Prof. Dr. Andreas Podelski
Dr. Matthias Heizmann
Christian Schilling

Delivery: December 5th, 2016
16:15 via the post boxes
Discussion: December 7th, 2016

# Tutorial for Cyber-Physical Systems - Discrete Models

## Exercise Sheet 7

**Exercise 1: Liveness properties** 2 Points

Let $P$ and $P'$ be liveness properties over $AP$. Prove or disprove the following claims:

(a) $P \cup P'$ is a liveness property.

(b) $P \cap P'$ is a liveness property.

Recall that we use the following definition. An LT property $E \subseteq (2^{AP})^\omega$ is a liveness property iff $\mathit{pref}(E) = (2^{AP})^+$.

**Exercise 2: LT properties** 3 Points

Recall Exercise 3 from Sheet 5. We considered six LT properties with $AP = \{a, b\}$.

(a) State for each of these properties which of them are invariants, which are safety properties, which are liveness properties, and which are neither.

(Hint: some properties fall into several classes.)

(b) For those properties $P$ which are neither a safety nor a liveness property, find a decomposition of $P = P_s \cap P_l$ into a safety and a liveness property. Use $\omega$-regular expressions to describe $P_s$ and $P_l$.

For your reference, we list the properties again below.

(i) Every state satisfies $a$ or $b$.

(ii) There is no state satisfying $b$ before the first occurence of $a$.

(iii) Every $a$ will be eventually followed by $b$.

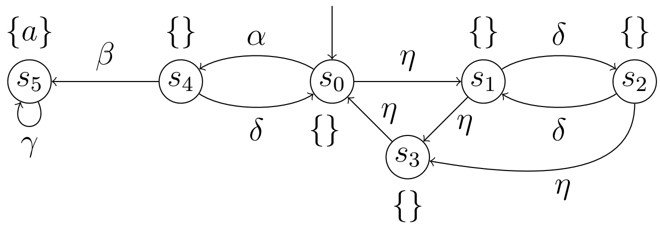
(iv) Exactly three states satisfy $a$.

(v) If there are infinitely many $a$, then there are infinitely many $b$.

(vi) There are only finitely many $a$.

**Exercise 3: Fairness** 2 Points

Consider the following transition system:




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

(a) $\mathcal{F}_1 = (\{\{\gamma\}\}, \emptyset, \emptyset)$

(b) $\mathcal{F}_2 = (\{\{\alpha\}, \{\gamma\}\}, \emptyset, \emptyset)$

(c) $\mathcal{F}_3 = (\{\{\alpha, \gamma\}\}, \emptyset, \emptyset)$

(d) $\mathcal{F}_4 = (\emptyset, \{\{\beta\}\}, \emptyset)$

(e) $\mathcal{F}_5 = (\emptyset, \{\{\alpha\}, \{\beta\}\}, \emptyset)$

(f) $\mathcal{F}_6 = (\emptyset, \{\{\alpha\}, \{\beta\}, \{\eta\}\}, \emptyset)$

(g) $\mathcal{F}_7 = (\emptyset, \emptyset, \{\{\alpha\}, \{\beta\}, \{\eta\}\})$

(h) $\mathcal{F}_8 = (\emptyset, \{\{\alpha\}, \{\beta\}\}, \{\{\eta\}\})$

*Note*: "eventually" is not to be confused with the German "eventuell".

**Exercise 4$^\star$: Invariant checking for infinite transition systems** 1 Point

In Exercise 3 on Sheet 6 we developed a breadth-first search algorithm for invariant checking of finite transition systems.

Now, we consider infinite transition systems. The algorithm does not terminate if the invariant is satisfied and there are infinitely many reachable states. In this exercise we analyze whether the algorithm still terminates if the invariant is *not* satisfied.

Let

$$TS_{\text{inf}}^{\neg\text{sat}} := \{(TS, \Phi) \mid TS \text{ is infinite and does not satisfy } \Phi\}$$

be the set of all such infinite transition systems together with an invariant that is not satisfied.

Does the algorithm always terminate for all transition systems and invariants in $TS_{\text{inf}}^{\neg\text{sat}}$? If not, state a sufficient but non-trivial restriction of $TS_{\text{inf}}^{\neg\text{sat}}$ such that the algorithm always terminates.