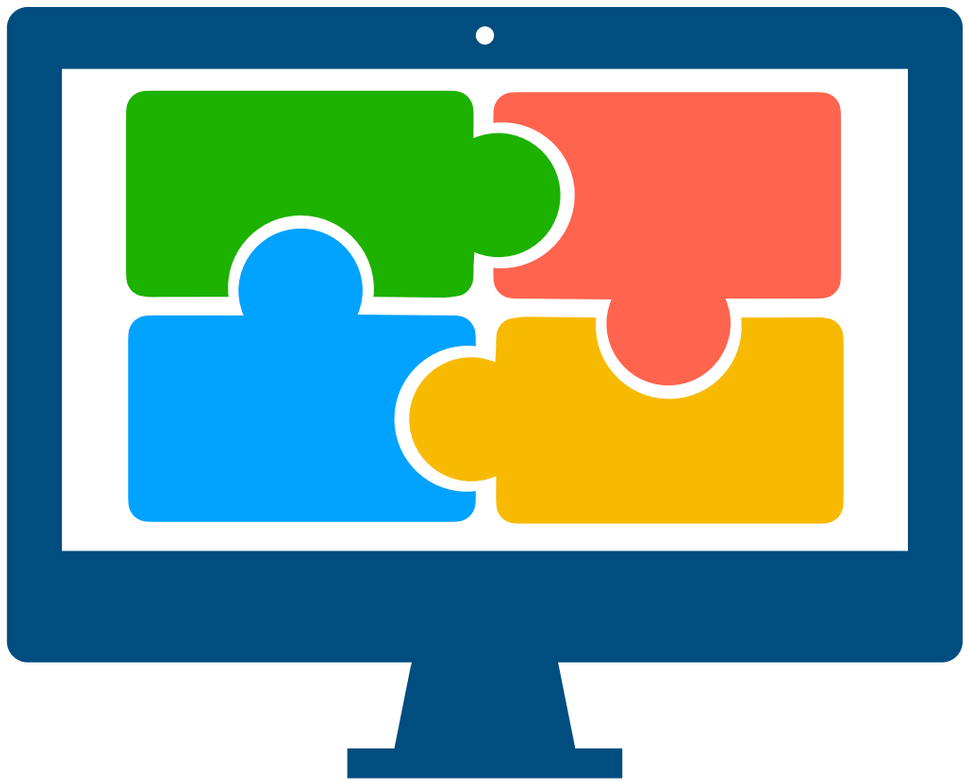

http://didawiki.di.unipi.it/doku.php/magistraleinformatica/psc/

PSC 2020/21 (375AA, 9CFU)

Principles for Software Composition

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

Exercises #2

Structural induction, rule induction and divergence

[**Ex. 1**] Complete the proof of termination of boolean expressions by structural induction.

$$b \ ::= \ v \ \mid \ a \ \mathsf{cmp} \ a \ \mid \ \neg b \ \mid \ b \ \mathsf{bop} \ b$$

$$P(b) \triangleq \forall \sigma.\ \exists u.\ \langle b, \sigma \rangle \longrightarrow u$$

Ex. 1, Termination Bexp

$$P(b) \triangleq \forall \sigma.\ \exists u.\ \langle b, \sigma \rangle \longrightarrow u$$

by structural induction

$\forall v \in \mathbb{B}.\ P(v)$

$\forall a_0, a_1.\ P(a_0 \,\mathsf{cmp}\, a_1)$

} see Lecture 05b

$\forall b.\ P(b) \Rightarrow P(\neg b)$

$\forall b_0, b_1.\ (P(b_0) \wedge P(b_1)) \Rightarrow P(b_0 \ \mathsf{bop}\ b_1)$

} to be done

Ex. 1, Termination Bexp

$$P(b) \triangleq \forall \sigma.\ \exists u.\ \langle b, \sigma \rangle \longrightarrow u$$

by structural induction

$\forall b.\ P(b) \Rightarrow P(\neg b)$ take a generic $b \in$ Bexp

we assume $P(b) \triangleq \forall \sigma.\ \exists w.\ \langle b, \sigma \rangle \longrightarrow w$

we want to prove $P(\neg b) \triangleq \forall \sigma.\ \exists u.\ \langle \neg b, \sigma \rangle \longrightarrow u$

