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

20 - Weak semantics
CCS syntax

\[ p, q ::= \begin{array}{l}
\text{nil} \quad \text{inactive process} \\
\text{x} \quad \text{process variable (for recursion)} \\
\mu.p \quad \text{action prefix} \\
p\backslash\alpha \quad \text{restricted channel} \\
p[\phi] \quad \text{channel relabelling} \\
p + q \quad \text{nondeterministic choice (sum)} \\
p|q \quad \text{parallel composition} \\
\text{rec } x. \ p \quad \text{recursion}
\end{array} \]

(operators are listed in order of precedence)
CCS op. semantics

Act) \[ \mu.p \xrightarrow{\mu} p \]

Res) \[ p \xrightarrow{\mu} q \quad \mu \not\in \{ \alpha, \bar{\alpha} \} \]
\[ p \backslash \alpha \xrightarrow{\mu} q \backslash \alpha \]

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

SumL) \[ p_1 \xrightarrow{\mu} q \]
\[ p_1 + p_2 \xrightarrow{\mu} q \]

SumR) \[ p_2 \xrightarrow{\mu} q \]
\[ p_1 + p_2 \xrightarrow{\mu} q \]

ParL) \[ p_1 \xrightarrow{\mu} q_1 \]
\[ p_1 | p_2 \xrightarrow{\mu} q_1 | p_2 \]

Com) \[ p_1 \xrightarrow{\lambda} q_1 \quad p_2 \xrightarrow{\bar{\lambda}} q_2 \]
\[ p_1 | p_2 \xrightarrow{\tau} q_1 | q_2 \]

ParR) \[ p_2 \xrightarrow{\mu} q_2 \]
\[ p_1 | p_2 \xrightarrow{\mu} p_1 | q_2 \]

Rec) \[ p[\text{rec } x. p / x] \xrightarrow{\mu} q \]
\[ \text{rec } x. p \xrightarrow{\mu} q \]
CCS
Weak transitions
Sequential buffer

\[ B_0^2 \triangleq in. B_1^2 \]
\[ B_1^2 \triangleq in. B_2^2 + \overline{out}. B_0^2 \]
\[ B_2^2 \triangleq \overline{out}. B_1^2 \]
Parallel buffer

\[ B_0^1 \triangleq \text{in}.B_1^1 \]

\[ B_1^1 \triangleq \overline{\text{out}.B_0^1} \]
Linked buffer

\[ B_0^1 \triangleq in.B_1^1 \]
\[ \eta(out) = c \]
\[ B_1^1 \triangleq \overline{out}.B_0^1 \]
\[ \phi(in) = c \]

\[ p \sim q \triangleq (p[\eta]\mid q[\phi]) \setminus c \]
Comparing buffers

are they all strong bisimilar?

\[ B_0^2 \xrightarrow{\text{in}} B_1^2 \]

\[ B_1^2 \xleftarrow{\text{out}} B_2^2 \]

\[ B_0^2 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^2 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^0 \]

\[ B_1^0 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]

\[ B_0^1 \xrightarrow{\text{in}} B_1^1 \]

\[ B_1^1 \xleftarrow{\text{out}} B_2^1 \]
Silent transitions

τ-transitions are silent, non observable they represent internal steps of the system they can be used just for bookkeeping can we abstract away from them? can we find a broader equivalence? necessary to relate an abstract specification (little use of τ) with a concrete implementation (lots/tons of τ)
Weak bisimulation game

cooler equivalence: more power to the defender!

Alice picks a process and an ordinary transition

Bob replies possibly using many additional silent transitions
arbitrarily many, but finitely many
such sequences are called weak transitions

\[ p \xrightarrow{\mu} q \]

what if Alice picks a silent transition?

