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*

February 10, 2006

Solution

Solution 1

(2 + 4 + 4 points)

approach:	2
$closure(closure(P)) \subseteq closure(P)$	4
$closure(P) \subseteq closure(closure(P))$	4

Let P denote an LT property. Then $closure(P)$ is a safety property:

Proof:
We show that $closure(P) = closure(closure(P))$.

"$\subseteq$": Let $\sigma \in closure(P)$. From the definition of *closure* one infers

$$pref(\sigma) \subseteq pref(P). \tag{1}$$

By definition, $closure(P) = \left\{\sigma' \in \left(2^{AP}\right)^{\omega} \mid pref(\sigma') \subseteq pref(P)\right\}$. Therefore

$$\begin{aligned} \gamma \in P &\Longrightarrow pref(\gamma) \subseteq pref(P) \\ &\Longrightarrow \gamma \in closure(P) \end{aligned}$$

It follows, that for any LT-property P, we have $P \subseteq closure(P)$.

Since $P \subseteq closure(P)$ we have

$$pref(P) \subseteq pref(closure(P)) \tag{2}$$

By transitivity of the set inclusion $\subseteq$, we can infer from (1) and (2):

$$pref(\sigma) \subseteq pref(closure(P))$$

Therefore $\sigma \in closure(closure(P))$.

"$\supseteq$": Let $\sigma \in closure(closure(P))$. We have to prove that $\sigma \in closure(P)$. By definition of $closure(P)$, this is equivalent to showing that $pref(\sigma) \subseteq pref(P)$:

Let $\hat{\sigma} \in pref(\sigma)$. By definition,

$$closure(closure(P)) = \left\{\sigma' \in \left(2^{AP}\right)^{\omega} \mid pref(\sigma') \subseteq pref(closure(P))\right\}$$

$\Longrightarrow \hat{\sigma} \in pref(closure(P))$ (* $\sigma \in closure(closure(P))$ *)
$\Longrightarrow \exists \sigma' \in closure(P)$ such that $\hat{\sigma} \in pref(\sigma')$ and $pref(\sigma') \subseteq pref(P)$.
$\Longrightarrow \hat{\sigma} \in pref(P)$.

Therefore we have shown that $pref(\sigma) \subseteq pref(P)$.

Solution 2

(3 + 4 + 3 points)

(a) $P = Words\big((a \to \bigcirc\neg b)\mathsf{W}(a \wedge b)\big)$ is a safety property:

By definition, P is a safety property iff

$$\forall \sigma \in (2^{AP})^\omega \setminus P. \quad \exists \hat{\sigma} \in pref(\sigma). \quad P \cap \Big\{\sigma' \in \big(2^{AP}\big)^\omega \mid \hat{\sigma} \in pref(\sigma')\Big\} = \emptyset.$$

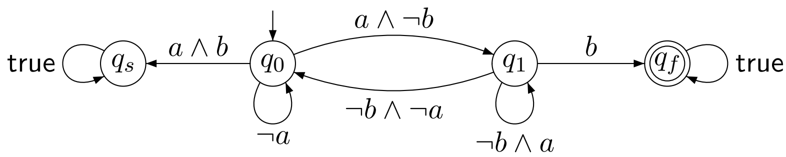
According to the LTL semantics of W and $\bigcirc$, we have

$$(2^{AP})^\omega \setminus P = Words(\neg\varphi) = \mathcal{L}_\omega\Big((\{b\} + \{a\}^*.\emptyset)^*.\{a\}^+.(\{a,b\} + \{b\}).(2^{AP})^\omega\Big).$$

Choose $\sigma \in Words(\neg\varphi)$.
Then there exists $k \geq 0$ such that $\sigma[k] = \{a\}$ and $b \in \sigma[k{+}1]$ and forall $i < k$: $a \in \sigma[i] \to b \notin \sigma[i{+}1]$.
Therefore $\hat{\sigma} = \sigma[0..k+1]$ is a minimal bad prefix for σ.

$\Longrightarrow$ For each $\sigma \in (2^{AP})^\omega \setminus P$, there exists a bad prefix.
$\Longrightarrow$ P is a safety property.

