Prof. Dr. Ir. J.-P. Katoen
A. Mereacre & H. Yue

# Advanced Model Checking
# Summer term 2009

## – Series 5 –

Hand in on May 25'th before the exercise class.

### Exercise 1 $(1 + 1 + 1 = 3$ points)

Figure 1 shows on its left a transition system $TS$ and on its right a reduced system $\hat{TS}$ that results from choosing $ample(s) = \{\alpha\}$. Check whether $TS$ and $\hat{TS}$ are stutter trace equivalent. If they are not, indicate which of the conditions $(A1) - (A4)$ is (are) violated.

Answer the same question for the transition system in the reduction shown in Figures 2 and 3, where different colors indicate different state labels.

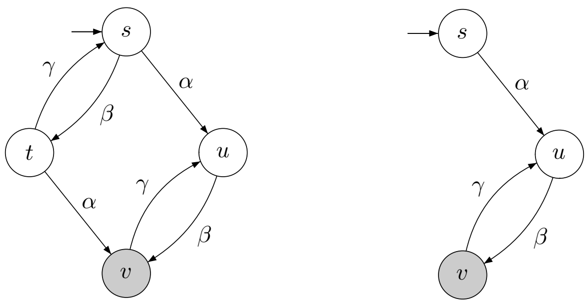



Abbildung 1: Transition system $TS$ (left) and $\hat{TS}$ (right) for the Exercise 1

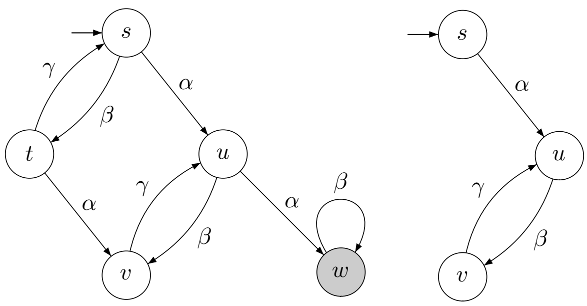



Abbildung 2: Transition system $TS$ (left) and $\hat{TS}$ (right) for the Exercise 1

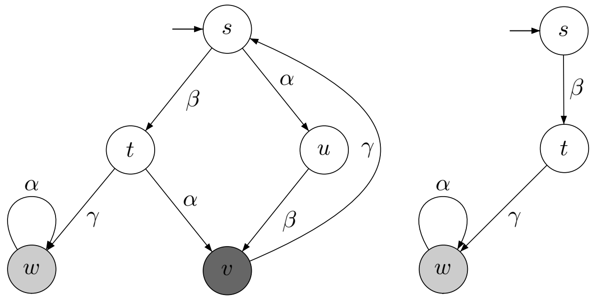
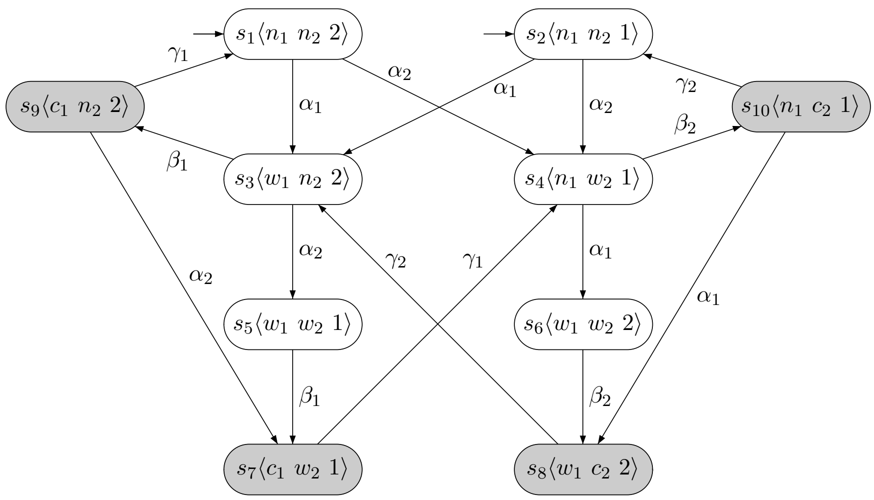



Abbildung 3: Transition system $TS$ (left) and $\hat{TS}$ (right) for the Exercise 1

## Exercise 2 **($1 + 1 = 2$ points)**

Consider the transition system $TS_{Pet}$ for the Peterson mutual exclusion algorithm.

