Model Checking
Exercises with (Some) Solutions

Teacher: Luca Tesei

Master of Science in Computer Science - University of Camerino

Contents

1 Linear Temporal Logic

Exercise 1.1. *Consider the following LTL formulas:*

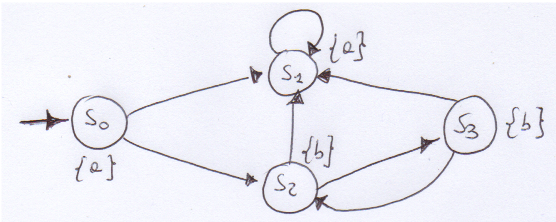
$$\varphi_1 = \Box(a \vee b) \qquad \varphi_2 = (\Box a) \vee (\Box b)$$

Let $\Sigma = 2^{AP}$ *and* $AP = \{a, b\}$.

1. *Derive two NBAs* $\mathcal{A}_1$ *and* $\mathcal{A}_2$ *on the alphabet* Σ *for the formulas* φ_1 *and* φ_2. *More precisely, it must hold* $\mathcal{L}_\omega(\mathcal{A}_1) = \mathcal{L}_\omega(\varphi_1)$ *and* $\mathcal{L}_\omega(\mathcal{A}_2) = \mathcal{L}_\omega(\varphi_2)$.

2. *Construct a GNBA* $\mathcal{G}$ *that accepts the intersection of the two languages of* $\mathcal{A}_1$ *and* $\mathcal{A}_2$, *i.e.* $\mathcal{L}_\omega(\mathcal{G}) = \mathcal{L}_\omega(\mathcal{A}_1) \cap \mathcal{L}_\omega(\mathcal{A}_2)$.

Exercise 1.2. *Consider the following transition system* TS *on* $AP = \{a, b\}$:

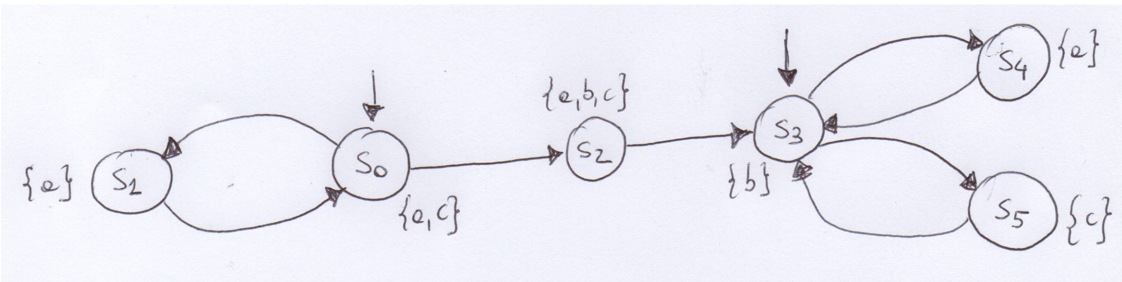


and the following LTL formula $\varphi = \Box\Diamond\neg a$.

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 1.3. *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* $\pi \not\models \varphi_i$.

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

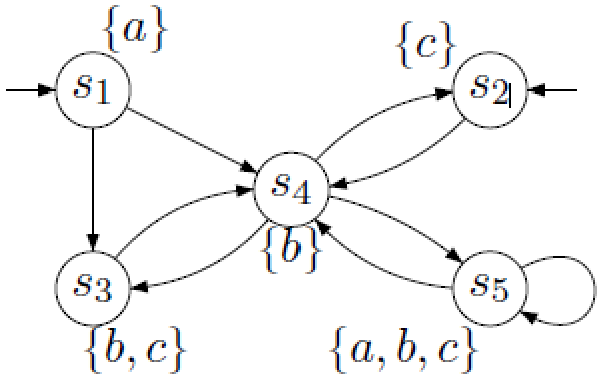
2. *Consider the following fairness assumptions written as LTL formulas:*

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

(a) **(2 points)** *Decide whether or not* $TS \models_{\text{fair}} \varphi_1$ *under the three different fairness conditions* ψ^i_{fair}, $i \in \{1,2,3\}$, **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^i_{fair}.

