Introduction to Model Checking 2015:
Exercise 3.

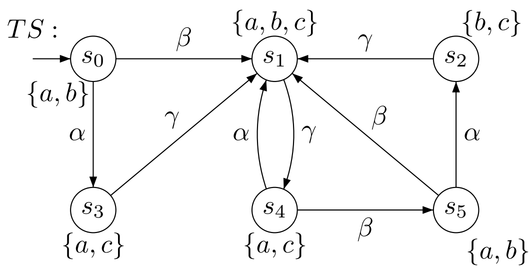
Supervised by: Dr. Prof. Joost-Pieter Katoen

Hand in before: 13th May | Assisted by: Dr. N. Jansen & S. Chakraborty

---

Exercise 1 *(2 Points)*

Consider the following transition system TS



and the regular safety property

$$P_{safe} = \begin{array}{c}\text{“always if } a \text{ is valid and } b \wedge \neg c \text{ was valid somewhere before,} \\ \text{then neither } a \text{ nor } b \text{ holds thereafter at least until } c \text{ holds”}\end{array}$$

As an example, it holds:

$$\begin{aligned}
\{b\}\emptyset\{a,b\}\{a,b,c\} &\in pref(P_{safe}) \\
\{a,b\}\{a,b\}\emptyset\{b,c\} &\in pref(P_{safe}) \\
\{b\}\{a,c\}\{a\}\{a,b,c\} &\in BadPref(P_{safe}) \\
\{b\}\{a,c\}\{a,c\}\{a\} &\in BadPref(P_{safe})
\end{aligned}$$

Questions:

1. *Define an NFA $\mathcal{A}$ such that $\mathcal{L}(\mathcal{A}) = MinBadPref(P_{safe})$.*
2. *Decide whether $TS \models P_{safe}$ using the $TS \otimes \mathcal{A}$ construction.*
   Provide a counterexample if $TS \not\models P_{safe}$.

Exercise 2 *(4 Points)*

Let us introduce the notion of quantitative fairness $\psi := \overset{\infty}{\underset{p}{\exists}}\varphi$, *where φ is a linear time property and p is a real number. We are not only interested in something happening (say φ) infinitely often, but also the frequency of the happenings, say p.*

For the sake of simplicity consider φ to be a atomic propositions (or their conjunctions). For a finite word x, let $\mathsf{freq}_\varphi(x)$ be the number of times φ is true in x. For example, $x = \{a\}\{b\}\{a\}\{c\}\{c\}\{c\}\{a\}\{c\}$, $\mathsf{freq}_a(x) = 3$.

For an infinite word w, let w_n be the finite prefix of length n, i.e., $w = w_n \cdot v$, where $|w_n| = n$ and $v \in \Sigma^\omega$. The semantics of quantitative fairness is as follows:

$$w \models \overset{\infty}{\underset{p}{\exists}}\varphi \quad \textit{iff} \quad \lim_{n\to\infty} \inf\left(\frac{1}{n}\mathsf{freq}_\varphi(w_n)\right) = p$$

For example, the word $w = a^\omega$ satisfies $\overset{\infty}{\underset{p}{\exists}} a$ with $p = 1$. Show the following:

1. *For any word w and letter a, $\lim\limits_{n\to\infty} \inf \dfrac{1}{n}\mathsf{freq}_a(w_n) \leq 1$.*
2. *Show that $\overset{\infty}{\underset{p}{\exists}} a$ with $p = 1$ is not same as $\overset{\infty}{\forall} a$. That is, find a word w such that $w \models \overset{\infty}{\underset{p}{\exists}} a$ and $w \not\models \overset{\infty}{\forall} a$.* [1]

---

[1] Recall $\overset{\infty}{\forall}$ is “for all, but finitely many ...” form lecture slides 7

3. *Show that if* $w \models \overset{\infty}{\underset{p}{\exists}} a$ *and* $w \models \overset{\infty}{\underset{p}{\exists}} b$*, where* a, b *are atomic proposition and* $p = 1$*, then* $w \models \overset{\infty}{\underset{p}{\exists}}(a \wedge b)$*.*

Exercise 3 *Consider a class of Transition systems imaginatively named as the* Lasso Transition systems *(LTS). These transition systems have the following property: The out-degree of states in a cycle of the TS is exactly one. The simple LTS ($T_{c,d}$) is shown in figure 1. The length of the path from $s_0 \rightsquigarrow s_l$ is c and the length of the loop ($s_l \rightsquigarrow s_l$) is $d+1$ (the number of distinct states in the loop is d).*

Let $L_{\varphi,d'}$ be a linear time property defined as follows:

$$L_{\varphi,d'} = \{w \in (2^{AP})^\omega \mid \textit{ if } w[i] \models \varphi \textit{ then } i \textit{ is a multiple of } d'\}$$

where φ is an atomic proposition. We want to model check a simple LTS $T_{c,d}$ (figure 1) where only state $s_l \models \varphi$, against $L_{\varphi,d'}$.

$$T_{c,d} \models L_{\varphi,d'}$$

The general algorithmic approach would be as follows:

- *Make a NFA for $\neg L^{fin}_{\varphi,d'}$. (Since $L^{fin}_{\varphi,d'} = \{w \in (2^{AP})^* \mid$ if $w[i] \models \varphi$ then i is a multiple of $d'\}$ is regular.) This is the set of BadPref of $L_{\varphi,d'}$*
- *Take the cross product of the said NFA with $T_{c,d}$.*
- *Check for empty-ness.*

Do the following:

1. *Show that the time complexity of model checking by the above procedure is $O(cd' + dd')$.*
2. *Find an algorithm that can decide $T_{c,d} \models L_{\varphi,d'}$ in time*

$$O(\log c \log d' + \log d \log d')$$

   (or even better).

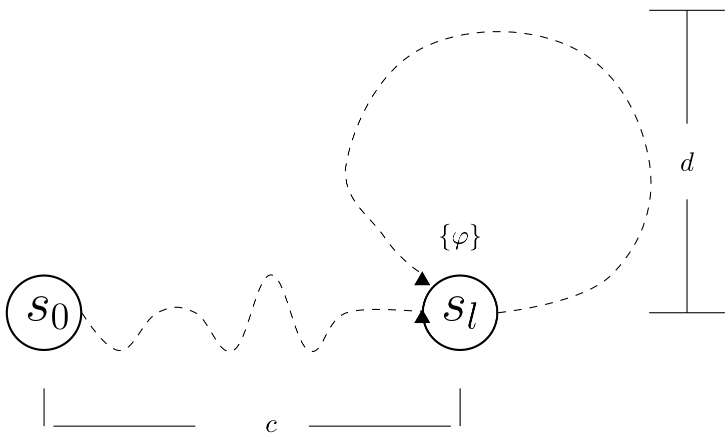


Figure 1: A simple lasso transition system $T_{c,d}$