Systems Verification Lab
Exercises on Regular Properties, Linear Time Logic and Computation Tree Logic with (Some) Solutions

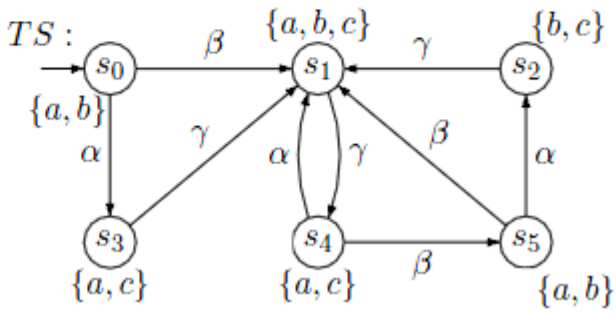
Teacher: Luca Tesei

Master of Science in Computer Science - University of Camerino

Contents

1 Regular Properties

Exercise 1.1. *Consider the following transition system TS:*



and the regular safety property

$$P_{safe} = \text{"always if } a \text{ is valid and } b \wedge \neg c \text{ was valid somewhere before, then } a \text{ and } b \text{ do not hold thereafter at least until } c \text{ holds"}$$

As an example, it holds:

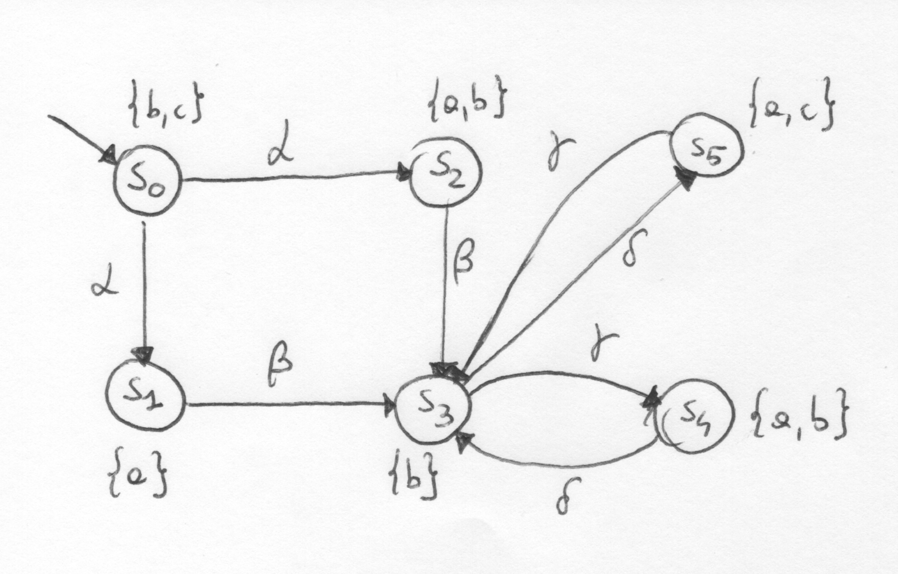
$$\begin{aligned}
\{b\}\emptyset\{a,b\}\{a,b,c\} &\in pref(P_{safe}) \\
\{a,b\}\{a,b\}\emptyset\{b,c\} &\in pref(P_{safe}) \\
\{b\}\{a,c\}\{a\}\{a,b,c\} &\in BadPref(P_{safe}) \\
\{b\}\{a,c\}\{a,c\}\{a\} &\in BadPref(P_{safe})
\end{aligned}$$

Questions:

(a) Define an NFA A such that $L(A) = MinBadPref(P_{safe})$

(b) Decide whether $TS \models P_{safe}$ *using the* $TS \otimes A$ *construction. Provide a counterexample if* $TS \not\models P_{safe}$

Exercise 1.2. *Consider the following transition system* TS*:*



and the regular safety property

P_{safe} = *"always if* b *is holding and* a *was held somewhere before, then* c *must* **not** *hold in the position just after the current* b*"*

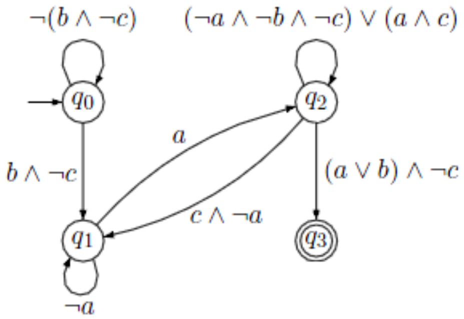
1. *Define an NFA* $\mathcal{A}$ *such that* $\mathcal{L}(\mathcal{A}) = \text{MinBadPref}(P_{\text{safe}})$

2. *Decide whether* $\text{TS} \models P_{\text{safe}}$ *using the* $\text{TS} \otimes \mathcal{A}$ *construction. Provide a counterexample if* $\text{TS} \not\models P_{\text{safe}}$

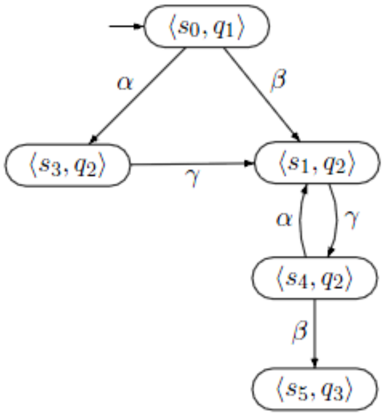
Solutions

Solution of Exercise 1.1

- The NFA that accepts the set of minimal bad prefixes:



- First we apply the $TS \otimes \mathcal{A}$ construction which yields:



A counterexample to $TS \models P_{safe}$ is given by the following initial path fragment in $TS \otimes \mathcal{A}$:

$$\pi_{\otimes} = \langle s_0, q_1 \rangle \langle s_3, q_2 \rangle \langle s_1, q_2 \rangle \langle s_4, q_2 \rangle \langle s_5, q_3 \rangle$$

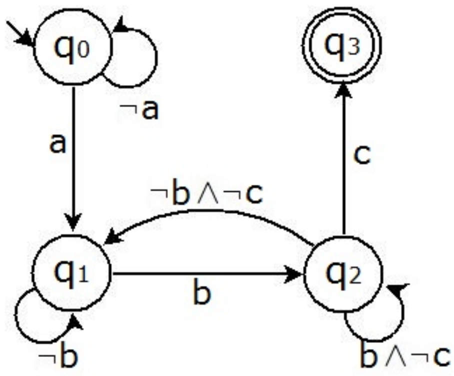
By projection on the state component, we get a path in the underlying transition system:

$$\pi = s_0 s_3 s_1 s_4 s_5 \text{ with } trace(\pi) = \{a, b\}\{a, c\}\{a, b, c\}\{a, c\}\{a, b\}$$

Obviously, $trace(\pi) \in BadPref(P_{safe})$, so we have $Traces_{fin}(TS) \cap BadPref(P_{safe}) \neq \emptyset$. By lemma 3.25, this is equivalent to $TS \not\models P_{safe}$.

Solution of Exercise 1.2

1. An NFA accepting the minimal bad prefixes for the property is $\mathcal{A}$:



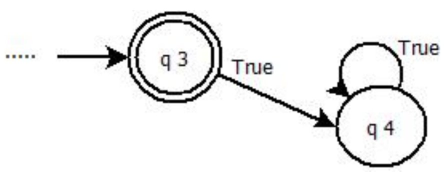
where:
$\neg a \equiv \{\{\}, \{b\}, \{c\}, \{b, c\}\}$
$a \equiv \{\{a\}, \{a, b\}, \{a, c\}, \{a, b, c\}\}$
The union of $\neg a$ and a is 2^{AP}

$\neg b \equiv \{\{\}, \{a\}, \{c\}, \{a, c\}\}$
$b \equiv \{\{b\}, \{a, b\}, \{b, c\}, \{a, b, c\}\}$
The union of $\neg b$ and b is 2^{AP}

$c \equiv \{\{c\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$
$b \wedge \neg c \equiv \{\{b\}, \{a, b\}\}$
$\neg b \wedge \neg c \equiv \{\{\}, \{a\}\}$
The union of c, $b \wedge \neg c$ and $\neg b \wedge \neg c$ is 2^{AP}

So the NFA is non-blocking apart from state q_3.

2. To apply the product $TS \otimes \mathcal{A}$, $\mathcal{A}$ should be non-blocking. Our $\mathcal{A}$ is deterministic and becomes non-blocking if we add a state q_4 and let



or alternatively we can add a self-loop on q_3. In this case the automaton would recognize all bad prefixes, not just the minimal ones. Let us consider $\mathcal{A}'$ made on one of these two ways.

Let's construct the product:
$L(s_0) = \{b, c\}$ $\delta(q_0, \{b, c\}) = \{q_0\}$
So the unique initial state of $TS \otimes \mathcal{A}'$ is $< s_0, q_0 >$

$$
\begin{tikzcd}[column sep=small]
 & {} \arrow[r] & < s_0, q_0 > \arrow[dl] \arrow[dr] & \\
 & < s_1, q_1 > \arrow[d] & & < s_2, q_1 > \arrow[d, phantom, "\vdots"] \\
 & < s_3, q_2 > \arrow[d] & & {} \\
 & < s_5, q_3 > \overset{*}{\dots} & &
\end{tikzcd}
$$

From $< s_0, q_0 >$:

- $s_0 \longrightarrow s_1$ $L(s_1) = \{a\}$
  $\delta(q_0, \{a\}) = \{q_1\}$.
- $s_0 \longrightarrow s_2$ $L(s_2) = \{a, b\}$
  $\delta(q_0, \{a, b\}) = \{q_1\}$.

