university of groningen

Basic Approaches to the Semantics of Computation (BaSC)

Lecture 5: Rule Induction

Jorge A. Pérez

Bernoulli Institute for Mathematics, Computer Science, and AI
University of Groningen, Groningen, the Netherlands

November 27, 2025

Well-Founded Induction

Let $\prec \subseteq A \times A$ be a well-founded relation.

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

- A general proof principle, aka Noetherian induction.
- Derived from Theorem 4.5, direction **(2)** $\Rightarrow$ **(1)**.

Well-Founded Induction

Let $\prec \subseteq A \times A$ be a well-founded relation.

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

- A general proof principle, aka Noetherian induction.
- Derived from Theorem 4.5, direction **(2)** $\Rightarrow$ **(1)**.
- When proving $P(a)$ for some a, we can exploit the assumption $\forall b \prec a. P(b)$.
- A base case is any element of A such that the set $\{b \in A \mid b \prec a\}$ is empty.

Well-Founded Induction

Let $\prec \subseteq A \times A$ be a well-founded relation.

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

- A general proof principle, aka Noetherian induction.
- Derived from Theorem 4.5, direction **(2)** $\Rightarrow$ **(1)**.
- When proving $P(a)$ for some a, we can exploit the assumption $\forall b \prec a. P(b)$.
- A base case is any element of A such that the set $\{b \in A \mid b \prec a\}$ is empty.

We can **instantiate the principle**, by choosing specific A and $\prec$.

An Instance: Structural Induction

- Set: $A = T_\Sigma$ (closed terms)
- Well-founded relation: immediate subterm relation
  $\prec = \{(t_i, f(t_1, \ldots, t_n)) \mid f \in \Sigma_n, i \in [1..n]\}$

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

$$\rightsquigarrow$$

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

Structural Induction for Commands

Given the syntax of commands:

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

We have that structural induction is as follows:

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

Determinacy by Structural Induction

Base Cases

$$P(\textbf{skip})$$

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

Inductive Cases

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

$$\forall b, c_0, c_1.\ P(c_0) \wedge P(c_1) \Rightarrow P(\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1)$$

$$\forall b, c.\ P(c) \Rightarrow P(\textbf{while } b \textbf{ do } c)$$

Determinacy by Structural Induction

Base Cases

$$P(\textbf{skip})$$

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

Inductive Cases

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

$$\forall b, c_0, c_1.\, P(c_0) \wedge P(c_1) \Rightarrow P(\textbf{if}\ b\ \textbf{then}\ c_0\ \textbf{else}\ c_1)$$

$$\forall b, c.\, P(c) \Rightarrow P(\textbf{while}\ b\ \textbf{do}\ c)$$

The case for **while** b **do** c fails, due to the recursive definition of its semantics:

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

one of the premises is as complex as the conclusion!

Where is the Problem?

$$\forall b, c.\, P(c) \;\Rightarrow\; P(\textbf{while}\ b\ \textbf{do}\ c)$$

- Consider arbitrary b and c. Our inductive hypothesis:
  $P(c) \triangleq \forall \sigma, \sigma_1, \sigma_2 \in \mathbb{M}.\, (\langle c, \sigma\rangle \longrightarrow \sigma_1 \wedge \langle c, \sigma\rangle \longrightarrow \sigma_2) \Rightarrow \sigma_1 = \sigma_2$

Where is the Problem?

$$\forall b, c.\, P(c) \;\Rightarrow\; P(\textbf{while } b \textbf{ do } c)$$

- Consider arbitrary b and c. Our inductive hypothesis:
  $P(c) \triangleq \forall \sigma, \sigma_1, \sigma_2 \in \mathbb{M}. (\langle c, \sigma \rangle \longrightarrow \sigma_1 \wedge \langle c, \sigma \rangle \longrightarrow \sigma_2) \Rightarrow \sigma_1 = \sigma_2$
- We want to prove

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

Where is the Problem?

