



Exam in *Introduction to Model Checking* for
Bachelor of Science, Master of Science and Diploma students
February 17, 2014

Solution

Question 1

(5 + 5 points)

Let P be an LT property. Further let $P_{\text{safe}} = \text{closure}(P)$ be a safety property. Prove:

- (a) Every bad prefix of P_{safe} is also a bad prefix of P .
- (b) Every bad prefix of P is also a bad prefix of P_{safe} .

Hint: one way to prove this, is to assume the contrary and deduce a contradiction.

Solution: _____

(a)

$$\begin{aligned}
 & \hat{\sigma} \in \text{BadPref}(P_{\text{safe}}) \\
 \iff & P_{\text{safe}} \cap \{\sigma \in (2^{AP})^\omega \mid \hat{\sigma} \sqsubseteq \sigma\} = \emptyset \\
 \iff & \text{closure}(P) \cap \{\sigma \in (2^{AP})^\omega \mid \hat{\sigma} \sqsubseteq \sigma\} = \emptyset \\
 \stackrel{*}{\Rightarrow} & P \cap \{\sigma \in (2^{AP})^\omega \mid \hat{\sigma} \sqsubseteq \sigma\} = \emptyset \\
 \iff & \hat{\sigma} \in \text{BadPref}(P)
 \end{aligned}$$

where (*) is the fact that for any LT property Q it holds that $Q \subseteq \text{closure}(Q)$.

(b) We have to show that

$$P \cap \{\sigma \in (2^{AP})^\omega \mid \hat{\sigma} \sqsubseteq \sigma\} = \emptyset \quad (1)$$

$$\Rightarrow \text{closure}(P) \cap \{\sigma \in (2^{AP})^\omega \mid \hat{\sigma} \sqsubseteq \sigma\} = \emptyset . \quad (2)$$

Therefore assume this is not true. Then

$$P \cap \{\sigma \in (2^{AP})^\omega \mid \hat{\sigma} \sqsubseteq \sigma\} = \emptyset \quad (3)$$

$$\text{and } \text{closure}(P) \cap \{\sigma \in (2^{AP})^\omega \mid \hat{\sigma} \sqsubseteq \sigma\} \neq \emptyset . \quad (4)$$

Then the intersection in (2) contains at least one trace σ' . By definition of *closure*, equation (4) can then be written as

$$\{\sigma \in (2^{AP})^\omega \mid \text{pref}(\sigma) \subseteq \text{pref}(P)\} \cap \{\sigma \in (2^{AP})^\omega \mid \hat{\sigma} \sqsubseteq \sigma\} \supseteq \{\sigma'\} .$$

From this we see that *every* prefix $\hat{\sigma}$ of σ' must also be a prefix of P . Thus it cannot be a bad prefix of P which contradicts (3). Hence the assumption is wrong and the statement is true.

Question 2

(3 + 5 + 2 points)

- (a) Prove or disprove that the following two LTL formula are equivalent: $\Diamond \bigcirc a \equiv \bigcirc \Diamond a$.
- (b) Show there is **no** equivalent LTL formula for the CTL formula $\forall \Diamond \forall \bigcirc a$.
- (c) Assume we know that $\forall \bigcirc \forall \Diamond a \equiv \bigcirc \Diamond a$ which means that for all transition systems TS :

$$TS \models_{CTL} \forall \bigcirc \forall \Diamond a \iff TS \models_{LTL} \bigcirc \Diamond a .$$

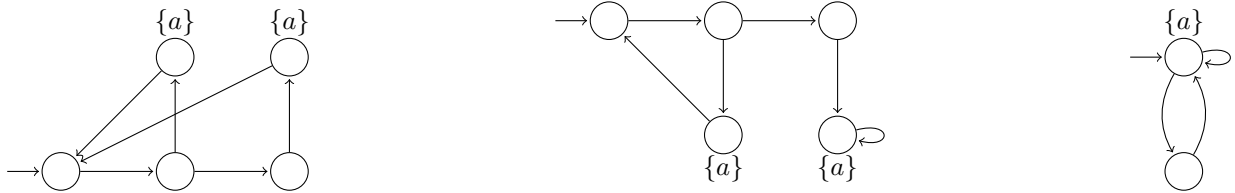
Based on this assumption and the results above argue whether the two CTL formulas $\forall \Diamond \forall \bigcirc a$ and $\forall \bigcirc \forall \Diamond a$ are equivalent.