From $< s_1, q_1 >$:

- $s_1 \longrightarrow s_3$ $L(s_3) = \{b\}$
  $\delta(q_1, \{b\}) = \{q_2\}$.

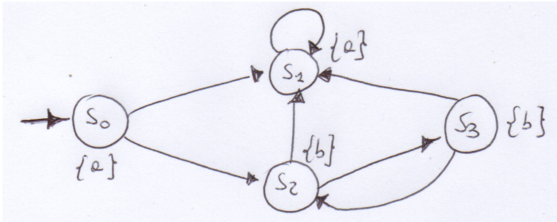
From $< s_3, q_2 >$:

- $s_3 \longrightarrow s_5$ $L(s_5) = \{a, c\}$
  $\delta(q_2, \{a, c\}) = \{q_3\}$.

we can stop constructing $TS \otimes \mathcal{A}'$ because we can already decide that $TS \not\models P_{safe}$.
Indeed in $TS \otimes \mathcal{A}'$ a state in which q_3 is present is reachable *. The path gives us a counter-example for the property:
$s_0 s_1 s_3 s_5 ...$ whose trace is $\{b, c\}\{a\}\{b\}\{a, c\}... \not\models P_{safe}$

2 Linear Temporal Logic

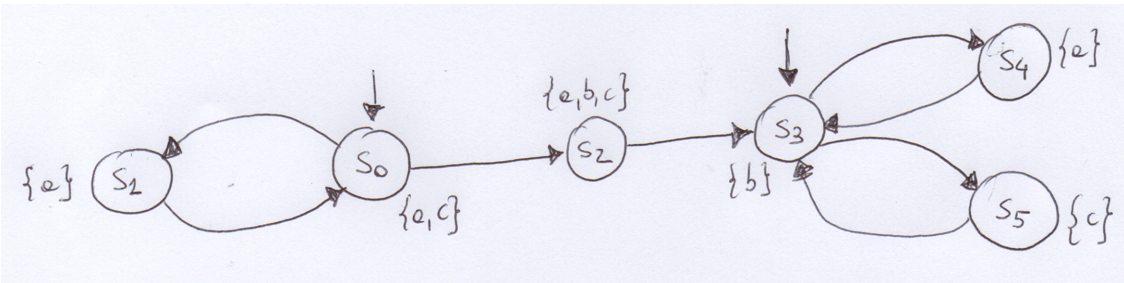
Exercise 2.1. *Consider the following transition system TS on $AP = \{a, b\}$:*



and the following LTL formula $\varphi = \Box\Diamond\neg a$.

1. *Derive an NBAs $\mathcal{A}$ for the formula $\neg\varphi$, i.e. such that $\mathcal{L}_\omega(\mathcal{A}) = \mathcal{L}_\omega(\neg\varphi)$.*
2. *Tell whether or not it holds $TS \models \varphi$ by constructing $TS \otimes \mathcal{A}$ and checking the proper persistence property related to the accepting states of $\mathcal{A}$. If $TS \not\models \varphi$ then provide a counterexample, i.e. give a path $\pi \in Paths(TS)$ such that $\pi \not\models \varphi$.*
   Hint: it is not required to construct all the transition system $TS \otimes \mathcal{A}$, but only the reachable portion that is needed to answer to the question.

Exercise 2.2. *Consider the following transition system TS on $AP = \{a, b, c\}$.*



1. *Decide, for each LTL formula φ_i below, whether or not $TS \models \varphi_i$. Justify your answers! If $TS \not\models \varphi_i$ provide a path $\pi \in Paths(TS)$ such that $\pi \not\models \varphi_i$.*

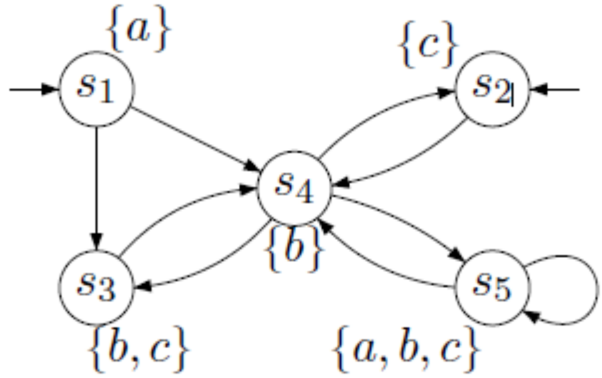
$$\varphi_1 = \Diamond b \qquad \varphi_2 = \bigcirc\bigcirc(c \vee b)$$
$$\varphi_3 = \Diamond(a \wedge b \wedge c) \qquad \varphi_4 = (\bigcirc\bigcirc\bigcirc a) \vee (\Diamond\Box a)$$
$$\varphi_5 = (a \vee b)\,\mathcal{U}\,(a \vee c) \qquad \varphi_6 = \Box(b \longrightarrow (\bigcirc\Diamond c))$$

2. *Consider the following fairness assumptions written as LTL formulas:*

$$\psi_1^{\text{fair}} = \Box\Diamond c \longrightarrow \Box\Diamond b \qquad \psi_2^{\text{fair}} = \Box\Diamond a \qquad \psi_3^{\text{fair}} = \Box\Diamond b \longrightarrow ((\Box\Diamond a) \wedge (\Box\Diamond c))$$

   (a) **(2 points)** *Decide whether or not $TS \models_{\text{fair}} \varphi_1$ under the three different fairness conditions ψ_{fair}^i, $i \in \{1, 2, 3\}$,* **separately**. *Whenever $TS \not\models_{\text{fair}} \varphi_1$ provide a path $\pi \in Paths(TS)$ such that $\pi \not\models \varphi_1$ and arguing that π is fair with respect to ψ_{fair}^i.*

   (b) **(2 points)** *Decide whether or not $TS \models_{\text{fair}} \varphi_6$ under the three different fairness conditions ψ_{fair}^i, $i \in \{1, 2, 3\}$,* **separately**. *Whenever $TS \not\models_{\text{fair}} \varphi_6$ provide a path $\pi \in Paths(TS)$ such that $\pi \not\models \varphi_6$ and arguing that π is fair with respect to ψ_{fair}^i.*

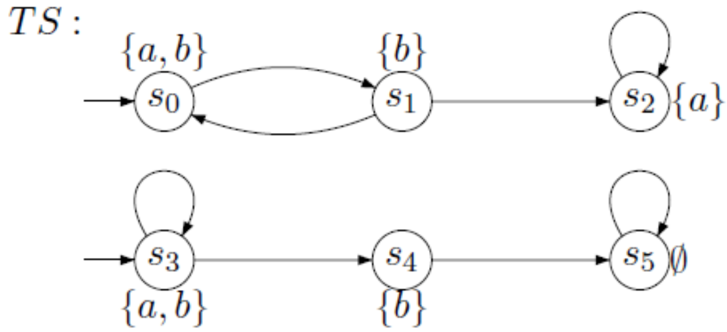


Exercise 2.3. *Consider the transition system TS over the set of atomic proposition $AP = \{a, b, c\}$: Decide for each of the LTL formulas φ_i holds. Justify your answer!*

If $TS \not\models \varphi_i$, provide a path $\pi \in paths(TS)$ such that $\pi \not\models \varphi_i$.

$\varphi_1 = \Diamond\Box c$	$\varphi_4 = \Box a$
$\varphi_2 = \Box\Diamond c$	$\varphi_5 = a\mathcal{U}\Box(b \vee c)$
$\varphi_3 = \bigcirc\neg c \longrightarrow \bigcirc\bigcirc c$	$\varphi_6 = (\bigcirc\bigcirc b)\mathcal{U}(b \vee c)$

Exercise 2.4. *Let $AP = \{a, b, c\}$. Consider the transition system TS over AP outlined below*



and the LTL fairness assumption $fair = (\Box\Diamond(a \wedge b) \longrightarrow \Box\Diamond\neg c) \wedge (\Box\Diamond(a \wedge b) \longrightarrow \Box\Diamond\neg b)$.
a) Specify the fair paths of TS!
b) Decide for each of the following LTL formulas φ_i whether it holds $TS \models_{fair} \varphi_i$:

$$\varphi_1 = \bigcirc\neg a \longrightarrow \Diamond\Box a \qquad \varphi_2 = b\mathcal{U}\Box\neg b \qquad \varphi_3 = b\mathcal{W}\Box\neg b$$

In case $TS \not\models_{fair} \varphi_i$, indicate a path $\pi \in \in FairPaths(TS)$ for which $\pi \not\models \varphi$ holds.