$$\forall b, c.\, P(c) \;\Rightarrow\; P(\textbf{while}\ b\ \textbf{do}\ c)$$

- Consider arbitrary b and c. Our inductive hypothesis:
  $P(c) \triangleq \forall \sigma, \sigma_1, \sigma_2 \in \mathbb{M}.\, (\langle c, \sigma\rangle \longrightarrow \sigma_1 \land \langle c, \sigma\rangle \longrightarrow \sigma_2) \Rightarrow \sigma_1 = \sigma_2$
- We want to prove

  $$P(\textbf{while}\ b\ \textbf{do}\ c) \triangleq \forall \sigma, \sigma_1, \sigma_2 \in \mathbb{M}.$$
  $$(\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \sigma_1 \land \langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2) \Rightarrow \sigma_1 = \sigma_2$$

- Take $\sigma, \sigma_1, \sigma_2$ such that $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \sigma_1$ and $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2$.
  We want to prove $\sigma_1 = \sigma_2$.

Where is the Problem?

$$\forall b, c.\, P(c) \;\Rightarrow\; P(\textbf{while}\ b\ \textbf{do}\ c)$$

- Consider arbitrary b and c. Our inductive hypothesis:
  $P(c) \triangleq \forall \sigma, \sigma_1, \sigma_2 \in \mathbb{M}. (\langle c, \sigma\rangle \longrightarrow \sigma_1 \wedge \langle c, \sigma\rangle \longrightarrow \sigma_2) \Rightarrow \sigma_1 = \sigma_2$
- We want to prove

  $P(\textbf{while}\ b\ \textbf{do}\ c) \triangleq \forall \sigma, \sigma_1, \sigma_2 \in \mathbb{M}.$
  $(\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \sigma_1 \wedge \langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2) \Rightarrow \sigma_1 = \sigma_2$
- Take $\sigma, \sigma_1, \sigma_2$ such that $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \sigma_1$ and $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2$. We want to prove $\sigma_1 = \sigma_2$.
- By determinacy of boolean expressions, there are two cases: $\langle b, \sigma\rangle \longrightarrow \texttt{tt}$ and $\langle b, \sigma\rangle \longrightarrow \texttt{ff}$. The issue is when $\langle b, \sigma\rangle \longrightarrow \texttt{tt}$.

Where is the Problem? (cont.)

- Consider the goal $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \sigma_1$, assuming $\langle b, \sigma\rangle \longrightarrow \mathtt{tt}$.

Where is the Problem? (cont.)

- Consider the goal $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \boxed{\sigma_1}$, assuming $\langle b, \sigma\rangle \longrightarrow \texttt{tt}$.
- The only applicable rule is

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

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

Where is the Problem? (cont.)

- Consider the goal $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \boxed{\sigma_1}$, assuming $\langle b, \sigma\rangle \longrightarrow \texttt{tt}$.
- The only applicable rule is

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

  hence $\boxed{\sigma_1} = \boxed{\sigma_1'}$ with $\langle c, \sigma\rangle \longrightarrow \boxed{\sigma_1''}$ and $\langle \textbf{while}\ b\ \textbf{do}\ c, \boxed{\sigma_1''}\rangle \longrightarrow \boxed{\sigma_1'}$.
- Similarly, since $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \boxed{\sigma_2}$,

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

Where is the Problem? (cont.)

- Consider the goal $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \sigma_1$, assuming $\langle b, \sigma\rangle \longrightarrow \texttt{tt}$.
- The only applicable rule is

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

  hence $\sigma_1 = \sigma'_1$ with $\langle c, \sigma\rangle \longrightarrow \sigma''_1$ and $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma''_1\rangle \longrightarrow \sigma'_1$.
- Similarly, since $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \sigma_2$,
  it must be $\sigma_2 = \sigma'_2$ with $\langle c, \sigma\rangle \longrightarrow \sigma''_2$ and $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma''_2\rangle \longrightarrow \sigma'_2$.
- By the inductive hypothesis $P(c)$, we have $\sigma''_1 = \sigma''_2$.