Bob can just leave the other process idle
i.e. can choose not to move
Weak transitions

\[ p \xrightarrow{\tau} q \quad \text{iff} \quad p \xrightarrow{\tau}^* q \]
\[ p = q \lor p \xrightarrow{\tau} \ldots \xrightarrow{\tau} q \]

\[ p \text{ can reach } q \text{ via a (possibly empty) finite sequence of } \tau\text{-transitions} \]

\[ p \xrightarrow{\lambda} q \quad \text{iff} \quad \exists p', q'. \; p \xrightarrow{\tau} p' \xrightarrow{\lambda} q' \xrightarrow{\tau} q \]

\[ p \text{ can reach } q \text{ via a } \lambda\text{-transition possibly preceded and followed by empty/finite sequences of } \tau\text{-transitions} \]
Example

\[
\begin{array}{c}
\text{Example} \\
\begin{array}{c}
B_1^1 \sim B_0^1 \\
\text{in} \\
B_0^1 \sim B_0^1 \\
\text{out} \\
B_0^1 \sim B_1^1 \\
\tau \\
B_1^1 \sim B_1^1 \\
\text{out} \\
B_1^1 \sim B_1^1 \\
\text{in} \\
B_0^1 \sim B_0^1 \\
\text{out} \\
B_0^1 \sim B_0^1 \\
\text{in} \\
B_0^1 \sim B_0^1 \\
\tau \\
B_0^1 \sim B_0^1 \\
\text{out} \\
B_0^1 \sim B_0^1 \\
\end{array}
\end{array}
\]
CCS
weak bisimulation
Weak bisimulation

\( R \) is a \textit{weak} bisimulation if

\[
\forall p, q. \ (p, q) \in R \Rightarrow \left\{ \begin{array}{l}
\forall \mu, p'. p \xrightarrow{\mu} p' \Rightarrow \exists q'. q \xrightarrow{\mu} q' \land p' R q' \\
\land \ \text{Alice plays}
\end{array} \right.
\]

\[
\forall \mu, q'. q \xrightarrow{\mu} q' \Rightarrow \exists p'. p \xrightarrow{\mu} p' \land p' R q'
\]

\text{weak transitions}

Alice plays

Bob replies
Weak bisimilarity:

\[ p \approx q \iff \exists R \text{ a weak bisimulation with } (p, q) \in R \]

**TH.** Weak bisimilarity is an equivalence relation

**TH.** Any strong bisimulation is a weak bisimulation

**Cor.** Strong bisimilarity implies weak bisimilarity
Weaker bisimilarity?

what if we give extra power to Alice as well?

\[ \forall p, q. (p, q) \in R \Rightarrow \]

\[ \forall \mu, p'. p \xrightarrow{\mu} p' \Rightarrow \exists q'. q \xrightarrow{\mu} q' \land p' \mathrel{R} q' \]
\[ \land \quad \text{Alice plays} \]

\[ \forall \mu, q'. q \xrightarrow{\mu} q' \Rightarrow \exists p'. p \xrightarrow{\mu} p' \land p' \mathrel{R} q' \]
\[ \land \quad \text{Bob replies} \]

weak transitions

nothing changes: we still get the same weak bisimilarity
Example

\[ R \triangleq \left\{ (B_0^2, B_0^1 \sim B_0^1), (B_1^2, B_1^1 \sim B_1^1), (B_1^2, B_1^1 \sim B_1^1), (B_2^2, B_1^1 \sim B_1^1) \right\} \]

is a weak bisimulation relation
Example

\[ B_0^2 \xrightarrow{\text{out}} B_1^2 \xleftarrow{\text{in}} B_1^1 \xrightarrow{\text{in}} B_0^1 \xleftarrow{\text{in}} B_0^1 \xrightarrow{\tau} B_0^1 \xleftarrow{\text{in}} B_1^1 \xrightarrow{\text{in}} B_0^1 \xleftarrow{\text{in}} B_0^1 \xrightarrow{\text{in}} B_1^1 \xleftarrow{\text{in}} B_0^1 \xrightarrow{\text{out}} B_1^2 \xleftarrow{\text{out}} B_1^2 \xrightarrow{\text{out}} B_1^2 \xleftarrow{\text{out}} B_1^2 \]
Example

$B_0^2$ $B_1^2$ $B_1^1$ $B_0^1$ $B_0^1$ $B_1^1$ $B_1^0$ $B_1^1$ $B_0^1$ $B_1^1$ $B_0^1$

$B_2^2$ $R$ $B_1^1$ $R$ $B_0^1$ $B_1^1$ $R$ $B_0^1$ $B_1^1$ $R$ $B_0^1$

$B_0^1$ $B_0^1$ $B_0^1$ $B_1^1$
Example

\[ B_1^2 \text{ stays idle!} \]

\[ R \]

\[ B_1^2 \overset{\tau}{\rightarrow} B_1^1 \]

