RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

LEHRSTUHL FÜR INFORMATIK II

RWTH Aachen · D-52056 Aachen · GERMANY

Winter term 2005/06

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

Exam in *Model Checking*

March 31, 2006

Solution

Solution 1

(1 + 4 + 5 points)

(a) We start by computing the closure of φ:

$$closure(\varphi) = \{\,\mathsf{true}\,, \mathsf{false}\,, a, \neg a, \bigcirc a, \neg \bigcirc a, \\ (a \wedge \bigcirc a), \neg(a \wedge \bigcirc a), \varphi, \neg\varphi\,\}$$

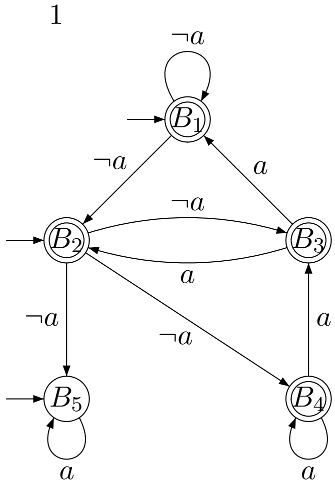
The elementary sets are:

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

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

$$Q = \{B_1, B_2, B_3, B_4, B_5\}$$
$$Q_0 = \{B_1, B_2, B_5\}$$
$$\mathcal{F} = \big\{F_{(a \wedge \bigcirc a)\mathsf{U}\neg a}\big\}$$
$$F_{(a \wedge \bigcirc a)\mathsf{U}\neg a} = \{B_1, B_2, B_3, B_4\}$$

The transition relation δ is given by the following graph representation:

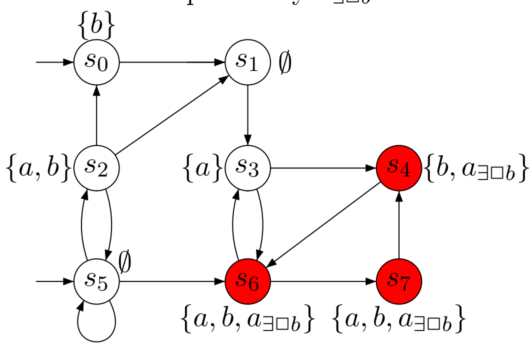


Solution 2

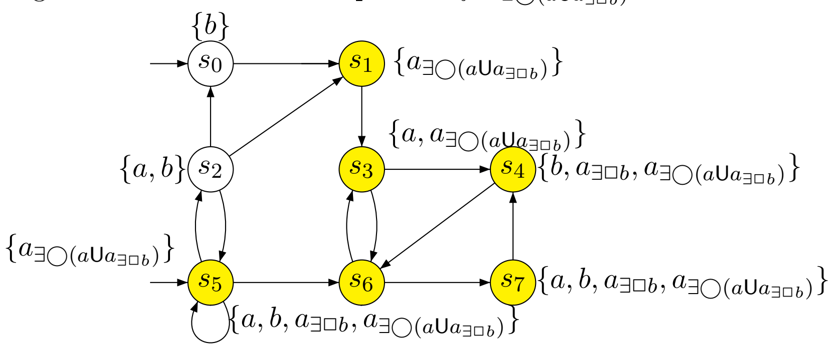
(2 + 4 + 4 points)

We consider the maximal proper state subformulas $Sub(\Phi)$:

1. $\Psi = a$: $Sat(a) = \{s_2, s_3, s_6, s_7\}$
2. $\Psi = b$: $Sat(b) = \{s_0, s_2, s_4, s_6, s_7\}$
3. $\Psi = \exists\Box b$:
   The following equivalence is used to compute $Sat(\exists\Box b)$:
   $$s \models_{\text{CTL}^*} \exists\varphi \quad\iff\quad s \models_{\text{CTL}^*} \neg\forall\neg\varphi \quad\iff\quad s \not\models_{\text{CTL}^*} \forall\neg\varphi \quad\iff\quad s \not\models_{\text{LTL}} \neg\varphi$$
   According to the LTL semantics, we have $Sat_{\text{LTL}}(\neg\Box b) = Sat_{\text{LTL}}(\Diamond\neg b) = \{s_0, s_1, s_2, s_3, s_5\}$. Then, $S \setminus Sat_{\text{LTL}}(\neg\Box b) = \{s_4, s_6, s_7\}$ is the satisfaction set $Sat_{\text{CTL}^*}(\exists\Box b)$:
   $$Sat_{\text{CTL}^*}(\exists\Box b) = \{s_4, s_6, s_7\}.$$
   The labeling is extended by a fresh atomic proposition $a_{\exists\Box b}$ according to $Sat_{\text{CTL}^*}(\exists\Box b)$.
   The corresponding subformula $\exists\Box b$ of Φ is replaced by $a_{\exists\Box b}$.