Where is the Problem? (cont.)

- Consider the goal $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \boxed{\sigma_1}$, assuming $\langle b, \sigma\rangle \longrightarrow \texttt{tt}$.
- The only applicable rule is

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

  hence $\boxed{\sigma_1} = \boxed{\sigma'_1}$ with $\langle c, \sigma\rangle \longrightarrow \boxed{\sigma''_1}$ and $\langle \textbf{while}\ b\ \textbf{do}\ c, \boxed{\sigma''_1}\rangle \longrightarrow \boxed{\sigma'_1}$.
- Similarly, since $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma\rangle \longrightarrow \boxed{\sigma_2}$,
  it must be $\boxed{\sigma_2} = \boxed{\sigma'_2}$ with $\langle c, \sigma\rangle \longrightarrow \boxed{\sigma''_2}$ and $\langle \textbf{while}\ b\ \textbf{do}\ c, \boxed{\sigma''_2}\rangle \longrightarrow \boxed{\sigma'_2}$.
- By the inductive hypothesis $P(c)$, we have $\boxed{\sigma''_1} = \boxed{\sigma''_2}$.
- Thus, $\langle \textbf{while}\ b\ \textbf{do}\ c, \boxed{\sigma''_2}\rangle \longrightarrow \boxed{\sigma'_1}$ and $\langle \textbf{while}\ b\ \textbf{do}\ c, \boxed{\sigma''_2}\rangle \longrightarrow \boxed{\sigma'_2}$, but there is no inductive hypothesis $P(\textbf{while}\ b\ \textbf{do}\ c)$!

A Recursive Definition!

this premise is as complex as the conclusion!

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

To prove determinacy we need another induction principle: rule induction.

Derivations

A logical system is a set of axioms and inference rules:

$$R = \left\{ \frac{}{z}, \frac{x_1 \quad \cdots \quad x_n}{y}, \ldots \right\}$$

Derivations

A logical system is a set of axioms and inference rules:

$$R = \left\{ \frac{}{z}, \frac{x_1 \quad \cdots \quad x_n}{y}, \cdots \right\}$$

A derivation in the logical system R is written $d \Vdash_R y$ where

- either $d = \left(\frac{}{y} \right)$ is an axiom of R;
- or $d = \left(\frac{d_1 \quad \cdots \quad d_n}{y} \right)$ for some derivations $d_1 \Vdash_R x_1, \cdots, d_n \Vdash_R x_n$

  such that $\left(\frac{x_1 \quad \cdots \quad x_n}{y} \right)$ is an inference rule of R.

Derivations

A logical system is a set of axioms and inference rules:

$$R = \left\{ \frac{}{z}, \frac{x_1 \quad \cdots \quad x_n}{y}, \cdots \right\}$$

A derivation in the logical system R is written $d \Vdash_R y$ where

- either $d = \left(\frac{}{y} \right)$ is an axiom of R;
- or $d = \left(\frac{d_1 \quad \cdots \quad d_n}{y} \right)$ for some derivations $d_1 \Vdash_R x_1, \cdots, d_n \Vdash_R x_n$

  such that $\left(\frac{x_1 \quad \cdots \quad x_n}{y} \right)$ is an inference rule of R.

We define $D_R \triangleq \{d \mid d \Vdash_R y\}$.

Immediate Subderivation Relation

$$A = D_R$$

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

Immediate Subderivation Relation

$$A = D_R$$

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

Example

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

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

Measuring Derivations

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

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

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

Example

$$\mathsf{height}\left(\frac{}{2 \longrightarrow 2}\right) = 1 \qquad \mathsf{height}\left(\frac{\frac{}{1 \longrightarrow 1} \quad \frac{}{2 \longrightarrow 2}}{(1 \oplus 2) \longrightarrow 3}\right) = 2$$

$\prec$ on Derivations is Well-Founded

- The measure height is useful:to connect $\prec$ with well-founded relations for $\mathbb{N}$
- By definition, if $d \prec d'$ then $\mathsf{height}(d) < \mathsf{height}(d')$.
- Any descending chain in $\prec$ induces a descending chain in $<$
- Since $<$ is well-founded so is $\prec$.

