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*

March 30, 2009

Solution

Solution 1

(10 points)

Let P be a linear time property. Prove that P is a liveness property *if and only if* $\mathit{closure}(P) = \left(2^{AP}\right)^{\omega}$.

Solution:
P is a liveness property iff $\mathit{closure}(P) = \left(2^{AP}\right)^{\omega}$.

$\Longrightarrow$ Let P be a liveness property. Then $\mathit{pref}(P) = \left(2^{AP}\right)^{\star}$. Hence

$$\begin{aligned}\mathit{closure}(P) &= \left\{\sigma' \in \left(2^{AP}\right)^{\omega} \mid \mathit{pref}(\sigma) \subseteq \mathit{pref}(P)\right\}\\ &= \left\{\sigma' \in \left(2^{AP}\right)^{\omega} \mid \mathit{pref}(\sigma) \subseteq \left(2^{AP}\right)^{\star}\right\}\\ &= \left(2^{AP}\right)^{\omega}.\end{aligned}$$

$\Longleftarrow$ Let $\mathit{closure}(P) = \left(2^{AP}\right)^{\omega}$. We show that $\mathit{pref}(P) = \left(2^{AP}\right)^{\star}$: Therefore assume that there exists $\hat{\sigma} \in \left(2^{AP}\right)^{\star} \setminus \mathit{pref}(P)$. Then $\mathit{pref}(\hat{\sigma}\sigma'') \not\subseteq \mathit{pref}(P)$ for all $\sigma'' \in \left(2^{AP}\right)^{\omega}$ and hence $\hat{\sigma}\sigma'' \notin \mathit{closure}(P)$. In this way, we obtain a contradiction to our assumption. Therefore, $\mathit{pref}(P) \supseteq \left(2^{AP}\right)^{\star}$ and our claim follows.

Solution 2

(10 points)

Let P denote the linear time property over the set $AP = \{a, b\}$ of atomic propositions such that P consists of all infinite traces $\sigma = A_0 A_1 A_2 \cdots \in \left(2^{AP}\right)^\omega$ that satisfy

$$\forall i \geq 0.\ (A_i = \emptyset \implies \exists k \geq i.\ (b \in A_k \wedge \forall j \in \{i, \ldots, k-1\}\, .\, a \notin A_j))\, .$$

(a) Specify an LTL formula φ such that $Words(\varphi) = P$.

(b) Give an ω–regular expression for P.

(c) Apply the decomposition theorem and give ω–regular expressions for P_{safe} and P_{live}.

Solution:

(a) $\Box\left((\neg a \wedge \neg b) \rightarrow (\neg a)\mathsf{U} b\right)$

(b) Let $E = (\{a\} + \{b\} + \{a, b\} + \emptyset^+.(\{b\} + \{a, b\}))$.
Then $P = \mathcal{L}_\omega(E^\omega)$.

(c) We obtain the safety and liveness properties as follows:

$$\begin{aligned}
P_{safe} &= closure(P) \\
&= \mathcal{L}_\omega\left(E^\omega + E^\star.\emptyset^\omega\right) \\
&= \mathcal{L}_\omega\Big(\left(\{a\} + \{b\} + \{a, b\} + \emptyset^+.(\{b\} + \{a, b\})\right)^\omega + \left(\{a\} + \{b\} + \{a, b\} + \emptyset^+.(\{b\} + \{a, b\})\right)^\star.\emptyset^\omega\Big) \\
\bar{P}_{safe} &= \left(2^{AP}\right)^\star.\emptyset.\{a\}.\left(2^{AP}\right)^\omega \\
P_{live} &= P \cup \Big(\left(2^{AP}\right)^\omega \setminus P_{safe}\Big) \\
&= P \cup \bar{P}_{safe} \\
&= (\{a\} + \{b\} + \{a, b\} + \emptyset^+.(\{b\} + \{a, b\}))^\omega + \left(2^{AP}\right)^\star.\emptyset.\{a\}.\left(2^{AP}\right)^\omega .
\end{aligned}$$

Solution 3

(4 + 5 + 1 points)

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

(a) Compute all elementary sets with respect to *closure*(φ)!
Hint: There are 7 elementary sets.

(b) Use the algorithm from the lecture to construct the GNBA $\mathcal{G}_\varphi$ with $\mathcal{L}_\omega(\mathcal{G}_\varphi) = \mathit{Words}(\varphi)$:

- Define the set of initial states and the acceptance component.
- Depict the transition relation of $\mathcal{G}_\varphi$.
  Hint: It suffices to consider the reachable elementary sets only!