Exercise 2.5. *Consider the following LTL formula:*

$$\varphi = \Box(b \longrightarrow (b\,\mathcal{U}\,(a \wedge \neg b)))$$

1. *Put the formula $\neg\varphi$ in Positive Normal Form containing the weak until operator $\mathcal{W}$ as dual of the until.*

2. *Convert $\neg\varphi$ into an equivalent LTL formula ψ that is constructed according to the following grammar:*

$$\Phi ::= true \mid false \mid \Phi \wedge \Phi \mid \neg\Phi \mid \bigcirc\Phi \mid \Phi\,\mathcal{U}\,\Phi$$

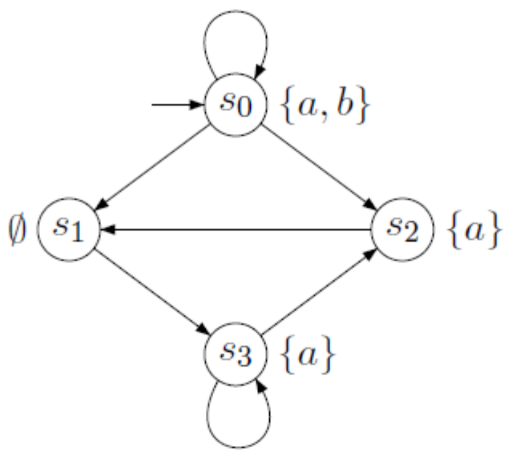
then, construct the set closure(ψ) and derive at least one set B that is elementary set with respect to closure(ψ).

Exercise 2.6. *Transform the LTL–formula $\varphi = \neg\Diamond(\neg(a\mathcal{U}c) \longrightarrow ((b \wedge \neg d)\mathcal{U}a))$ in positive normal form, once using the W–operator and once using the R–operator.*

Exercise 2.7. *We consider model checking of $\omega-$regular LT properties which are defined by LTL formulas. Therefore let φ_1 and φ_2 be as follows:*

$\varphi_1 = \Box\Diamond a \longrightarrow \Box\Diamond b$

$\varphi_2 = \Diamond(a \wedge \bigcirc a)$



Further, our model is represented by the transition system TS over $AP = \{a, b\}$ which is given as outlined on the right. We check whether $TS| = \varphi_i$ for $i = 1, 2$ using the nested depth–first search algorithm from the lecture. Therefore proceed as follows:

a) Derive an NBA A_i for the LTL formula $\neg\varphi_i$ (for $i = 1, 2$). More precisely, for A_i it must hold $L_\omega(A_i) = L_\omega(\neg\varphi_i)$.
Hint: Four, respectively three states suffice.

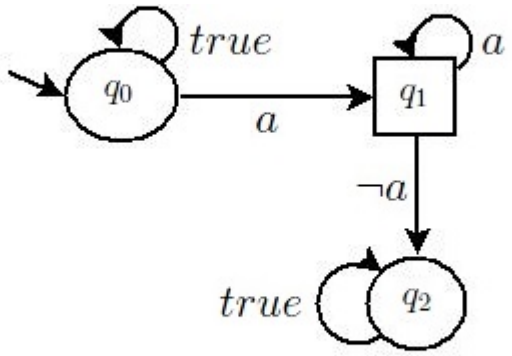
b) Outline the reachable fragment of the product transition system $TS \otimes A_i$.

c) Sketch the main steps of the nested depth–first search algorithm for the persistency check on $TS \otimes A_i$.
d) Provide the counterexample computed by the algorithm if $TS \nvDash \varphi_i$.

Solutions

Solution of Exercise 2.1

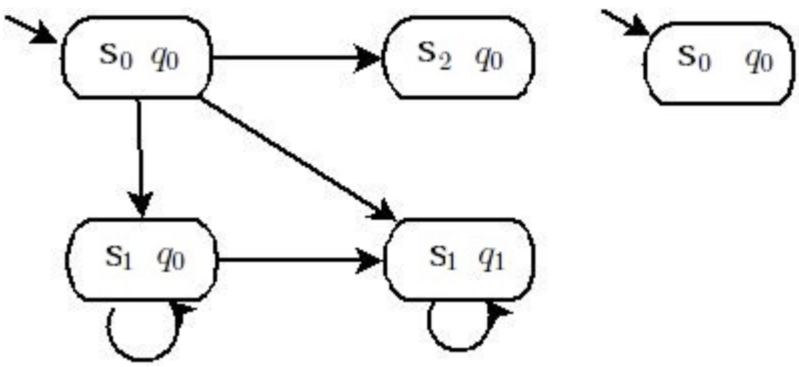
1. We first note the $\neg\varphi \equiv \neg\Box\Diamond\neg a \equiv \Diamond\Box a$
   An NBA $\mathcal{A}$ for $\Diamond\Box a$ is the following

   where:
   $a \equiv \{\{a\}, \{a, b\}\}$
   $\neg a \equiv \{\{\}, \{b\}\}$
   $true \equiv \{\{a\}, \{b\}, \{a, b\}, \{\}\}$
   $F = \{q_1\}$

2. Let's start constructing the product $TS \otimes A$

   The initial state are those (s_0, x) where
   $x \in \delta(q_0, L(s_0)) =$
   $\delta(q_0, \{a\}) =$
   $\{q_0, q_1\}$
   that is, there are two initial states: (s_0, q_0) and (s_0, q_1)

   $from(s_0, q_0)$:
   $s_0 \rightarrow s_1, \delta(q_0, L(s_1)) =$
   $\delta(q_0, \{a\}) = \{q_0, q_1\}$

$s_0 \to s_2, \delta(q_0, L(s_2)) =$
$\delta(q_0, \{b\}) = \{q_0\}$

$from(s_1, q_1)$:
$s_1 \to s_1, \delta(q_1, L(s_1)) =$
$\delta(q_1, \{a\}) = \{q_1\}$

$from(s_1, q_0)$:
$s_1 \to s_1, \delta(q_0, L(s_1)) =$
$\delta(q_0, \{a\}) = \{q_0, q_1\}$

We can stop constructing the product because it is now clear that there is a reachable strongly connected component (SCC) in which q_1 is visited infinitely often.

This means that $L_\omega(TS \otimes A) \neq \emptyset$, thus there is a behaviour in TS that violates the formula $\varphi = \Box\Diamond\neg a$.
Thus $TS \not\models \varphi$ and a counterexample is the path $\pi : s_0(s_1)^\omega$

Solution of Exercise 2.2

1. $TS \not\models \Diamond b$

   Counterexample: $\pi = (s_0 s_1)^\omega$

   $TS \models \bigcirc \bigcirc (c \vee b)$

   Because the following are the all the possible prefixes of paths of TS:
   $s_0\ s_1\ s_0$...
   $s_0\ s_2\ s_3$...
   $s_3\ s_4\ s_3$
   $s_3\ s_5\ s_3$
   third state of each paths (s_0 and s_3) satisfies $(c \vee b)$

   $TS \not\models \Diamond(a \wedge b \wedge c)$

   Because all the runs that start in s_3 never reach the state s_2 that is the only one in which $a \wedge b \wedge c$ is true

   $TS \not\models (\bigcirc \bigcirc \bigcirc a) \vee (\Diamond\Box a)$

   Because of the run $s_3\ s_4\ s_3\ s_5\ (s_3\ s_5)^\omega$ in which the first "s_5" $\not\models a$ and $(s_3\ s_5)^\omega \not\models (\Diamond\Box a)$

   $TS \models (a \vee b)\,\mathcal{U}\,(a \vee c)$

   In all runs:
   s_0... , $s_0 \models (a \vee b)\,\mathcal{U}\,(a \vee c)$
   $s_3\ s_4$ ... $s_3 \models (a \vee b)$, $s_4 \models (a \vee b)$
   $s_3\ s_5$ ... $s_3 \models (a \vee b)$, $s_5 \models (a \vee b)$

   $TS \not\models \Box(b \longrightarrow (\bigcirc\Diamond c))$

   Because of the runs s_0 ... $s_0\ s_2\ s_3\ s_4\ (s_3\ s_4)^\omega$ in which: $s_2 = b\ s_3 = \Diamond c$ and $(s_3\ s_4)^\omega$ is never c

2.
- In case of fairness $\psi_1^{\text{fair}} = \Box\Diamond c \longrightarrow \Box\Diamond b$
  the path $(s_0\ s_1)^\omega$ is not fair, thus $TS \models_{\text{fair}} \varphi_1$ under the fairness condition ψ_1^{fair}.