(b) The following NFA $\mathcal{A}$ recognizes $BadPref(P)$:



(c) $P' = Words\big((a \to \bigcirc\neg b)\mathsf{U}(a \wedge b)\big)$ is <u>not</u> a safety property:
Consider $\sigma = \emptyset^\omega$. Obviously $\sigma \notin P'$ but any prefix $\hat{\sigma}$ of σ can be prolonged by the suffix $\{a,b\}^\omega$:

$$\forall \hat{\sigma} \in pref(\sigma). \quad \hat{\sigma}.(\{a,b\})^\omega \in P'.$$

The resulting trace is in P'; therefore no bad prefixes can be defined for σ.

The following observation leads to a straightforward decomposition of P' (cf. lecture notes, p. 243):

$$\varphi\mathsf{U}\psi \quad \equiv \quad (\varphi\mathsf{W}\psi) \wedge \Diamond\psi$$

Therefore we have

$$(a \to \bigcirc\neg b)\mathsf{U}(a \wedge b) \equiv (a \to \bigcirc\neg b)\mathsf{W}(a \wedge b) \wedge \Diamond(a \wedge b).$$

Considering the sets of words according to this equivalence, we have

$$Words\big((a \to \bigcirc\neg b)\mathsf{U}(a \wedge b)\big) = Words\big((a \to \bigcirc\neg b)\mathsf{W}(a \wedge b)\big) \cap Words\big(\Diamond(a \wedge b)\big).$$

Now we can decompose P' into a safety property P_{safe} and a liveness property P_{life} as follows:

$$P_{safe} = Words\big((a \to \bigcirc\neg b)\mathsf{W}(a \wedge b)\big)$$
$$P_{live} = Words\big(\Diamond(a \wedge b)\big)$$

In part (a), we already showed that $P = P_{safe} = Words\big((a \to \bigcirc\neg b)\mathsf{W}(a \wedge b)\big)$ is a safety property.

It remains to show that P_{live} is indeed a liveness property:
$P_{live} = Words\big(\Diamond(a \wedge b)\big) = \mathcal{L}_\omega\big((2^{\{a,b\}})^*.\{a,b\}.(2^{\{a,b\}})^\omega\big)$.
Therefore $pref(P_{live}) = (2^{\{a,b\}})^*$ and by definition, P_{live} is a liveness property.

Solution 3

(1 + 4 + 5 points)

(a) Let $\psi = \Box(a \leftrightarrow \bigcirc\neg a)$ and $AP = \{a\}$.
First we transform ψ into the equivalent basic LTL-formula φ:

$$
\begin{aligned}
\psi &= \Box(a \leftrightarrow \bigcirc\neg a) \\
&= \neg\Diamond\neg(a \leftrightarrow \bigcirc\neg a) && (*\ \Box\varphi \equiv \neg\Diamond\neg\varphi\ *) \\
&= \neg\Diamond\neg((a \wedge \bigcirc\neg a) \vee (\neg a \wedge \neg\bigcirc\neg a)) && (*\ \text{bijunktion}\ *) \\
&= \neg\Diamond\big(\neg(a \wedge \bigcirc\neg a) \wedge \neg(\neg a \wedge \neg\bigcirc\neg a)\big) && (*\ \text{deMorgan}\ *) \\
&= \neg\big[\mathsf{true}\,\mathsf{U}\big(\neg\underbrace{(a \wedge \bigcirc\neg a)}_{\varphi_1} \wedge \neg\underbrace{(\neg a \wedge \neg\bigcirc\neg a)}_{\varphi_2}\big)\big] = \varphi && (*\ \Diamond\varphi \equiv \mathsf{true}\,\mathsf{U}\varphi\ *)
\end{aligned}
$$

(b) Now we compute $closure(\varphi)$:

$$
\begin{aligned}
closure(\varphi) = \{\,&\mathsf{true}, \mathsf{false}, a, \neg a, \bigcirc\neg a, \neg\bigcirc\neg a, \\
&\varphi_1, \neg\varphi_1, \varphi_2, \neg\varphi_2, \\
&\neg\varphi_1 \wedge \neg\varphi_2, \neg(\neg\varphi_1 \wedge \neg\varphi_2), \\
&\mathsf{true}\,\mathsf{U}(\neg\varphi_1 \wedge \neg\varphi_2), \neg\,[\mathsf{true}\,\mathsf{U}(\neg\varphi_1 \wedge \neg\varphi_2)]\ \}
\end{aligned}
$$