take a generic σ

consider the goal $\langle \neg b, \sigma \rangle \longrightarrow u \quad \nwarrow_{u = \neg w} \langle b, \sigma \rangle \longrightarrow w$

by inductive hypothesis $P(b)$, such w exists

we conclude by taking $u = \neg w$

Ex. 1, Termination Bexp

$$P(b) \triangleq \forall \sigma.\ \exists u.\ \langle b, \sigma \rangle \longrightarrow u$$

by structural induction

$\forall b_0, b_1.\ (P(b_0) \wedge P(b_1)) \Rightarrow P(b_0 \text{ bop } b_1)$ take $b_0, b_1 \in$ Bexp

we assume $P(b_i) \triangleq \forall \sigma.\ \exists u_i.\ \langle b_i, \sigma \rangle \longrightarrow u_i$

we want to prove $P(b_0 \text{ bop } b_1) \triangleq \forall \sigma.\ \exists u.\ \langle b_0 \text{ bop } b_1, \sigma \rangle \longrightarrow u$

take a generic σ

consider the goal $\langle b_0 \text{ bop } b_1, \sigma \rangle \longrightarrow u$

$\nwarrow_{u = u_0\ bop\ u_1}\ \langle b_0, \sigma \rangle \longrightarrow u_0, \langle b_1, \sigma \rangle \longrightarrow u_1$

by inductive hypotheses $P(b_0)$ and $P(b_1)$, such u_0, u_1 exist

we conclude by taking $u = u_0\ bop\ u_1$

[**Ex. 2**] Extend the syntax of arithmetic expressions with the operator $a_0 \sqcap a_1$ whose big-step operational semantics is given by the rules:

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

1. Prove termination or exhibit a counterexample.

2. Prove determinacy or exhibit a counterexample.

Ex. 2, termination

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

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

Ex. 2, determinacy

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 $m = m'$

Ex. 2, determinacy (ctd)

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

Only the rule $\dfrac{\langle a_0, \sigma \rangle \longrightarrow n \quad \langle a_1, \sigma \rangle \longrightarrow n}{\langle a_0 \sqcap a_1, \sigma \rangle \longrightarrow n}$ 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 $m = m'$

Ex. 2, determinacy

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)

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

We want to prove

$P(\langle a_0 \sqcap a_1, \sigma\rangle \longrightarrow n) \stackrel{\triangle}{=} \forall n'.\ \langle a_0 \sqcap a_1, \sigma\rangle \longrightarrow n' \Rightarrow n = n'$

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

We want to prove $n = n'$

Ex. 2, determinacy (ctd)

$$P(\langle a_0, \sigma\rangle \longrightarrow n) \stackrel{\triangle}{=} \forall n'.\ \langle a_0, \sigma\rangle \longrightarrow n' \Rightarrow n = n'$$

$$P(\langle a_1, \sigma\rangle \longrightarrow n) \stackrel{\triangle}{=} \forall n'.\ \langle a_1, \sigma\rangle \longrightarrow n' \Rightarrow n = n'$$

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

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

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

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

[**Ex. 3**] Extend the syntax of arithmetic expressions with the operator $a_0 \sqcup a_1$ whose big-step operational semantics is given by the rule:

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

1. Prove termination or exhibit a counterexample.

2. Prove determinacy or exhibit a counterexample.

Ex. 3, termination

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

Inductive case (ctd)

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

Either rules $\dfrac{\langle a_0, \sigma \rangle \longrightarrow n_0}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_0}$ $\dfrac{\langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \sqcup a_1, \sigma \rangle \longrightarrow n_1}$ 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 $m = m_0$)

Ex. 3, determinacy

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

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

$$1 \neq 2$$

[**Ex. 4**] 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.

Ex. 4, divergence

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

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

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

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

[**Ex. 5**] Prove determinacy of boolean expressions by rule induction.