  In case of fairness $\psi_2^{\text{fair}} = \Box\Diamond a$
  the runs s_0 ... $s_0\ s_2\ s_3$ ... $s_3\ (s_3\ s_4)^\omega$ are not fair.
  This does not effect the satisfaction of φ_1:
  $TS \not\models_{\text{fair}} \varphi_1$ because the run $(s_0\ s_1)^\omega$ is fair for ψ_2^{fair}

  In case of ψ_3^{fair}: $\Box\Diamond b \longrightarrow ((\Box\Diamond a) \wedge (\Box\Diamond c))$
  the runs s_0 ... $s_0\ s_2\ s_3$ ... $s_3\ (s_3\ s_4)^\omega$, s_0 ... $s_0\ s_2\ s_3$ ... $s_3\ (s_3\ s_5)^\omega$ are not fair.
  This, again, does not effect the satisfaction of φ_1.
  $TS \not\models_{\text{fair}} \varphi_1$ under ψ_3^{fair} because $(s_0\ s_1)^\omega$ is fair in ψ_3^{fair}
- In the previous case we discussed the runs that are not fair under ψ_1^{fair},ψ_2^{fair},ψ_3^{fair}.
  $TS \not\models_{\text{fair}} \varphi_6$ with ψ_1^{fair} because the paths s_0 ... $s_0\ s_2\ (s_3\ s_4)^\omega$ are fair for ψ_1^{fair}
  $TS \not\models_{\text{fair}} \varphi_6$ with ψ_2^{fair} because the paths s_0 ... $s_0\ s_2\ (s_3\ s_4)^\omega$ are fair for ψ_2^{fair}
  $TS \models_{\text{fair}} \varphi_6$ with ψ_3^{fair} because the paths s_0 ... $s_0\ s_2\ (s_3\ s_4)^\omega$ are not fair for ψ_3^{fair}

Solution of Exercise 2.3

We have to decide the validity of the given LTL formulas wrt.
the transition system on the right. This yields:

$\varphi_1 = \Diamond\Box c$	*no* $s_2 s_4 s_2 s_4 \ldots$
$\varphi_2 = \Box\Diamond c$	*yes*
$\varphi_3 = \bigcirc\neg c \longrightarrow \bigcirc\bigcirc c$	*yes*
$\varphi_4 = \Box a$	*no* $s_2 \ldots$
$\varphi_5 = a\mathcal{U}\Box(b \vee c)$	*yes*
$\varphi_6 = (\bigcirc\bigcirc b)\mathcal{U}(b \vee c)$	*no* $s_1 s_4 s_2 \ldots$

Solution of Exercise 2.4

$a)$ The fair paths of TS are defined by

$$fair = (\Box\Diamond(a \wedge b) \longrightarrow \Box\Diamond\neg c) \wedge (\Box\Diamond(a \wedge b) \longrightarrow \Box\Diamond\neg b) :$$

The conclusion in the first conjunction $(\Box\Diamond(a \wedge b) \longrightarrow \Box\Diamond\neg c)$ is fulfilled by every path, since no state in TS is labeled with c. Formally, we have $\Box\neg c \longrightarrow \Box\Diamond\neg c$ and therefore our claim holds. Consider the second part $(\Box\Diamond(a \wedge b) \longrightarrow \Box\Diamond\neg b)$ of fair: Its premise is fulfilled only on the path $\pi = s_3^\omega$. But $\pi \not\models \Box\Diamond\neg b$. Therefore π is the only unfair path in TS:

$$FairPaths(TS) = \mathcal{L}_\omega((s_0 s_1)^\omega + (s_0 s_1)^+ s_2^\omega + s_3^+ s_4 s_5^\omega)$$

$b)$

- $\varphi_1 = \bigcirc\neg a \longrightarrow \Diamond\Box a$
  Consider the path $\pi_1 = s_3 s_4 s_5^\omega \in FairPaths(TS)$. For its corresponding trace

  $$trace(\pi_1) = \sigma_1 = \{a, b\}\{b\}\emptyset^\omega$$

  it holds $\sigma_1 \in Words(\bigcirc\neg a)$, but $\sigma_1 \notin Words(\Diamond\Box a)$.
  $\Rightarrow \sigma_1 \notin Words(\bigcirc\neg a \longrightarrow \Diamond\Box a)$
  $\Rightarrow TS \not\models_{fair} \bigcirc\neg a \longrightarrow \Diamond\Box a$

- $\varphi_2 = b\mathcal{U}\Box\neg b$
  Consider the path $\pi_2 = (s_0 s_1)^\omega \in FairPaths(TS)$. Here, we have
  $$trace(\pi_2) = \sigma_2 = (\{a,b\}\{b\})^\omega$$
  and $\sigma_2 \nvDash_{fair} b\mathcal{U}\Box\neg b$ since there exists no $i \geq$ s.t. $\sigma_2[i...] \vDash \Box\neg b$.
  $\Rightarrow TS \nvDash_{fair} b\mathcal{U}\Box\neg b$

- $\varphi_3 = b\mathcal{W}\Box\neg b$
  It holds $TS \vDash_{fair} \varphi_1$

Solution of Exercise 2.5

1. $\neg\varphi = \neg\Box(b \longrightarrow (b\,\mathcal{U}\,(a \wedge \neg b))) \equiv$
   $\equiv \Diamond\neg(b \longrightarrow (b\,\mathcal{U}\,(a \wedge \neg b))) \equiv$
   $\equiv \Diamond\neg(\neg b \vee (b\,\mathcal{U}\,(a \wedge \neg b))) \equiv$
   $\equiv \Diamond(\neg\neg b \wedge \neg(b\,\mathcal{U}\,(a \wedge \neg b))) \equiv$
   $\equiv \Diamond(b \wedge (b \wedge \neg(a \wedge \neg b))\mathcal{W}(\neg b \wedge \neg(a \wedge \neg b))) \equiv$
   $\equiv \Diamond(b \wedge (b \wedge (\neg a \vee b))\mathcal{W}(\neg b \wedge (\neg a \vee b)))$
   the last form is in PNF.

2. As in the previous case $\neg\varphi \equiv \Diamond(b \wedge \neg(b\mathcal{U}(a \wedge \neg b)))$
   So $\neg\varphi \equiv true\,\mathcal{U}\,(b \wedge \neg(b\,\mathcal{U}\,(a \wedge \neg b)))$
   Let $\varphi \equiv true\,\mathcal{U}(b \wedge \neg(b\,\mathcal{U}\,(a \wedge \neg b)))$
   $\mathrm{closure}(\psi) = \{true, a, b, a \wedge \neg b, (b\mathcal{U}(a \wedge \neg b)), b \wedge \neg((b\,\mathcal{U}\,(a \wedge \neg b))), \varphi\} \cup$
   $\{false, \neg a, \neg b, \neg(a \wedge \neg b), \neg(b\,\mathcal{U}\,(a \wedge \neg b)), \neg(b \wedge \neg((b\,\mathcal{U}\,(a \wedge \neg b)))), \neg\varphi\}$
   an example of elementary set is $B = \{true, a, \neg b, (b\,\mathcal{U}\,(a \wedge \neg b)), \neg(b \wedge \neg((b\,\mathcal{U}\,(a \wedge \neg b)))), \varphi\}$

Solution of Exercise 2.6

We have the following LTL formula:

$$\begin{aligned}\varphi = \neg\Diamond\big(\neg(a\mathsf{U}c) \rightarrow ((b \wedge \neg d)\mathsf{U}a)\big) &\equiv \Box\neg\big((a\mathsf{U}c) \vee ((b \wedge \neg d)\mathsf{U}a)\big) && (^*\ \Diamond\varphi \equiv \neg\Box\neg\varphi \text{ and } \varphi \rightarrow \psi \equiv \neg\varphi \vee \psi\ ^*)\\ &\equiv \Box\big(\neg(a\mathsf{U}c) \wedge \neg((b \wedge \neg d)\mathsf{U}a)\big) && (^*\ \text{deMorgan}\ ^*)\end{aligned}$$

a) PNF with W–operator (weak until): Rewrite rule for until: $\neg(\varphi\mathsf{U}\psi) \rightsquigarrow (\varphi \wedge \neg\psi)\mathsf{W}(\neg\varphi \wedge \neg\psi)$. We obtain for φ as above:

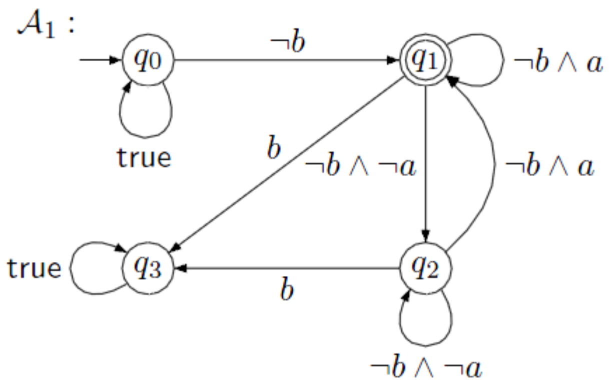
$$\begin{aligned}\varphi &\equiv \Box\big((a \wedge \neg c)\mathsf{W}(\neg a \wedge \neg c) \wedge (b \wedge \neg d \wedge \neg a)\mathsf{W}(\neg(b \wedge \neg d) \wedge \neg a)\big)\\ &\equiv \big((a \wedge \neg c)\mathsf{W}(\neg a \wedge \neg c) \wedge (b \wedge \neg d \wedge \neg a)\mathsf{W}((\neg b \vee d) \wedge \neg a)\big)\mathsf{W}\mathsf{false}\end{aligned}$$

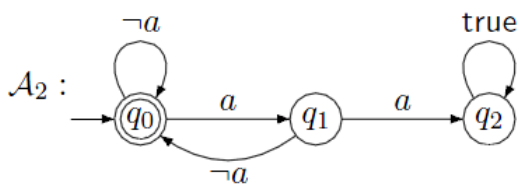
b) PNF with R–operator (release): Rewrite rule for until: $\neg(\varphi\mathsf{U}\psi) \rightsquigarrow \neg\varphi\mathsf{R}\neg\psi$. We obtain for φ as above:

$$\begin{aligned}\varphi &\equiv \Box\big(\neg a\mathsf{R}\neg c \wedge \neg(b \wedge \neg d)\mathsf{R}\neg a\big)\\ &\equiv \mathsf{false}\mathsf{R}(\neg a\mathsf{R}\neg c \wedge (\neg b \vee d)\mathsf{R}\neg a)\end{aligned}$$

