\frac{x_1, \dots, x_n}{y} \right) \in R \right\}$$

(immediate subderivation relation)

Immediate subderivation

Take $A = D_R$

$$\prec = \left\{ \left(d_i, \frac{d_1, \dots, d_n}{y} \right) \mid d_1 \Vdash_R x_1, \dots, d_n \Vdash_R x_n, \left(\frac{x_1, \dots, x_n}{y} \right) \in R \right\}$$

(immediate subderivation relation)

Example

Immediate subderivation

Take $A = D_R$

$$\prec = \left\{ \left(d_i, \frac{d_1, \dots, d_n}{y} \right) \mid d_1 \Vdash_R x_1, \dots, d_n \Vdash_R x_n, \left(\frac{x_1, \dots, x_n}{y} \right) \in R \right\}$$

(immediate subderivation relation)

Example

$$R = \left\{ \frac{}{N \longrightarrow n}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \oplus E_1 \longrightarrow n_0 + n_1}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \otimes E_1 \longrightarrow n_0 \cdot n_1} \right\}$$

Immediate subderivation

Take $A = D_R$

$$\prec = \left\{ \left(d_i, \frac{d_1, \dots, d_n}{y} \right) \mid d_1 \Vdash_R x_1, \dots, d_n \Vdash_R x_n, \left(\frac{x_1, \dots, x_n}{y} \right) \in R \right\}$$

(immediate subderivation relation)

Example

$$R = \left\{ \frac{}{N \longrightarrow n}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \oplus E_1 \longrightarrow n_0 + n_1}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \otimes E_1 \longrightarrow n_0 \cdot n_1} \right\}$$

$$\overline{2 \longrightarrow 2}$$

Immediate subderivation

Take $A = D_R$

$$\prec = \left\{ \left(d_i, \frac{d_1, \dots, d_n}{y} \right) \mid d_1 \Vdash_R x_1, \dots, d_n \Vdash_R x_n, \left(\frac{x_1, \dots, x_n}{y} \right) \in R \right\}$$

(immediate subderivation relation)

Example

$$R = \left\{ \frac{}{N \longrightarrow n}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \oplus E_1 \longrightarrow n_0 + n_1}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \otimes E_1 \longrightarrow n_0 \cdot n_1} \right\}$$

$$\frac{}{2 \longrightarrow 2} \prec \frac{\frac{}{1 \longrightarrow 1} \quad \frac{}{2 \longrightarrow 2}}{(1 \oplus 2) \longrightarrow 3}$$

Immediate subderivation

Take $A = D_R$

$$\prec = \left\{ \left(d_i, \frac{d_1, \dots, d_n}{y} \right) \mid d_1 \Vdash_R x_1, \dots, d_n \Vdash_R x_n, \left(\frac{x_1, \dots, x_n}{y} \right) \in R \right\}$$

(immediate subderivation relation)

Example

$$R = \left\{ \overline{N \longrightarrow n}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \oplus E_1 \longrightarrow n_0 + n_1}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \otimes E_1 \longrightarrow n_0 \cdot n_1} \right\}$$

$$\overline{2 \longrightarrow 2} \prec \frac{\overline{1 \longrightarrow 1} \quad \overline{2 \longrightarrow 2}}{(1 \oplus 2) \longrightarrow 3} \prec$$

Immediate subderivation

Take $A = D_R$

$$\prec = \left\{ \left(d_i, \frac{d_1, \dots, d_n}{y} \right) \mid d_1 \Vdash_R x_1, \dots, d_n \Vdash_R x_n, \left(\frac{x_1, \dots, x_n}{y} \right) \in R \right\}$$

(immediate subderivation relation)

Example

$$R = \left\{ \frac{}{N \longrightarrow n}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \oplus E_1 \longrightarrow n_0 + n_1}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \otimes E_1 \longrightarrow n_0 \cdot n_1} \right\}$$

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

Lemma

$D_R, \prec$ is w.f.

Lemma

$D_R, \prec$ is w.f.

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

Lemma

$D_R, \prec$ is w.f.

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

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

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

Lemma

$D_R, \prec$ is w.f.

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

$$\begin{aligned} height\left(\frac{}{y}\right) &\triangleq 1 && \text{if } (\frac{}{y}) \in R \\ height\left(\frac{d_1, \dots, d_n}{y}\right) &\triangleq 1 + \max_{i \in [1, n]} height(d_i) && \text{if } d_1 \Vdash_R x_1, \dots, d_n \Vdash_R x_n, (\frac{x_1, \dots, x_n}{y}) \in R \end{aligned}$$

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

Lemma

$D_R, \prec$ is w.f.

