RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

LEHRSTUHL FÜR INFORMATIK 2
RWTH Aachen · D-52056 Aachen
http://moves.rwth-aachen.de/

Prof. Dr. Ir. J.-P. Katoen
C. Dehnert & F. Sher

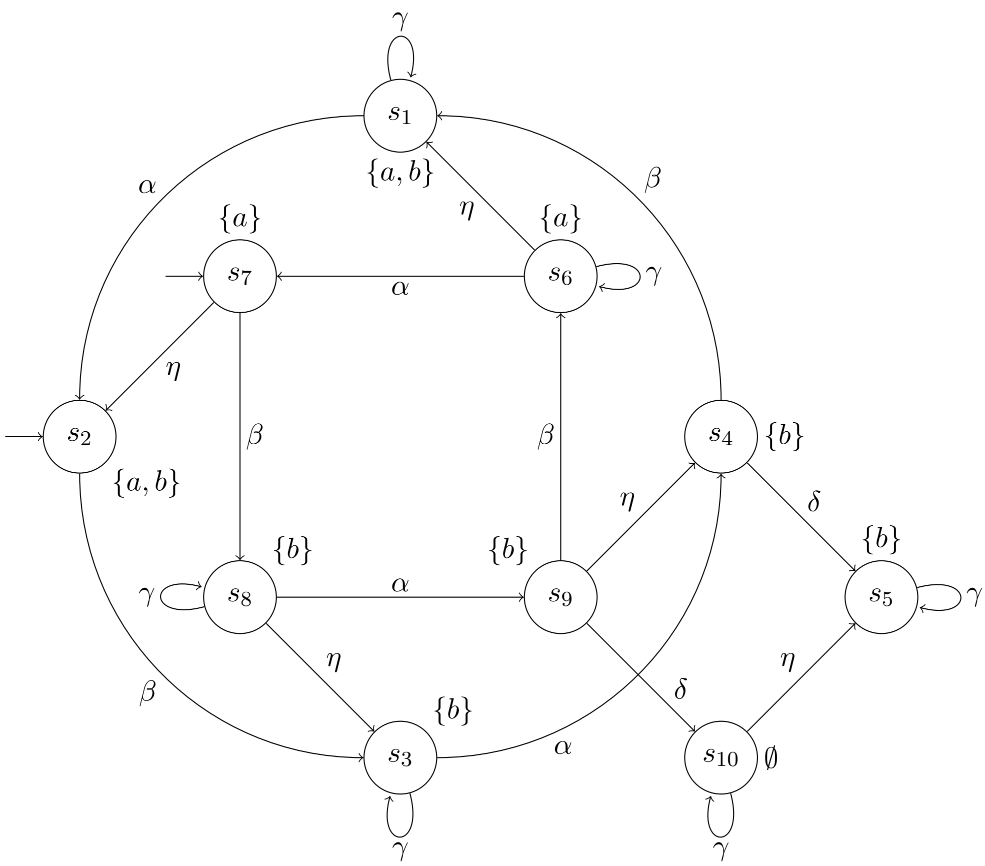
Advanced Model Checking
Summer term 2014

– Series 8 –

Hand in on **18 June** before the exercise class.

Exercise 1 (4 points)

Consider the following transition system TS.



(i) For each of the following ample sets, indicate whether it satisfies conditions (A1) to (A3). Justify your answer in case a condition is violated.

a) $ample(s_6) = \{\alpha, \gamma\}$

b) $ample(s_7) = \{\beta\}$

c) $ample(s_8) = \{\alpha\}$

d) $ample(s_9) = \{\beta, \delta, \eta\}$

e) $ample(s_{10}) = \{\gamma, \eta\}$

(ii) Is condition (A4) met if the ample sets are chosen according to (i)?

(iii) If the conditions (A1) through (A4) do not hold, provide a minimal extension of the ample sets that fixes this issue. Justify your answer.

Exercise 2 **(2 points)**

Definition 1 *Let $TS_i = (S_i, Act_i, \to_i, I_i, AP, L_i)$ be transition systems for $i \in \{1,2\}$. 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 $\nu_1, \nu_2 \colon S_1 \times S_2 \to \mathbb{N}$ such that for all $(s_1, s_2) \in \mathcal{R}$:

(i) $L_1(s_1) = L_2(s_2)$

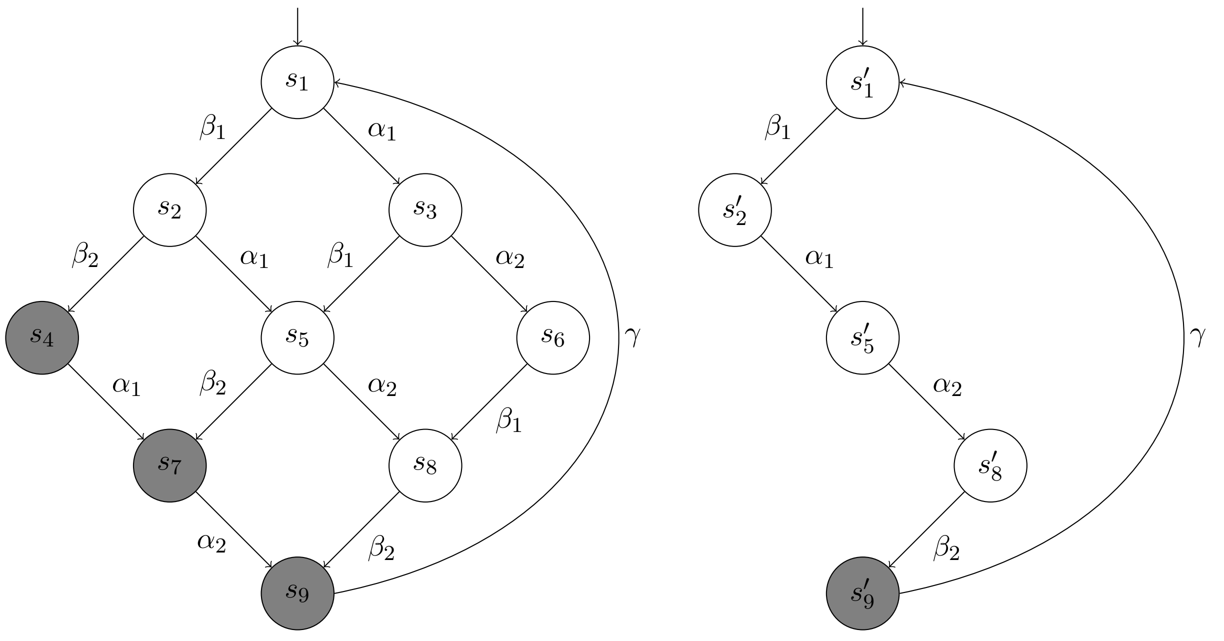
(ii) For all $s_1' \in \mathrm{Post}(s_1)$, at least one of the following three conditions holds:

- *(1)* $\exists s_2' \in \mathrm{Post}(s_2)$ *such that* $(s_1', s_2') \in \mathcal{R}$
- *(2)* $(s_1', s_2) \in \mathcal{R}$ *and* $\nu_1(s_1', s_2) < \nu_1(s_1, s_2)$
- *(3)* $\exists s_2' \in \mathrm{Post}(s_2)$ *such that* $(s_1, s_2') \in \mathcal{R}$ *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, ν_i^- denotes the function $S_2 \times S_1 \to \mathbb{N}$ that results from ν_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).*

Consider the following to transition systems TS and $\widehat{TS}$ where $\widehat{TS}$ results from TS by choosing the appropriate ample sets. States of equal color are labeled equally.

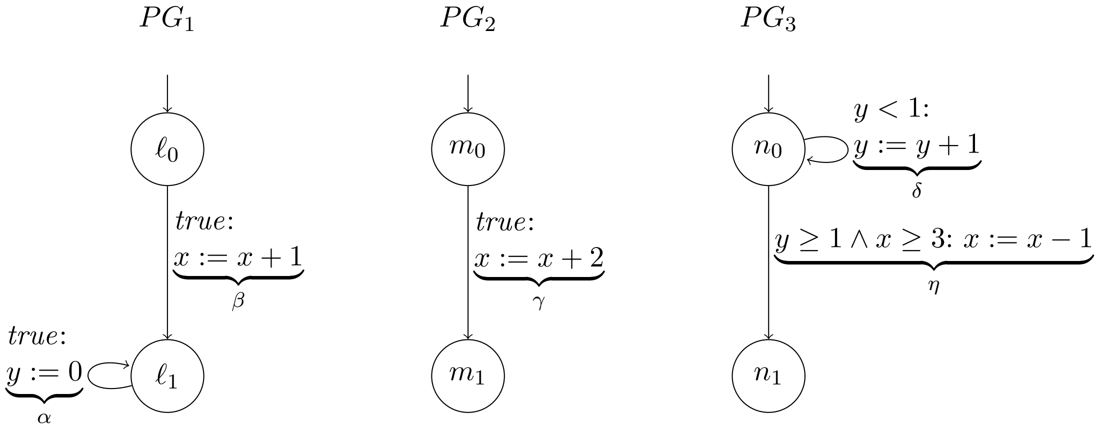


(i) How is normed bisimulation equivalence related to divergence-sensitive stutter bisimulation equivalence? Justify your answer.

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

Exercise 3 **(4 points)**

Consider the following three program graphs PG_1, PG_2, PG_3 over the shared variables x and y.



(i) Prove or refute that the invariant $\varphi = \square\neg n_1$ holds on $TS(PG_1 \parallel PG_2 \parallel PG_3)$ (where only n_1 is considered as an atomic proposition) with the initial condition $x = 0 \wedge y = 0$. For this, use the POR-based algorithm presented in the lecture (slide 151); in particular use the presented method to derive ample sets (slide 219) and the local criterion (slide 262) for (A2). Whenever you are required to pick a process (i.e., program graph) by any of the algorithms, try PG_2 first, then PG_1 and only then PG_3. Choosing the order of explored actions (in the ample set) is up to you. Write down all steps that you performed.