(b) **(2 points)** *Decide whether or not* $TS \models_{\text{fair}} \varphi_6$ *under the three different fairness conditions* ψ^i_{fair}, $i \in \{1,2,3\}$, **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^i_{fair}.

Exercise 1.4. *Consider the transition system TS over the set of atomic proposition* $AP = \{a, b, c\}$*:*

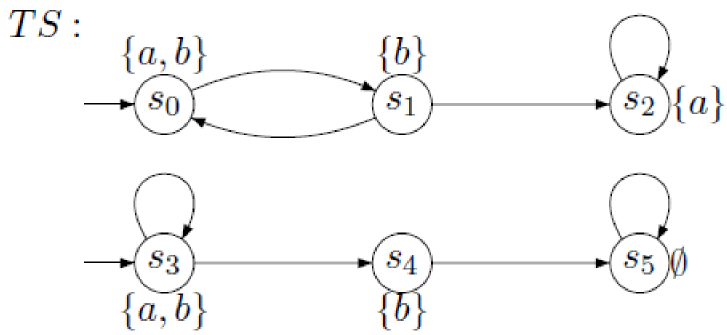


Decide for each of the LTL formulas φ_i *holds. Justify your answer!*

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

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

Exercise 1.5. *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 1.6. *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:*

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

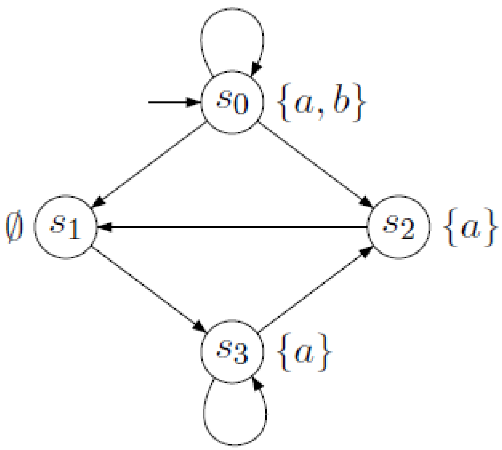
   then, construct the set $closure(\psi)$ and derive at least one set B that is elementary set with respect to $closure(\psi)$.

Exercise 1.7. *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 1.8. *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 $TS \otimes A_i$.

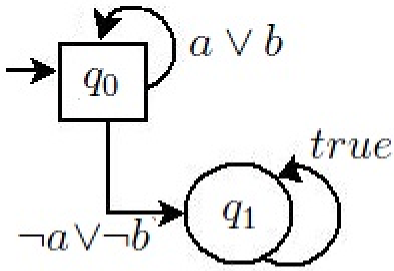
d) Provide the counterexample computed by the algorithm if $TS \not\models \varphi_i$.

Solutions

Solution of Exercise 1.1

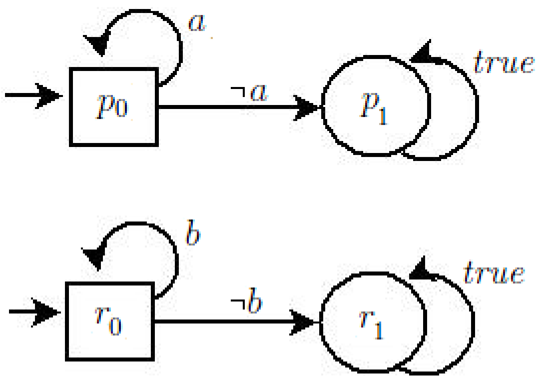
1. $\sum = AP = (2^{AP})^\omega$

   For the formula $\varphi_1 = \Box(a \vee b)$ the NBA $\mathcal{A}_\infty$ is:

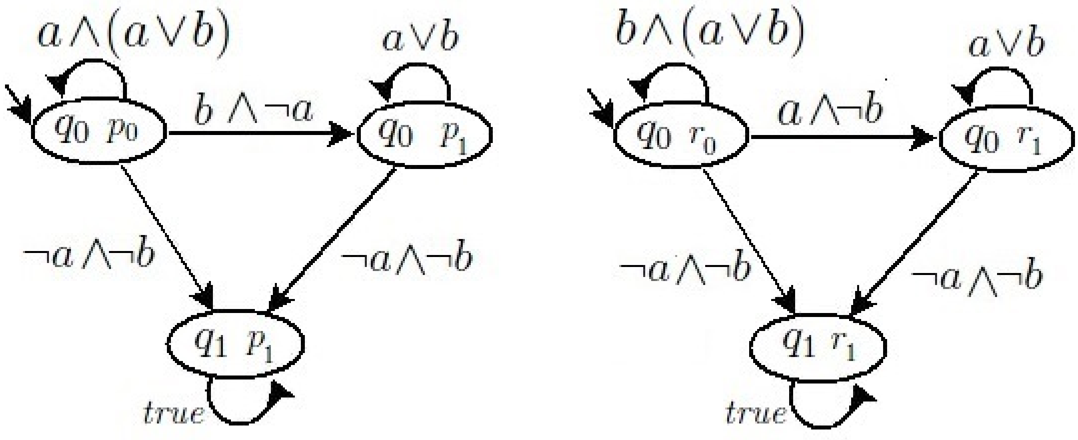
   Where:
   $(a \vee b) \equiv \{\{a\}, \{b\}, \{a, b\}\}$
   $(\neg a \vee \neg b) \equiv \{\{\}\}$
   $F_1 = \{q_0\}$

   For the formula $\varphi_2 = (\Box a) \vee (\Box b)$ the NBA $\mathcal{A}_\in$ is:

   Where:
   $a \equiv \{\{a\}, \{a, b\}\}$
   $\neg a \equiv \{\{\}, \{b\}\}$
   $b \equiv \{\{b\}, \{a, b\}\}$
   $\neg b \equiv \{\{\}, \{a\}\}$
   $F_2 = \{\{p_0\}, \{r_0\}\}$

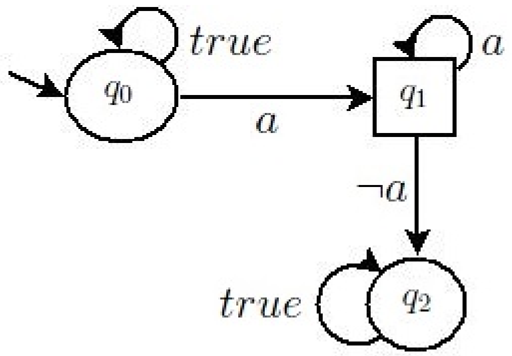
2. Let us construct $G = (\{q_0, q_1\} \times \{p_0, p_1, r_0, r_1\}, \sum, ...)$



where
$a \wedge (a \vee b) \equiv \{\{a\}, \{a, b\}\}$
$b \wedge (a \vee b) \equiv \{\{b\}, \{a, b\}\}$
The accepts sets are: $\mathcal{F} = \{\{q_0, p_0\}, \{q_0, p_1\}, \{q_0, r_0\}, \{q_0, r_1\}, \}$
$\{\{q_1, p_0\}, \{r_1, q_0\}\}$ are not reachable.