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

$$\begin{aligned} height\left(\frac{}{y}\right) &\triangleq 1 && \text{if } (\frac{}{y}) \in R \\ height\left(\frac{d_1, \dots, d_n}{y}\right) &\triangleq 1 + \max_{i \in [1, n]} height(d_i) && \text{if } d_1 \Vdash_R x_1, \dots, d_n \Vdash_R x_n, (\frac{x_1, \dots, x_n}{y}) \in R \end{aligned}$$

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

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

Lemma

$D_R, \prec$ is w.f.

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

$$\begin{aligned} height\left(\frac{}{y}\right) &\triangleq 1 && \text{if } (\frac{}{y}) \in R \\ height\left(\frac{d_1, \dots, d_n}{y}\right) &\triangleq 1 + \max_{i \in [1, n]} height(d_i) && \text{if } d_1 \Vdash_R x_1, \dots, d_n \Vdash_R x_n, (\frac{x_1, \dots, x_n}{y}) \in R \end{aligned}$$

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

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

Corollary

$$D_R, \prec^+ \text{ is w.f.}$$

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

Corollary

$$D_R, \prec^+ \text{ is w.f.}$$

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

Example

$$R = \left\{ \frac{}{N \longrightarrow n}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \oplus E_1 \longrightarrow n_0 + n_1}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \otimes E_1 \longrightarrow n_0 \cdot n_1} \right\}$$

Corollary

$$D_R, \prec^+ \text{ is w.f.}$$

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

Example

$$R = \left\{ \frac{}{N \longrightarrow n}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \oplus E_1 \longrightarrow n_0 + n_1}, \frac{E_0 \longrightarrow n_0 \quad E_1 \longrightarrow n_1}{E_0 \otimes E_1 \longrightarrow n_0 \cdot n_1} \right\}$$

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

Rule induction

Typical properties

It is very often the case that the property of a derivation is only concerned with the conclusion of the derivation

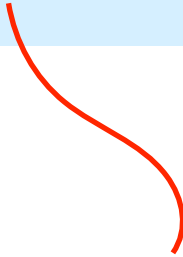
$$d \Vdash_R y \quad \Rightarrow \quad P(d) \Leftrightarrow Q(y)$$

$$P\left(\frac{d_1, \dots, d_n}{y}\right) \triangleq Q(y)$$

in such cases we can avoid to mention derivations at all

Rule induction principle

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


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

Rule induction principle

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

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

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

Rule induction simplified

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

Rule induction simplified

assuming that premises are theorems
may be not even necessary

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

Induction schemes

properties of numbers $P(n)$ mathematical induction

Induction schemes

properties of numbers $P(n)$ mathematical induction

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

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

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

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 $P(F)$ rule induction

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 $P(F)$ rule induction

one proof obligation for each inference rule

Determinacy: two views

properties of terms

$P(t)$

structural induction

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

Determinacy: two views

properties of terms

$P(t)$

structural induction

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

properties of formulas

$P(F)$

rule induction

Determinacy: two views

properties of terms

$P(t)$

structural induction

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

properties of formulas

$P(F)$

rule induction

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

Determinacy of commands

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

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

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

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

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

Base case

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

Base case

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

We want to prove

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

Base case

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

We want to prove

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

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

Base case

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

We want to prove

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

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

We want to prove $\sigma = \sigma_2$

Base case

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

We want to prove

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

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

We want to prove $\sigma = \sigma_2$

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

Base case

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

We want to prove

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

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 $\frac{}{\langle \mathbf{skip}, \sigma \rangle \longrightarrow \sigma}$ is applicable, hence $\sigma_2 = \sigma$

Base case

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

Base case

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $\langle a, \sigma \rangle \longrightarrow m$

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

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

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

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

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

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

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

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)

$$P(\langle c_0, \sigma \rangle \longrightarrow \sigma'') \triangleq \forall \sigma_2''. \langle c_0, \sigma \rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma'' \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2'. \langle c_1, \sigma'' \rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

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)

$$P(\langle c_0, \sigma \rangle \longrightarrow \sigma'') \triangleq \forall \sigma_2''. \langle c_0, \sigma \rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma'' \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2'. \langle c_1, \sigma'' \rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

We want to prove

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

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)

$$P(\langle c_0, \sigma \rangle \longrightarrow \sigma'') \triangleq \forall \sigma_2''. \langle c_0, \sigma \rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma'' \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2'. \langle c_1, \sigma'' \rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

We want to prove

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

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

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)

$$P(\langle c_0, \sigma \rangle \longrightarrow \sigma'') \triangleq \forall \sigma_2''. \langle c_0, \sigma \rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma'' \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2'. \langle c_1, \sigma'' \rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

We want to prove

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

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

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

Inductive case (cont.)