4. $\Psi = \exists\bigcirc(a \mathsf{U} a_{\exists\Box b})$:
   The above equivalence for existentially quantified path formulas yields:
   $$s \models_{\text{CTL}^*} \exists\bigcirc(a \mathsf{U} a_{\exists\Box b}) \quad\iff\quad s \not\models_{\text{LTL}} \neg\bigcirc(a \mathsf{U} a_{\exists\Box b}).$$
   By the equivalence $\neg\bigcirc(a \mathsf{U} a_{\exists\Box b}) \equiv \bigcirc\neg(a \mathsf{U} a_{\exists\Box b})$, the satisfaction set of $\neg(a \mathsf{U} a_{\exists\Box b})$ can be inferred:
   $$\begin{aligned} Sat_{\text{LTL}}(\neg(a \mathsf{U} a_{\exists\Box b})) &= \{s_0, s_1, s_2, s_5\} \\ Sat_{\text{LTL}}(\bigcirc\neg(a \mathsf{U} a_{\exists\Box b})) &= \{s_0, s_2\} \\ Sat_{\text{CTL}^*}(\exists\bigcirc(a \mathsf{U} a_{\exists\Box b})) &= S \setminus Sat_{\text{LTL}}(\bigcirc\neg(a \mathsf{U} a_{\exists\Box b})) \\ &= S \setminus \{s_0, s_2\} \\ &= \{s_1, s_3, s_4, s_5, s_6, s_7\} \end{aligned}$$
   The labeling is extended by a new atomic prop. $a_{\exists\bigcirc(a\mathsf{U}a_{\exists\Box b})}$ according to $Sat_{\text{CTL}^*}(\exists\bigcirc(a \mathsf{U} a_{\exists\Box b}))$.
   Again, the corresponding subformula Ψ of Φ is replaced by $a_{\exists\bigcirc(a\mathsf{U}a_{\exists\Box b})}$:



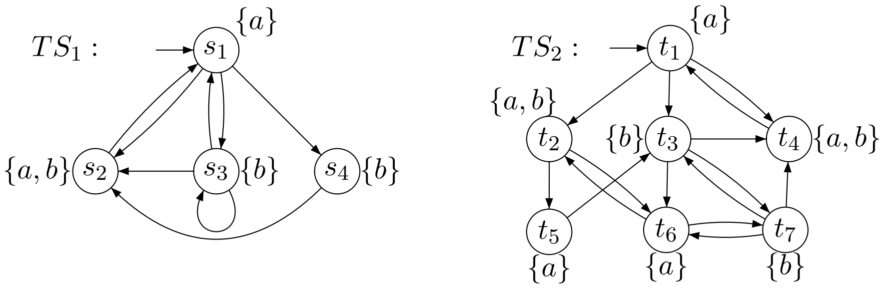
5. $\Psi = \forall\Diamond\Box a_{\exists\bigcirc(a\mathsf{U}a_{\exists\Box b})}$:
   In the case of universal quantification, we can directly apply the LTL–semantics:
   $$Sat_{\text{LTL}}(\Diamond\Box a_{\exists\bigcirc(a\mathsf{U}a_{\exists\Box b})}) = \{s_0, s_1, s_3, s_4, s_6, s_7\}.$$

Because of $s_5 \in Q_0$, but $s_5 \notin Sat(\Phi)$, this yields $TS \not\models_{\text{CTL}^*} \Phi$.

Solution 3

(7 + 3 points)

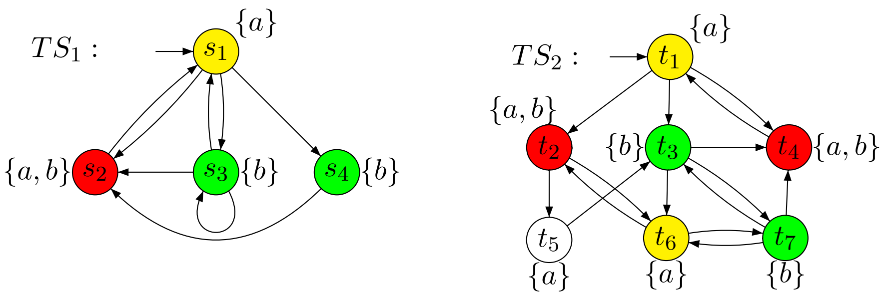
The two transition systems were given as follows:



(a) $TS_1 \not\sim TS_2$.
Argument: Consider the CTL-formula $\Phi = \exists \bigcirc (b \wedge \forall \bigcirc (a \wedge b))$.
Then $TS_1 \models \Phi$ and $TS_2 \not\models \Phi$. Therefore TS_1 and TS_2 cannot be bisimilar.

