

Advanced Model Checking Summer term 2014

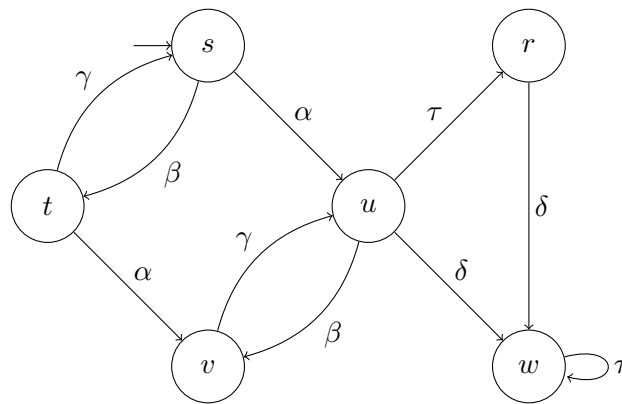
– Series 7 –

Hand in on 4 June before the exercise class.

Exercise 1

(2 points)

Consider the following transitions system TS with the action set $Act = \{\alpha, \beta, \gamma, \delta, \tau\}$ in which all states are equally labeled. Determine for each pair of actions whether they are independent.



Solution:

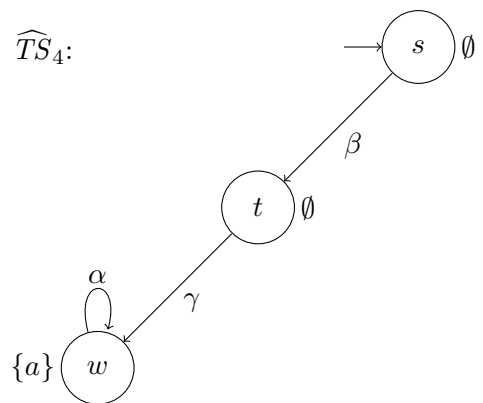
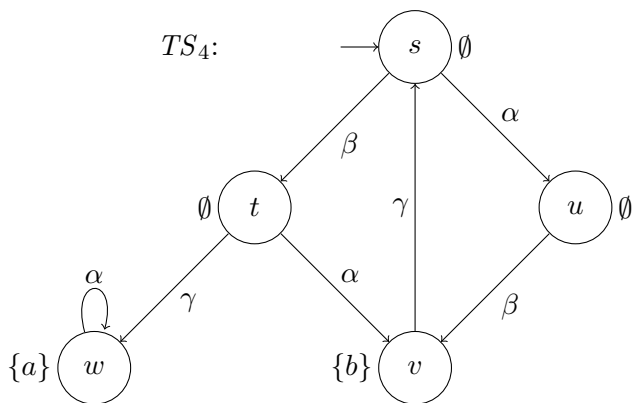
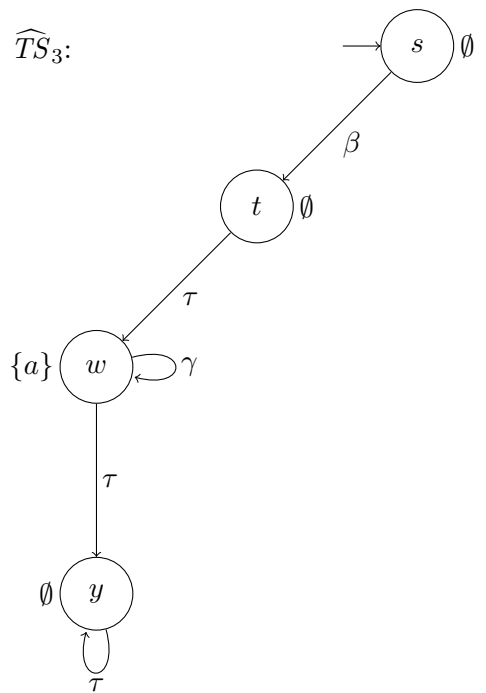
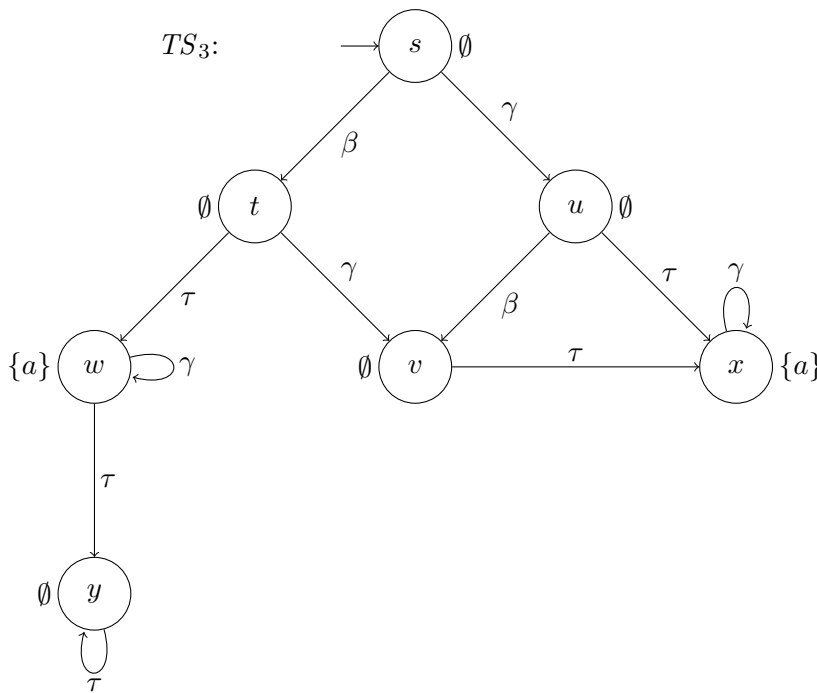
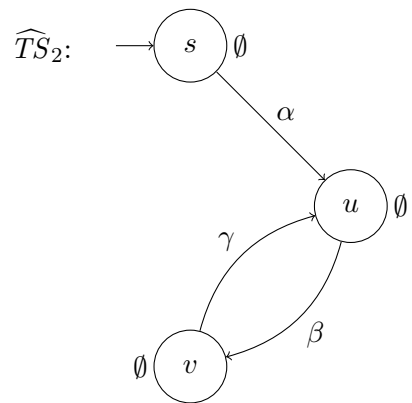
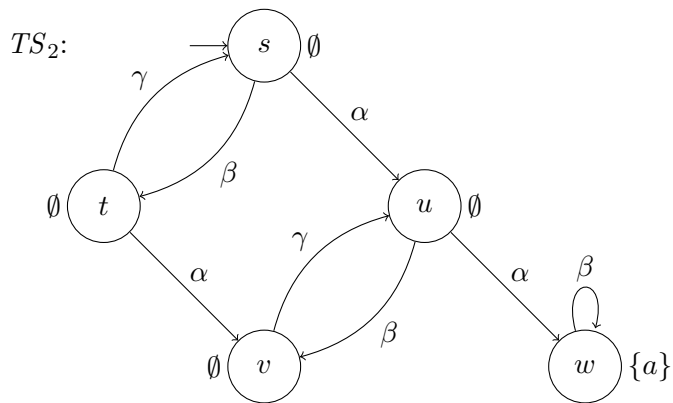