$$P(\langle c_0, \sigma \rangle \longrightarrow \sigma'') \triangleq \forall \sigma_2''. \langle c_0, \sigma \rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma'' \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2'. \langle c_1, \sigma'' \rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

Consider the goal

Inductive case (cont.)

$$P(\langle c_0, \sigma \rangle \longrightarrow \sigma'') \triangleq \forall \sigma_2''. \langle c_0, \sigma \rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma'' \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2'. \langle c_1, \sigma'' \rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

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

Inductive case (cont.)

$$P(\langle c_0, \sigma \rangle \longrightarrow \sigma'') \triangleq \forall \sigma_2''. \langle c_0, \sigma \rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma'' \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2'. \langle c_1, \sigma'' \rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

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

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

Inductive case (cont.)

$$P(\langle c_0, \sigma \rangle \longrightarrow \sigma'') \triangleq \forall \sigma_2''. \langle c_0, \sigma \rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma'' \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2'. \langle c_1, \sigma'' \rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

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

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

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

Inductive case (cont.)

$$P(\langle c_0, \sigma \rangle \longrightarrow \sigma'') \triangleq \forall \sigma_2''. \langle c_0, \sigma \rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma'' \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2'. \langle c_1, \sigma'' \rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

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

Only the rule $\frac{\langle c_0, \sigma \rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma'' \rangle \longrightarrow \sigma'}{\langle c_0 ; c_1, \sigma \rangle \longrightarrow \sigma'}$ 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 $\sigma'' = \sigma_2''$

Inductive case (cont.)

$$P(\langle c_0, \sigma \rangle \longrightarrow \sigma'') \triangleq \forall \sigma_2''. \langle c_0, \sigma \rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma'' \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2'. \langle c_1, \sigma'' \rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

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

Only the rule $\frac{\langle c_0, \sigma \rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma'' \rangle \longrightarrow \sigma'}{\langle c_0 ; c_1, \sigma \rangle \longrightarrow \sigma'}$ 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 $\langle c_1, \sigma'' \rangle \longrightarrow \sigma_2'$

Inductive case (cont.)

$$P(\langle c_0, \sigma \rangle \longrightarrow \sigma'') \triangleq \forall \sigma_2''. \langle c_0, \sigma \rangle \longrightarrow \sigma_2'' \Rightarrow \sigma'' = \sigma_2''$$

$$P(\langle c_1, \sigma'' \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2'. \langle c_1, \sigma'' \rangle \longrightarrow \sigma_2' \Rightarrow \sigma' = \sigma_2'$$

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

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

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

Inductive case

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

We assume

Inductive case

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

We assume

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

Inductive case

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

We assume

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

(inductive hypothesis)

$$P(\langle c_1, \sigma \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2. \langle c_1, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$$

Inductive case

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

We assume

$$\langle b, \sigma \rangle \longrightarrow \text{ff} \quad (\text{inductive hypothesis})$$

$$P(\langle c_1, \sigma \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2. \langle c_1, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$$

We want to prove

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

Inductive case

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

We assume

$$\langle b, \sigma \rangle \longrightarrow \text{ff} \quad (\text{inductive hypothesis})$$

$$P(\langle c_1, \sigma \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2. \langle c_1, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$$

We want to prove

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

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

Inductive case

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

We assume

$$\langle b, \sigma \rangle \longrightarrow \text{ff} \quad (\text{inductive hypothesis})$$

$$P(\langle c_1, \sigma \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2. \langle c_1, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$$

We want to prove

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

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

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

Inductive case (cont.)

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

$$P(\langle c_1, \sigma \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2. \langle c_1, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$$

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

Inductive case (cont.)

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

$$P(\langle c_1, \sigma \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2. \langle c_1, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$$

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

By determinacy of Bexp

Inductive case (cont.)

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

$$P(\langle c_1, \sigma \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2. \langle c_1, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$$

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

By determinacy of Bexp

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

Inductive case (cont.)

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

$$P(\langle c_1, \sigma \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2. \langle c_1, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$$

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

By determinacy of Bexp

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

hence $\sigma_2 = \sigma'_2$ with $\langle c_1, \sigma \rangle \longrightarrow \sigma'_2$

Inductive case (cont.)

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

$$P(\langle c_1, \sigma \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2. \langle c_1, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$$

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

By determinacy of Bexp

only the rule $\frac{\langle b, \sigma \rangle \longrightarrow \text{ff} \quad \langle c_1, \sigma \rangle \longrightarrow \sigma'}{\langle \text{if } b \text{ then } c_0 \text{ else } c_1, \sigma \rangle \longrightarrow \sigma'}$ 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

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

Analogous to the previous case and thus omitted

Base case

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

Base case

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

We assume

Base case

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

We assume

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

Base case

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

We assume

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

We want to prove

Base case

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

We assume

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

We want to prove

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

Base case

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

We assume

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

We want to prove

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

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

Base case

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

We assume

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

We want to prove

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

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

We want to prove $\sigma = \sigma_2$

Inductive case (cont.)

