RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

LEHRSTUHL FÜR INFORMATIK 2

RWTH Aachen · D-52056 Aachen · GERMANY

Winter term 2008/09

Prof. Dr. Ir. J.-P. Katoen

Exam in *Model Checking*

February 27, 2009

Solution

Solution 1 (10 points)

Let P and P' be safety properties. Prove that $\mathit{BadPref}(P) \cap \mathit{BadPref}(P') = \mathit{BadPref}(P \cup P')$.
Solution:

$$\begin{aligned}
\hat{\sigma} \in \mathit{BadPref}(P) \cap \mathit{BadPref}(P') &\iff P \cap \left\{\sigma' \in \left(2^{AP}\right)^{\omega} \mid \hat{\sigma} \in \mathit{pref}(\sigma')\right\} = \emptyset \\
&\quad\wedge P' \cap \left\{\sigma' \in \left(2^{AP}\right)^{\omega} \mid \hat{\sigma} \in \mathit{pref}(\sigma')\right\} = \emptyset \\
&\iff \left(P \cup P'\right) \cap \left\{\sigma' \in \left(2^{AP}\right)^{\omega} \mid \hat{\sigma} \in \mathit{pref}(\sigma')\right\} = \emptyset \\
&\iff \hat{\sigma} \in \mathit{BadPref}(P \cup P').
\end{aligned}$$

Solution 2 (5 + 4 + 1 points)

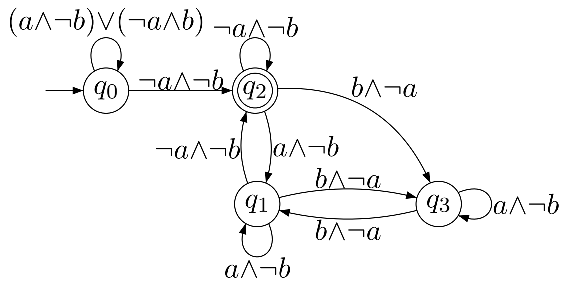
Consider the linear-time property P over $AP = \{a, b\}$:

"$(\neg a \wedge \neg b)$ holds infinitely often and $(a \wedge b)$ never holds and
between any two occurrences of $(\neg a \wedge \neg b)$, the number of states where b holds is even."

1. Provide an NBA $\mathcal{A}$ over 2^{AP} such that $\mathcal{L}_\omega(\mathcal{A}) = P$.
   Hint: Parts (b) and (c) can be solved without a solution for part (a).
2. Formally prove or disprove the following statements:
   - P is a safety property.
   - P is a liveness property.
3. Let $\mathcal{A}'$ be an NBA over 2^{AP}. Then $P' = \mathcal{L}_\omega(\mathcal{A}')$ is the linear-time property defined by $\mathcal{A}'$.
   Is it always the case that there exists an LTL-formula φ such that $P' = Words(\varphi)$?
   Justify your answer!

Solution:

1. An NBA $\mathcal{A}$ over 2^{AP} with $\mathcal{L}_\omega(\mathcal{A}) = P$ is depicted below:



2. P can be characterized by the ω-regular expression E derived as follows:

$$L_{q_0,q_2} = (\{a\} + \{b\})^\star.\emptyset$$
$$L_{q_2,q_2} = (\{b\}.\{a\}^\star.\{b\}.\{a\}^\star)^\star.\emptyset$$
$$E = L_{q_0,q_2}.L^\omega_{q_2,q_2} = \big(\{a\} + \{b\}\big)^\star.\Big(\emptyset.\big(\{b\}.\{a\}^\star.\{b\}.\{a\}^\star\big)^\star\Big)^\omega.$$

   We disprove that P is

   - a safety property: $\sigma = \emptyset\{a\}^\omega \in \big(2^{AP}\big)^\omega \setminus P$. Note that for all $\hat{\sigma} \in pref\,(\emptyset\{a\}^\omega)$ it holds that $\hat{\sigma}.\emptyset^\omega \in P$. Thus no bad prefix exists for σ and P is not a safety property.
   - a liveness property: $\{a, b\} \notin pref(P)$. Hence $pref(P) \neq \big(2^{AP}\big)^\star$.

3. No. LTL is strictly less expressive than the class of ω-regular languages. See Remark 5.43.

Solution 3 (4 + 4 + 2 points)

Let $\varphi = (a \wedge \bigcirc a) \mathsf{U} (a \wedge \neg \bigcirc a)$ be an LTL–formula over $AP = \{a\}$.

1. Compute all elementary sets with respect to φ.
2. Construct the GNBA $\mathcal{G}_\varphi$ according to the algorithm from the lecture such that $\mathcal{L}_\omega(\mathcal{G}_\varphi) = \mathit{Words}(\varphi)$.
3. Give an ω-regular expression E such that $\mathcal{L}_\omega(\mathcal{G}_\varphi) = \mathcal{L}_\omega(E)$.