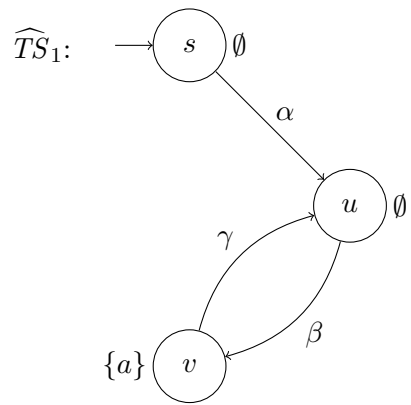
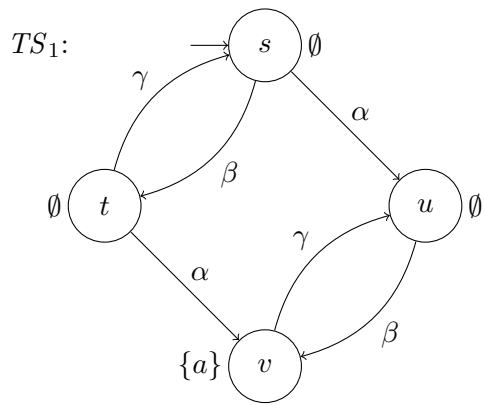
	α	β	γ	δ	τ
α	X	y	y	y*	y*
β		X	y*	n	n
γ			X	y*	y*
δ				X	y
τ					X

where y means “yes”, y^* means “yes, because they are never simultaneously enabled” and n means “no”.

Exercise 2

(3 points)

Consider the following four pairs $(TS_i, \widehat{TS}_i)$ of transition systems where $\widehat{TS}_i$ results from reducing TS_i using the appropriate ample sets. Check for each pair $(TS_i, \widehat{TS}_i)$ whether the two transitions systems are stutter trace equivalent and indicate **all** of the ample set conditions (A1)-(A4) that are violated.



