

Modeling Concurrent and Probabilistic Systems

Lecture 9: Observation Congruence

Joost-Pieter Katoen Thomas Noll

Software Modeling and Verification Group
RWTH Aachen University
noll@cs.rwth-aachen.de

<http://www-i2.informatik.rwth-aachen.de/i2/mcps09/>

Summer Semester 2009

- 1 Repetition: Weak Bisimulation
- 2 Definition of Observation Congruence
- 3 Properties of Observation Congruence
- 4 Decidability of Observation Congruence

Definition

- Given $w \in Act^*$, $\widehat{w} \in (N \cup \overline{N})^*$ denotes the sequence of non- τ -actions in w (in particular, $\widehat{\tau^n} = \varepsilon$ for every $n \in \mathbb{N}$).
- For $w = \alpha_1 \dots \alpha_n \in Act^*$ and $P, Q \in Prc$, we let

$$P \xrightarrow{\textcolor{red}{w}} Q \iff P \xrightarrow{\tau}^* \xrightarrow{\alpha_1} \xrightarrow{\tau}^* \dots \xrightarrow{\alpha_n} \xrightarrow{\tau}^* Q$$

(and hence: $\xrightarrow{\varepsilon} = \xrightarrow{\tau}^*$).

- A relation $\rho \subseteq Prc \times Prc$ is called a **weak bisimulation** if $P\rho Q$ implies, for every $\alpha \in Act$,
 - $P \xrightarrow{\alpha} P' \implies$ ex. $Q' \in Prc$ such that $Q \xrightarrow{\widehat{\alpha}} Q'$ and $P' \rho Q'$
 - $Q \xrightarrow{\alpha} Q' \implies$ ex. $P' \in Prc$ such that $P \xrightarrow{\widehat{\alpha}} P'$ and $P' \rho Q'$
- $P, Q \in Prc$ are called **weakly bisimilar** (notation: $P \approx Q$) if there exists a weak bisimulation ρ such that $P\rho Q$.

Properties

- ① $P \sim Q \implies P \approx Q$
- ② \approx is an equivalence relation
- ③ $LTS(P) = LTS(Q) \implies P \approx Q$
- ④ $P \approx Q \implies \widehat{Tr}(P) = \widehat{Tr}(Q)$
- ⑤ \approx is (non- τ) deadlock sensitive
- ⑥ For every $P \in Prc$, $P \approx \tau.P$
- ⑦ \approx is **not a congruence**:

It is true that $b.\text{nil} \approx \tau.b.\text{nil}$
but $a.\text{nil} + b.\text{nil} \not\approx a.\text{nil} + \tau.b.\text{nil}$

- 1 Repetition: Weak Bisimulation
- 2 Definition of Observation Congruence
- 3 Properties of Observation Congruence
- 4 Decidability of Observation Congruence

Goal: introduce an equivalence which has most of the desirable properties of \approx and which is preserved under all CCS operators

Definition 9.1

$P, Q \in Prc$ are called **observationally congruent** (notation: $P \simeq Q$) if, for every $\alpha \in Act$,

- ① $P \xrightarrow{\alpha} P' \implies$ ex. $Q' \in Prc$ such that $Q \xrightarrow{\alpha} Q'$ and $P' \approx Q'$
- ② $Q \xrightarrow{\alpha} Q' \implies$ ex. $P' \in Prc$ such that $P \xrightarrow{\alpha} P'$ and $P' \approx Q'$

Remark: \simeq differs from \approx only in the use of $\xrightarrow{\alpha}$ rather than $\xrightarrow{\hat{\alpha}}$, i.e., it requires τ -actions from P or Q to be simulated by at least one τ -step in the other process. This only applies to the first step; the successors just have to satisfy $P' \approx Q'$ (and not $P' \simeq Q'$).