Solution: _____

(a)

$$\begin{aligned}
 \sigma \models \Diamond \bigcirc a &= \{\sigma \in (2^{AP})^\omega \mid \exists j \geq 0 : \sigma[j..] \models \bigcirc a\} \\
 &= \{\sigma \in (2^{AP})^\omega \mid \exists j \geq 0 : \sigma[j+1..] \models a\} \\
 &= \{\sigma \in (2^{AP})^\omega \mid \exists j \geq 1 : \sigma[j..] \models a\} \\
 &= \{\sigma \in (2^{AP})^\omega \mid \sigma[1..] \models \Diamond a\} \\
 &= \sigma \models \bigcirc \Diamond a
 \end{aligned}$$

- (b) According to Draghicescu/Clarke we know that if there is an equivalent LTL formula for $\Phi = \forall \Diamond \forall \bigcirc a$, it must be $\varphi = \Diamond \bigcirc a$. However we can find a transition system TS such that $TS \models \varphi$ and $TS \not\models \Phi$:



So no equivalent LTL formula exists!

(c)

$$\begin{aligned}
 \forall \bigcirc \forall \Diamond a &\stackrel{\text{assumption}}{\equiv} \bigcirc \Diamond a \\
 &\stackrel{a)}{\equiv} \Diamond \bigcirc a \\
 &\stackrel{b)}{\not\equiv} \forall \Diamond \forall \bigcirc a
 \end{aligned}$$

Question 3

(1 + 3 + 6 points)

Let $\psi = (\Box a) \cup b$ and $AP = \{a, b\}$.

- (a) Transform ψ into an equivalent basic LTL-formula φ . The basic LTL syntax is given by the following context free grammar:

$$\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc \varphi \mid \varphi_1 \cup \varphi_2$$

- (b) Compute all elementary sets with respect to $\text{closure}(\varphi)$

Hint: There are 7 elementary sets.

- (c) Use the algorithm from the lecture to construct the GNBA $\mathcal{G}_\varphi$ with $\mathcal{L}_\omega(\mathcal{G}_\varphi) = \text{Words}(\varphi)$. Therefore
- define its set of initial states and its acceptance component,
 - and for each elementary set B , define $\delta(B, B \cap AP)$.

Solution: _____

- (a) Let $\psi = (\Box a) \cup b$ and $AP = \{a, b\}$.

First we transform ψ into the equivalent basic LTL-formula φ :

$$\begin{aligned} \psi &= (\Box a) \cup b \\ &= (\neg \Diamond \neg a) \cup b \\ &= (\neg(\text{true} \cup \neg a)) \cup b \\ &= \varphi \end{aligned}$$

- (b) Now we compute $\text{closure}(\varphi)$ (optional):

$$\begin{aligned} \text{closure}(\varphi) = \{ &\text{true}, \text{false}, a, \neg a, b, \neg b, \\ &\text{true} \cup \neg a, \neg(\text{true} \cup \neg a), \\ &\varphi, \neg\varphi \} \end{aligned}$$

The elementary sets are:

	true	a	b	$\text{true} \cup \neg a$	φ
B_1	1	0	0	1	0
B_2	1	0	1	1	1
B_3	1	1	0	0	0
B_4	1	1	1	0	1
B_5	1	1	0	1	0
B_6	1	1	1	1	1
B_7	1	1	0	0	1

- (c) The GNBA $\mathcal{G}_\varphi = (Q, \Sigma, \delta, Q_0, \mathcal{F})$ is defined by:

$$\begin{aligned} Q &= \{B_1, B_2, B_3, B_4, B_5, B_6, B_7\} \\ \Sigma &= 2^{\{a, b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\} \\ Q_0 &= \{B_2, B_4, B_6, B_7\} \\ \mathcal{F} &= \{F_{\text{true} \cup \neg a}, F_\varphi\} \\ F_{\text{true} \cup \neg a} &= \{B_1, B_2, B_3, B_4, B_7\} \\ F_\varphi &= \{B_1, B_2, B_3, B_4, B_5, B_6\} \end{aligned}$$

The transition relation δ is given by the following table:

from \ to	B_1	B_2	B_3	B_4	B_5	B_6	B_7
B_1	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
B_2	$\{b\}$	$\{b\}$	$\{b\}$	$\{b\}$	$\{b\}$	$\{b\}$	$\{b\}$
B_3			$\{a\}$				
B_4			$\{a, b\}$	$\{a, b\}$			$\{a, b\}$
B_5	$\{a\}$	$\{a\}$			$\{a\}$	$\{a\}$	
B_6	$\{a, b\}$	$\{a, b\}$			$\{a, b\}$	$\{a, b\}$	
B_7				$\{a\}$			$\{a\}$

