Exam in *Principles of Model Checking*

Course number 192114100

Prof. Dr. Joost-Pieter Katoen

November 1, 2016, 08:45 – 11:15

Family name: ______________________________

First name: ______________________________

Student number: ______________________________

Please note the following hints:

- Keep your student id card ready.
- The only allowed materials are
  - a copy of the book,
  - a copy of the lecture slides.
  - a dictionary.

  Other materials (e.g., exercises, solutions, handwritten notes) are not admitted.
- Write your name and student number on every sheet.
- Write with blue or black ink; do not use a pencil.
- Any attempt at deception leads to failure for this exam, even if it is detected only later.
- The editing time is **150 minutes**.

Question	Possible	Received
1	10	
2	10	
3	10	
4	10	
5	10	
Total	50	
Grade		

Question 1

(10 points)

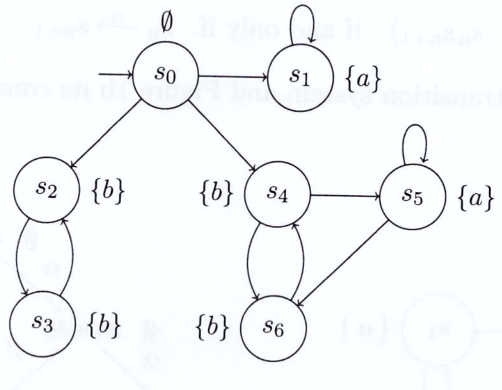
Let $\varphi = (\Diamond a) \cup b$ and $AP = \{ a, b \}$.
Questions:

(a) Give the elementary sets for φ. *Hint: There are 8 sets.*

(b) Use the algorithm from the lecture to construct the GNBA $\mathcal{G}_\varphi$ such that $\mathcal{L}_\omega(\mathcal{G}_\varphi) = \mathit{Words}(\varphi)$.
Hint: You can give the transitions in a list or tabular form.

Question 2

(10 points)



Consider the *TS* depicted above with the fairness assumption fair $= \Phi_1 \wedge \Phi_2$ where

$$\Phi_1 = \Box\Diamond\,(b \rightarrow \forall\bigcirc\, b)$$
$$\Phi_2 = \Box\Diamond\, a \rightarrow \Box\Diamond\, b$$

Hint: In the following, you may give the results of standard-CTL model checking queries directly.

Questions:

(a) Give $Sat_{\text{fair}}(\exists\Box\,\text{true})$.

(b) Decide whether

$$TS \models_{\text{fair}} \exists\bigcirc\,((\exists\Box\, b) \wedge (\neg\forall\Box\,\neg a))$$

using the model-checking algorithm for CTL with fairness from the lecture. *Provide all satisfaction sets you compute. Also provide intermediate results for any SCCs you consider during the computation.*

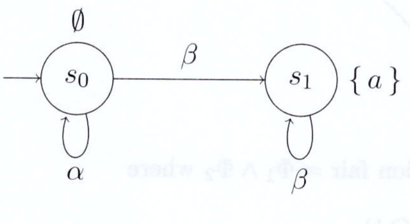
Question 3

(10 points)

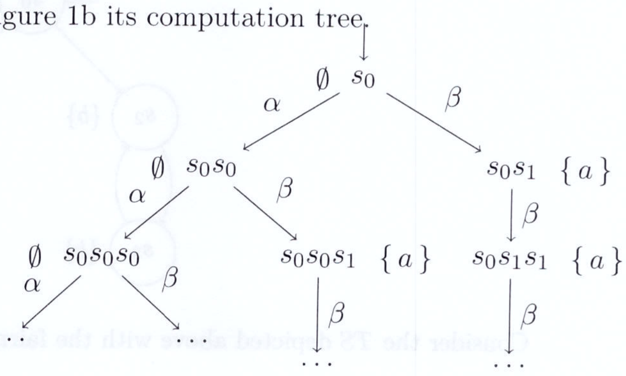
Let $TS = (S, Act, \rightarrow, s_0, AP, L)$ be a a (possibly infinitely branching) transition system with no terminal states. The *computation tree* of *TS* is the transition system $\text{CT}(TS) = (S^+, Act, \rightarrow_{\text{CT}}, s_0, AP, L_{\text{CT}})$ where