Solution:

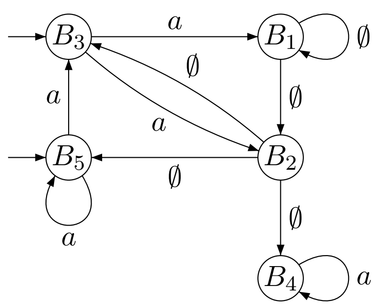
1. The elementary sets are:

	a	$\bigcirc a$	$a \wedge \bigcirc a$	$a \wedge \neg \bigcirc a$	φ
B_1	0	0	0	0	0
B_2	0	1	0	0	0
B_3	1	0	0	1	1
B_4	1	1	1	0	0
B_5	1	1	1	0	1

2. The GNBA $\mathcal{G}_\varphi = \left(Q, 2^{AP}, \delta, Q_0, \mathcal{F}\right)$ is defined by:

$$Q = \{B_1, B_2, B_3, B_4, B_5\}$$
$$Q_0 = \{B_3, B_5\}$$
$$\mathcal{F} = \{F_\varphi\}$$
$$F_\varphi = \{B_1, B_2, B_3, B_4\}$$

The transition relation δ is given by the following graph:



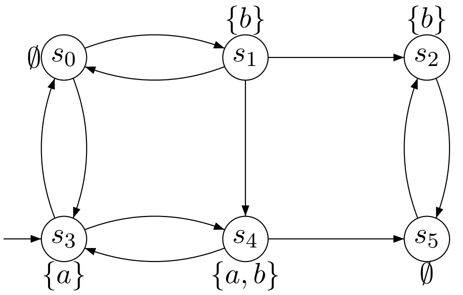
3. We derive $\mathcal{L}_\omega(\mathcal{G}_\varphi) = \mathit{Words}(\varphi) = \{a\}^+ \emptyset \left(2^{AP}\right)^\omega$.

Solution 4 (3 + 4 + 3 points)

Compute $Sat_{sfair}(\Phi)$ for the CTL-formula Φ and the strong fairness assumption *sfair*:

$$\Phi = \exists\Box a$$
$$sfair = \Box\Diamond a \rightarrow \Box\Diamond\exists\,(\neg a)\,\mathsf{U}\,(\forall\bigcirc b)$$

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



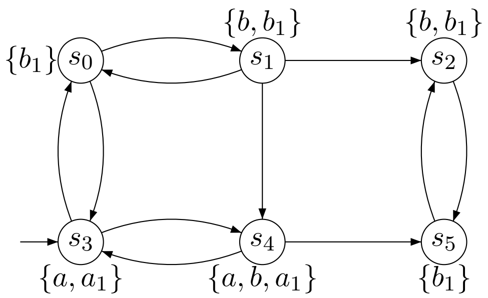
Proceed in the following steps:

1. Determine $Sat\,(\exists\,(\neg a)\,\mathsf{U}\,(\forall\bigcirc b))$ (without fairness).
2. Determine $Sat_{sfair}(\exists\Box\,\mathsf{true})$.
3. Determine $Sat_{sfair}(\Phi)$.

Solution:

1. $Sat(\exists(\neg a)\mathsf{U}(\forall\bigcirc b))$:
   Consider the state subformula $\forall\bigcirc b$. Then $Sat(\forall\bigcirc b) = \{s_5\}$.
   Further, $Sat(\neg a) = \{s_0, s_1, s_2, s_5\}$.
   Using the backward search starting in s_5 we derive $Sat(\exists(\neg a)\mathsf{U}(\forall\bigcirc b)) = \{s_0, s_1, s_2, s_5\}$.

   Now we relabel states in $Sat(a)$ with a_1 and those in $Sat(\exists(\neg a)\mathsf{U}(\forall\bigcirc b))$ with b_1 to encode the strong fairness constraint in the transition system:

2. Compute $Sat_{sfair}(\exists\Box\mathsf{true})$:

   - The SCCs of $G[\mathsf{true}]$ of $TS[\mathsf{true}]$ are:

   $$C_1 = \{s_0, s_3\} \qquad C_2 = \{s_0, s_1\}$$
   $$C_3 = \{s_3, s_4\} \qquad C_4 = \{s_2, s_5\}$$
   $$C_{1,2} = \{s_0, s_1, s_3\} \qquad C_{1,3} = \{s_0, s_3, s_4\}$$
   $$C_{1,2,3} = \{s_0, s_1, s_3, s_4\}$$

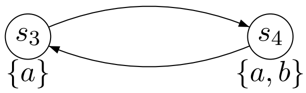
   Then $T = \{C_1, C_2, C_{1,2}, C_{1,2,3}, C_4\}$. Some examples for this:
   - $C_3 \notin T$ because $C_3 \cap Sat(a) = \{s_3\}$ but $C_3 \cap Sat(\exists(\neg a)\mathsf{U}(\forall\bigcirc b)) = \emptyset$.

- $C_1 \in T$ because $C_1 \cap Sat(a) = \{s_3\}$ and also $C_1 \cap Sat(\exists(\neg a)\mathsf{U}(\forall \bigcirc b)) = \{s_0\}$.