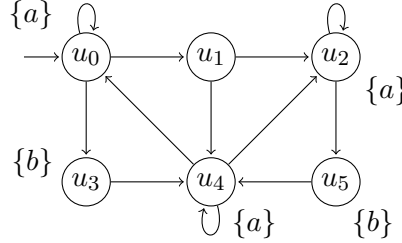
Question 4

(2 + 1 + 6 + 1 points)

Decide if $TS \models_{fair} \Phi$ for the CTL-formula Φ and the fairness assumption $fair$:

$$\Phi = \forall \square (a \rightarrow (\exists \bigcirc a \wedge \forall \diamond b))$$

$$fair = (\square \diamond (\neg a \wedge \neg b) \rightarrow \square \diamond b) \wedge (\diamond \square a \rightarrow \square \diamond b)$$

where TS over $AP = \{a, b\}$ is given by:

Proceed in the following steps:

- (a) Determine
- $Sat_{fair}(\exists \square \text{true})$
- .

Therefore give reachable strongly connected node sets that satisfy the fairness assumption.

- (b) Rewrite
- Φ
- into
- Ψ
- in existential normal form.

- (c) Determine
- $Sat_{fair}(\Psi)$
- .

Therefore determine $Sat_{fair}(\dots)$ for all subformulas starting with the smallest. You may give these sets directly but when determining $Sat_{fair}(\exists \square \Upsilon)$, give G_Υ , its SCCs and check fairness.

- (d) Decide
- $TS \models_{fair} \Phi$
- .

Solution: _____

- (a) First check the state formulae of the fairness assumptions (trivial here).

Next find all the state in which the fairness assumption is realisable and label those with a_{fair} . Consider the strongly connected node set $D = \{u_0, u_3, u_4\}$ (or analogously $\{u_2, u_5, u_4\}$): We have that $D \cap Sat(b) \neq \emptyset$ and hence the consecution of both fairness constraints is satisfied. Furthermore D is reachable from every state. Thus $Sat_{fair}(\exists \square \text{true}) = S$. Hence label all states with a_{fair} .

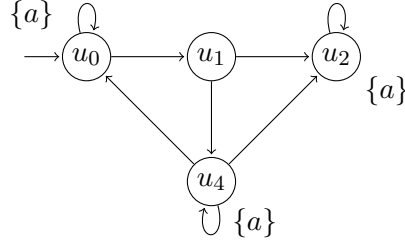
- (b)

$$\begin{aligned} \Phi &= \forall \square (a \rightarrow (\exists \bigcirc a \wedge \forall \diamond b)) \\ &\equiv \neg \exists \diamond \neg (a \rightarrow (\exists \bigcirc a \wedge \forall \diamond b)) \\ &\equiv \neg \exists \diamond \neg (\neg a \vee (\exists \bigcirc a \wedge \forall \diamond b)) \\ &\equiv \neg \exists \diamond (a \wedge (\neg \exists \bigcirc a \vee \neg \forall \diamond b)) \\ &\equiv \neg \exists \diamond (a \wedge (\neg \exists \bigcirc a \vee \exists \square \neg b)) \\ &= \Psi . \end{aligned}$$

- (c)
- $Sat_{fair}(a) = Sat(a \wedge a_{fair}) = \{u_0, u_2, u_4\}$
 - $Sat_{fair}(b) = Sat(b \wedge a_{fair}) = \{u_3, u_5\}$

- $Sat_{fair}(\neg b) = S \setminus Sat_{fair}(b) = \{u_0, u_1, u_2, u_4\}$
- $Sat_{fair}(\exists \bigcirc a) = Sat(\exists \bigcirc (a \wedge a_{fair})) = \{u_0, u_1, u_2, u_3, u_4, u_5\}$
- $Sat_{fair}(\neg \exists \bigcirc a) = S \setminus Sat_{fair}(\exists \bigcirc a) = \emptyset$
- $Sat_{fair}(\exists \Box \neg b) = \dots$

Digraph $G_{\neg b}$:



There two (non-trivial) SCCs: $C_1 = \{u_0, u_1, u_4\}$ and $C_2 = \{u_2\}$.

