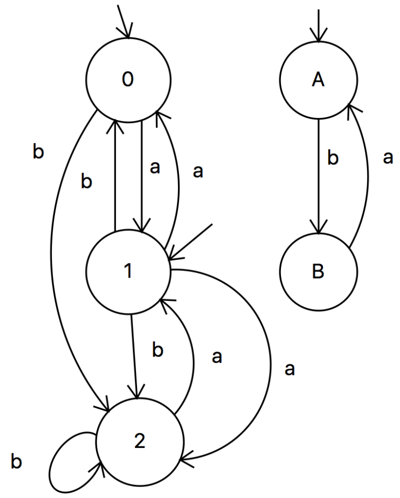
Master of Science in Computer Science - University of Camerino
Reactive Systems Verification A. Y. 2016/2017
Written Test of 12th July 2017 (Appello II)
Teacher: Luca Tesei

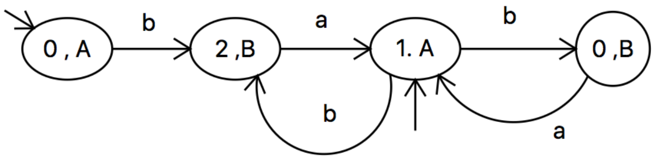
EXERCISE 1 (6 points)

Consider the two following transition systems.



1. Draw the transition system resulting from their product using handshaking with the handshake action set $H = \{a, b\}$.

Solution



EXERCISE 2 (9 points)

Consider the alphabet $AP = \{A, B, C, D\}$ and the following linear time properties:

(a) Whenever A holds then B does not hold for two steps

(b) B and C hold together only finitely many times

(c) If C holds infinitely many times then D holds only finitely many times

(d) C holds at least once and whenever D holds also A must hold

For each property:

1. formalise it using set expressions and first order logic;
2. formalise it in LTL (you can use the operators next, until, box and diamond, together with all boolean connectives);

3. tell if it is a safety, liveness or mixed property; in case it is a safety property provide an NFA for the language of the **minimal** bad prefixes.

Solution

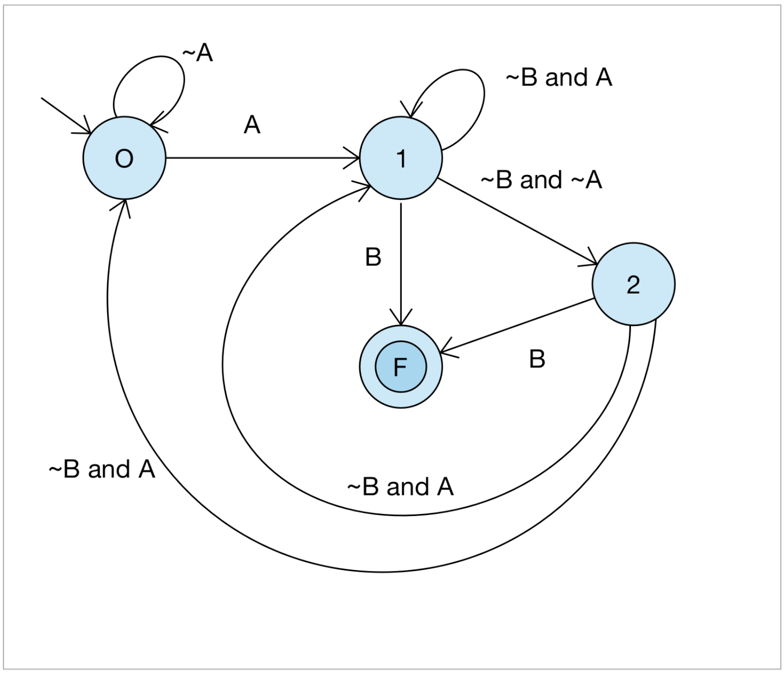
(a) This is a safety property. The set of all words belonging to the property is

$$\left\{X_0X_1\ldots \in \left(2^{AP}\right)^\omega \mid \forall i \in \mathbb{N}.A \in X_i \Rightarrow (B \notin X_{i+1} \land B \notin X_{i+2})\right\}$$