Solution of Exercise 1.2

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



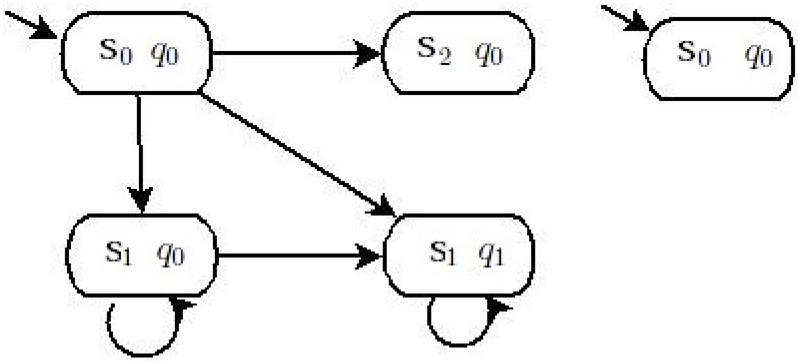
   where:
   $a \equiv \{\{a\}, \{a, b\}\}$
   $\neg a \equiv \{\{\}, \{b\}\}$
   $true \equiv \{\{a\}, \{b\}, \{a, b\}, \{\}\}$
   $F = \{q_1\}$

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)



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

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

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

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

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 1.3

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 1.4

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* $s_2s_4s_2s_4$...
$\varphi_2 = \Box\Diamond c$	*yes*
$\varphi_3 = \bigcirc\neg c \longrightarrow \bigcirc\bigcirc c$	*yes*
$\varphi_4 = \Box a$	*no* s_2...
$\varphi_5 = a\mathcal{U}\Box(b \vee c)$	*yes*
$\varphi_6 = (\bigcirc\bigcirc b)\mathcal{U}(b \vee c)$	*no* $s_1s_4s_2$...

Solution of Exercise 1.5

$a)$ 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:

$$FairPaths(TS) = \mathcal{L}_\omega((s_0s_1)^\omega + (s_0s_1)^+s_2^\omega + s_3^+s_4s_5^\omega)$$

$b)$

- $\varphi_1 = \bigcirc\neg a \longrightarrow \Diamond\Box a$
  Consider the path $\pi_1 = s_3s_4s_5^\omega \in FairPaths(TS)$. 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 $\pi_2 = (s_0s_1)^\omega \in FairPaths(TS)$. Here, we have

  $$trace(\pi_2) = \sigma_2 = (\{a,b\}\{b\})^\omega$$

  and $\sigma_2 \not\models_{fair} b\mathcal{U}\Box\neg b$ since there exists no $i \geq$ s.t. $\sigma_2[i...] \models \Box\neg b$.
  $\Rightarrow TS \not\models_{fair} b\mathcal{U}\Box\neg b$

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

Solution of Exercise 1.6

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 1.7

We have the following LTL formula:

$$\varphi = \neg\Diamond(\neg(a\mathsf{U}c) \rightarrow ((b \wedge \neg d)\mathsf{U}a)) \equiv \Box\neg((a\mathsf{U}c) \vee ((b \wedge \neg d)\mathsf{U}a)) \qquad \text{(* } \Diamond\varphi \equiv \neg\Box\neg\varphi \text{ and } \varphi \rightarrow \psi \equiv \neg\varphi \vee \psi \text{*)}$$
$$\equiv \Box(\neg(a\mathsf{U}c) \wedge \neg((b \wedge \neg d)\mathsf{U}a)) \qquad \text{(* deMorgan *)}$$

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:

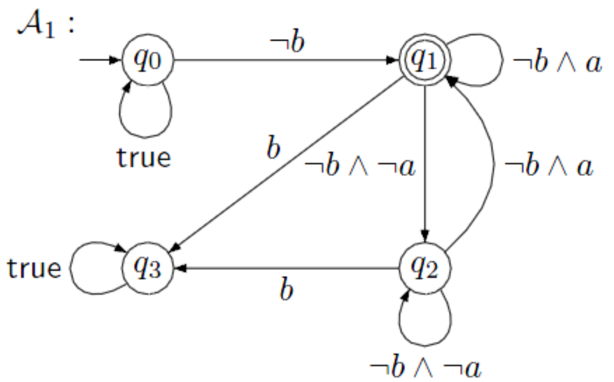
$$\varphi \equiv \Box((a \wedge \neg c)\mathsf{W}(\neg a \wedge \neg c) \wedge (b \wedge \neg d \wedge \neg a)\mathsf{W}(\neg(b \wedge \neg d) \wedge \neg a))$$
$$\equiv ((a \wedge \neg c)\mathsf{W}(\neg a \wedge \neg c) \wedge (b \wedge \neg d \wedge \neg a)\mathsf{W}((\neg b \vee d) \wedge \neg a))\mathsf{W}\mathsf{false}$$