(c) Informally describe the language $\mathcal{L}_\omega(\mathcal{G}_\varphi)$.

Solution:

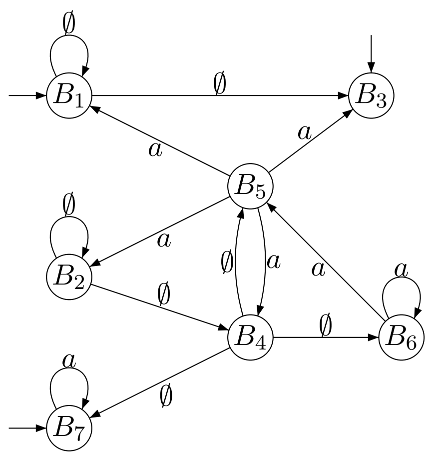
(a) The elementary sets are:

	a	$\bigcirc a$	$\neg a \mathsf{U} a$	$a \wedge \bigcirc a$	φ
B_1	0	0	0	0	1
B_2	0	0	1	0	0
B_3	0	1	0	0	1
B_4	0	1	1	0	0
B_5	1	0	1	0	0
B_6	1	1	1	1	0
B_7	1	1	1	1	1

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

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

The transition relation δ is given by the following graph representation (where also the unreachable parts are outlined — not necessary in the exam):

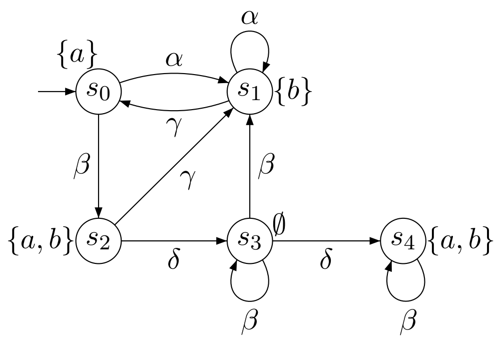


(c) The accepted language $\mathcal{L}_\omega(\mathcal{G}_\varphi)$ is the singleton $\{\emptyset^\omega\}$.

Solution 4

(2 + 4 + 4 points)

Let P denote the set of traces $\sigma = A_0A_1A_2 \dots \in \left(2^{AP}\right)^\omega$ over $AP = \{a, b\}$ such that there exist infinitely many indices $k \geq 0$ with $A_k = \emptyset$. Consider the following transition system TS:



For each of the fairness assumptions

(a) $\mathcal{F}_1 = \left(\left\{\{\alpha\}\right\}, \left\{\{\beta\}, \{\delta, \gamma\}\right\}, \emptyset\right)$ and

(b) $\mathcal{F}_2 = \left(\left\{\{\alpha\}\right\}, \left\{\{\beta\}, \{\delta\}, \{\gamma\}\right\}, \emptyset\right)$:

Decide whether $TS \models_{\mathcal{F}_i} P$ for $i = 1, 2$. Justify your answers!

Solution:
We consider each of the fairness assumptions $\mathcal{F}_i$ for $i \in \{1, 2\}$: We have $TS \models_{\mathcal{F}_i} P$ iff $\mathit{FairTraces}_{\mathcal{F}_i}(TS) \subseteq P$. Because of $\overset{\infty}{\exists}\, k.\ A_k = \emptyset$, each trace has to visit s_3 infinitely many times.

(a) $TS \not\models_{\mathcal{F}_1} P$: Consider the execution $\pi = (s_0s_2s_1s_1)^\omega$. It is $\mathcal{F}_1$-fair but $\pi \not\models \Box\Diamond(\neg a \land \neg b)$.

(b) $TS \models_{\mathcal{F}_2} P$:

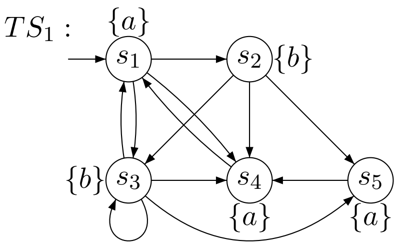
- Any trace that reaches s_4 is not $\mathcal{F}_2$-fair as α is executed only finitely many times. This is in contradiction to our $\mathcal{F}_{2,ucond} = \left\{\{\alpha\}\right\}$.
- Therefore $s_3 \xrightarrow{\delta} s_4$ is never taken.
- Because of $\{\gamma\} \in \mathcal{F}_{2,strong}$, the α-loop of s_1 cannot be taken infinitely long.
- Because of $\{\beta\} \in \mathcal{F}_{2,strong}$, we take the transition $s_0 \xrightarrow{s}{}_2$ infinitely often.
- Because of $\{\delta\} \in \mathcal{F}_{2,strong}$, we take the transition $s_2 \xrightarrow{s}{}_3$ infinitely often.