$\prec$ on Derivations is Well-Founded

- The measure height is useful:to connect $\prec$ with well-founded relations for $\mathbb{N}$
- By definition, if $d \prec d'$ then $\text{height}(d) < \text{height}(d')$.
- Any descending chain in $\prec$ induces a descending chain in $<$
- Since $<$ is well-founded so is $\prec$.

Consider $\prec^+$, the transitive closure of $\prec$. We have, e.g.,

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

- Corollary: $\prec^+$ is well-founded.

Induction on Derivations

Because $\prec$ is well-founded, we can now instantiate the induction principle!

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

A Variant: Rule Induction

Recall: $I_R \triangleq \{y \mid \Vdash_R y\}$ is the set of all theorems of R.

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

A Variant: Rule Induction

Recall: $I_R \triangleq \{y \mid \Vdash_R y\}$ is the set of all theorems of R.

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

Having $\{x_1, \ldots, x_n\} \subseteq I_R$ means assuming a derivation d_i for each theorem x_i. Without this assumption, we have a simplified variant:

$$\frac{\forall \left(\dfrac{x_1 \cdots x_n}{y}\right) \in R.\, (P(x_1) \land \cdots \land P(x_n)) \Rightarrow P(y)}{\forall x \in I_R.\, P(x)}$$

Induction Schemes

Properties of numbers $P(n) \rightsquigarrow$ **Mathematical induction**

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

Induction Schemes

Properties of numbers $P(n) \rightsquigarrow$ **Mathematical induction**

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

Properties of terms $P(t) \rightsquigarrow$ **Structural induction**

One proof obligation for each function symbol

Induction Schemes

Properties of numbers $P(n) \rightsquigarrow$ **Mathematical induction**

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

Properties of terms $P(t) \rightsquigarrow$ **Structural induction**

One proof obligation for each function symbol

Properties of formulas $P(F) \rightsquigarrow$ **Rule induction**

One proof obligation for each inference rule

Two Views of Determinacy

Properties of terms $P(t)$ $\rightsquigarrow$ Structural induction

$$P(c) \triangleq \forall \sigma, \sigma_1, \sigma_2 \in \mathbb{M}.\, (\langle c, \sigma \rangle \longrightarrow \sigma_1 \wedge \langle c, \sigma \rangle \longrightarrow \sigma_2) \Rightarrow \sigma_1 = \sigma_2$$

Two Views of Determinacy

Properties of terms $P(t)$ $\rightsquigarrow$ Structural induction

$$P(c) \triangleq \forall \sigma, \sigma_1, \sigma_2 \in \mathbb{M}. \, (\langle c, \sigma \rangle \longrightarrow \sigma_1 \land \langle c, \sigma \rangle \longrightarrow \sigma_2) \Rightarrow \sigma_1 = \sigma_2$$

Properties of formulas $P(F)$ $\rightsquigarrow$ Rule induction

$$P(\langle c, \sigma \rangle \longrightarrow \sigma_1) \triangleq \forall \sigma_2 \in \mathbb{M}. \, \langle c, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

IMP Semantics (Commands)

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

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

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

- $P(\langle c, \sigma\rangle \longrightarrow \sigma_1) \triangleq \forall \sigma_2 \in \mathbb{M}.\, \langle c, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$
- $\forall c, \sigma, \sigma_1 . P(\langle c, \sigma\rangle \longrightarrow \sigma_1)$?

Determinacy: Base Case #1

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

We want to prove

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

Take σ_2 such that $\langle \textbf{skip}, \sigma \rangle \longrightarrow \sigma_2$. We want to prove that $\sigma = \sigma_2$.