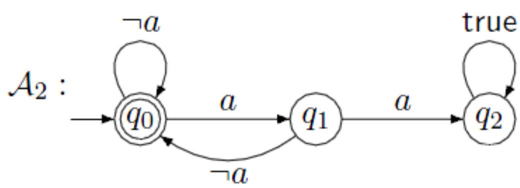
b) PNF with R–operator (release): Rewrite rule for until: $\neg(\varphi\mathsf{U}\psi) \rightsquigarrow \neg\varphi\mathsf{R}\neg\psi$. We obtain for φ as above:

$$\varphi \equiv \Box(\neg a\mathsf{R}\neg c \wedge \neg(b \wedge \neg d)\mathsf{R}\neg a)$$
$$\equiv \mathsf{false}\mathsf{R}(\neg a\mathsf{R}\neg c \wedge (\neg b \vee d)\mathsf{R}\neg a)$$

Solution of Exercise 1.8

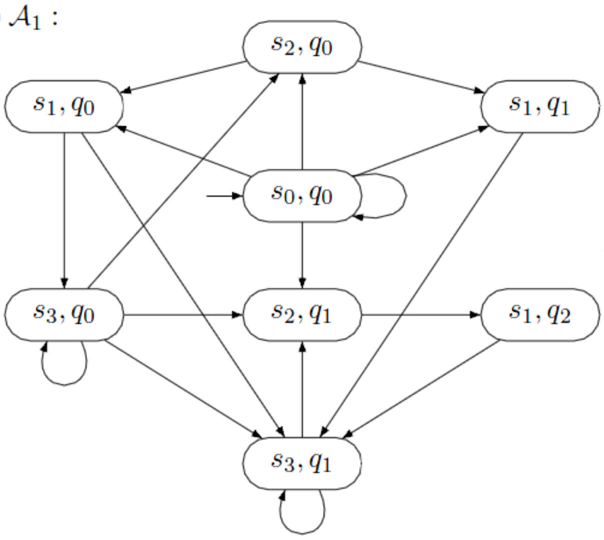
$a)$ The automata accepting the complement languages of φ_1 and φ_2 are:



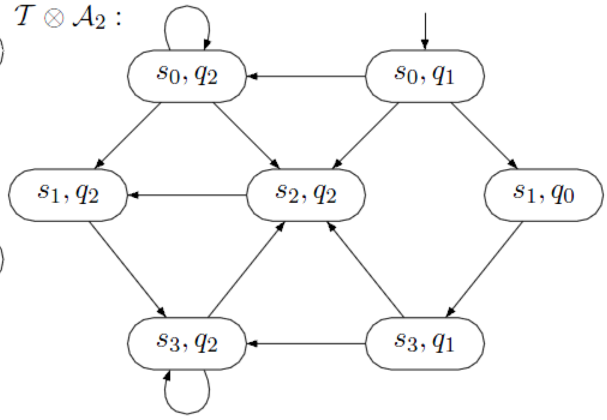


$b)$ The reachable fragments of $T \otimes A_i$ for $i = 1, 2$ are as follows:

$\mathcal{T} \otimes \mathcal{A}_1$:



$\mathcal{T} \otimes \mathcal{A}_2$:



$c)$ 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: $< s_0, q_0 >, < s_1, q_1 >, < s_3, q_1 >, < s_2, q_1 >, < s_1, q_2 >, < s_3, q_1 >$
$TS \vDash \varphi_2$.