Prof. Dr. Ir. Joost-Pieter Katoen

Sebastian Junges, Lutz Klinkenberg

Model Checking (Winter Term 2019/2020)

— Exercise Sheet 10 (due 31.01.2020) —

General Remarks

- The exercises are to be solved in groups of *three* students.
- You may hand in your solutions for the exercises just before the exercise class starts at 12:15 or by dropping them into the "Introduction to Model Checking" box at our chair *before 12:00*. Do *not* hand in your solutions via L2P or via e-mail.
- If a task asks you to justify your answer, an explanation of your reasoning is sufficient. If you are required to prove a statement, you need to give a *formal* proof.

Exercise 1 (Symbolic bisimulation): (1 point)

Let $\overline{x}, \overline{x}'$ and $\overline{b}$ be three vectors of Boolean variables of size $n > 0$ and let a_i denote the i-th variable in a vector $\overline{a}$. Assume that the transition relation of a transition system TS with state space $S = Eval(\overline{x})$ is given by means of a switching function $\Delta : Eval(\overline{x}, \overline{x}') \to \{0, 1\}$ (as seen in the lecture). Let $Q = \{B_0, \ldots, B_{2^n-1}\}$ be a partition of the state space ($S = \dot{\bigcup}_{i=0}^{2^n-1} B_i$ and $B_i = \emptyset$ is possible) represented as a switching function $f_Q : Eval(\overline{x}, \overline{b}) \to \{0, 1\}$ defined by

$$f_Q(s, B_i) = 1 \iff s \in B_i$$

(a) Using the available switching functions and the usual operations on them, define another switching function $f_{sig^Q} : Eval(\overline{x}, \overline{b}) \to \{0, 1\}$ given by

$$f_{sig^Q}(s, B_i) = 1 \iff \exists s' \in Post(s) : s' \in B_i$$

(b) Let the characteristic functions $\chi_{Sat(c)}(s)$ and $\chi_{Sat(d)}(s)$ for the only two atomic propositions $c, d \in AP$ in TS be given. Define a switching function $f_{Q^*} : Eval(\overline{x}, \overline{b}) \to \{0, 1\}$ that represents the partition $Q^* = \{\{s | L(s) = A\} | A \in 2^{AP}\}$, i.e., the coarsest partition that respects the labeling.

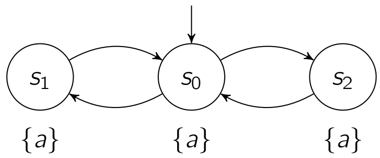
You may use the usual operations on switching functions as well as the "special" switching functions $i|_{\overline{b}} : Eval(\overline{b}) \to \{0, 1\}$ that evaluate to 1 if and only if the input is the binary encoding of the number i.

(c) Conceptually explain how the functions $f_Q(s, B_i)$ and $f_{sig^Q}(s, B_i)$ can be used to compute the coarsest bisimulation equivalence on TS.

Exercise 2 (Bounded paths): (1 point)

For LTL formula φ we write $TS \models_k \exists\varphi$ iff there exists a path $\pi \in Paths(TS)$ for which $\pi \models_k \varphi$. Notations like $TS \models_k \forall\varphi$ and $TS \models \exists\varphi$ are analogous.
Consider the transition system TS depicted below.
Determine all $k \geq 0$ for which the following holds.

a) $TS \models_k \forall\Box a$

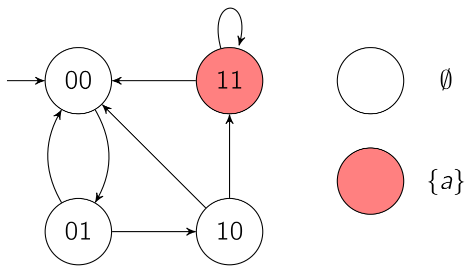


b) $TS \models_k \exists\Box a$

Justify your answers!

Exercise 3 (Bounded model checking): **(1 point)**

Perform bounded model checking on the following transition system TS.



(a) TS (b) Legend

(a) Let a state s be represented as $s = (s[0], s[1])$. Give the SAT representation of the transition relation $T(s, s')$, the initial state(s) $I(s)$ and the atomic proposition $a(s)$.

(b) Given the property $p := \Box(\neg a \vee \neg a)$ and the bound $k := 3$ generate the SAT encoding for the bounded model checking problem $[\![TS, \neg p]\!]_3$ by especially specifying:

- The unfolding of the transition relation: $[\![TS]\!]_3$
- The loop condition: L_3
- The translation for paths without loops: $[\![\neg p]\!]_3^0$
- The translation for paths with loops: ${}_\ell[\![\neg p]\!]_3^0$ (for variable ℓ)

(c) Try to find a satisfying assigment for the SAT encoding and give the resulting counterexample if one can be found.

Exercise 4 (Bounded semantics): **(1 point)**

Proof the following statements for finite transition systems TS without terminal states and LTL formulas of the form

$$\varphi ::= a \mid \neg a \mid \Box a \mid \Diamond a \mid a$$

where a is an atomic proposition.

a) For any $\pi \in Paths(TS)$ and $k \geq 0$ it holds that $\pi \models_k \varphi \implies \pi \models \varphi$.

b) If $TS \models \exists\varphi$ then there exists $k \geq 0$ with $TS \models_k \exists\varphi$.