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

Ex. 5, determinacy Bexp

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

by rule induction

$$\frac{}{\langle v,\sigma\rangle \longrightarrow v}$$

we need to prove $P(\langle v,\sigma\rangle \longrightarrow v) \triangleq \forall u'.\ \langle v,\sigma\rangle \longrightarrow u' \Rightarrow v = u'$

take u' such that $\langle v,\sigma\rangle \longrightarrow u'$

we need to prove $v = u'$

consider the goal $\langle v,\sigma\rangle \longrightarrow u'$

it must be $\nwarrow_{u'=v} \Box$

Ex. 5, determinacy Bexp

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

by rule induction

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

we assume $\langle a_i,\sigma\rangle \longrightarrow n_i$

we need to prove

$P(\langle a_0 \text{ cmp } a_1,\sigma\rangle \longrightarrow n_0\ cmp\ n_1) \triangleq \forall u'.\ \langle a_0 \text{ cmp } a_1,\sigma\rangle \longrightarrow u' \Rightarrow n_0\ cmp\ n_1 = u'$

take u' such that $\langle a_0 \text{ cmp } a_1,\sigma\rangle \longrightarrow u'$

we need to prove $n_0\ cmp\ n_1 = u'$

consider the goal $\langle a_0 \text{ cmp } a_1,\sigma\rangle \longrightarrow u'$

it must be $\nwarrow_{u'=m_0\ cmp\ m_1}\ \langle a_0,\sigma\rangle \longrightarrow m_0, \langle a_1,\sigma\rangle \longrightarrow m_1$

by determinacy of Aexp $n_0 = m_0$ and $n_1 = m_1$

thus $n_0\ cmp\ n_1 = m_0\ cmp\ m_1 = u'$

Ex. 5, determinacy Bexp

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

by rule induction

$$\frac{\langle b,\sigma\rangle \longrightarrow v}{\langle \neg b,\sigma\rangle \longrightarrow \neg v}$$

we assume $P(\langle b,\sigma\rangle \longrightarrow v) \triangleq$
$\forall w.\ \langle b,\sigma\rangle \longrightarrow w \Rightarrow v = w$

we need to prove

$P(\langle \neg b,\sigma\rangle \longrightarrow \neg v) \triangleq \forall u'.\ \langle \neg b,\sigma\rangle \longrightarrow u' \Rightarrow \neg v = u'$

take u' such that $\langle \neg b,\sigma\rangle \longrightarrow u'$

we need to prove $\neg v = u'$

consider the goal $\langle \neg b,\sigma\rangle \longrightarrow u'$

it must be $\nwarrow_{u'=\neg w} \langle b,\sigma\rangle \longrightarrow w$

by inductive hypothesis $v = w$

thus $\neg v = \neg w = u'$

Ex. 5, determinacy Bexp

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

by rule induction

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

we assume $P(\langle b_i, \sigma\rangle \longrightarrow v_i) \stackrel{\triangle}{=}$
$\forall u_i.\ \langle b_i, \sigma\rangle \longrightarrow u_i \Rightarrow v_i = u_i$

we need to prove

$P(\langle b_0 \text{ bop } b_1, \sigma\rangle \longrightarrow v_0\ bop\ v_1) \stackrel{\triangle}{=} \forall u'.\ \langle b_0 \text{ bop } b_1, \sigma\rangle \longrightarrow u' \Rightarrow v_0\ bop\ v_1 = u'$

take u' such that $\langle b_0 \text{ bop } b_1, \sigma\rangle \longrightarrow u'$

we need to prove $v_0\ bop\ v_1 = u'$

consider the goal $\langle b_0 \text{ bop } b_1, \sigma\rangle \longrightarrow u'$

it must be $\nwarrow_{u' = u_0\ bop\ u_1} \langle b_0, \sigma\rangle \longrightarrow u_0, \langle b_1, \sigma\rangle \longrightarrow u_1$

by inductive hypotheses $v_0 = u_0$ and $v_1 = u_1$

thus $v_0\ bop\ v_1 = u_0\ bop\ u_1 = u'$

[**Ex. 6**] Let b be a boolean expression and c a command. Consider the command

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

Prove by rule induction that:

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

Ex. 6, loop exit

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

by structural induction? $\qquad$ by rule induction?

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

the predicate matches with the conclusions of two rules only

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

Ex. 6, loop exit

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

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

by rule induction

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

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

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

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

immediate (by assumption)

Ex. 6, loop exit

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

by rule induction

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

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

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

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

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

$P(\langle w, \sigma''\rangle \longrightarrow \sigma') \stackrel{\triangle}{=} \langle b, \sigma'\rangle \longrightarrow \textbf{ff}$

we need to prove $P(\langle w, \sigma\rangle \longrightarrow \sigma') \stackrel{\triangle}{=} \langle b, \sigma'\rangle \longrightarrow \textbf{ff}$

immediate (by inductive hypothesis)