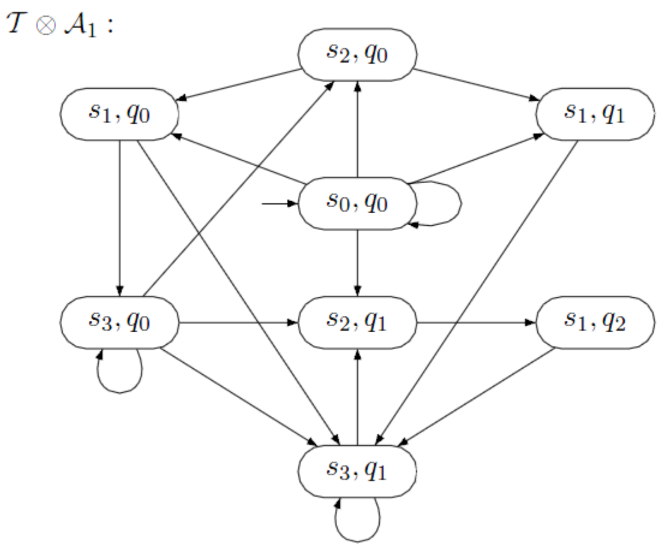
Solution of Exercise 2.7

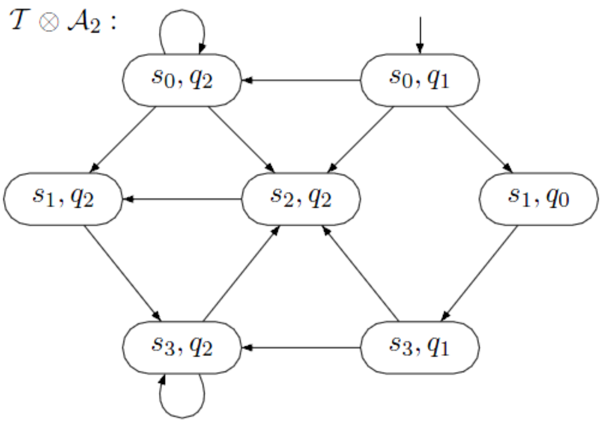
$a)$ The automata accepting the complement languages of φ_1 and φ_2 are:





$b)$ The reachable fragments of $T \otimes A_i$ for $i = 1, 2$ are as follows:





$c)$ Sketch the main steps of the nested depth-first search algorithm for the persistency check on $T \otimes A_i$: We check for the persistence property "eventually forever ¬F".

1. Constructed the product $T \otimes A_1$, we can see that there is a reachable strongly connected component (SCC) in which q_1 is visited infinitely often.

   This means that $L_\omega(TS \otimes A_1) \neq \emptyset$, thus there is a behaviour in TS that violates the formula φ_1. So, $TS \nvDash \varphi_1$

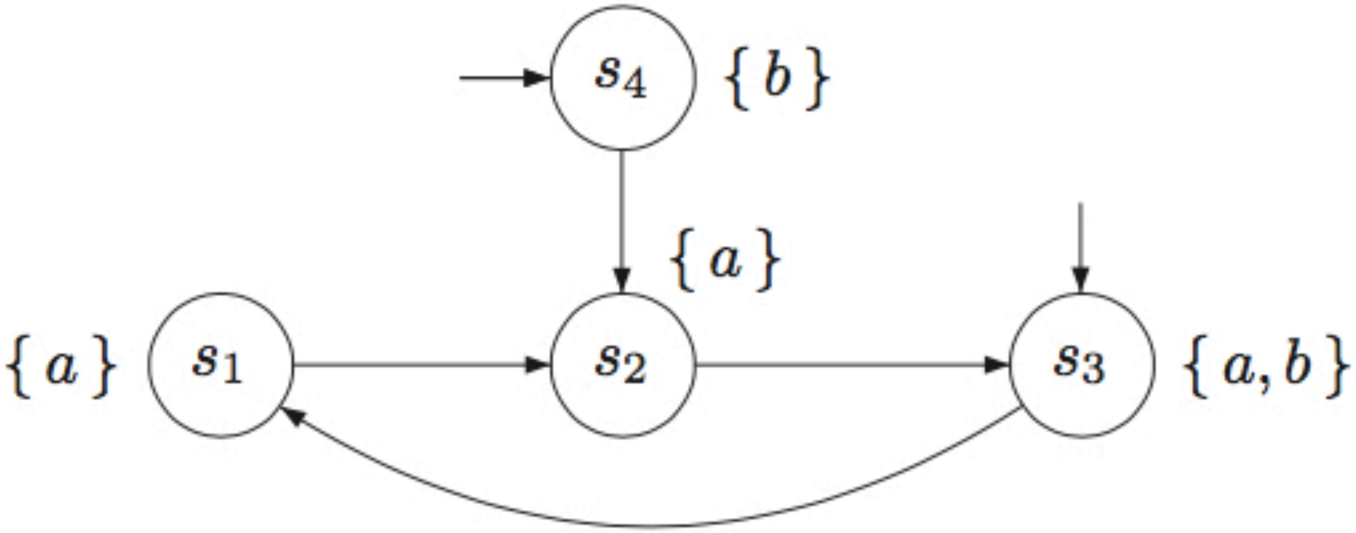
2. Constructed the product $T \otimes A_2$, we can see that there not a reachable strongly connected component (SCC) in which q_0 is visited infinitely often.

   This means that $L_\omega(TS \otimes A_2) = \emptyset$, thus there is not a behaviour in TS that violates the formula φ_2.
   So, $TS \vDash \varphi_2$

$d)$
$TS \nvDash \varphi_1$. counterexample: $< s_0, q_0 >, < s_1, q_1 >, < s_3, q_1 >, < s_2, q_1 >, < s_1, q_2 >, < s_3, q_1 >$
$TS \vDash \varphi_2$.

3 LTL Exercises from Book

EXERCISE 5.1. Consider the following transition system over the set of atomic propositions $\{a, b\}$:



Indicate for each of the following LTL formulae the set of states for which these formulae are fulfilled:

(a) $\bigcirc\, a$

(b) $\bigcirc\bigcirc\bigcirc\, a$

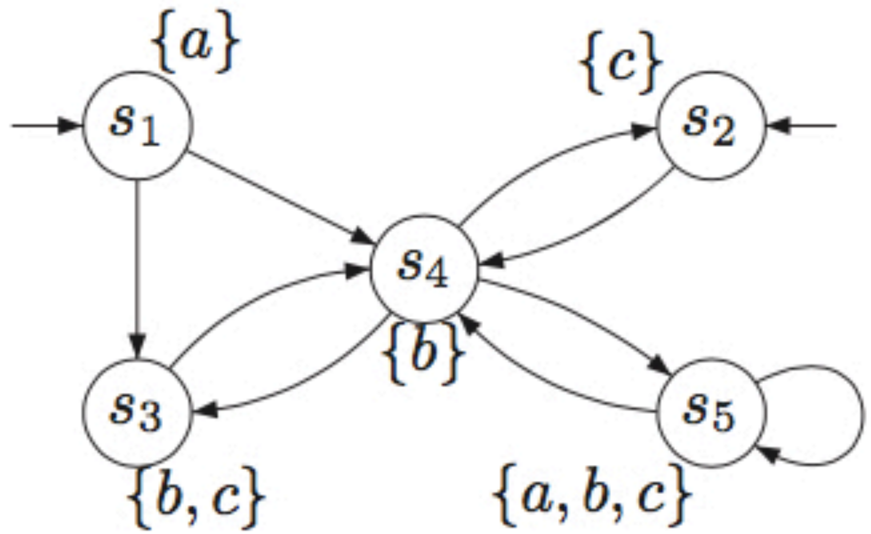
(c) $\Box\, b$

(d) $\Box\Diamond\, a$

(e) $\Box\,(b \,\mathsf{U}\, a)$

(f) $\Diamond\,(a \,\mathsf{U}\, b)$

EXERCISE 5.2. Consider the transition system TS over the set of atomic propositions $AP = \{a, b, c\}$:



Decide for each of the LTL formulae φ_i below, whether $TS \models \varphi_i$ holds. Justify your answers! If $TS \not\models \varphi_i$, provide a path $\pi \in Paths(TS)$ such that $\pi \not\models \varphi_i$.

$$
\begin{aligned}
\varphi_1 &= \Diamond \Box c \\
\varphi_2 &= \Box \Diamond c \\
\varphi_3 &= \bigcirc \neg c \rightarrow \bigcirc \bigcirc c \\
\varphi_4 &= \Box a \\
\varphi_5 &= a \, \mathsf{U} \, \Box (b \vee c) \\
\varphi_6 &= (\bigcirc \bigcirc b) \, \mathsf{U} \, (b \vee c)
\end{aligned}
$$

EXERCISE 5.4. Suppose we have two users, *Peter* and *Betsy*, and a single printer device *Printer*. Both users perform several tasks, and every now and then they want to print their results on the *Printer*. Since there is only a single printer, only one user can print a job at a time. Suppose we have the following atomic propositions for *Peter* at our disposal:

- *Peter.request* ::= indicates that *Peter* requests usage of the printer;
- *Peter.use* ::= indicates that *Peter* uses the printer;
- *Peter.release* ::= indicates that *Peter* releases the printer.