Then $Sat_{sfair}(\exists\Box\mathsf{true}) = \{s \in S \mid Reach_{TS}(s) \cap \bigcup T \neq \emptyset\} = S$.
Extend the labeling accordingly by a fresh atomic proposition a_{fair} (omitted here).

3. Compute $Sat_{fair}(\exists\Box a)$:

   - Then $G[a]$ of $TS[a]$ is the graph

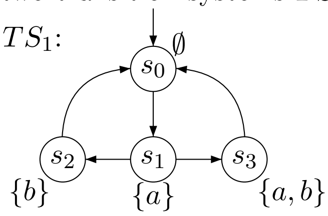


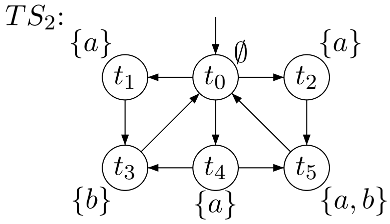
Further, there is only one SCC in $G[a]$: $C_3 = \{s_3, s_4\}$. But as $C_3 \notin T$ — C_3 satisfies a_1 infinitely often, but never b_1 — it is not fair. Hence $Sat_{sfair}(\exists\Box a) = \emptyset$.

Solution 5a

((2 + 1) + (3 + 3 + 1) points)

Consider the two transition systems TS_1 and TS_2:





1. Prove or disprove $TS_1 \sim TS_2$.

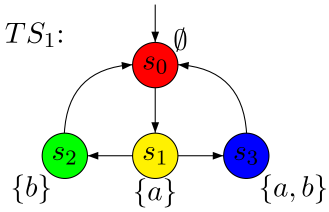
2. Prove or disprove $TS_1 \simeq TS_2$.

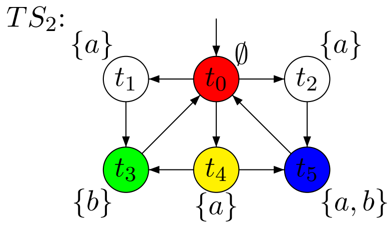
Solution:

1. $TS_1 \not\sim TS_2$:
   A distinguishing CTL-formula is $\forall\Box\,(a \rightarrow \exists\bigcirc\,(a \wedge b))$.
   Then $TS_1 \models \Phi$ and $TS_2 \not\models \Phi$ (because of t_1).

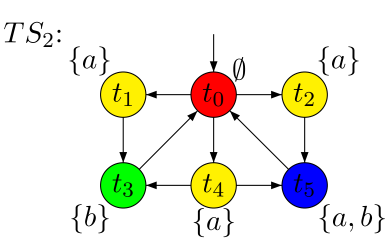
2. $TS_1 \simeq TS_2$:

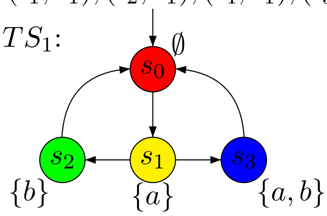
   - $TS_1 \preceq TS_2$ with simulation relation $\mathcal{R} = \{(s_0, t_0), (s_1, t_4), (s_2, t_3), (s_3, t_5)\}$:





   - $TS_2 \preceq TS_1$ with simulation relation $\mathcal{R} = \{(t_0, s_0), (t_1, s_1), (t_2, s_1), (t_4, s_1), (t_3, s_2), (t_5, s_3)\}$:





   Hence, $TS_1 \preceq TS_2$ and $TS_2 \preceq TS_1$. Therefore $TS_1 \simeq TS_2$.

Solution 5b
(10 points)

Let $\Phi = \forall a \mathsf{U} (\neg\exists\Box b)$. Prove or disprove the following statement:

There exists an LTL-formula φ that is equivalent to Φ.

Solution:
Let $\Phi = \forall a \mathsf{U} (\neg\exists\Box b)$. Then $\varphi = a \mathsf{U} \neg\Box b$ (by Thm. 6.18). We prove that $\Phi \equiv \varphi$:

$$\begin{aligned}
s \models \Phi &\iff \forall \pi \in \mathit{Paths}(s).\ \exists k \geq 0.\ (\pi[k] \models \neg\exists\Box b \wedge \forall j < k.\ \pi[j] \models a)\\
&\iff \forall \pi \in \mathit{Paths}(s).\ \exists k \geq 0.\ (\pi[k] \models \forall\Diamond\neg b \wedge \forall j < k.\ \pi[j] \models a)\\
&\iff \forall \pi \in \mathit{Paths}(s).\ \exists k \geq 0.\ \big(\forall \pi' \in \mathit{Paths}(\pi[k]).\ \exists i \geq 0.\ \pi'[i] \models \neg b \wedge \forall j < k.\ \pi[j] \models a\big)\\
&\iff \forall \pi \in \mathit{Paths}(s).\ \exists k \geq 0.\ (\pi[k] \models \Diamond\neg b \wedge \forall j < k.\ \pi[j] \models a)\\
&\iff s \models a \mathsf{U} \Diamond\neg b\\
&\iff s \models a \mathsf{U} \neg\Box b.
\end{aligned}$$