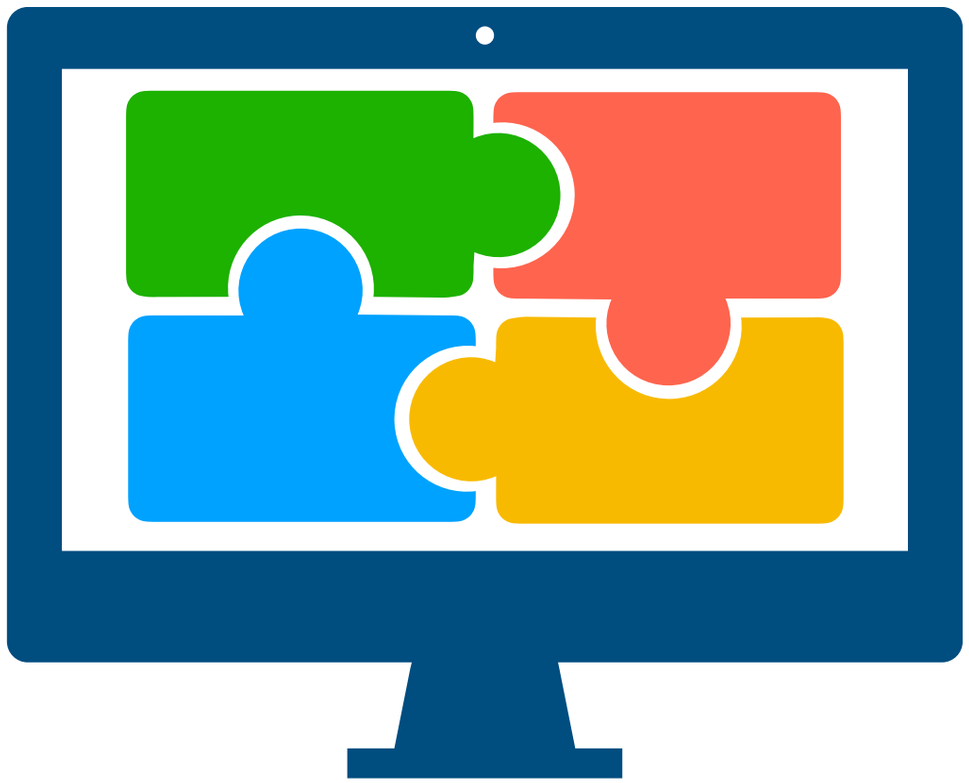


http://didawiki.di.unipi.it/doku.php/magistraleinformatica/psc/

PSC 2020/21 (375AA, 9CFU)

Principles for Software Composition

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

17b - CCS: guarded processes

CCS

guarded processes

CCS op. semantics

Act) $$\frac{}{\mu.p \xrightarrow{\mu} p}$$

Res) $$\frac{p \xrightarrow{\mu} q \quad \mu \notin \{\alpha, \overline{\alpha}\}}{p\backslash\alpha \xrightarrow{\mu} q\backslash\alpha}$$

Rel) $$\frac{p \xrightarrow{\mu} q}{p[\phi] \xrightarrow{\phi(\mu)} q[\phi]}$$

SumL) $$\frac{p_1 \xrightarrow{\mu} q}{p_1 + p_2 \xrightarrow{\mu} q}$$

SumR) $$\frac{p_2 \xrightarrow{\mu} q}{p_1 + p_2 \xrightarrow{\mu} q}$$

ParL) $$\frac{p_1 \xrightarrow{\mu} q_1}{p_1|p_2 \xrightarrow{\mu} q_1|p_2}$$

Com) $$\frac{p_1 \xrightarrow{\lambda} q_1 \quad p_2 \xrightarrow{\overline{\lambda}} q_2}{p_1|p_2 \xrightarrow{\tau} q_1|q_2}$$