For *Betsy*, similar predicates are defined. Specify in LTL the following properties:

(a) Mutual exclusion, i.e., only one user at a time can use the printer.

(b) Finite time of usage, i.e., a user can print only for a finite amount of time.

(c) Absence of individual starvation, i.e., if a user wants to print something, he/she eventually is able to do so.

(d) Absence of blocking, i.e., a user can always request to use the printer

(e) Alternating access, i.e., users must strictly alternate in printing.

EXERCISE 5.6. Which of the following equivalences are correct? Prove the equivalence or provide a counterexample that illustrates that the formula on the left and the formula on the right are not equivalent.

(a) $\Box\varphi \rightarrow \Diamond\psi \equiv \varphi \,\mathsf{U}\, (\psi \vee \neg\varphi)$

(b) $\Diamond\Box\varphi \rightarrow \Box\Diamond\psi \equiv \Box\big(\varphi \,\mathsf{U}\, (\psi \vee \neg\varphi)\big)$

(c) $\Box\Box(\varphi \vee \neg\psi) \equiv \neg\Diamond(\neg\varphi \wedge \psi)$

(d) $\Diamond(\varphi \wedge \psi) \equiv \Diamond\varphi \wedge \Diamond\psi$

(e) $\Box\varphi \wedge \bigcirc\Diamond\varphi \equiv \Box\varphi$

(f) $\Diamond\varphi \wedge \bigcirc\Box\varphi \equiv \Diamond\varphi$

(g) $\Box\Diamond\varphi \rightarrow \Box\Diamond\psi \equiv \Box\big(\varphi \rightarrow \Diamond\psi\big)$

(h) $\neg(\varphi_1 \,\mathsf{U}\, \varphi_2) \equiv \neg\varphi_2 \,\mathsf{W}\, (\neg\varphi_1 \wedge \neg\varphi_2)$

(i) $\bigcirc\Diamond\varphi_1 \equiv \Diamond\bigcirc\varphi_2$

(j) $(\Diamond\Box\varphi_1) \wedge (\Diamond\Box\varphi_2) \equiv \Diamond(\Box\varphi_1 \wedge \Box\varphi_2)$

(k) $(\varphi_1 \,\mathsf{U}\, \varphi_2) \,\mathsf{U}\, \varphi_2 \equiv \varphi_1 \,\mathsf{U}\, \varphi_2$

EXERCISE 5.11. Consider the transition system TS in Figure 5.25 with the set $AP = \{a, b, c\}$ of atomic propositions. Note that this is a single transition system with two initial states. Consider the LTL fairness assumption

$$fair = (\Box\Diamond(a \wedge b) \rightarrow \Box\Diamond\neg c) \wedge (\Diamond\Box(a \wedge b) \rightarrow \Box\Diamond\neg b).$$

Questions:

(a) Determine the fair paths in TS, i.e., the initial, infinite paths satisfying *fair*

(b) For each of the following LTL formulae:

$$\begin{aligned}
\varphi_1 &= \Diamond\Box a \\
\varphi_2 &= \bigcirc\neg a \longrightarrow \Diamond\Box a \\
\varphi_3 &= \Box a \\
\varphi_4 &= b \,\mathsf{U}\, \Box\neg b \\
\varphi_5 &= b \,\mathsf{W}\, \Box\neg b \\
\varphi_6 &= \bigcirc\bigcirc b \,\mathsf{U}\, \Box\neg b
\end{aligned}$$

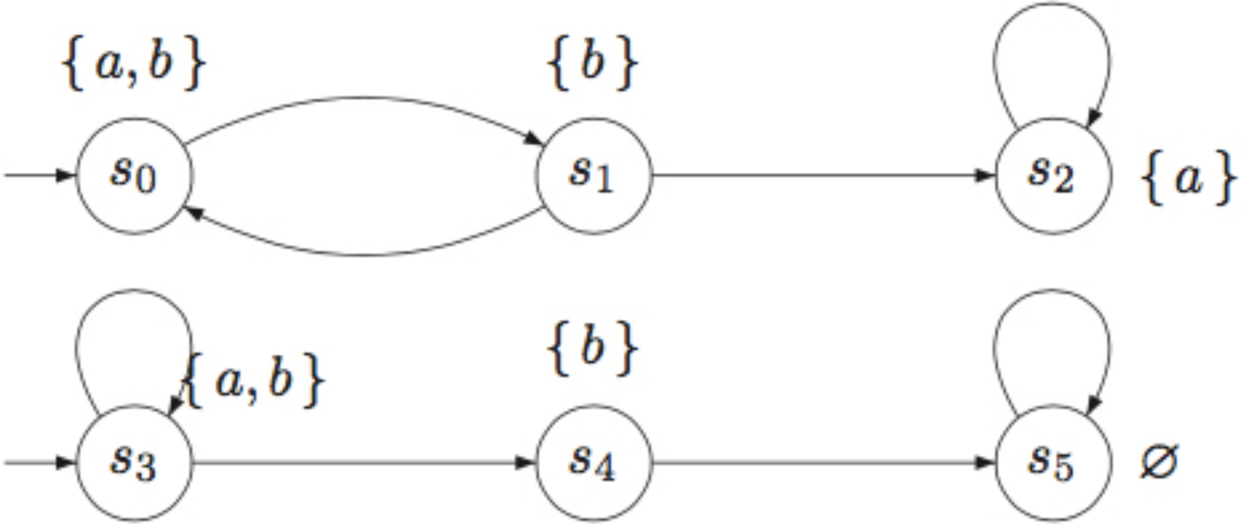


Figure 5.25: Transition system for Exercise 5.11.

determine whether $TS \models_{fair} \varphi_i$. In case $TS \not\models_{fair} \varphi_i$, indicate a path $\pi \in Paths(TS)$ for which $\pi \not\models \varphi_i$.

EXERCISE 5.13. Provide an NBA for each of the following LTL formulae:

$$\Box(a \vee \neg \bigcirc b) \quad \text{and} \quad \Diamond a \ \vee \ \Box\Diamond(a \leftrightarrow b) \quad \text{and} \quad \bigcirc \bigcirc (a \vee \Diamond\Box b).$$

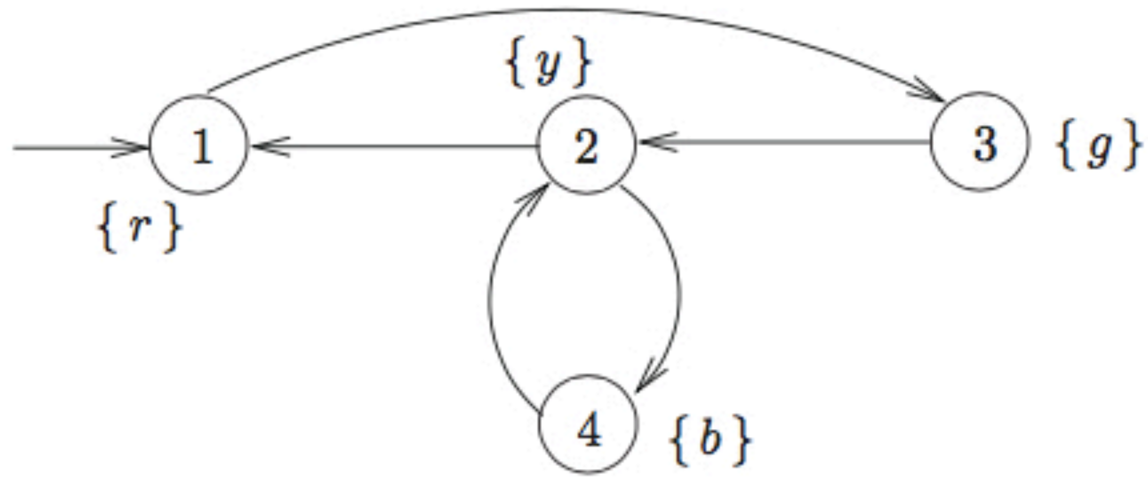
EXERCISE 5.17. Let $\psi = \Box\,(a \leftrightarrow \bigcirc \neg a)$ and $AP = \{\, a \,\}$.

