



Tutorials for Verification
Exercise sheet 4

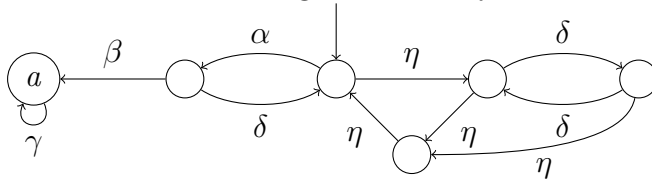
Exercise 1: Safety properties

Let TS and TS' be transition systems with terminal states. Prove or refute the equivalence of the following statements.

- (a) $Traces(TS) = Traces(TS')$
- (b) $TS \models P_{safe}$ iff $TS' \models P_{safe}$

Exercise 2: Fairness

Consider the following transition system:



Under which fairness assumptions \mathcal{F}_i does the system satisfy the property “eventually a ”? Justify your answer.

- $\mathcal{F}_1 = (\{\{\gamma\}\}, \emptyset, \emptyset)$
- $\mathcal{F}_2 = (\{\{\alpha\}, \{\gamma\}\}, \emptyset, \emptyset)$
- $\mathcal{F}_3 = (\{\{\alpha, \gamma\}\}, \emptyset, \emptyset)$
- $\mathcal{F}_4 = (\emptyset, \{\{\beta\}\}, \emptyset)$
- $\mathcal{F}_5 = (\emptyset, \{\{\alpha\}, \{\beta\}\}, \emptyset)$
- $\mathcal{F}_6 = (\emptyset, \{\{\alpha\}, \{\beta\}, \{\eta\}\}, \emptyset)$
- $\mathcal{F}_7 = (\emptyset, \emptyset, \{\{\alpha\}, \{\beta\}, \{\eta\}\})$
- $\mathcal{F}_8 = (\emptyset, \{\{\alpha\}, \{\beta\}\}, \{\{\eta\}\})$

Exercise 3: Fairness entailments

Let TS be a transition system and P a liveness property (over AP).

$$\begin{aligned} \mathcal{F}_0 &= (\emptyset, \emptyset, \emptyset) \\ \mathcal{F}_{w1} &= (\emptyset, \emptyset, \{\{\alpha, \beta\}\}) & \mathcal{F}_{w2} &= (\emptyset, \emptyset, \{\{\alpha\}, \{\beta\}\}) \\ \mathcal{F}_{s1} &= (\emptyset, \{\{\alpha, \beta\}\}, \emptyset) & \mathcal{F}_{s2} &= (\emptyset, \{\{\alpha\}, \{\beta\}\}, \emptyset) \\ \mathcal{F}_{u1} &= (\{\{\alpha, \beta\}\}, \emptyset, \emptyset) & \mathcal{F}_{u2} &= (\{\{\alpha\}, \{\beta\}\}, \emptyset, \emptyset) \end{aligned}$$

Prove or refute the following entailments:

- (a) $TS \models_{\mathcal{F}_0} P \Rightarrow TS \models_{\mathcal{F}_{w1}} P$
- (b) $TS \models_{\mathcal{F}_{w1}} P \Rightarrow TS \models_{\mathcal{F}_{w2}} P$
- (c) $TS \models_{\mathcal{F}_{w2}} P \Rightarrow TS \models_{\mathcal{F}_{w1}} P$
- (d) $TS \models_{\mathcal{F}_{w1}} P \Rightarrow TS \models_{\mathcal{F}_{s1}} P$
- (e) $TS \models_{\mathcal{F}_{s1}} P \Rightarrow TS \models_{\mathcal{F}_{s2}} P$
- (f) $TS \models_{\mathcal{F}_{s2}} P \Rightarrow TS \models_{\mathcal{F}_{s1}} P$
- (g) $TS \models_{\mathcal{F}_{s1}} P \Rightarrow TS \models_{\mathcal{F}_{u1}} P$
- (h) $TS \models_{\mathcal{F}_{s2}} P \Rightarrow TS \models_{\mathcal{F}_{u1}} P$
- (i) $TS \models_{\mathcal{F}_{u1}} P \Rightarrow TS \models_{\mathcal{F}_{u2}} P$
- (j) $TS \models_{\mathcal{F}_{u2}} P \Rightarrow TS \models_{\mathcal{F}_{u1}} P$

Exercise 4: Model checking regular safety properties

Let $AP = \{x = 2, crit_1\}$ and $\Sigma = 2^{AP}$. Let P_{safe} be the safety property “process 1 never enters its critical section from a state where $x = 2$ ”. Here entering the critical section means a transition from a state where $crit_1$ does not hold to a state where $crit_1$ holds.

- (a) Construct a NFA for the minimal bad prefixes of P_{safe} .
- (b) Apply the algorithm of the lecture to check whether $TS_{Pet} \models P_{safe}$ (TS_{Pet} denotes Petersen’s banking system). If the property does not hold give the counterexample that is returned by the algorithm.

Exercise 5: ω -regular expressions

- (a) Let $\Sigma = \{send, ack, idle\}$. Give ω -regular expressions for the following properties:
 - (i) There is no *ack* before the first *send*.
 - (ii) From some point on there is only *idle*.
 - (iii) There is a *send*, which is eventually followed by an *ack*.
 - (iv) There are only finitely many *sends*.
 - (v) There are infinitely many *ack*.
 - (vi) Every *send* is eventually followed by an *ack*. *Hint*: combine some of the previous properties.
- (b) Let E, E_1, E_2, F, F_1, F_2 be regular expressions with $\varepsilon \notin \mathcal{L}(F) \cup \mathcal{L}(F_1) \cup \mathcal{L}(F_2)$. Prove or disprove the following equivalences for ω -regular expressions:
 - (i) $(E_1 + E_2).F^\omega \equiv E_1.F^\omega + E_2.F^\omega$
 - (ii) $E.(F_1 + F_2)^\omega \equiv E.F_1^\omega + E.F_2^\omega$
 - (iii) $E.(F.F^*)^\omega \equiv E.F^\omega$
 - (iv) $(E^*.F)^\omega \equiv E^*.F^\omega$