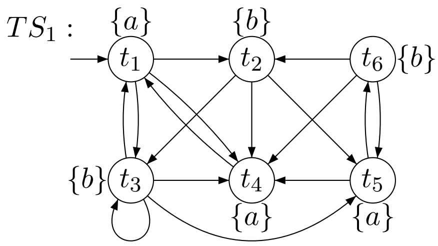
Therefore $\mathit{FairTraces}_{\mathcal{F}_1}(TS) \subseteq P$ and $TS \models_{\mathcal{F}_1} P$.

Solution 5a

(4 + 6 points)

Consider the following transition systems TS_1 and TS_2:



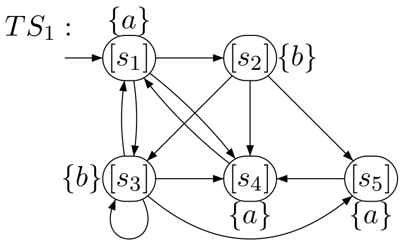


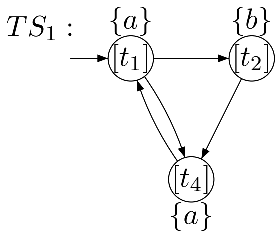
(a) Compute $TS_1/\sim$ and $TS_2/\sim$.

(b) Decide whether $TS_1 \sim TS_2$. Explain your answer.

Solution:

(a) The quotient transition systems for TS_1 and TS_2 are:





$\mathcal{R} = \mathsf{Id}$

$[s_1] = \{s_1\}$ $\quad [s_2] = \{s_2\}$

$[s_3] = \{s_3\}$ $\quad [s_4] = \{s_4\}$

$[s_5] = \{s_5\}$

$\mathcal{R} = \{(t_1, t_5), (t_2, t_3), (t_2, t_6)\}^*$

$[t_1] = \{t_1, t_5\}$

$[t_2] = \{t_2, t_3, t_6\}$

$[t_4] = \{t_4\}$

(b) $TS_1 \not\sim TS_2$: Note that $s_1 \not\sim t_1$ as s_1 has successors in three equivalence classes whereas t_1 only has successors to $[t_2]$ and to $[t_4]$.

Solution 5b

(4 + 6 points)

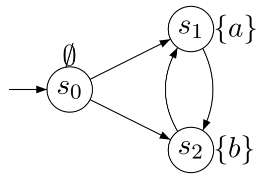
Let φ be an LTL-formula, $TS = (S, Act, \to, I, AP, L)$ be a transition system and $s \in S$.

(a) Prove or disprove: $s \models \varphi \iff s \not\models \neg\varphi$.

(b) Prove that $\Diamond(a \wedge \Box b)\mathsf{W}\neg b \equiv \Diamond(\neg b \vee \Box(a \wedge b))$.

Solution:

(a) Let $\varphi = \bigcirc a$ and consider the transition system



Then $s_0 \not\models \neg \bigcirc a$ (because of $\pi = s_0 s_1$) and $s_0 \not\models \bigcirc a$ (because of $\pi = s_0 s_2$). Therefore $s_0 \models \varphi \not\Leftrightarrow s_0 \not\models \neg\varphi$.

(b) We proceed as follows:

$$\begin{aligned}
\Diamond(a \wedge \Box b)\mathsf{W}(\neg b) &\equiv \Diamond\,[(a \wedge \Box b)\mathsf{U}(\neg b) \vee \Box(a \wedge \Box b)] \\
&\equiv \Diamond(a \wedge \Box b)\mathsf{U}(\neg b) \vee \Diamond\Box(a \wedge \Box b) \\
&\equiv \Diamond\neg b \vee \Diamond(\Box a \wedge \Box\Box b) \\
&\equiv \Diamond\neg b \vee \Diamond(\Box a \wedge \Box b) \\
&\equiv \Diamond\neg b \vee \Diamond\Box(a \wedge b) \\
&\equiv \Diamond(\neg b \vee \Box(a \wedge b)).
\end{aligned}$$