Determinacy: Base Case #1

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

We want to prove

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

Take σ_2 such that $\langle \textbf{skip}, \sigma \rangle \longrightarrow \sigma_2$. We want to prove that $\sigma = \sigma_2$.

- Consider the goal $\langle \textbf{skip}, \sigma \rangle \longrightarrow \sigma_2$.
- Only the rule $\frac{}{\langle \textbf{skip}, \sigma \rangle \longrightarrow \sigma}$ is applicable, hence $\sigma = \sigma_2$.

Determinacy: Base Case #2

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

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 such that $\langle x := a, \sigma \rangle \longrightarrow \sigma_2$. We want to prove that $\sigma[n/x] = \sigma_2$.

Determinacy: Base Case #2

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

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 such that $\langle x := a, \sigma \rangle \longrightarrow \sigma_2$. We want to prove that $\sigma[n/x] = \sigma_2$.

Determinacy: Base Case #2

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

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 such that $\langle x := a, \sigma \rangle \longrightarrow \sigma_2$. We want to prove that $\sigma[n/x] = \sigma_2$.

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

Determinacy: Base Case #2

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

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 such that $\langle x := a, \sigma \rangle \longrightarrow \sigma_2$. We want to prove that $\sigma[n/x] = \sigma_2$.

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

Determinacy: Base Case #2

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

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 such that $\langle x := a, \sigma \rangle \longrightarrow \sigma_2$. We want to prove that $\sigma[n/x] = \sigma_2$.

- Consider the goal $\langle x := a, \sigma \rangle \longrightarrow \sigma_2$.
- Only the rule $\dfrac{\langle a, \sigma \rangle \longrightarrow n}{\langle x := a, \sigma \rangle \longrightarrow \sigma[n/x]}$ 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 arithmetic expressions we have $n = m$, and thus $\sigma_2 = \sigma[m/x] = \sigma[n/x]$.

Determinacy: Inductive Case #1

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

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 that $\sigma' = \sigma_2$.

Determinacy: Inductive Case #1 (cont.)

We assume (inductive hypotheses):

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

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

Determinacy: Inductive Case #1 (cont.)

We assume (inductive hypotheses):

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

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

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

Determinacy: Inductive Case #1 (cont.)

We assume (inductive hypotheses):

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

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

- 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 $\langle c_1, \sigma_2''\rangle \longrightarrow \sigma_2'$.

Determinacy: Inductive Case #1 (cont.)

We assume (inductive hypotheses):

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

- 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 IH $P(\langle c_0, \sigma\rangle \longrightarrow \sigma'')$, we have $\sigma'' = \sigma_2''$ and thus $\langle c_1, \sigma''\rangle \longrightarrow \sigma_2'$.

Determinacy: Inductive Case #1 (cont.)

We assume (inductive hypotheses):

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

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

- 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 IH $P(\langle c_0, \sigma\rangle \longrightarrow \sigma'')$, we have $\sigma'' = \sigma_2''$ and thus $\langle c_1, \sigma''\rangle \longrightarrow \sigma_2'$.
- By IH $P(\langle c_1, \sigma''\rangle \longrightarrow \sigma')$, we have $\sigma' = \sigma_2'$ and we conclude: $\sigma' = \sigma_2$.

Determinacy: Inductive Case #2

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

We assume $\langle b, \sigma\rangle \longrightarrow \mathtt{ff}$ and the 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
$P(\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \longrightarrow \sigma') \triangleq \forall \sigma_2.\, \langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2.$
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 that
$\sigma' = \sigma_2$.

Determinacy: Inductive Case #2 (cont.)

We assume:

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

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

Determinacy: Inductive Case #2 (cont.)

We assume:

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

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

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

Determinacy: Inductive Case #2 (cont.)