ParR) $$\frac{p_2 \xrightarrow{\mu} q_2}{p_1|p_2 \xrightarrow{\mu} p_1|q_2}$$

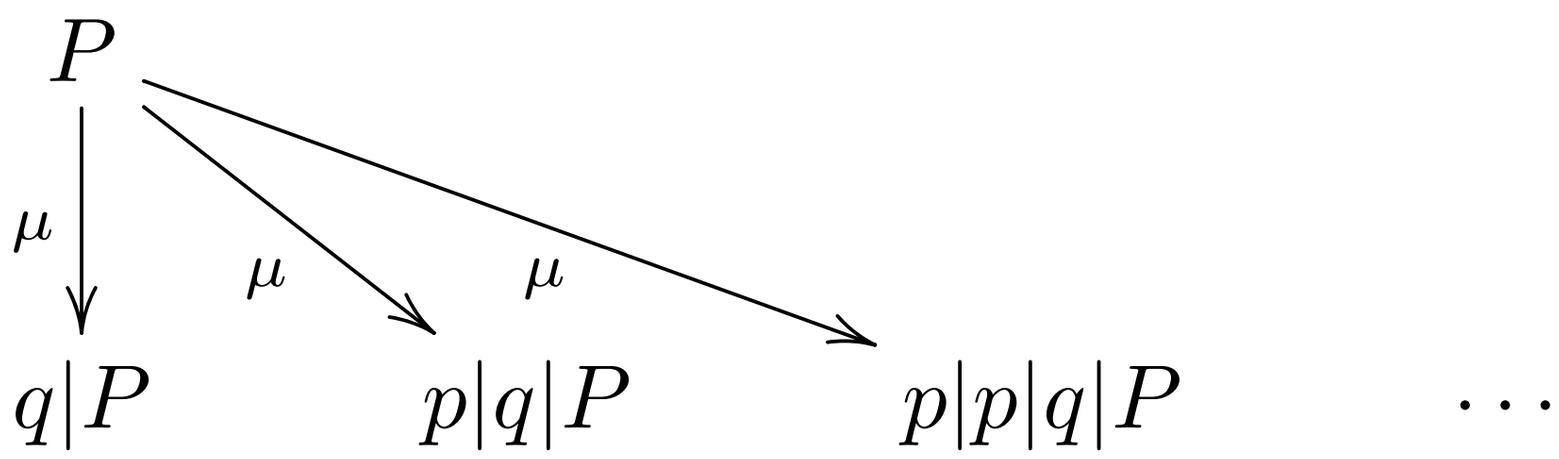
Rec) $$\frac{p\left[{}^{\mathbf{rec}\ x.\ p}/_{x}\right] \xrightarrow{\mu} q}{\mathbf{rec}\ x.\ p \xrightarrow{\mu} q}$$

CCS: guarded processes

the allowed form of recursion is very general

there are processes with infinitely many outgoing transitions

suppose $p \xrightarrow{\mu} q$ take $P \triangleq \mathbf{rec}\ x.\ p|x$ $P \triangleq p|P$



such processes are called *infinitely branching* and are BAD

CCS: guarded processes

guarded processes guarantee that process variables occur under a prefix (recursion is guarded by some action)

let X be a set of process variables

$G(p, X)$ all recursively defined names are guarded in p

if a name in X occurs free in p it is prefixed by an action

$$G(\mathbf{nil}, X) \triangleq \mathbf{true} \qquad G(p[\phi], X) \triangleq G(p, X)$$

$$G(x, X) \triangleq x \notin X \qquad G(p + q, X) \triangleq G(p, X) \wedge G(q, X)$$

$$G(\mu.p, X) \triangleq G(p, \emptyset) \qquad G(p|q, X) \triangleq G(p, X) \wedge G(q, X)$$

$$G(p\backslash\alpha, X) \triangleq G(p, X) \qquad G(\mathbf{rec}\ x.\ p, X) \triangleq G(p, X \cup \{x\})$$

a closed process p is *guarded* if $G(p, \emptyset)$ holds true

Exercise: guarded?