Solution:

- TS_1 and $\widehat{TS}_1$: Obviously, the two transition systems are not stutter trace equivalent. While $\emptyset^\omega \in \text{Traces}(TS_1)$, the only trace in $\widehat{TS}_1$ is $\emptyset(\emptyset\{a\})^\omega$. (A3) is violated since $\text{ample}(s) = \{\alpha\} \neq \text{Act}(s)$, but α is not a stutter action.
- TS_2 and $\widehat{TS}_2$: The two transition systems are not stutter trace equivalent, since $\emptyset\emptyset\{a\}^\omega \in \text{Traces}(TS_1)$, but the only trace in $\widehat{TS}_2$ is $\emptyset^\omega$. Conditions (A2), (A3) and (A4) are violated. (A2) is violated (at s and u) since α and β are not independent. Hence, for example $s \xrightarrow{\beta} t$ is an execution fragment in TS violating (A2). (A3) is violated, because, e.g., α is not a stutter action and thus choosing $\text{ample}(s) = \{\alpha\}$ is illegal. (A4) is violated at u since α is in no ample set on the cycle $u \Rightarrow v \Rightarrow u$ in $\widehat{TS}_2$.
- TS_3 and $\widehat{TS}_3$: Actually, the two transition systems are stutter trace equivalent. However, choosing ample sets this way violates (A2) and (A3). γ and τ are not independent, so $t \xrightarrow{\gamma} v$ is a counterexample for (A2). (A3) is violated, since $\text{ample}(t) = \{\tau\} \neq \text{Act}(t)$, but τ is not a stutter action.
- TS_4 and $\widehat{TS}_4$: The two transition systems are not stutter trace equivalent. $(\emptyset\emptyset\{b\})^\omega \in \text{Traces}(TS_4)$, but the single trace $\emptyset\emptyset\{a\}^\omega \in \text{Traces}(\widehat{TS}_4)$ does not contain an $\{b\}$. Conditions (A2) and (A3) are violated. Much like for TS_3 and $\widehat{TS}_3$, γ and α are not independent, so $t \xrightarrow{\alpha} v$ is a counterexample for (A2) and γ is not a stutter action (and therefore (A3) is violated).

Exercise 3

(2 points)

For $1 \leq i \leq n$, let $TS_i = (S_i, \text{Act}_i, \rightarrow_i, I_i, AP, L_i)$ be an action-deterministic transition system such that $\text{Act}_i \cap \text{Act}_j \cap \text{Act}_k = \emptyset$ for $1 \leq i < j < k \leq n$. Consider the parallel composition with synchronization over common actions, i.e., the transition system

$$TS = TS_1 \parallel TS_2 \parallel \dots \parallel TS_n.$$

For each state $s = \langle s_1, \dots, s_n \rangle$ of TS , let $\text{Act}_i(s) = \text{Act}_i \cap \text{Act}(s)$ be the set of actions of TS_i that are enabled in s . Show that the dependency condition (A2) holds for all sets $\text{ample}(\cdot)$ if for each state s of TS the following two conditions hold:

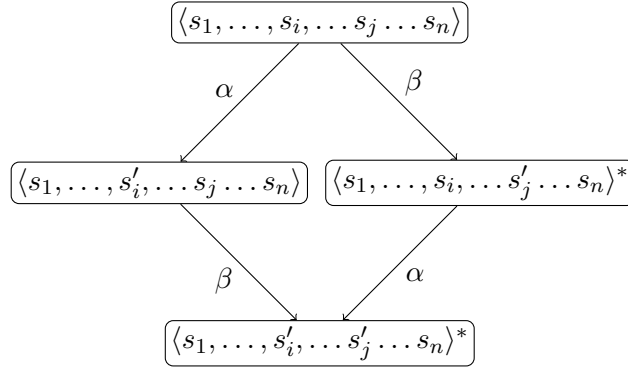
- (i) If $\text{ample}(s) \neq \text{Act}(s)$, then $\text{ample}(s) = \text{Act}_i(s)$ for some $i \in \{1, \dots, n\}$.
- (ii) If $\text{ample}(s) = \text{Act}_i(s) \neq \text{Act}(s)$ for some $i \in \{1, \dots, n\}$, then $\text{ample}(s) \cap \left(\bigcup_{\substack{1 \leq j \leq n \\ j \neq i}} \text{Act}_j \right) = \emptyset$.