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

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

Inductive case (cont.)

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

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

By determinacy of Bexp

Inductive case (cont.)

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

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

By determinacy of Bexp

Only the rule $\frac{\langle b, \sigma \rangle \longrightarrow \text{ff}}{\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma}$ is applicable

Inductive case (cont.)

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

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

By determinacy of Bexp

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

Inductive case

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

Inductive case

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

We assume

Inductive case

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

We assume

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

Inductive case

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

We assume

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

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

Inductive case

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

We assume

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

(inductive hypotheses)

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

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

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)

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

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

We want to prove

Inductive case

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

We assume

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

(inductive hypotheses)

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

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

We want to prove

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

Inductive case

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

We assume

$$\langle b, \sigma \rangle \longrightarrow \texttt{tt} \quad (\text{inductive hypotheses})$$

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

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

We want to prove

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

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

Inductive case

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

We assume

$$\langle b, \sigma \rangle \longrightarrow \texttt{tt} \quad (\text{inductive hypotheses})$$

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

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

We want to prove

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

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

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

Inductive case (cont.)

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

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

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

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

Inductive case (cont.)

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

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

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

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

By determinacy of Bexp

Inductive case (cont.)

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

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

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

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

By determinacy of Bexp

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

Inductive case (cont.)

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

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

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

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

By determinacy of Bexp

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

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

Inductive case (cont.)

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

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

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

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

By determinacy of Bexp

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

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

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

Inductive case (cont.)

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

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

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

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

By determinacy of Bexp

only the rule
$$\frac{\langle b, \sigma \rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma \rangle \longrightarrow \sigma'' \quad \langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma'' \rangle \longrightarrow \sigma'}{\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma'}$$
 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 $\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma'' \rangle \longrightarrow \sigma_2'$

Inductive case (cont.)

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

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

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

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

By determinacy of Bexp

only the rule
$$\frac{\langle b, \sigma \rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma \rangle \longrightarrow \sigma'' \quad \langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma'' \rangle \longrightarrow \sigma'}{\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma'}$$
 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 $P(\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma'' \rangle \longrightarrow \sigma')$

Inductive case (cont.)

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

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

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

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

By determinacy of Bexp

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

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

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

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

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

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

Determinacy of commands

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

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

Structural induction, rule induction and divergence

Exercise: $a_0 \sqcap a_1$

Extend the syntax of arithmetic expressions with the operator $a_0 \sqcap a_1$ whose big-step operational semantics is defined by the rule

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$

1. Prove termination or exhibit a counterexample.
2. Prove determinacy or exhibit a counterexample.

Exercise: $a_0 \sqcap a_1$

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$

Exercise: $a_0 \sqcap a_1$

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$

$$\langle 1 \sqcap 2, \sigma \rangle \not\rightarrow$$

Exercise: $a_0 \sqcap a_1$

by structural induction

$$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcap a_1)$$

Exercise: $a_0 \sqcap a_1$

by structural induction

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcap a_1)$ Take generic a_0, a_1

Exercise: $a_0 \sqcap a_1$

by structural induction

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcap a_1)$ Take generic a_0, a_1

We assume

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

Exercise: $a_0 \sqcap a_1$

by structural induction

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcap a_1)$ Take generic a_0, a_1

We assume (inductive hypotheses)

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

Exercise: $a_0 \sqcap a_1$

by structural induction

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcap a_1)$ 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

Exercise: $a_0 \sqcap a_1$

by structural induction

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcap a_1)$ 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

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

Exercise: $a_0 \sqcap a_1$

by structural induction

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcap a_1)$ 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

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

Take generic σ, m, m' such that $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m$ and $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m'$

Exercise: $a_0 \sqcap a_1$

by structural induction

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcap a_1)$ 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

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

Take generic σ, m, m' such that $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m$ and $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m'$

We want to prove $m = m'$

Exercise: $a_0 \sqcap a_1$

Exercise: $a_0 \sqcap a_1$

Consider the goal $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m$

Exercise: $a_0 \sqcap a_1$

Consider the goal $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m$

Only the rule
$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$
 is applicable

Exercise: $a_0 \sqcap a_1$

Consider the goal $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m$

Only the rule
$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$
 is applicable

hence $\langle a_0, \sigma \rangle \longrightarrow m$ and $\langle a_1, \sigma \rangle \longrightarrow m$

