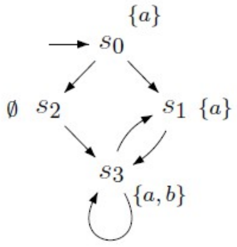
Software Validation and Verification
Second Exercise Sheet – Linear Time Properties

Exercise 1

Consider the transition system below and formally define its traces.



Exercise 2

Let $AP = \{a, b\}$ and let P be the LT property of all infinite words $\sigma = A_0A_1A_2 \cdots \in \left(2^{AP}\right)^\omega$ such that there exists $n \geq 0$ with $a \in A_i$ for $0 \leq i < n$, $\{a, b\} = A_n$ and $b \in A_j$ for infinitely many $j \geq 0$. Provide a decomposition $P = P_{safe} \cap P_{live}$ into a safety and into a liveness property.

Exercise 3

Recall the definition of AP-deterministic transition systems (cf. Series 1, Exercise 1). Let TS and TS′ be transition systems with the same set of atomic propositions AP. Prove the following relationship between trace inclusion and finite trace inclusion:

a) For AP-deterministic TS and TS′:

$$\mathit{Traces}(\mathsf{TS}) = \mathit{Traces}(\mathsf{TS}') \text{ if and only if } \mathit{Traces}_{\mathit{fin}}(\mathsf{TS}) = \mathit{Traces}_{\mathit{fin}}(\mathsf{TS}').$$

b) Give concrete examples of TS and TS′ where at least one of the transition systems is not AP-deterministic, and

$$\mathit{Traces}(\mathsf{TS}) \not\subseteq \mathit{Traces}(\mathsf{TS}') \quad \text{and} \quad \mathit{Traces}_{\mathit{fin}}(\mathsf{TS}) = \mathit{Traces}_{\mathit{fin}}(\mathsf{TS}').$$

Exercise 4

Consider the set AP of atomic propositions defined by $\text{AP} = \{x = 0, x > 1\}$ and consider a nonterminating sequential computer program P that manipulates the variable x.

a) Formulate the following informally stated properties as LT properties:

a) initially x differs from zero

b) initially x is equal to zero, but at some point x exceeds one

c) x exceeds one only finitely many times

d) x exceeds one infinitely often

e) the value of x alternates between zero and one

b) Determine which of the provided LT properties are safety properties? Which are liveness properties? Justify your answers by a formal argument.

Exercise 5

Let P denote the set of traces of the form $\sigma = A_0 A_1 A_2 \ldots \in \left(2^{AP}\right)^\omega$ such that

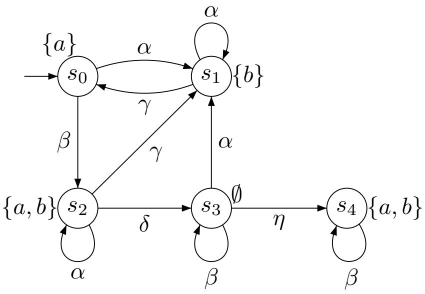
$$\overset{\infty}{\exists}\, k.\ A_k = \{a, b\} \quad \wedge \quad \exists n \geq 0.\ \forall k > n.\ \big(a \in A_k \Rightarrow b \in A_{k+1}\big).$$

Consider the following fairness assumptions with respect to the transition system TS outlined on the right:

1. $\mathcal{F}_1 = \big(\{\{\alpha\}\}, \{\{\beta\}, \{\delta, \gamma\}, \{\eta\}\}, \emptyset\big)$.
   Decide whether $TS \models_{\mathcal{F}_1} P$.

2. $\mathcal{F}_2 = \Big(\{\{\alpha\}\}, \{\{\beta\}, \{\gamma\}\}, \{\{\eta\}\}\Big)$.
   Decide whether $TS \models_{\mathcal{F}_2} P$.

Justify your answers!



α
$\{a\}$
α
s_0
s_1
$\{b\}$
γ
β
γ
α
$\emptyset$
$\{a,b\}$
s_2
δ
s_3
η
s_4
$\{a,b\}$
α
β
β