(For more details of the algorithm, cf. page 45-47 of the book.)




**Questions:**

(a) Which actions are independent?

(b) Apply the partial order reduction approach to $TS_{Pet}$ with "small" ample sets according to Algorithm 38 (page 622 of the book) for checking the invariant "always $\neg(crit_1 \wedge crit_2)$", where $AP = \{crit_1, crit_2\}$. Note that $c_i$ in the figure is an abbreviation for $crit_i$.

## Exercise 3 **(2 points)**

Let $TS = (S, Act, \rightarrow, I, AP, L)$ be an action-deterministic transition system and let $\mathcal{I}_{st}$ be the set of all pairs $(\alpha, \beta) \in Act \times Act$ of independent actions $\alpha$ and $\beta$ where $\alpha$ or $\beta$ (or both) is a stutter action. Let *stutter permutation equivalence* $\cong_{perm}$ be the finest equivalence on $Act^*$ such that

$$\bar{\gamma}\alpha\beta\bar{\delta} \cong_{perm} \bar{\gamma}\beta\alpha\bar{\delta}$$

if $\bar{\gamma}, \bar{\delta} \in Act^*$ and $(\alpha, \beta) \in \mathcal{I}_{st}$.

The extension of $\cong_{perm}$ to an equivalence for infinite action sequences is defined as follows. If $\tilde{\alpha} = \alpha_1\alpha_2\alpha_3...$ and $\tilde{\beta} = \beta_1\beta_2\beta_3...$ are actions sequences in $Act^\omega$, then $\tilde{\alpha} \sqsubseteq_{perm} \tilde{\beta}$ if for all finite prefixes $\alpha_1...\alpha_n$ of $\tilde{\alpha}$ there exists a finite prefix $\beta_1...\beta_m$ of $\tilde{\beta}$ with $m \geq n$ and a finite word $\bar{\gamma} \in Act^*$ such that

$$\alpha_1 ... \alpha_n \bar{\gamma} \cong_{perm} \beta_1 ... \beta_m$$

We then define the binary relation $\cong_{perm}^{\omega}$ on $Act^{\omega}$ by

$$\tilde{\alpha} \cong_{perm}^{\omega} \tilde{\beta} \quad \text{iff} \quad \tilde{\alpha} \sqsubseteq_{perm} \tilde{\beta} \quad \text{and} \quad \tilde{\beta} \sqsubseteq_{perm} \tilde{\alpha}$$

**Questions:**

(a) Show that $\cong_{perm}^{\omega}$ is an equivalence.

## Exercise 4 **($1 + 2 = 3$ points)**

Consider the following definition:

**Definition 1** *Let $TS_i = (S_i, Act_i, \rightarrow_i, I_i, AP, L_i)$ be transition systems over $AP$. A* normed simulation *for $(TS_1, TS_2)$ is a triple $(\mathcal{R}, \nu_1, \nu_2)$ consisting of a binary relation $\mathcal{R} \in S_1 \times S_2$ such that:*

$$\forall s_1 \in I_1 . \exists s_2 \in I_2 . (s_1, s_2) \in \mathcal{R}$$

*and functions $\nu_1, \nu_2 : S_1 \times S_2 \rightarrow \mathbf{N}$ such that for all $(s_1, s_2) \in \mathcal{R}$:*

*(I)* $L_1(s_1) = L_2(s_2)$

*(II) For all $s_1' \in Post(s_1)$, at least one of the following three conditions holds:*