(a) Show that ψ can be transformed into the following equivalent basic LTL formula

$$\varphi = \neg\left[\,\text{true}\,\mathsf{U}\,(\neg\,(a \wedge \bigcirc \neg a) \wedge \neg\,(\neg a \wedge \neg \bigcirc\, \neg a))\right].$$

4 CTL Exercises from Book

EXERCISE 6.1. Consider the following transition system over $AP = \{b, g, r, y\}$:

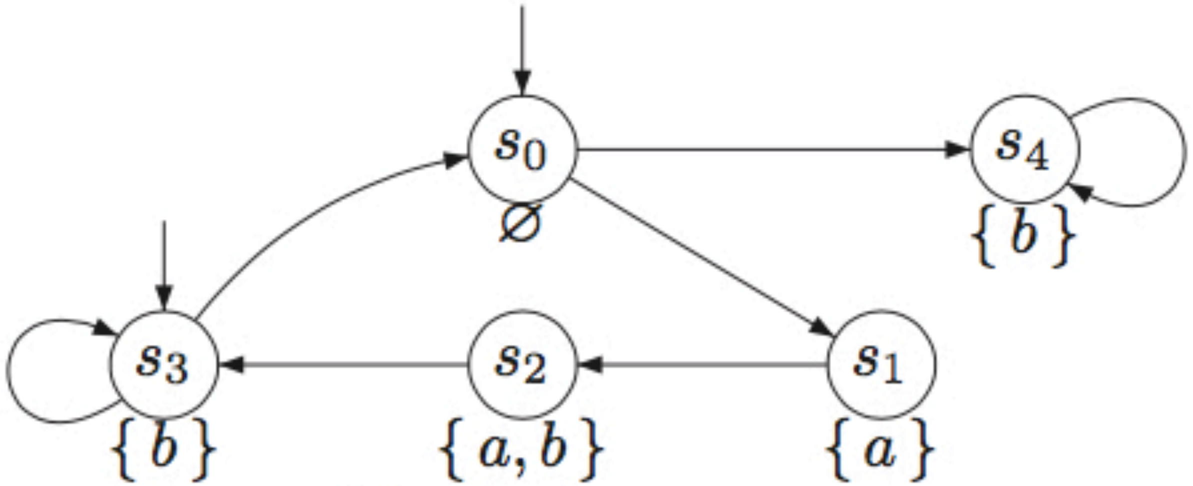


The following atomic propositions are used: r (red), y (yellow), g (green), and b (black). The model is intended to describe a traffic light that is able to blink yellow. You are requested to indicate for each of the following CTL formulae the set of states for which these formulae hold:

(a)	$\forall\Diamond\, y$	(g)	$\exists\Box\, \neg g$
(b)	$\forall\Box\, y$	(h)	$\forall(b\, \mathsf{U}\, \neg b)$
(c)	$\forall\Box\, \forall\Diamond\, y$	(i)	$\exists(b\, \mathsf{U}\, \neg b)$
(d)	$\forall\Diamond\, g$	(j)	$\forall(\neg b\, \mathsf{U}\, \exists\Diamond\, b)$
(e)	$\exists\Diamond\, g$	(k)	$\forall(g\, \mathsf{U}\, \forall(y\, \mathsf{U}\, r))$
(f)	$\exists\Box\, g$	(l)	$\forall(\neg b\, \mathsf{U}\, b)$

EXERCISE 6.2. Consider the following CTL formulae and the transition system TS outlined on the right:

$$\begin{aligned}
\Phi_1 &= \forall(a \,\mathsf{U}\, b) \vee \exists \bigcirc (\forall\Box\, b) \\
\Phi_2 &= \forall\Box\, \forall(a \,\mathsf{U}\, b) \\
\Phi_3 &= (a \wedge b) \rightarrow \exists\Box\, \exists \bigcirc \forall(b \,\mathsf{W}\, a) \\
\Phi_4 &= (\forall\Box\, \exists\Diamond\, \Phi_3)
\end{aligned}$$



Determine the satisfaction sets $Sat(\Phi_i)$ and decide whether $TS \models \Phi_i$ $(1 \leqslant i \leqslant 4)$.

EXERCISE 6.3. Which of the following assertions are correct? Provide a proof or a counterexample.

(a) If $s \models \exists\Box\, a$, then $s \models \forall\Box\, a$.

(b) If $s \models \forall\Box\, a$, then $s \models \exists\Box\, a$.

(c) If $s \models \forall\Diamond\, a \lor \forall\Diamond\, b$, then $s \models \forall\Diamond\,(a \lor b)$.

(d) If $s \models \forall\Diamond\,(a \lor b)$, then $s \models \forall\Diamond\, a \lor \forall\Diamond\, b$.

EXERCISE 6.4. Let Φ and Ψ be arbitrary CTL formulae. Which of the following equivalences for CTL formulae are correct?

(a) $\forall\bigcirc\forall\Diamond\Phi \equiv \forall\Diamond\forall\bigcirc\Phi$

(b) $\exists\bigcirc\exists\Diamond\Phi \equiv \exists\Diamond\exists\bigcirc\Phi$

(c) $\forall\bigcirc\forall\Box\Phi \equiv \forall\Box\forall\bigcirc\Phi$

(d) $\exists\bigcirc\exists\Box\Phi \equiv \exists\Box\exists\bigcirc\Phi$

(e) $\exists\Diamond\exists\Box\Phi \equiv \exists\Box\exists\Diamond\Phi$

(f) $\forall\Box(\Phi \Rightarrow (\neg\Psi \wedge \exists\bigcirc\Phi)) \equiv (\Phi \Rightarrow \neg\forall\Diamond\Psi)$

(g) $\forall\Box(\Phi \Rightarrow \Psi) \equiv (\exists\bigcirc\Phi \Rightarrow \exists\bigcirc\Psi)$

(h) $\neg\forall(\Phi \;\mathsf{U}\; \Psi) \equiv \exists(\Phi \;\mathsf{U}\; \neg\Psi)$

(i) $\exists((\Phi \wedge \Psi) \;\mathsf{U}\; (\neg\Phi \wedge \Psi)) \equiv \exists(\Phi \;\mathsf{U}\; (\neg\Phi \wedge \Psi))$

(j) $\forall(\Phi \;\mathsf{W}\; \Psi) \equiv \neg\exists(\neg\Phi \;\mathsf{W}\; \neg\Psi)$

(k) $\exists(\Phi \;\mathsf{U}\; \Psi) \equiv \exists(\Phi \;\mathsf{U}\; \Psi) \wedge \exists\Diamond\Psi$

(l) $\exists(\Psi \;\mathsf{W}\; \neg\Psi) \vee \forall(\Psi \;\mathsf{U}\; \text{false}) \equiv \exists\bigcirc\Phi \vee \forall\bigcirc\neg\Phi$

(m) $\forall\Box\Phi \wedge (\neg\Phi \vee \exists\bigcirc\exists\Diamond\neg\Phi) \equiv \exists X\neg\Phi \wedge \forall\bigcirc\Phi$

(n) $\forall\Box\forall\Diamond\Phi \equiv \Phi \wedge (\forall\bigcirc\forall\Box\forall\Diamond\Phi) \vee \forall\bigcirc(\forall\Diamond\Phi \wedge \forall\Box\forall\Diamond\Phi)$

(o) $\forall\Box\Phi \equiv \Phi \vee \forall\bigcirc\forall\Box\Phi$

EXERCISE 6.7. Transform the following CTL formulae into ENF and PNF. Show all intermediate steps.

$$\Phi_1 = \forall(\,(\neg a)\,\mathsf{W}\,(b \rightarrow \forall \bigcirc c)\,)$$

$$\Phi_2 = \forall \bigcirc \left(\, \exists((\neg a)\,\mathsf{U}\,(b \wedge \neg c)) \;\vee\; \exists\Box\,\forall \bigcirc a \,\right)$$

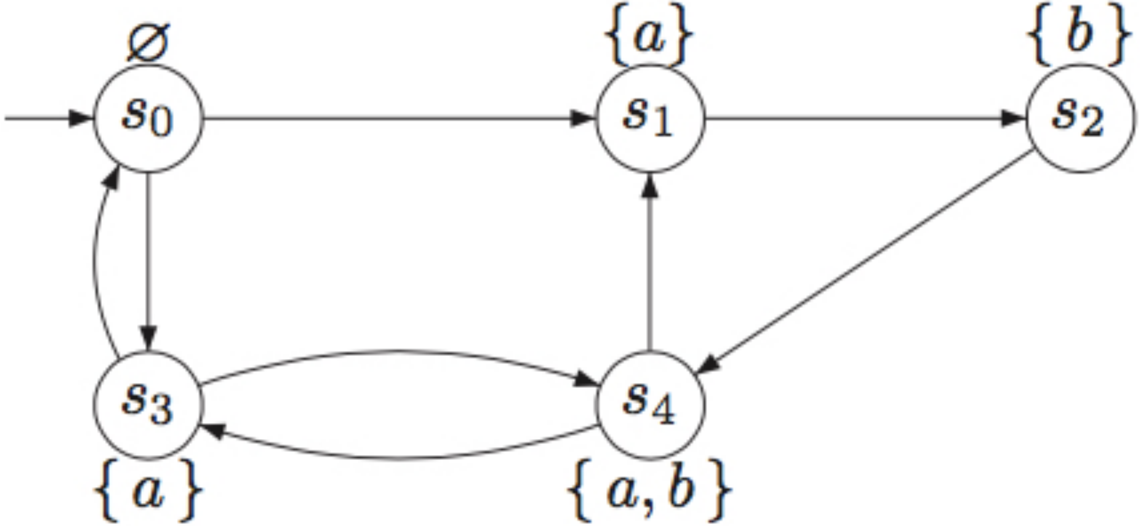
Exercise 6.9. Consider the CTL formula

$$\Phi = \forall\Box\left(a \rightarrow \forall\Diamond\left(b \wedge \neg a\right)\right)$$

and the following CTL fairness assumption:

$$\mathit{fair} = \forall\Diamond\,\forall\bigcirc\left(a \wedge \neg b\right) \rightarrow \forall\Diamond\,\forall\bigcirc\left(b \wedge \neg a\right) \wedge \Diamond\,\Box\,\exists\Diamond\, b \rightarrow \Box\,\Diamond\, b.$$

Prove that $TS \models_{fair} \Phi$ where transition system TS is depicted below.