We assume:

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

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

- Consider the goal $\langle \textbf{if}\ b\ \textbf{then}\ c_0\ \textbf{else}\ c_1, \sigma \rangle \longrightarrow \sigma_2$.
- By determinacy of boolean expressions, only the rule $\dfrac{\langle b, \sigma \rangle \longrightarrow \texttt{ff} \quad \langle c_1, \sigma \rangle \longrightarrow \sigma'}{\langle \textbf{if}\ b\ \textbf{then}\ c_0\ \textbf{else}\ c_1, \sigma \rangle \longrightarrow \sigma'}$ applies, hence $\sigma_2 = \sigma_2'$, with $\langle c_1, \sigma \rangle \longrightarrow \sigma_2'$.

Determinacy: Inductive Case #2 (cont.)

We assume:

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

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

- Consider the goal $\langle \textbf{if}\ b\ \textbf{then}\ c_0\ \textbf{else}\ c_1, \sigma \rangle \longrightarrow \sigma_2$.
- By determinacy of boolean expressions, only the rule $\dfrac{\langle b, \sigma \rangle \longrightarrow \mathtt{ff} \quad \langle c_1, \sigma \rangle \longrightarrow \sigma'}{\langle \textbf{if}\ b\ \textbf{then}\ c_0\ \textbf{else}\ c_1, \sigma \rangle \longrightarrow \sigma'}$ applies, hence $\sigma_2 = \sigma_2'$, with $\langle c_1, \sigma \rangle \longrightarrow \sigma_2'$.
- By IH $P(\langle c_1, \sigma \rangle \longrightarrow \sigma')$, we then have $\sigma' = \sigma_2' = \sigma_2$, and we are done.

Determinacy: Inductive Case #3

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

This case is analogous to the previous one.

Determinacy: Base Case #3

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

We assume $\langle b, \sigma \rangle \longrightarrow \texttt{ff}$. We want to prove

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

Take σ_2 such that $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma \rangle \longrightarrow \sigma_2$. We want to prove that $\sigma = \sigma_2$.

Determinacy: Base Case #3

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

We assume $\langle b, \sigma \rangle \longrightarrow \texttt{ff}$. We want to prove

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

Take σ_2 such that $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma \rangle \longrightarrow \sigma_2$. We want to prove that $\sigma = \sigma_2$.

- Consider the goal $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma \rangle \longrightarrow \sigma_2$.
- By determinacy of boolean expressions, only the rule $\dfrac{\langle b, \sigma \rangle \longrightarrow \texttt{ff}}{\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma \rangle \longrightarrow \sigma}$ is applicable, hence $\sigma_2 = \sigma$.

Determinacy: Inductive Case #4

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

We assume $\langle b, \sigma \rangle \longrightarrow \mathtt{tt}$ and the inductive hypotheses:

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

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

We want to prove
$P(\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma \rangle \longrightarrow \sigma') \triangleq \forall \sigma_2. \langle \textbf{while}\ b\ \textbf{do}\ c, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma' = \sigma_2$.
Take σ_2 such that $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma \rangle \longrightarrow \sigma_2$. We want to prove that $\boxed{\sigma' = \sigma_2}$.

Determinacy: Inductive Case #4 (cont.)

We assume $\langle b, \sigma \rangle \longrightarrow \texttt{tt}$ and the inductive hypotheses:

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

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

Determinacy: Inductive Case #4 (cont.)

We assume $\langle b, \sigma \rangle \longrightarrow \texttt{tt}$ and the inductive hypotheses:

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

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

- Consider the goal $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma \rangle \longrightarrow \sigma_2$.
- By determinacy of boolean expressions, 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 IH $P(\langle c, \sigma \rangle \longrightarrow \sigma'')$, $\sigma'' = \sigma_2''$ thus $\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma'' \rangle \longrightarrow \sigma_2'$.
- By IH $P(\langle \textbf{while}\ b\ \textbf{do}\ c, \sigma'' \rangle \longrightarrow \sigma')$, $\sigma' = \sigma_2'$ and we conclude $\sigma' = \sigma_2$.
- This concludes the case (and the proof of determinacy).

The End