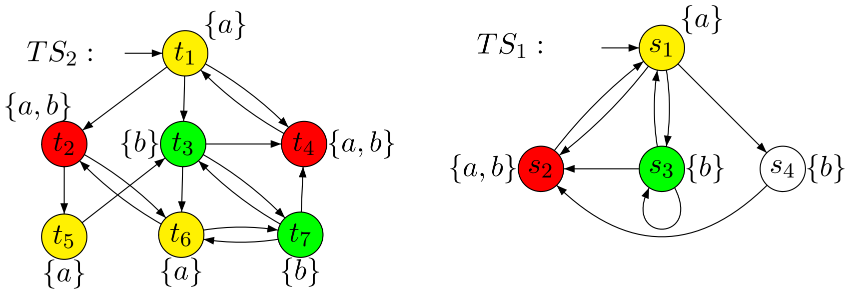
(b) $TS_1 \simeq TS_2$. To show this, we consider the cases:

- $TS_1 \preceq TS_2$:
  Graphically, the simulation relation is outlined below:



$$\mathcal{R} = \{(s_1,t_1),(s_2,t_4),(s_2,t_2),(s_3,t_3),(s_4,t_3),(s_3,t_7),(s_1,t_6),(s_4,t_7)\}$$

- $TS_2 \preceq TS_1$:
  The simulation order can be outlined graphically as follows:



$$\mathcal{R} = \{(t_1,s_1),(t_2,s_2),(t_3,s_3),(t_4,s_2),(t_5,s_1),(t_6,s_1),(t_7,s_3)\}$$

$\Longrightarrow TS_1 \simeq TS_2$.

Solution 4

(2 + 4 + 4 points)

(a) We first consider P_1:

(i) The linear time property P_1 can be described by the following ω-regular expression:

$$P_1 = \mathcal{L}_\omega\big(\emptyset^*.\{a\}.\,(\emptyset + \{b\} + \{a,b\} + \{a\}.\{b\})^\omega\big)$$

(ii) According to Lemma 3.36, any LT-property can be decomposed into a safety and a liveness property:

$$P = \underbrace{closure(P)}_{P_{safe}} \cap \underbrace{\Big(P \cup \Big(\big(2^{AP}\big)^\omega \setminus closure(P)\Big)\Big)}_{P_{live}}.$$

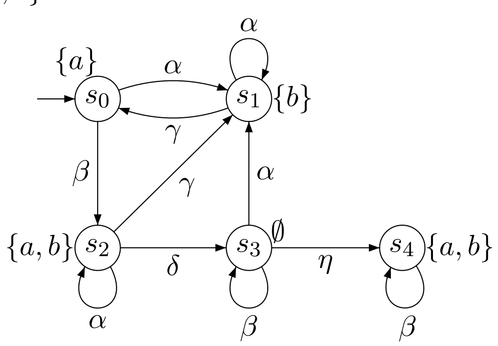
Application to P_1 yields

$$\begin{aligned} P_{safe} &= closure(P) \\ &= \mathcal{L}_\omega\big(\emptyset^*.\{a\}.\,(\emptyset + \{b\} + \{a,b\} + \{a\}.\{b\})^\omega + \emptyset^\omega\big) \end{aligned}$$

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

(iii) Since $pref(P_{live}) = \big(2^{AP}\big)^*$, P_{live} is a liveness property.
As $closure(P) = closure(closure(P))$, P_{safe} is a safety property.

(b) We consider each of the fairness assumptions $\mathcal{F}_i$ for $i \in \{1, 2\}$:



We have $TS \models_{\mathcal{F}_i} P_2$ iff $FairTraces_{\mathcal{F}_i}(TS) \subseteq P_2$. Because of $\overset{\infty}{\exists}\, k.\ A_k = \{a, b\}$, each trace has to visit at least one of s_2 or s_4 infinitely many times. Additionally, from some point onwards, each a-state must be followed by a state that is annotated with (at least) b.

(i) $TS \models_{\mathcal{F}_1} P_2$:

- Any trace that reaches s_4 is not $\mathcal{F}_1$-fair as α is executed only finitely many times. This is in contradiction to our $\mathcal{F}_{1,ucond} = \big\{\{\alpha\}\big\}$.
- Therefore $s_3 \xrightarrow{\eta} s_4$ is never taken.
- Because of $\{\eta\} \in \mathcal{F}_{1,strong}$ and because η actions cannot be executed infinitely often (in fact, only once from s_3 to s_4), the state s_3 must not be visited infinitely often.
- The transitions $s_1 \xrightarrow{\alpha} s_1$ and $s_2 \xrightarrow{\alpha} s_2$ cannot be taken infinitely often because of the enabled γ transitions to s_0 or s_1, respectively.
- As β is enabled in s_0, all $\mathcal{F}_1$–fair paths visit exactly s_0, s_1 and s_2 infinitely often.

Therefore $FairTraces_{\mathcal{F}_1}(TS) \subseteq P_2$ and $TS \models_{\mathcal{F}_1} P_2$.

(ii) $TS \not\models_{\mathcal{F}_2} P_2$:
Consider the path $\pi = (s_0 s_2 s_3 s_1)^\omega$ with its corresponding trace $\sigma = (\{a\}\{a,b\}\emptyset\{b\})^\omega$.
We have $\pi \in FairPaths_{\mathcal{F}_2}(TS)$, but $\sigma \notin P_2$.
$\Longrightarrow FairTraces_{\mathcal{F}_2}(TS) \not\subseteq P_2$.