$R \triangleq \mathbf{rec}\ x.\ \alpha.x + \beta$

$G(R, \emptyset)$? 

$$G(\mathbf{rec}\ x.\ \alpha.x + \beta, \emptyset) = G(\alpha.x + \beta, \{x\})$$

$$= G(\alpha.x, \{x\}) \wedge G(\beta, \{x\})$$

$$= G(x, \emptyset) \wedge G(\mathbf{nil}, \emptyset)$$

$$= x \notin \emptyset \wedge \mathbf{true}$$

$$= \mathbf{true}$$

Exercise: guarded?

$T \triangleq \mathbf{rec}\ x.\ (\alpha|x) + \beta$

$G(T, \emptyset)?$ 

$$G(\mathbf{rec}\ x.\ (\alpha|x) + \beta, \emptyset) = G((\alpha|x) + \beta, \{x\})$$

$$= G(\alpha|x, \{x\}) \wedge G(\beta, \{x\})$$

$$= G(\alpha, \{x\}) \wedge G(x, \{x\}) \wedge G(\mathbf{nil}, \emptyset)$$

$$= G(\mathbf{nil}, \emptyset) \wedge x \notin \{x\} \wedge \mathbf{true}$$

$$= \mathbf{true} \wedge \mathbf{false}$$

$$= \mathbf{false}$$

Exercise: guarded?

$U \triangleq \mathbf{rec}\ x.\ \alpha|\beta.x$

$G(U, \emptyset)?$ 

$$G(\mathbf{rec}\ x.\ \alpha|\beta.x, \emptyset) = G(\alpha|\beta.x, \{x\})$$

$$= G(\alpha, \{x\}) \wedge G(\beta.x, \{x\})$$

$$= G(\mathbf{nil}, \emptyset) \wedge G(x, \emptyset)$$

$$= \mathbf{true} \wedge x \notin \emptyset$$

$$= \mathbf{true}$$

Exercise: guarded?

$\mathbf{rec}\ x.\ x$  unguarded

$\mathbf{rec}\ x.\ \alpha.\mathbf{rec}\ y.\ x$  guarded

$\mathbf{rec}\ x.\ \alpha.\mathbf{rec}\ y.\ x + y$  unguarded

$\mathbf{rec}\ x.\ \alpha.\mathbf{rec}\ y.\ x|y$  unguarded

$\mathbf{rec}\ x.\ \alpha.\mathbf{rec}\ y.\ x|\beta.y$  guarded

Properties of guarded processes

Guarded variables

TH. $G(p, X \cup \{x\}) \Rightarrow G(p, X)$

TH. $G(p, X) \wedge x \notin \mathsf{fv}(p) \Rightarrow G(p, X \cup \{x\})$

proofs by structural induction on p (omitted)

Substitutions preserve guardedness

TH. $G(p, X) \wedge \bigwedge_{i \in [1,n]} G(p_i, X) \Rightarrow G(p[{}^{p_1}/_{x_1}, \cdots, {}^{p_n}/_{x_n}], X)$

proof by structural induction on p (omitted)

Transitions preserve guardedness

TH. $G(p, X) \wedge p \xrightarrow{\mu} q \Rightarrow G(q, \emptyset)$

proof by rule induction on $p \xrightarrow{\mu} q$ (omitted)

Guarded processes are finitely branching

TH. $G(p, \emptyset) \Rightarrow \forall \mu.\ \{q \mid p \xrightarrow{\mu} q\}$ is a finite set

we prove a stronger property:

