



**PSC 2023/24** (375AA, 9CFU)

Principles for Software Composition

Roberto Bruni

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

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

**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  $R$ .

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

# 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)

## 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.

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

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

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

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

## Example

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

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

# 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

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

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

in such cases we can avoid to mention derivations at all

# 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

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

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

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

properties of formulas

$P(F)$

rule induction

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

# 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

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

We want to prove

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

Take  $\sigma_2$  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

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

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

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

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

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

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

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



# Inductive case

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

We assume

(inductive hypotheses)

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

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

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

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

# Inductive case (ctd)

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

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

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

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

We assume

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

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

We want to prove

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

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

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

# Inductive case (ctd)

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

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

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

By determinacy of Bexp

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

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

By inductive hypothesis  $P(\langle c_1, \sigma \rangle \longrightarrow \sigma')$ , we then have  $\sigma' = \sigma'_2 = \sigma_2$

# Inductive case

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

Analogous to the previous case and thus omitted

# Base case

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

We assume

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

We want to prove

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

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

We want to prove  $\sigma = \sigma_2$

# Inductive case (ctd)

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

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

By determinacy of Bexp

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

# Inductive case

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

We assume

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

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

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

We want to prove

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

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

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



# Inductive case (ctd)

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

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

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

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

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

# Determinacy of commands

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

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

# Badge exercise



Suppose we extend the syntax of arithmetic expressions

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

where  $x++$  evaluates to the current value of  $x$  but then increment  $x$  as a side-effect

1. Redefine the operational semantics of  $A_{\text{exp}}$ ,  $B_{\text{exp}}$  and  $Com$  to take side-effects into account and discuss all problematic issues and the subsequent design choices
2. Find two arithmetic expressions  $a_0$  and  $a_1$  such that the evaluation of  $a_0+a_1$  is different from  $a_1+a_0$ , if possible