Goal: introduce an equivalence which has most of the desirable properties of \approx and which is preserved under all CCS operators

Definition 9.1

$P, Q \in Prc$ are called **observationally congruent** (notation: $P \simeq Q$) if, for every $\alpha \in Act$,

- ① $P \xrightarrow{\alpha} P' \implies$ ex. $Q' \in Prc$ such that $Q \xrightarrow{\alpha} Q'$ and $P' \approx Q'$
- ② $Q \xrightarrow{\alpha} Q' \implies$ ex. $P' \in Prc$ such that $P \xrightarrow{\alpha} P'$ and $P' \approx Q'$

Remark: \simeq differs from \approx only in the use of $\xrightarrow{\alpha}$ rather than $\xrightarrow{\hat{\alpha}}$, i.e., it requires τ -actions from P or Q to be simulated by at least one τ -step in the other process. This only applies to the first step; the successors just have to satisfy $P' \approx Q'$ (and not $P' \simeq Q'$).

Definition of Observation Congruence I

Goal: introduce an equivalence which has most of the desirable properties of \approx and which is preserved under all CCS operators

Definition 9.1

$P, Q \in Prc$ are called **observationally congruent** (notation: $P \simeq Q$) if, for every $\alpha \in Act$,

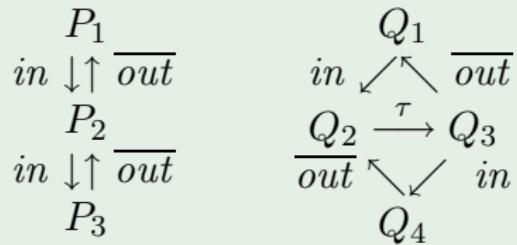
- ① $P \xrightarrow{\alpha} P' \implies$ ex. $Q' \in Prc$ such that $Q \xrightarrow{\alpha} Q'$ and $P' \approx Q'$
- ② $Q \xrightarrow{\alpha} Q' \implies$ ex. $P' \in Prc$ such that $P \xrightarrow{\alpha} P'$ and $P' \approx Q'$

Remark: \simeq differs from \approx only in the use of $\xrightarrow{\alpha}$ rather than $\xrightarrow{\widehat{\alpha}}$, i.e., it requires τ -actions from P or Q to be simulated by at least one τ -step in the other process. This only applies to the first step; the successors just have to satisfy $P' \approx Q'$ (and not $P' \simeq Q'$).

Definition of Observation Congruence II

Example 9.2

① Sequential and parallel two-place buffer:



$P_1 \simeq Q_1$ since $P_1 \approx Q_1$ (cf. Example 8.3) and neither P_1 nor Q_1 has initial τ -steps

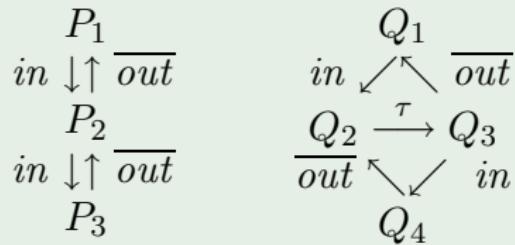
② $\tau.b.nil \not\simeq b.nil$ (since $\tau.b.nil \xrightarrow{\tau}$ but $b.nil \not\xrightarrow{\tau}$)
⇒ counterexample to congruence of \approx does not apply

③ $b.\tau.nil \simeq b.nil$ (since $\tau.nil \approx nil$)

Definition of Observation Congruence II

Example 9.2

① Sequential and parallel two-place buffer:



$P_1 \simeq Q_1$ since $P_1 \approx Q_1$ (cf. Example 8.3) and neither P_1 nor Q_1 has initial τ -steps

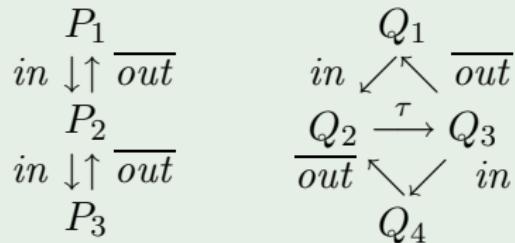
② $\tau.b.nil \not\simeq b.nil$ (since $\tau.b.nil \xrightarrow{\tau}$ but $b.nil \not\xrightarrow{\tau}$)
 \Rightarrow counterexample to congruence of \approx does not apply

③ $b.\tau.nil \simeq b.nil$ (since $\tau.nil \approx nil$)

Definition of Observation Congruence II

Example 9.2

① Sequential and parallel two-place buffer:



$P_1 \simeq Q_1$ since $P_1 \approx Q_1$ (cf. Example 8.3) and neither P_1 nor Q_1 has initial τ -steps

② $\tau.b.nil \not\simeq b.nil$ (since $\tau.b.nil \xrightarrow{\tau}$ but $b.nil \not\xrightarrow{\tau}$)
 \Rightarrow counterexample to congruence of \approx does not apply

③ $b.\tau.nil \simeq b.nil$ (since $\tau.nil \approx nil$)

- 1 Repetition: Weak Bisimulation
- 2 Definition of Observation Congruence
- 3 Properties of Observation Congruence
- 4 Decidability of Observation Congruence

Properties of Observation Congruence I

Corollary 9.3

For every $P, Q \in Prc$,

- ① $P \sim Q \implies P \simeq Q$
- ② $P \simeq Q \implies P \approx Q$

Proof.

- ① since $\xrightarrow{\alpha} \subseteq \xrightarrow{\alpha}$ and $\sim \subseteq \approx$
- ② since $\xrightarrow{\alpha} \subseteq \xrightarrow{\hat{\alpha}}$

□

Remark: this implies that

- processes with **identical LTSs** are \simeq -equivalent,
- \simeq -equivalent processes are (non- τ) **trace equivalent**, and
- \simeq is (non- τ) **deadlock sensitive**.

Exercise 5 shows that both inclusions are proper.

Properties of Observation Congruence I

Corollary 9.3

For every $P, Q \in Prc$,

- ① $P \sim Q \implies P \simeq Q$
- ② $P \simeq Q \implies P \approx Q$

Proof.

- ① since $\xrightarrow{\alpha} \subseteq \xrightarrow{\alpha}$ and $\sim \subseteq \approx$
- ② since $\xrightarrow{\alpha} \subseteq \xrightarrow{\hat{\alpha}}$

□

Remark: this implies that

- processes with **identical LTSs** are \simeq -equivalent,
- \simeq -equivalent processes are (non- τ) **trace equivalent**, and
- \simeq is (non- τ) **deadlock sensitive**.

Exercise 5 shows that both inclusions are proper.

Corollary 9.3

For every $P, Q \in Prc$,

- ① $P \sim Q \implies P \simeq Q$
- ② $P \simeq Q \implies P \approx Q$

Proof.

- ① since $\xrightarrow{\alpha} \subseteq \xrightarrow{\alpha}$ and $\sim \subseteq \approx$
- ② since $\xrightarrow{\alpha} \subseteq \xrightarrow{\hat{\alpha}}$

□

Remark: this implies that

- processes with **identical LTSs** are \simeq -equivalent,
- \simeq -equivalent processes are (non- τ) **trace equivalent**, and
- \simeq is (non- τ) **deadlock sensitive**.

Exercise 5 shows that both inclusions are proper.

Theorem 9.4

\simeq is a CCS congruence.

Proof.

- ① “equivalence” part: see Theorem 9.6
- ② “congruence” part: omitted



Theorem 9.4

\simeq is a CCS congruence.

Proof.

- ① “equivalence” part: see Theorem 9.6
- ② “congruence” part: omitted



A characterization of \simeq in terms of \approx :

Theorem 9.5

For every $P, Q \in Prc$,

$$P \simeq Q \iff P + R \approx Q + R \text{ for every } R \in Prc.$$

Proof.

on the board



Remark: together with Corollary 9.3 and Theorem 9.4, this shows that \simeq is the largest congruence contained in \approx

A characterization of \simeq in terms of \approx :

Theorem 9.5

For every $P, Q \in Prc$,

$$P \simeq Q \iff P + R \approx Q + R \text{ for every } R \in Prc.$$

Proof.

on the board



Remark: together with Corollary 9.3 and Theorem 9.4, this shows that \simeq is the largest congruence contained in \approx

A characterization of \simeq in terms of \approx :

Theorem 9.5

For every $P, Q \in Prc$,

$$P \simeq Q \iff P + R \approx Q + R \text{ for every } R \in Prc.$$

Proof.

on the board



Remark: together with Corollary 9.3 and Theorem 9.4, this shows that \simeq is the **largest congruence contained in \approx**

Theorem 9.6

\simeq is an equivalence relation.