Exercise: $a_0 \sqcap a_1$

Consider the goal $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m$

Only the rule
$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$
 is applicable

hence $\langle a_0, \sigma \rangle \longrightarrow m$ and $\langle a_1, \sigma \rangle \longrightarrow m$

Similarly, since $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m'$

Exercise: $a_0 \sqcap a_1$

Consider the goal $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m$

Only the rule
$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$
 is applicable

hence $\langle a_0, \sigma \rangle \longrightarrow m$ and $\langle a_1, \sigma \rangle \longrightarrow m$

Similarly, since $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m'$

it must be $\langle a_0, \sigma \rangle \longrightarrow m'$ and $\langle a_1, \sigma \rangle \longrightarrow m'$

Exercise: $a_0 \sqcap a_1$

Consider the goal $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m$

Only the rule
$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$
 is applicable

hence $\langle a_0, \sigma \rangle \longrightarrow m$ and $\langle a_1, \sigma \rangle \longrightarrow m$

Similarly, since $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow m'$

it must be $\langle a_0, \sigma \rangle \longrightarrow m'$ and $\langle a_1, \sigma \rangle \longrightarrow m'$

By inductive hypotheses, we conclude $m = m'$

Exercise: $a_0 \sqcap a_1$

by rule induction

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$

Exercise: $a_0 \sqcap a_1$

by rule induction

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$

We assume

(inductive hypotheses)

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

Exercise: $a_0 \sqcap a_1$

by rule induction

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$

We assume (inductive hypotheses)

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

We want to prove

$$P(\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n) \triangleq \forall n'. \langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n' \Rightarrow n = n'$$

Exercise: $a_0 \sqcap a_1$

by rule induction

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$

We assume (inductive hypotheses)

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

We want to prove

$$P(\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n) \triangleq \forall n'. \langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n' \Rightarrow n = n'$$

Take n' such that $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n'$

Exercise: $a_0 \sqcap a_1$

by rule induction

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$

We assume (inductive hypotheses)

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

We want to prove

$$P(\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n) \triangleq \forall n'. \langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n' \Rightarrow n = n'$$

Take n' such that $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n'$

We want to prove $n = n'$

Exercise: $a_0 \sqcap a_1$

$$P(\langle a_0, \sigma \rangle \longrightarrow n) \triangleq \forall n'. \langle a_0, \sigma \rangle \longrightarrow n' \Rightarrow n = n'$$

$$P(\langle a_1, \sigma \rangle \longrightarrow n) \triangleq \forall n'. \langle a_1, \sigma \rangle \longrightarrow n' \Rightarrow n = n'$$

Consider the goal $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n'$

Exercise: $a_0 \sqcap a_1$

$$P(\langle a_0, \sigma \rangle \longrightarrow n) \triangleq \forall n'. \langle a_0, \sigma \rangle \longrightarrow n' \Rightarrow n = n'$$

$$P(\langle a_1, \sigma \rangle \longrightarrow n) \triangleq \forall n'. \langle a_1, \sigma \rangle \longrightarrow n' \Rightarrow n = n'$$

Consider the goal $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n'$

Only the rule
$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$
 is applicable

Exercise: $a_0 \sqcap a_1$

$$P(\langle a_0, \sigma \rangle \longrightarrow n) \triangleq \forall n'. \langle a_0, \sigma \rangle \longrightarrow n' \Rightarrow n = n'$$

$$P(\langle a_1, \sigma \rangle \longrightarrow n) \triangleq \forall n'. \langle a_1, \sigma \rangle \longrightarrow n' \Rightarrow n = n'$$

Consider the goal $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n'$

Only the rule
$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$
 is applicable

hence $\langle a_0, \sigma \rangle \longrightarrow n'$ and $\langle a_1, \sigma \rangle \longrightarrow n'$

Exercise: $a_0 \sqcap a_1$

$$P(\langle a_0, \sigma \rangle \longrightarrow n) \triangleq \forall n'. \langle a_0, \sigma \rangle \longrightarrow n' \Rightarrow n = n'$$

$$P(\langle a_1, \sigma \rangle \longrightarrow n) \triangleq \forall n'. \langle a_1, \sigma \rangle \longrightarrow n' \Rightarrow n = n'$$

Consider the goal $\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n'$

Only the rule
$$\frac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$$
 is applicable

hence $\langle a_0, \sigma \rangle \longrightarrow n'$ and $\langle a_1, \sigma \rangle \longrightarrow n'$

By inductive hypotheses, we conclude $n = n'$

Exercise: $a_0 \sqcup a_1$

Extend the syntax of arithmetic expressions with the operator $a_0 \sqcup a_1$ whose big-step operational semantics is defined by the rule

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n_0}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_0} \quad \frac{\langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_1}$$