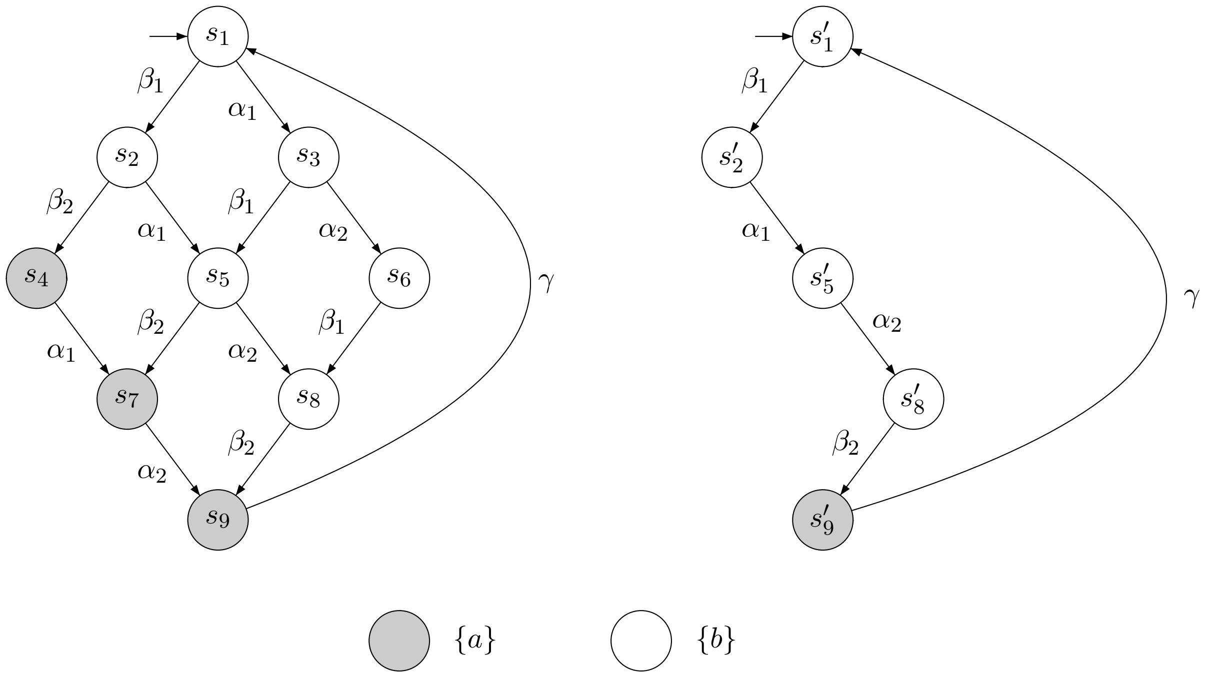
- *1)* $\exists s_2' \in Post(s_2) . (s_1', s_2') \in \mathcal{R}$
- *2)* $(s_1', s_2) \in \mathcal{R}$ *and* $\nu_1(s_1', s_2) < \nu_1(s_1, s_2)$
- *3)* $\exists s_2' \in Post(s_2) . (s_1, s_2') \in \mathcal{R}$ *and* $\nu_2(s_1, s_2') < \nu_2(s_1, s_2)$

*A* normed bisimulation *for $(TS_1, TS_2)$ is a normed simulation $(\mathcal{R}, \nu_1, \nu_2)$ for $(TS_1, TS_2)$ such that $(\mathcal{R}^{-1}, \nu_1^-, \nu_2^-)$ is a normed simulation for $(TS_2, TS_1)$. Here $\nu_i^-$ denotes the function $S_2 \times S_1 \rightarrow \mathbf{N}$ that results from $\nu_i$ by swapping the arguments, i.e. $\nu_i^-(u, v) = \nu_i(v, u)$ for all $u \in S_2$ and $v \in S_1$.*

*$TS_1$ and $TS_2$ are* normed bisimilar*, denoted $TS_1 \approx^n TS_2$, if there exists a normed bisimulation for $(TS_1, TS_2)$.*

**Questions:**

For two transition systems $TS$ (left) and $\widehat{TS}$ (right) show that:




(a) The ample sets *ample*(.) which reduce $TS$ to $\widehat{TS}$ satisfy conditions (A1)-(A5).

(b) Provide a normed bisimulation for $(TS, \widehat{TS})$.