$$\langle s_0 s_1 \ldots s_n \rangle \xrightarrow{\alpha}_{\text{CT}} \langle s_0 s_1 \ldots s_n s_{n+1} \rangle \text{ if and only if } s_n \xrightarrow{\alpha} s_{n+1} \quad \text{and} \quad L_{\text{CT}}(s_0 s_1 \ldots s_n) = L(s_n).$$

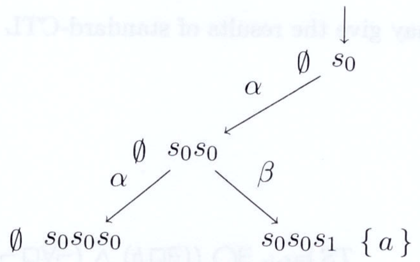
Figure 1a shows an example transition system and Figure 1b its computation tree.



(a) *TS*



(b) CT(*TS*)



(c) A prefix of CT(*TS*)

Figure 1

Let $\mathbb{T}$ denote the set of all computation trees and let Φ be a CTL state-formula. Then $TS \models \Phi$ if and only if $\text{CT}(TS) \models \Phi$. Hence, Φ defines a set of computation trees as follows

$$\mathcal{L}(\Phi) = \{ \text{CT}(TS) \in \mathbb{T} \mid TS \text{ is a transition system and } \text{CT}(TS) \models \Phi \}$$

A prefix of CT(*TS*) is the restriction of CT(*TS*) to a **finite** set of states $S_{\text{fin}} \subseteq S^+$ with

$$S_{\text{fin}} \neq \emptyset \quad \text{and} \quad s_0 s_1 \ldots s_n \in S_{\text{fin}} \text{ implies } s_0 s_1 \ldots s_{n-1} \in S_{\text{fin}}$$

Figure 1c shows one (of the infinitely many) prefix(es) of the computation tree in Figure 1b. Let $\textit{pref}(t)$ denote the set of prefixes of a computation tree t. For a set of computation trees T, we let $\textit{pref}(T) = \bigcup_{t \in T} \textit{pref}(t)$ and define the *closure* of T by $\textit{tcl}(T) = \{ t \in \mathbb{T} \mid \textit{pref}(t) \subseteq \textit{pref}(T) \}$. Then, by definition

(i) T is a (branching-time) *safety property* if and only if $\textit{tcl}(T) = T$, and

(ii) T is a (branching-time) *liveness property* if and only if $\textit{tcl}(T) = \mathbb{T}$

Questions:

(a) Prove that for all CTL formulas Φ for which $\mathcal{L}(\Phi)$ is both a safety and a liveness property, $\Phi \equiv \textit{true}$.