1. Prove termination or exhibit a counterexample.
2. Prove determinacy or exhibit a counterexample.

Exercise: $a_0 \sqcup a_1$

by structural induction

$$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcup a_1)$$

Exercise: $a_0 \sqcup a_1$

by structural induction

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcup a_1)$ Take generic a_0, a_1

Exercise: $a_0 \sqcup a_1$

by structural induction

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcup a_1)$ Take generic a_0, a_1

We assume $P(a_0) \triangleq \forall \sigma. \exists m_0. \langle a_0, \sigma \rangle \longrightarrow m_0$

$P(a_1) \triangleq \forall \sigma. \exists m_1. \langle a_1, \sigma \rangle \longrightarrow m_1$

Exercise: $a_0 \sqcup a_1$

by structural induction

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \sqcup a_1)$ Take generic a_0, a_1

We assume $P(a_0) \triangleq \forall \sigma. \exists m_0. \langle a_0, \sigma \rangle \longrightarrow m_0$

$P(a_1) \triangleq \forall \sigma. \exists m_1. \langle a_1, \sigma \rangle \longrightarrow m_1$

We want to prove $P(a_0 \sqcup a_1) \triangleq \forall \sigma. \exists m. \langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow m$

Exercise: $a_0 \sqcup a_1$

Take a generic σ and consider the goal $\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow m$

Exercise: $a_0 \sqcup a_1$

Take a generic σ and consider the goal $\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow m$

Either rules $\frac{\langle a_0, \sigma \rangle \longrightarrow n_0}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_0} \quad \frac{\langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_1}$ are applicable

Exercise: $a_0 \sqcup a_1$

Take a generic σ and consider the goal $\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow m$

Either rules $\frac{\langle a_0, \sigma \rangle \longrightarrow n_0}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_0} \quad \frac{\langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_1}$ are applicable

take the first

Exercise: $a_0 \sqcup a_1$

Take a generic σ and consider the goal $\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow m$

Either rules $\frac{\langle a_0, \sigma \rangle \longrightarrow n_0}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_0} \quad \frac{\langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_1}$ are applicable

take the first

$\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow m \nwarrow \langle a_0, \sigma \rangle \longrightarrow m$

Exercise: $a_0 \sqcup a_1$

Take a generic σ and consider the goal $\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow m$

Either rules $\frac{\langle a_0, \sigma \rangle \longrightarrow n_0}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_0} \quad \frac{\langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_1}$ are applicable

take the first

$$\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow m \nwarrow \langle a_0, \sigma \rangle \longrightarrow m$$

By inductive hypothesis $P(a_0)$, there is m_0 s.t. $\langle a_0, \sigma \rangle \longrightarrow m_0$

Exercise: $a_0 \sqcup a_1$

Take a generic σ and consider the goal $\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow m$

Either rules $\frac{\langle a_0, \sigma \rangle \longrightarrow n_0}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_0} \quad \frac{\langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_1}$ are applicable

take the first

$$\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow m \nwarrow \langle a_0, \sigma \rangle \longrightarrow m$$

By inductive hypothesis $P(a_0)$, there is m_0 s.t. $\langle a_0, \sigma \rangle \longrightarrow m_0$

And we are done (taking $m = m_0$)

Exercise: $a_0 \sqcup a_1$

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n_0}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_0} \quad \frac{\langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_1}$$

Exercise: $a_0 \sqcup a_1$

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n_0}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_0} \quad \frac{\langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_1}$$

$$\langle 1 \sqcup 2, \sigma \rangle \longrightarrow 1$$

Exercise: $a_0 \sqcup a_1$

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n_0}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_0} \quad \frac{\langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_1}$$

$$\langle 1 \sqcup 2, \sigma \rangle \longrightarrow 1 \quad \langle 1 \sqcup 2, \sigma \rangle \longrightarrow 2$$

Exercise: $a_0 \sqcup a_1$

$$\frac{\langle a_0, \sigma \rangle \longrightarrow n_0}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_0} \quad \frac{\langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_1}$$

$$\langle 1 \sqcup 2, \sigma \rangle \longrightarrow 1 \quad \langle 1 \sqcup 2, \sigma \rangle \longrightarrow 2$$

$$1 \neq 2$$

Exercise: Loop exit

Consider the command

$$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$$

Prove by rule induction that:

$$\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \text{false}$$

Exercise: Loop exit

$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$

$\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$

by structural induction?

by rule induction?

Exercise: Loop exit

$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$

$\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$

by rule induction?