(etc. for the other pairs)
Weak bis as a fixpoint

\[ \Psi(R) \triangleq \left\{ (p, q) \mid \forall \mu, p'. p \xrightarrow{\mu} p' \Rightarrow \exists q'. q \xrightarrow{\mu} q' \land p' R q' \right\} \]

\[ \Psi : \wp(\mathcal{P} \times \mathcal{P}) \rightarrow \wp(\mathcal{P} \times \mathcal{P}) \]

maps relations to relations

\[ R \subseteq \Psi(R) \]

a weak bisimulation

\[ \approx = \Psi(\approx) \]

weak bisimilarity is a fixpoint
CCS
problems with weak semantics
Problems with weak bis

with respect to weak transitions, guarded processes can have infinitely branching LTS

\[ P \triangleq \text{rec } x. \, \tau.x \mid \beta \]

\[ \begin{array}{c}
P \xrightarrow{\tau} P \mid \beta \xrightarrow{\tau} P \mid \beta \mid \beta \xrightarrow{\tau} \ldots \\
\beta \downarrow \quad \beta \downarrow \quad \beta \downarrow \\
\tau.P \quad \tau.P \mid \beta \quad \tau.P \mid \beta \mid \beta
\end{array} \]

many arrows omitted

assume \( p|\text{nil} = p \)

avoid \( \tau\)-prefixes?

\[ P \triangleq \text{rec } x. \, (\alpha.x \mid \overline{\alpha} \mid \beta) \setminus \alpha \]
Problems with weak bisimilarity is not a congruence (w.r.t. +)

take \( P \triangleq \alpha \) \hspace{1cm} Q \triangleq \tau.\alpha 

if \( P \xrightarrow{\alpha} \text{nil} \) then \( Q \xrightarrow{\alpha} \text{nil} \) \hspace{1cm} P \approx Q \quad \mathcal{C}[P] \not\approx \mathcal{C}[Q]

if \( Q \xrightarrow{\tau} \alpha \) then \( P \xrightarrow{\tau} P \)

take the context \( \mathcal{C}[] \triangleq [\cdot] + \beta \)

Alice plays \( \mathcal{C}[Q] \xrightarrow{\tau} \alpha \)

Bob can only reply \( \mathcal{C}[P] \xrightarrow{\tau} \mathcal{C}[P] \)

Alice plays \( \mathcal{C}[P] \xrightarrow{\beta} \text{nil} \)

Bob cannot reply \( \alpha \not\xrightarrow{\beta} \)

Alice wins!
Problems with weak bis

cannot distinguish between deadlock and silent divergence

\[
\text{rec } x. \tau.x \approx \text{nil}
\]

\[
\text{rec } x. \tau.x \xrightarrow{\tau} \text{rec } x. \tau.x \quad \text{nil} \xrightarrow{\tau} \text{nil}
\]
CCS
weak observational congruence
Weak obs congruence

\[ p \cong q \iff p \cong q \land \forall r. \ p + r \cong q + r \]

Equivalently

\[ p \cong q \iff \begin{cases} 
\forall p'. \ p \xrightarrow{\tau} p' \Rightarrow \exists q', q''. \ q \xrightarrow{\tau} q'' \Rightarrow q' \land p' \cong q' \\
\forall \lambda, p'. \ p \xrightarrow{\lambda} p' \Rightarrow \exists q'. \ q \xrightarrow{\lambda} q' \land p' \cong q'
\end{cases} \]

and vice versa

not a recursive definition! (refers to weak bisimilarity)

at the level of bisimulation game:

Bob is not allowed to use an idle move at the very first turn (at the following turns, ordinary weak bisimulation game)

TH. \( \cong \) is the largest congruence contained in \( \cong \)
Weak obs congruence

Note: \( \cong \) is not a weak bisimulation!

\[
P \triangleq \alpha \quad \text{and} \quad Q \triangleq \tau.\alpha
\]

\[
\begin{array}{ccc}
\beta.P & \cong & \beta.Q \\
\beta & \downarrow & \beta \\
P & \cong & Q
\end{array}
\]

\[P \not\approx Q\]

\[\cong \not\subseteq \Psi(\cong)\]
Weak obs congruence

All the laws for strong bisimilarity are still valid

Additionally: Milner’s $\tau$-laws

$p + \tau.p \simeq \tau.p$

$\mu.(p + \tau.q) \simeq \mu.(p + \tau.q) + \mu.q$

$\mu.\tau.p \simeq \mu.p$