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

Outline

Repetition: Definition of Weak Bisimulation

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 $w = \alpha_1 \ldots \alpha_n \in Act^*$ and $P, Q \in Prc$, we let

$$P \overset{w}{\Longrightarrow} Q \iff P \, (\overset{\tau}{\longrightarrow})^* \overset{\alpha_1}{\longrightarrow} (\overset{\tau}{\longrightarrow})^* \ldots (\overset{\tau}{\longrightarrow})^* \overset{\alpha_n}{\longrightarrow} (\overset{\tau}{\longrightarrow})^* \, Q$$

  (and hence: $\overset{\varepsilon}{\Longrightarrow} = (\overset{\tau}{\longrightarrow})^*$).
- A relation $\rho \subseteq Prc \times Prc$ is called a weak bisimulation if $P \rho Q$ implies, for every $\alpha \in Act$,
  1. $P \overset{\alpha}{\longrightarrow} P' \implies$ ex. $Q' \in Prc$ such that $Q \overset{\widehat{\alpha}}{\Longrightarrow} Q'$ and $P' \rho Q'$
  2. $Q \overset{\alpha}{\longrightarrow} Q' \implies$ ex. $P' \in Prc$ such that $P \overset{\widehat{\alpha}}{\Longrightarrow} P'$ 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 $P \rho Q$.

Repetition: Properties of Weak Bisimulation

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 $b.\mathsf{nil} \approx \tau.b.\mathsf{nil}$
   but $a.\mathsf{nil} + b.\mathsf{nil} \not\approx a.\mathsf{nil} + \tau.b.\mathsf{nil}$

Outline

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

Remark: $\simeq$ differs from $\approx$ only in the use of $\stackrel{\alpha}{\Longrightarrow}$ rather than $\stackrel{\widehat{\alpha}}{\Longrightarrow}$, 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:

$$
\begin{array}{c}
P_1 \\
in \downarrow\uparrow \overline{out} \\
P_2 \\
in \downarrow\uparrow \overline{out} \\
P_3
\end{array}
\qquad\qquad
\begin{array}{ccccc}
 & & Q_1 & & \\
in & \swarrow & & \nwarrow & \overline{out} \\
Q_2 & & \xrightarrow{\tau} & & Q_3 \\
\overline{out} & \nwarrow & & \swarrow & in \\
 & & Q_4 & &
\end{array}
$$

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

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

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

Outline

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 $\xRightarrow{\alpha} \subseteq \xRightarrow{\widehat{\alpha}}$

□

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 II

Theorem 9.4

$\simeq$ *is a CCS congruence.*

Proof.

1. "equivalence" part: see Theorem 9.6
2. "congruence" part: omitted

□

Properties of Observation Congruence II

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 $\approx$

Properties of Observation Congruence III

Theorem 9.6

$\simeq$ *is an equivalence relation.*

Proof.

on the board □

Properties of Observation Congruence V

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 □

Outline

The Problem

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 $S(P) := \{P' \in Prc \mid P \longrightarrow^* P'\}$) (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 $\sim\approx$)

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*

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

   be the set of P*'s* α*-successor blocks*
4. *Partition* $B = \sum_{i=1}^{k} B_i$ *such that*

   $$P, Q \in B_i \iff \alpha(P) = \alpha(Q)\alpha^*(P) = \alpha^*(Q) \textit{ for every } \alpha \in Act$$
5. *Let* $\Pi := (\Pi \setminus \{B\}) \cup \{B_1, \ldots, B_k\}$
6. *Continue with (2) until* Π *is stable*

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

The Partitioning Algorithm II

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:

$$\begin{aligned} & \text{Theorem 9.8 for } (S, Act, \longrightarrow) \\ \widehat{=} \quad & \text{Theorem 7.1 for } (S, Act, \longrightarrow') \\ & \text{where } \longrightarrow' := \bigcup_{\alpha \in Act} \overset{\widehat{\alpha}}{\Longrightarrow} \end{aligned}$$

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

Proof.

omitted □

Example 9.10

on the board