Exercise: Loop exit

$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$ $\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$
by rule induction?

$$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

Exercise: Loop exit

$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$ $\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$
by rule induction?

$$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

the predicate matches with the conclusions of two rules only

Exercise: Loop exit

$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$ $\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \text{ff}$
by rule induction?

$$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \text{ff}$$

the predicate matches with the conclusions of two rules only

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

Exercise: Loop exit

$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$ $\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \text{ff}$
by rule induction?

$$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \text{ff}$$

the predicate matches with the conclusions of two rules only

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

Exercise: Loop exit

$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$ $\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$
by rule induction

$$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

Exercise: Loop exit

$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$

$\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$

by rule induction

$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$

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

Exercise: Loop exit

$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$

$\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$

by rule induction

$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$

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

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

Exercise: Loop exit

$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$

$\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$

by rule induction

$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$

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

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

we need to prove $P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma) \triangleq \langle b, \sigma \rangle \longrightarrow \mathbf{ff}$

Exercise: Loop exit

$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c$

$\forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \text{ff}$

by rule induction

$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \text{ff}$

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

we assume $\langle b, \sigma \rangle \longrightarrow \text{ff}$

we need to prove $P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma) \triangleq \langle b, \sigma \rangle \longrightarrow \text{ff}$

immediate (by assumption)

Exercise: Loop exit

$$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c \qquad \forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

by rule induction

$$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

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

Exercise: Loop exit

$$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c \qquad \forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

by rule induction

$$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

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

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

$$\langle c, \sigma \rangle \longrightarrow \sigma''$$

$$\langle w, \sigma'' \rangle \longrightarrow \sigma'$$

$$P(\langle w, \sigma'' \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

Exercise: Loop exit

$$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c \qquad \forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

by rule induction

$$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

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

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

$$\langle c, \sigma \rangle \longrightarrow \sigma''$$

$$\langle w, \sigma'' \rangle \longrightarrow \sigma'$$

$$P(\langle w, \sigma'' \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

we need to prove $P(\langle w, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$

Exercise: Loop exit

$$w \stackrel{\text{def}}{=} \text{while } b \text{ do } c \qquad \forall \sigma, \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \Rightarrow \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

by rule induction

$$P(\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

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

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

$$\langle c, \sigma \rangle \longrightarrow \sigma''$$

$$\langle w, \sigma'' \rangle \longrightarrow \sigma'$$

$$P(\langle w, \sigma'' \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$$

we need to prove $P(\langle w, \sigma \rangle \longrightarrow \sigma') \triangleq \langle b, \sigma' \rangle \longrightarrow \mathbf{ff}$

immediate (by inductive hypothesis)

Exercise: Divergence

Consider the command

$$w \stackrel{\text{def}}{=} \textbf{while } x > y \textbf{ do } (x := x + 1 ; y := y - 1)$$

Find out the set S of memories σ such that $\langle w, \sigma \rangle \not\rightarrow$ and prove that this is the case by using the inference rule for divergence.

Exercise: Divergence

take $w \triangleq$ while $x > y$ do $\underbrace{(x := x + 1; y := y - 1)}_c$
take a generic σ

Exercise: Divergence

take $w \triangleq$ while $x > y$ do $\underbrace{(x := x + 1; y := y - 1)}_c$

take a generic σ

if $\sigma(x) \leq \sigma(y)$: $\langle w, \sigma \rangle \longrightarrow \sigma$

Exercise: Divergence

take $w \triangleq$ **while** $x > y$ **do** $\underbrace{(x := x + 1; y := y - 1)}_c$
take a generic σ

if $\sigma(x) \leq \sigma(y)$: $\langle w, \sigma \rangle \longrightarrow \sigma$

let $S \triangleq \{\sigma \mid \sigma(x) > \sigma(y)\}$

Exercise: Divergence

take $w \triangleq \text{while } x > y \text{ do } \underbrace{(x := x + 1; y := y - 1)}_c$
take a generic σ

if $\sigma(x) \leq \sigma(y)$: $\langle w, \sigma \rangle \longrightarrow \sigma$

let $S \triangleq \{\sigma \mid \sigma(x) > \sigma(y)\}$

- $\forall \sigma \in S. \langle x > y, \sigma \rangle \longrightarrow \text{tt}$
- $\forall \sigma \in S. \forall \sigma'. \langle x := x + 1; y := y - 1, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' \in S$

Exercise: Divergence

take $w \triangleq \text{while } x > y \text{ do } \underbrace{(x := x + 1; y := y - 1)}_c$
take a generic σ

if $\sigma(x) \leq \sigma(y)$: $\langle w, \sigma \rangle \longrightarrow \sigma$

let $S \triangleq \{\sigma \mid \sigma(x) > \sigma(y)\}$

- $\forall \sigma \in S. \langle x > y, \sigma \rangle \longrightarrow \text{tt}$ ✓
- $\forall \sigma \in S. \forall \sigma'. \langle x := x + 1; y := y - 1, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' \in S$