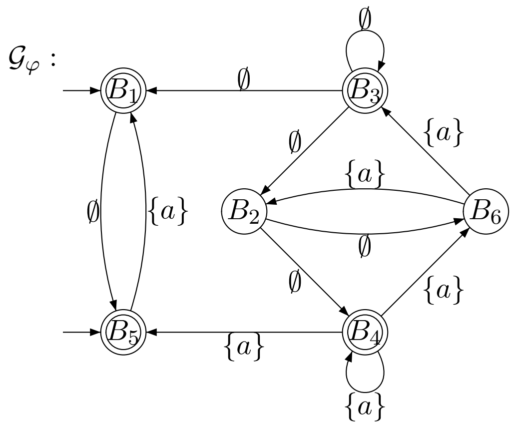
The elementary sets are:

	true	a	$\bigcirc\neg a$	$\overbrace{a \wedge \bigcirc\neg a}^{\varphi_1}$	$\overbrace{\neg a \wedge \neg\bigcirc\neg a}^{\varphi_2}$	$\neg\varphi_1 \wedge \neg\varphi_2$	$\mathsf{true}\,\mathsf{U}\,(\neg\varphi_1 \wedge \neg\varphi_2)$
B_1	1	0	0	0	1	0	0
B_2	1	0	0	0	1	0	1
B_3	1	0	1	0	0	1	1
B_4	1	1	0	0	0	1	1
B_5	1	1	1	1	0	0	0
B_6	1	1	1	1	0	0	1

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

$$
\begin{aligned}
Q &= \{B_1, B_2, B_3, B_4, B_5, B_6\} \\
\Sigma &= 2^{\{a\}} = \{\emptyset, \{a\}\} \\
Q_0 &= \{B_1, B_5\} \\
\mathcal{F} &= \{F_{\mathsf{true}\mathsf{U}(\neg\varphi_1 \wedge \neg\varphi_2)}\} \\
F_{\mathsf{true}\mathsf{U}(\neg\varphi_1 \wedge \neg\varphi_2)} &= \{B_1, B_3, B_4, B_5\}
\end{aligned}
$$

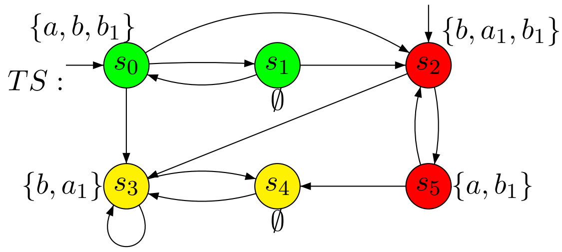
The transition relation δ is given by the following graph representation (where also the unreachable parts are outlined):



Solution 4 (2 + 4 + 4 points)

Let $fair = \Box\Diamond \underbrace{(b \wedge \neg a)}_{\Phi_1} \rightarrow \Box\Diamond \underbrace{\exists (b \mathsf{U} (a \wedge \neg b))}_{\Psi_1}$.

Introduce new atomic propositions a_1 and b_1 and extend the labeling accordingly:



The strongly connected components of TS are

$$C_1 = \{s_0, s_1\}$$
$$C_2 = \{s_2, s_5\}$$
$$C_3 = \{s_3, s_4\}$$

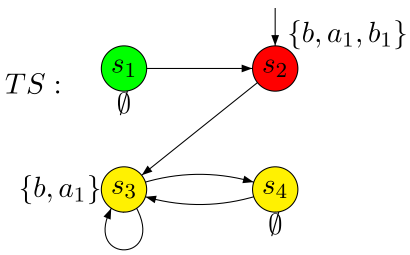
Each execution fragment ultimately stays in one of these SCCs. According to the fairness assumption $fair$ and the extended labeling, the SCC C_3 is excluded from this set, i.e. no fair path visits states in C_3 infinitely often.

We have $Sat_{fair}(\exists\Box\mathsf{true}) = \{s_0, s_1, s_2, s_5\}$.
Extend the labeling of those states with the new atomic proposition a_{fair}.