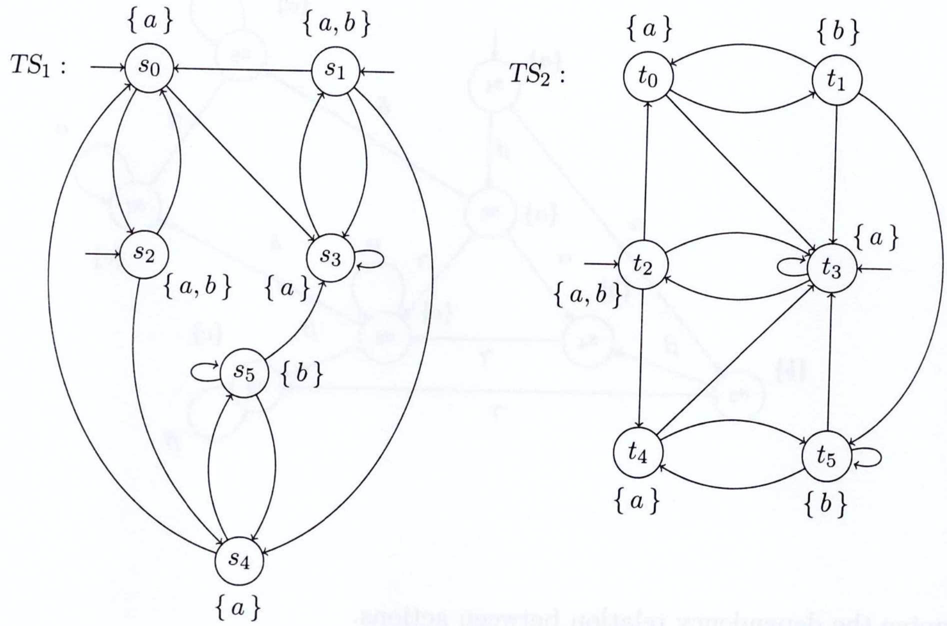
(b) Prove that for the CTL formula $\Phi = \forall \Diamond a$, $\mathcal{L}(\Phi)$ **is** a liveness property.

(c) Prove that for the CTL formula $\Phi' = \exists \Box a$, $\mathcal{L}(\Phi')$ is **not** a safety property.

Question 4

(10 points)

Let the two transition systems TS_1 and TS_2 be given as follows.



<u>Questions:</u>

(a) Determine $TS_1/\sim$ and provide the relation $\sim$.

(b) Prove or disprove $TS_1 \sim TS_2$.

(c) Consider the LTL formula

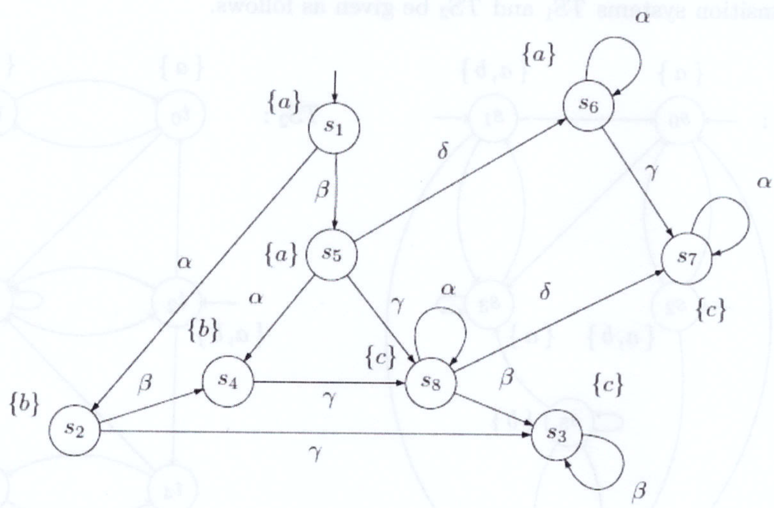
$$\varphi = \Box\Diamond\,(a \wedge b) \;\rightarrow\; \Diamond\Box\,(a \vee \neg b).$$

State whether $TS_1 \models \varphi$ and whether $TS_2 \models \varphi$. Briefly explain your answers.

Question 5

(10 points)

Consider the transition system depicted below:



Questions:

(a) Determine the dependency relation between actions.

(b) Determine which actions are stutter actions.

(c) Show that the following ample-set suggestion is incorrect: $ample(s_1) = \{\beta\}$, $ample(s_3) = \{\beta\}$, $ample(s_4) = \{\gamma\}$, $ample(s_5) = \{\alpha, \delta\}$, $ample(s_6) = \{\alpha\}$, $ample(s_8) = \{\beta\}$ and for the remaining states s_2 and s_7 the ample-set is empty.

(d) Provide the minimal ample sets that are correct.