Solution:

From (i) and (ii) it follows that

$$\begin{aligned} \text{ample}(s) = \text{Act}_i(s) \neq \text{Act}(s) &\implies \text{ample}(s) \cap \left(\bigcup_{\substack{1 \leq j \leq n \\ j \neq i}} \text{Act}_j \right) = \emptyset \\ &\implies \text{Act}_i(s) \cap \left(\bigcup_{\substack{1 \leq j \leq n \\ j \neq i}} \text{Act}_j \right) = \emptyset \\ &\implies \text{Act}_i(s) \cap \text{Act}_j = \emptyset \text{ for all } 1 \leq j \leq n, j \neq i \end{aligned}$$

Let $s = \langle s_1, \dots, s_n \rangle$ and $\alpha \in \text{Act}_i(s) = \text{ample}(s)$ and $\beta \in \text{Act}_j(s)$. According to the definition of parallel composition of transition systems (page 49 in the book), we have:



(*) Note that TS_j can synchronize with some other TS_k using β (so the state of TS_k may also change), but cannot change the state of TS_i .

Hence, we have that all actions $\alpha \in Act_i(s)$ are independent of $\bigcup_{\substack{1 \leq j \leq n \\ j \neq i}} Act_j$. In particular, this means that the antecedent of rule (A2) is never true, so the rule is by definition satisfied.

Exercise 4

(3 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 α and β where α or β (or both) is (are) a stutter action. Let *stutter permutation equivalence* $\cong_{perm}$ be the finest equivalence on Act^* such that

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

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

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

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

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

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

Solution:

In order to show that $\cong_{perm}^\omega$ is an equivalence, we need to prove transitivity, reflexivity and symmetry.

- **transitivity:** Let $\underbrace{\tilde{\alpha} \cong_{perm}^\omega \tilde{\beta}}_{(1)}$ and $\underbrace{\tilde{\beta} \cong_{perm}^\omega \tilde{\gamma}}_{(2)}$.

Assume that $\sqsubseteq_{perm}$ is transitive. Then from (1) and (2) we have $\tilde{\alpha} \sqsubseteq_{perm} \tilde{\beta}$, $\tilde{\beta} \sqsubseteq_{perm} \tilde{\gamma}$ and therefore $\tilde{\alpha} \sqsubseteq_{perm} \tilde{\gamma}$. $\tilde{\gamma} \sqsubseteq_{perm} \tilde{\alpha}$ follows analogously.

It remains to prove that $\sqsubseteq_{perm}$ is transitive. From $\tilde{\alpha} \sqsubseteq_{perm} \tilde{\beta}$, we get that for each finite prefix $\alpha_1\dots\alpha_n$ of $\tilde{\alpha}$ there exists a finite prefix $\beta_1\dots\beta_m$ of $\tilde{\beta}$, $m \geq n$ and a finite word $\bar{\delta}$ such that $\alpha_1\dots\alpha_n\bar{\delta} \cong_{perm} \beta_1\dots\beta_m$. Since $\tilde{\beta} \sqsubseteq_{perm} \tilde{\gamma}$, we know that there exists a finite prefix $\gamma_1\dots\gamma_k$ of $\tilde{\gamma}$, $k \geq m$ and a finite word $\bar{\delta}'$ such that $\beta_1\dots\beta_m\bar{\delta}' \cong_{perm} \gamma_1\dots\gamma_k$. But then $\gamma_1\dots\gamma_k$ is a prefix of $\tilde{\gamma}$, $k \geq n$ and $\bar{\delta}\bar{\delta}'$ is a finite word such that $\alpha_1\dots\alpha_n\bar{\delta}\bar{\delta}' \cong_{perm} \gamma_1\dots\gamma_k$. Therefore, $\tilde{\alpha} \sqsubseteq_{perm} \tilde{\gamma}$.

- **reflexivity:** Let $\tilde{\alpha} \in Act^\omega$.

Then for each finite prefix $\sigma = \alpha_1 \dots \alpha_n$ of $\tilde{\alpha}$ there exists another finite prefix σ' of $\tilde{\alpha}$, namely σ itself, such that $\sigma \cong_{\text{perm}} \sigma'$ since $\sigma \cong_{\text{perm}} \sigma$ (which holds since $\cong_{\text{perm}}$ is by definition an equivalence and hence reflexive). Therefore $\tilde{\alpha} \cong_{\text{perm}}^\omega \tilde{\alpha}$.

- **symmetry:**

$$\tilde{\alpha} \cong_{\text{perm}}^\omega \tilde{\beta} \Leftrightarrow \tilde{\alpha} \sqsubseteq_{\text{perm}} \tilde{\beta} \wedge \tilde{\beta} \sqsubseteq_{\text{perm}} \tilde{\alpha} \Leftrightarrow \tilde{\beta} \sqsubseteq_{\text{perm}} \tilde{\alpha} \wedge \tilde{\alpha} \sqsubseteq_{\text{perm}} \tilde{\beta} \Leftrightarrow \tilde{\beta} \cong_{\text{perm}}^\omega \tilde{\alpha}$$