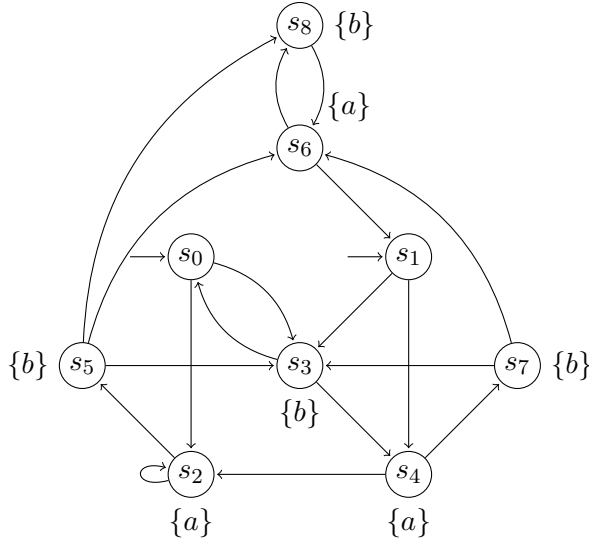
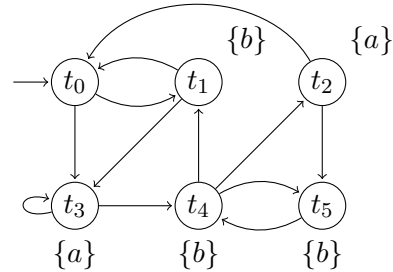
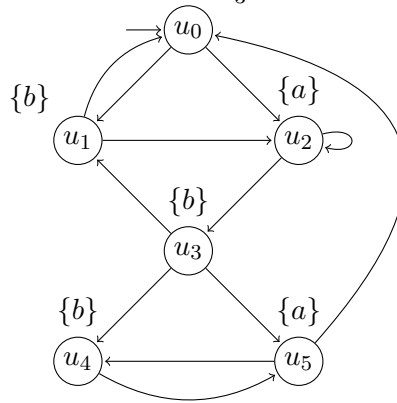
None of them satisfy the fairness assumption! Hence, $Sat_{fair}(\exists \Box \neg b) = \emptyset$.

- $Sat_{fair}(\neg \exists \bigcirc a \vee \exists \Box \neg b) = \emptyset$
- $Sat_{fair}(a \wedge (\neg \exists \bigcirc a \vee \exists \Box \neg b)) = \emptyset$
- $Sat_{fair}(\exists \Diamond (a \wedge (\neg \exists \bigcirc a \vee \exists \Box \neg b))) = \emptyset$
- $Sat_{fair}(\Psi) = S$

(d) Since $\Phi \equiv \Psi$, we have that $Sat_{fair}(\Phi) = Sat_{fair}(\Psi) = S \supseteq I$. And therefore $TS \models_{fair} \Phi$.

Question 5

(4 + 4 + 2 points)

Consider the three transition systems over $AP = \{a, b\}$: TS_1 : TS_2 : TS_3 :

- (a) Decide whether $TS_1 \sim TS_2$. In case the systems are bisimilar provide a bisimulation relation, otherwise give a distinguishing CTL formula.
- (b) Decide whether $TS_1 \sim TS_3$. In case the systems are bisimilar provide a bisimulation relation, otherwise give a distinguishing CTL formula.
- (c) Based on your answers to questions a) and b), give an argument whether $TS_2 \sim TS_3$.

Solution: _____

- (a) $TS_1 \not\sim TS_2$. A distinguishing CTL formula is:

$$\Phi = \exists \Diamond (b \rightarrow \exists \Box b)$$

or

$$\Phi = \exists \bigcirc (a \wedge \exists \bigcirc (b \wedge \exists \bigcirc (b \wedge \exists \bigcirc b)))$$

And we have $TS_1 \not\models \Phi$ but $TS_2 \models \Phi$.

- (b) $TS_1 \not\sim TS_3$. A distinguishing CTL formula is:

$$\Phi = \exists \bigcirc (b \wedge \exists \bigcirc (a \wedge \exists \bigcirc (b \wedge \exists \bigcirc (b \wedge \exists \bigcirc (a \wedge \exists \bigcirc (\neg a \wedge \neg b))))))$$

And we have $TS_1 \not\models \Phi$ but $TS_3 \models \Phi$.

- (c) From the discovered facts $TS_1 \not\sim TS_2$ and $TS_1 \not\sim TS_3$ no conclusion can be made. However the systems are not bisimilar which can be seen with the help of the CTL formula from part a).