Exercise: Divergence

take $w \triangleq \text{while } x > y \text{ do } \underbrace{(x := x + 1; y := y - 1)}_c$
take a generic σ

if $\sigma(x) \leq \sigma(y)$: $\langle w, \sigma \rangle \longrightarrow \sigma$

let $S \triangleq \{\sigma \mid \sigma(x) > \sigma(y)\}$

- $\forall \sigma \in S. \langle x > y, \sigma \rangle \longrightarrow \text{tt}$ ✓
- $\forall \sigma \in S. \forall \sigma'. \langle x := x + 1; y := y - 1, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' \in S$

in fact $\langle c, \sigma \rangle \longrightarrow \sigma' = \sigma[\sigma(x) + 1/x, \sigma(y) - 1/y]$

Exercise: Divergence

take $w \triangleq \text{while } x > y \text{ do } \underbrace{(x := x + 1; y := y - 1)}_c$
take a generic σ

if $\sigma(x) \leq \sigma(y)$: $\langle w, \sigma \rangle \longrightarrow \sigma$

let $S \triangleq \{\sigma \mid \sigma(x) > \sigma(y)\}$

- $\forall \sigma \in S. \langle x > y, \sigma \rangle \longrightarrow \mathbf{tt}$ ✓
- $\forall \sigma \in S. \forall \sigma'. \langle x := x + 1; y := y - 1, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' \in S$

in fact $\langle c, \sigma \rangle \longrightarrow \sigma' = \sigma[\sigma(x) + 1/x, \sigma(y) - 1/y]$

$$\sigma'(x) = \sigma(x) + 1 > \sigma(y) + 1 > \sigma(y) - 1 = \sigma'(y)$$

Exercise: Divergence

take $w \triangleq \text{while } x > y \text{ do } \underbrace{(x := x + 1; y := y - 1)}_c$
take a generic σ

if $\sigma(x) \leq \sigma(y)$: $\langle w, \sigma \rangle \longrightarrow \sigma$

let $S \triangleq \{\sigma \mid \sigma(x) > \sigma(y)\}$

- $\forall \sigma \in S. \langle x > y, \sigma \rangle \longrightarrow \text{tt}$ ✓
- $\forall \sigma \in S. \forall \sigma'. \langle x := x + 1; y := y - 1, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' \in S$

in fact $\langle c, \sigma \rangle \longrightarrow \sigma' = \sigma[\sigma(x) + 1/x, \sigma(y) - 1/y]$

$\sigma'(x) = \sigma(x) + 1 > \sigma(y) + 1 > \sigma(y) - 1 = \sigma'(y)$ thus $\sigma' \in S$

Exercise: Divergence

take $w \triangleq \text{while } x > y \text{ do } \underbrace{(x := x + 1; y := y - 1)}_c$
take a generic σ

if $\sigma(x) \leq \sigma(y)$: $\langle w, \sigma \rangle \longrightarrow \sigma$

let $S \triangleq \{\sigma \mid \sigma(x) > \sigma(y)\}$

- $\forall \sigma \in S. \langle x > y, \sigma \rangle \longrightarrow \text{tt}$ ✓
- $\forall \sigma \in S. \forall \sigma'. \langle x := x + 1; y := y - 1, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' \in S$ ✓

in fact $\langle c, \sigma \rangle \longrightarrow \sigma' = \sigma[\sigma(x) + 1/x, \sigma(y) - 1/y]$

$\sigma'(x) = \sigma(x) + 1 > \sigma(y) + 1 > \sigma(y) - 1 = \sigma'(y)$ thus $\sigma' \in S$

Exercise: Divergence

take $w \triangleq \text{while } x > y \text{ do } \underbrace{(x := x + 1; y := y - 1)}_c$
take a generic σ

if $\sigma(x) \leq \sigma(y)$: $\langle w, \sigma \rangle \longrightarrow \sigma$

let $S \triangleq \{\sigma \mid \sigma(x) > \sigma(y)\}$

- $\forall \sigma \in S. \langle x > y, \sigma \rangle \longrightarrow \text{tt}$ ✓
- $\forall \sigma \in S. \forall \sigma'. \langle x := x + 1; y := y - 1, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' \in S$ ✓

in fact $\langle c, \sigma \rangle \longrightarrow \sigma' = \sigma[\sigma(x) + 1/x, \sigma(y) - 1/y]$

$\sigma'(x) = \sigma(x) + 1 > \sigma(y) + 1 > \sigma(y) - 1 = \sigma'(y)$ thus $\sigma' \in S$

therefore, if $\sigma(x) > \sigma(y)$, then $\langle w, \sigma \rangle \not\longrightarrow$