Proof.

on the board



Theorem 9.6

\simeq is an equivalence relation.

Proof.

on the board



A characterization of \approx in terms of \simeq (reversal of Theorem 9.5):

Theorem 9.7

For every $P, Q \in Prc$,

$$P \approx Q \iff P \simeq Q \text{ or } P \simeq \tau.Q \text{ or } \tau.P \simeq Q.$$

Proof.

see Exercise 5



A characterization of \approx in terms of \simeq (reversal of Theorem 9.5):

Theorem 9.7

For every $P, Q \in Prc$,

$$P \approx Q \iff P \simeq Q \text{ or } P \simeq \tau.Q \text{ or } \tau.P \simeq Q.$$

Proof.

see Exercise 5



- 1 Repetition: Weak Bisimulation
- 2 Definition of Observation Congruence
- 3 Properties of Observation Congruence
- 4 Decidability of Observation Congruence

We now show that the **word problem for observation congruence**

Problem (Word problem for observation congruence)

Given: $P, Q \in Prc$

Question: $P \simeq Q?$

is decidable for finite-state processes (i.e., for those with $|S(P)|, |S(Q)| < \infty$ where $S(P) := \{P' \in Prc \mid P \xrightarrow{*} P'\}$)
(in general it is undecidable).

Since the definition of \simeq directly relies on \approx (cf. Def. 9.1), we first extend the partitioning algorithm from \sim (Theorem 7.1) to \approx .

We now show that the word problem for observation congruence

Problem (Word problem for observation congruence)

Given: $P, Q \in Prc$

Question: $P \simeq Q?$

is decidable for finite-state processes (i.e., for those with $|S(P)|, |S(Q)| < \infty$ where $S(P) := \{P' \in Prc \mid P \xrightarrow{*} P'\}$)
(in general it is undecidable).

Since the definition of \simeq directly relies on \approx (cf. Def. 9.1), we first extend the partitioning algorithm from \sim (Theorem 7.1) to \approx .

The Partitioning Algorithm I

Theorem 9.8 (Partitioning algorithm for \sim)

Input: LTS $(S, Act, \longrightarrow)$ (S finite)

Procedure: ① Start with initial partition $\Pi := \{S\}$

② Let $B \in \Pi$ be a block and $\alpha \in Act$ an action

③ For every $P \in B$, let

$$\alpha(P) := \{C \in \Pi \mid \text{ex. } P' \in C \text{ with } P \xrightarrow{\alpha} P'\}$$

be the set of P 's α -successor blocks

④ Partition $B = \sum_{i=1}^k B_i$ such that

$$P, Q \in B_i \iff \alpha(P) = \alpha(Q) \text{ for every } \alpha \in Act$$

⑤ Let $\Pi := (\Pi \setminus \{B\}) \cup \{B_1, \dots, B_k\}$

⑥ Continue with (2) until Π is stable

Output: Partition $\widehat{\Pi}$ of S

Then, for every $P, Q \in S$,

$$P \sim Q \iff \text{ex. } B \in \widehat{\Pi} \text{ with } P, Q \in B$$

The Partitioning Algorithm I

Theorem 9.8 (Partitioning algorithm for \approx)

Input: LTS $(S, Act, \longrightarrow)$ (S finite)

Procedure: ① Start with initial partition $\Pi := \{S\}$

② Let $B \in \Pi$ be a block and $\alpha \in Act$ an action

③ For every $P \in B$, let

$$\alpha^*(P) := \{C \in \Pi \mid \text{ex. } P' \in C \text{ with } P \xrightarrow{\alpha} P'\}$$

be the set of P 's α -successor blocks

④ Partition $B = \sum_{i=1}^k B_i$ such that

$$P, Q \in B_i \iff \alpha^*(P) = \alpha^*(Q) \text{ for every } \alpha \in Act$$

⑤ Let $\Pi := (\Pi \setminus \{B\}) \cup \{B_1, \dots, B_k\}$

⑥ Continue with (2) until Π is stable

Output: Partition $\widehat{\Pi}$ of S

Then, for every $P, Q \in S$,

$$P \approx Q \iff \text{ex. } B \in \widehat{\Pi} \text{ with } P, Q \in B$$

Remarks:

- ① Since S is finite, $\alpha^*(P)$ is effectively computable in step (3) of the algorithm.
- ② The \approx -partitioning algorithm can be interpreted as the application of the \sim -partitioning algorithm to an appropriately **modified LTS**:

$$\begin{aligned} & \text{Theorem 9.8 for } (S, Act, \rightarrow) \\ \hat{=} & \text{ Theorem 7.1 for } (S, Act, \rightarrow') \\ & \text{where } \rightarrow' := \bigcup_{\alpha \in Act} \xrightarrow{\hat{\alpha}} \end{aligned}$$

Proof.

similar to Theorem 7.1 (\sim -partitioning algorithm)



Remarks:

- ① Since S is finite, $\alpha^*(P)$ is effectively computable in step (3) of the algorithm.
- ② The \approx -partitioning algorithm can be interpreted as the application of the \sim -partitioning algorithm to an appropriately modified LTS:

$$\begin{aligned} & \text{Theorem 9.8 for } (S, Act, \rightarrow) \\ \hat{=} & \text{ Theorem 7.1 for } (S, Act, \rightarrow') \\ & \text{where } \rightarrow' := \bigcup_{\alpha \in Act} \xrightarrow{\hat{\alpha}} \end{aligned}$$

Proof.

similar to Theorem 7.1 (\sim -partitioning algorithm)



Decidability of Observation Congruence

Since the definition of \simeq requires the weak bisimilarity of the intermediate states after the first step, Theorem 9.8 yields the decidability of \simeq :

Theorem 9.9 (Decidability of \simeq)

Let $(S, Act, \longrightarrow)$ and $\widehat{\Pi}$ as in Theorem 9.8. Then, for every $P, Q \in S$,

$$P \simeq Q \iff \alpha^+(P) = \alpha^+(Q) \text{ for every } \alpha \in Act$$

where $\alpha^+(P) := \{C \in \widehat{\Pi} \mid \text{ex. } P' \in C \text{ with } P \xrightarrow{\alpha} P'\}$.

Proof.

omitted



Example 9.10

on the board

Decidability of Observation Congruence

Since the definition of \simeq requires the weak bisimilarity of the intermediate states after the first step, Theorem 9.8 yields the decidability of \simeq :

Theorem 9.9 (Decidability of \simeq)

Let $(S, Act, \longrightarrow)$ and $\widehat{\Pi}$ as in Theorem 9.8. Then, for every $P, Q \in S$,

$$P \simeq Q \iff \alpha^+(P) = \alpha^+(Q) \text{ for every } \alpha \in Act$$

where $\alpha^+(P) := \{C \in \widehat{\Pi} \mid \text{ex. } P' \in C \text{ with } P \xrightarrow{\alpha} P'\}$.

Proof.

omitted



Example 9.10

on the board

Decidability of Observation Congruence

Since the definition of \simeq requires the weak bisimilarity of the intermediate states after the first step, Theorem 9.8 yields the decidability of \simeq :

Theorem 9.9 (Decidability of \simeq)

Let $(S, Act, \longrightarrow)$ and $\widehat{\Pi}$ as in Theorem 9.8. Then, for every $P, Q \in S$,

$$P \simeq Q \iff \alpha^+(P) = \alpha^+(Q) \text{ for every } \alpha \in Act$$

where $\alpha^+(P) := \{C \in \widehat{\Pi} \mid \text{ex. } P' \in C \text{ with } P \xrightarrow{\alpha} P'\}$.

Proof.

omitted



Example 9.10

on the board

Decidability of Observation Congruence

Since the definition of \simeq requires the weak bisimilarity of the intermediate states after the first step, Theorem 9.8 yields the decidability of \simeq :

Theorem 9.9 (Decidability of \simeq)

Let $(S, Act, \longrightarrow)$ and $\widehat{\Pi}$ as in Theorem 9.8. Then, for every $P, Q \in S$,

$$P \simeq Q \iff \alpha^+(P) = \alpha^+(Q) \text{ for every } \alpha \in Act$$

where $\alpha^+(P) := \{C \in \widehat{\Pi} \mid \text{ex. } P' \in C \text{ with } P \xrightarrow{\alpha} P'\}$.

Proof.

omitted



Example 9.10

on the board