TH. $X = \{x_1, ..., x_n\} \qquad \sigma = [{}^{p_1}/_{x_1}, \cdots, {}^{p_n}/_{x_n}]$

$$G(p, X) \wedge \bigwedge_{i \in [1,n]} G(p_i, X) \Rightarrow \{q \mid \exists \mu.\ p\sigma \xrightarrow{\mu} q\} \text{ is a finite set}$$

proof: by structural induction on p

we only show some cases (and omit some details)

(see next slides)

TH. $X = \{x_1, ..., x_n\}$ $\quad \sigma = [{}^{p_1}/_{x_1}, \cdots, {}^{p_n}/_{x_n}]$ (continue)

$$G(p, X) \wedge \bigwedge_{i \in [1,n]} G(p_i, X) \Rightarrow \{q \mid \exists \mu.\ p\sigma \xrightarrow{\mu} q\} \text{ is a finite set}$$

proof: by structural induction on p

$p = \mathbf{nil}$ $\quad \mathbf{nil}\sigma = \mathbf{nil}$ $\quad \{q \mid \exists \mu.\ \mathbf{nil} \xrightarrow{\mu} q\} = \emptyset$

$p = x$ $\quad x \in X$ $\quad G(x, X) = \mathbf{false}$

$x \notin X$ $\quad x\sigma = x$ $\quad \{q \mid \exists \mu.\ x \xrightarrow{\mu} q\} = \emptyset$

$p = \mu'.p'$ $\quad \{q \mid \exists \mu.\ p\sigma \xrightarrow{\mu} q\} = \{p'\sigma\}$

TH. $X = \{x_1, ..., x_n\}$ $\quad \sigma = [{}^{p_1}/_{x_1}, \cdots, {}^{p_n}/_{x_n}]$ (continue)

$$G(p, X) \wedge \bigwedge_{i \in [1,n]} G(p_i, X) \Rightarrow \{q \mid \exists \mu.\ p\sigma \xrightarrow{\mu} q\} \text{ is a finite set}$$

proof: by structural induction on p

$p = p' \backslash \alpha$ $\quad p\sigma = p'\sigma \backslash \alpha \qquad G(p, X) = G(p', X)$

$$\{q \mid \exists \mu.\ p\sigma \xrightarrow{\mu} q\} = \{q' \backslash \alpha \mid \exists \mu \notin \{\alpha, \overline{\alpha}\}. p'\sigma \xrightarrow{\mu} q'\}$$

finite, by inductive hypothesis

$p = p'_0 + p'_1$ $\quad p\sigma = p'_0\sigma + p'_1\sigma \quad G(p, X) = G(p'_0, X) \wedge G(p'_1, X)$

$$\{q \mid \exists \mu.\ p\sigma \xrightarrow{\mu} q\} = \{q'_0 \mid \exists \mu.\ p'_0\sigma \xrightarrow{\mu} q'_0\} \cup \{q'_1 \mid \exists \mu.\ p'_1\sigma \xrightarrow{\mu} q'_1\}$$

finite, by inductive hypotheses

TH. $X = \{x_1, ..., x_n\}$ $\quad \sigma = [{}^{p_1}/_{x_1}, \cdots, {}^{p_n}/_{x_n}]$ (continue)

$G(p, X) \wedge \bigwedge_{i \in [1,n]} G(p_i, X) \Rightarrow \{q \mid \exists \mu.\ p\sigma \xrightarrow{\mu} q\}$ is a finite set

proof: by structural induction on p

$p = \mathbf{rec}\ x.p'$ without loss of generality $x \notin X \cup \bigcup_{i \in [1,n]} \mathrm{fv}(p_i)$

$$p\sigma = \mathbf{rec}\ x.\ p'\sigma$$

$$G(p, X) = G(p', X \cup \{x\})$$

$$\{q \mid \exists \mu.\ p\sigma \xrightarrow{\mu} q\} = \{q' \mid \exists \mu.\ p'\sigma[{}^{\mathbf{rec}\ x.\ p'\sigma}/_x] \xrightarrow{\mu} q'\}$$

finite, by inductive hypotheses