$\varnothing$
$\{a\}$
$\{b\}$
s_0
s_1
s_2
s_3
s_4
$\{a\}$
$\{a, b\}$

EXERCISE 6.14. Check for each of the following formula pairs (Φ_i, φ_i) whether the CTL formula Φ_i is equivalent to the LTL formula φ_i. Prove the equivalence or provide a counterexample that illustrates why $\Phi_i \not\equiv \varphi_i$.

(a) $\Phi_1 = \forall\Box\forall\bigcirc a$. and $\varphi_1 = \Box\bigcirc a$

(b) $\Phi_2 = \forall\Diamond\forall\bigcirc a$ and $\varphi_2 = \Diamond\bigcirc a$.

(c) $\Phi_3 = \forall\Diamond(a \wedge \exists\bigcirc a)$ and $\varphi_3 = \Diamond(a \wedge \bigcirc a)$.

(d) $\Phi_4 = \forall\Diamond a \ \vee \ \forall\Diamond b$ and $\varphi_4 = \Diamond(a \vee b)$.

(e) $\Phi_5 = \forall\Box(a \rightarrow \forall\Diamond b)$ and $\varphi_5 = \Box(a \rightarrow \Diamond b)$.

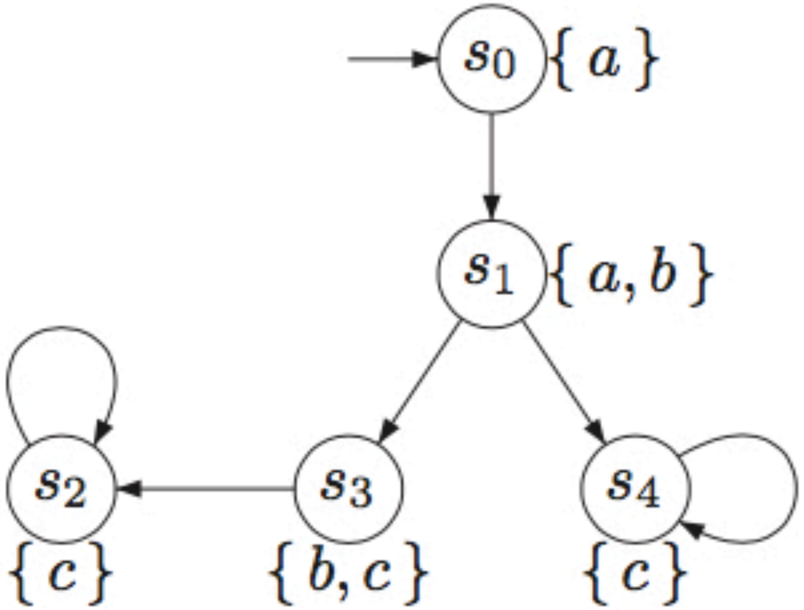
(f) $\Phi_6 = \forall(b \,\mathsf{U}\,(a \wedge \forall\Box b))$ and $\varphi_6 = \Diamond a \ \wedge \ \Box b$.

EXERCISE 6.16.

Consider the following CTL formulae

$$\Phi_1 = \exists\Diamond\,\forall\Box\, c \quad \text{and} \quad \Phi_2 = \forall(a \,\mathsf{U}\, \forall\Diamond\, c)$$

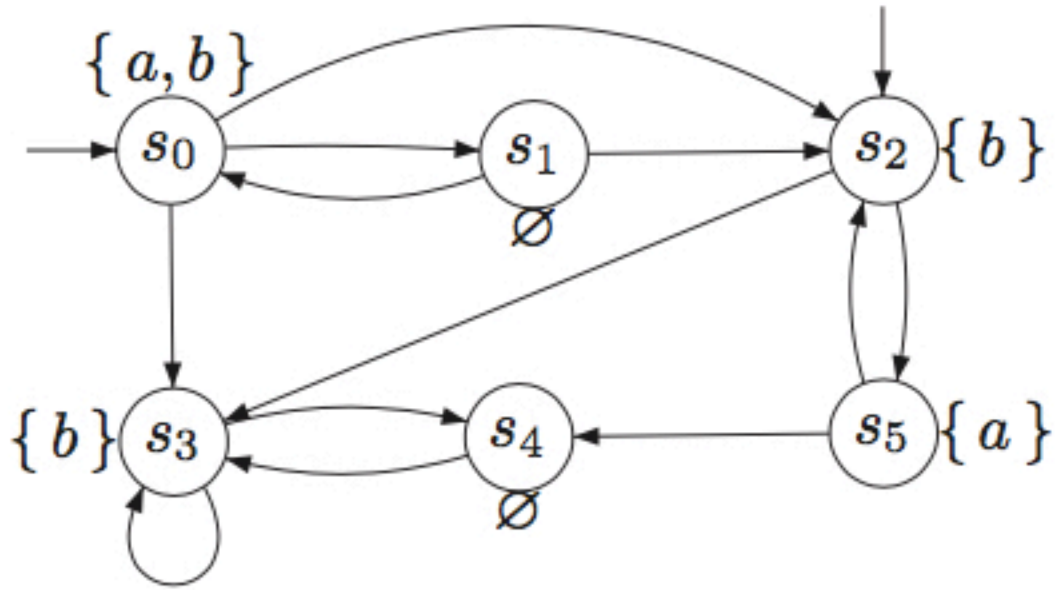
and the transition system TS outlined on the right. Decide whether $TS \models \Phi_i$ for $i = 1, 2$ using the CTL model-checking algorithm. Sketch its main steps.



EXERCISE 6.21. Consider the CTL formula Φ and the strong fairness assumption *sfair*:

$$\begin{aligned} \Phi &= \forall\Box\,\forall\Diamond\, a \\ \mathit{sfair} &= \Box\Diamond\,\underbrace{(b \wedge \neg a)}_{\Phi_1} \rightarrow \Box\Diamond\,\underbrace{\exists(b\,\mathsf{U}\,(a \wedge \neg b))}_{\Psi_1} \end{aligned}$$

and transition system TS over $AP = \{a, b\}$ which is given by



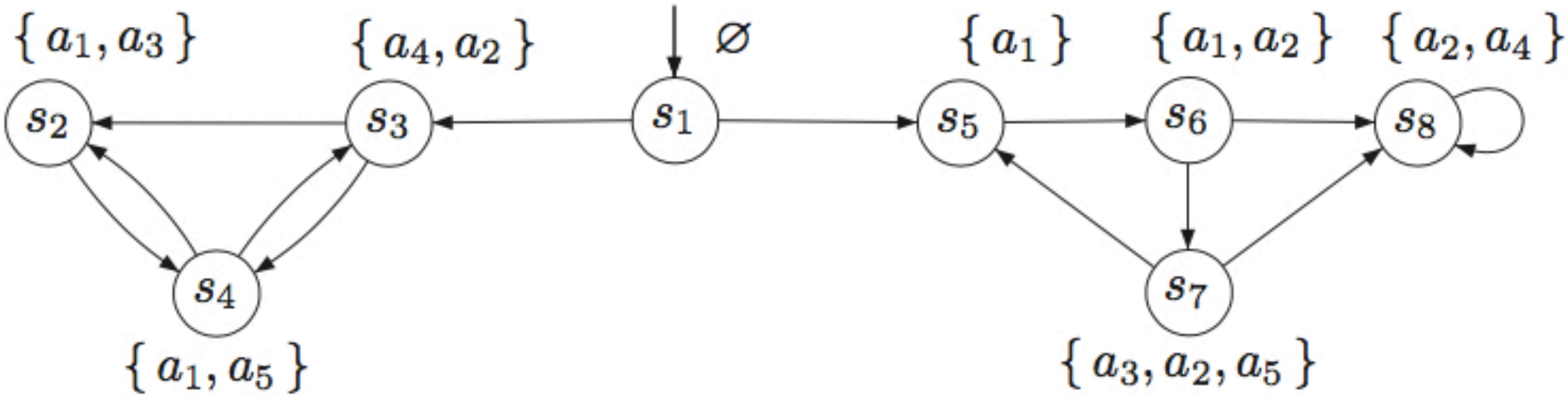
Questions:

(a) Determine $Sat(\Phi_1)$ and $Sat(\Psi_1)$ (without fairness).

(b) Determine $Sat_{sfair}(\exists\Box \text{ true})$.

(c) Determine $Sat_{sfair}(\Phi)$.

EXERCISE 6.23. Consider the following transition system TS over $AP = \{ a_1, \ldots, a_6 \}$.



Let $\Phi = \exists\bigcirc\ (a_1 \rightarrow \exists(a_1 \,\mathsf{U}\, a_2))$ and $sfair = sfair_1 \wedge sfair_2 \wedge sfair_3$ a strong CTL fairness assumption where

$$
\begin{aligned}
sfair_1 &= \Box\Diamond\ \forall\Diamond(a_1 \vee a_3) \longrightarrow \Box\Diamond a_4 \\
sfair_2 &= \Box\Diamond(a_3 \wedge \neg a_4) \longrightarrow \Box\Diamond a_5 \\
sfair_3 &= \Box\Diamond(a_2 \wedge a_5) \longrightarrow \Box\Diamond a_6
\end{aligned}
$$

Sketch the main steps for computing the satisfaction sets $Sat_{sfair}(\exists\Box\mathrm{true})$ and $Sat_{sfair}(\Phi)$.