Now consider the CTL-formula $\Phi = \forall\Box\forall\Diamond a$. Rewriting Φ into existential normal form yields:

$$\begin{aligned}\Phi &= \forall\Box\forall\Diamond a\\ &= \neg\exists\Diamond\neg\forall\Diamond a\\ &= \neg\exists\Diamond\exists\Box\neg a\\ &= \neg\exists(\mathsf{true}\,\mathsf{U}\exists\Box\neg a)\end{aligned}$$

- Compute the fair satisfaction set for subformula $\Phi = \exists\Box\neg a$: The state subgraph $G[\neg a]$ of TS is



  The only SCC in $G[\neg a]$ is C_3. But we have

  $$C_3 \cap Sat(a_1) \neq \emptyset$$
  $$C_3 \cap Sat(b_1) = \emptyset$$

  Therefore $T = \emptyset$ and $Sat_{fair}(\exists\Box\neg a) = \{s \in S \mid Reach_{G[\neg a]}(s) \cap T \neq \emptyset\} = \emptyset$.
  Introduce new atomic proposition $a_{\exists\Box\neg a}$ and extend the labeling of TS according to $Sat_{fair}(\exists\Box\neg a)$ (In this case, no state labels are extended since $Sat_{fair}(\exists\Box\neg a) = \emptyset$).

- Now consider $\Phi = \exists(\mathsf{true}\,\mathsf{U} a_{\exists\Box\neg a})$:

  $$Sat_{fair}(\exists(\mathsf{true}\,\mathsf{U} a_{\exists\Box\neg a})) = Sat(\exists(\mathsf{true}\,\mathsf{U}(a_{\exists\Box\neg a} \wedge a_{fair}))) = \emptyset$$

- Therefore $Sat_{fair}(\neg a_{\exists(\mathsf{true}\mathsf{U}\exists\Box\neg a)}) = \{s \in S \mid a_{\exists(\mathsf{true}\mathsf{U}\exists\Box\neg a)} \notin L(s)\}$.
  This yields $Sat_{fair}(\neg a_{\exists(\mathsf{true}\mathsf{U}\exists\Box\neg a)}) = S$.

Solution 5 (3 ∗ 1 + 3 + 4 points)

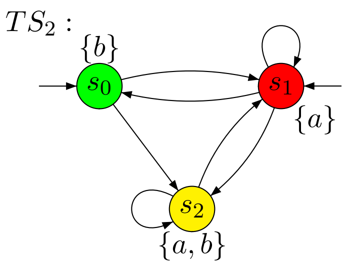
$TS_i \sim TS_j$ decision	3*1
formula:	3
bisimulation relation	4

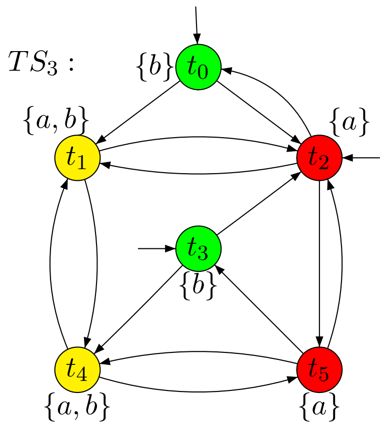
- $TS_1 \not\sim TS_2$:
  Let $\Phi = \forall\Box\big((a \wedge \neg b) \rightarrow \exists \bigcirc (b \wedge \neg a)\big)$.
  We have $TS_1 \not\models \Phi$ because $r_2 \models a \wedge \neg b$, but there does not exist an $b \wedge \neg a$ successor state of r_2. On the other hand, $TS_2 \models \Phi$: The only state in TS_2 that models $(a \wedge \neg b)$ is s_1 and we have that $s_0 \in Post(s_1)$ and $s_0 \models b \wedge \neg a$.

- $TS_2 \sim TS_3$:
  The following relation $\mathcal{R} \subseteq S_2 \times S_3$ is a bisimulation relation:

$$\begin{aligned}\mathcal{R} := \{\, & (s_0, t_0), (s_0, t_3),\\ & (s_1, t_2), (s_1, t_5),\\ & (s_2, t_1), (s_2, t_4)\ \}\end{aligned}$$

  Graphically, this is outlined as follows:





- Now it follows directly that $TS_1 \not\sim TS_3$ (again by Φ).