An LTL formula expressing the property is

$$\Box(A \Rightarrow (\bigcirc\neg B \land \bigcirc\bigcirc\neg B))$$

An NFA accepting all the minimal bad prefixes is the following one ($\sim$ stands for $\neg$)



(b) This is a liveness property. The set of all words belonging to the property is

$$\left\{X_0X_1\ldots \in \left(2^{AP}\right)^\omega \mid \overset{\infty}{\forall} i \in \mathbb{N}.D \notin X_i \lor C \notin X_i\right\}$$

An LTL formula expressing the property is

$$\Diamond\Box(\neg B \lor \neg C)$$

(c) This is a liveness property. The set of all words belonging to the property is

$$\left\{X_0X_1\ldots \in \left(2^{AP}\right)^\omega \mid \left(\overset{\infty}{\exists} i \in \mathbb{N}: C \in X_i\right) \Rightarrow \left(\overset{\infty}{\forall} i \in \mathbb{N}.D \notin X_i\right)\right\}$$

An LTL formula expressing the property is

$$(\Box\Diamond C) \Rightarrow (\Diamond\Box\neg D)$$

(d) This is a mixed property. The set of all words belonging to the property is

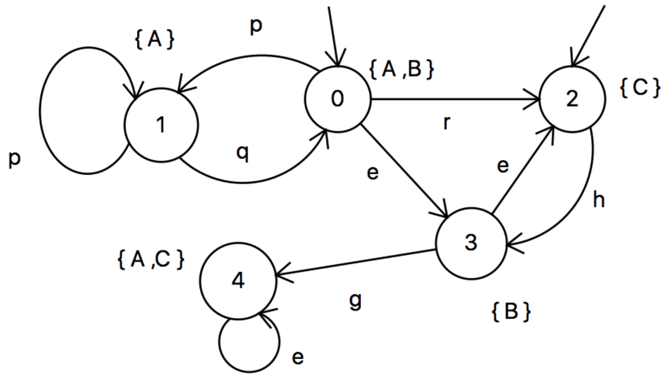
$$\left\{X_0 X_1 \ldots \in \left(2^{AP}\right)^\omega \mid (\exists i \in \mathbb{N}\colon C \in X_i) \wedge (\forall i \in \mathbb{N}. D \in X_i \Rightarrow A \in X_i)\right\}$$

An LTL formula expressing the property is

$$\Diamond C \Rightarrow \Box(D \Rightarrow A)$$

EXERCISE 3

Consider the following transition system TS on $AP = \{A, B, C\}$.



1. **(3 points)** 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 $\pi \not\models \varphi_i$.

$$\varphi_1 = \bigcirc \bigcirc A$$
$$\varphi_2 = \Box(A \Rightarrow \Diamond C)$$
$$\varphi_3 = \Diamond\Box(A \vee C)$$

2. Consider the following fairness assumptions:

$$\psi_1^{\text{fair}} = \{\{\}, \{q\}, \{r\}\} \qquad \psi_2^{\text{fair}} = \{\{\}, \{r\}, \{q\}\}$$
$$\psi_3^{\text{fair}} = \{\{\}, \{g\}, \{e\}\} \qquad \psi_4^{\text{fair}} = \{\{\}, \{\}, \{g, e\}\}$$

   (a) **(3 points)** Decide whether or not $TS \models_{\text{fair}} \varphi_2$ under the four different fairness conditions ψ^i_{fair}, $i \in \{1, 2, 3, 4\}$, **separately**. Whenever $TS \not\models_{\text{fair}} \varphi_2$ 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) **(3 points)** Decide whether or not $TS \models_{\text{fair}} \varphi_3$ under the four different fairness conditions ψ^i_{fair}, $i \in \{1, 2, 3, 4\}$, **separately**. Whenever $TS \not\models_{\text{fair}} \varphi_3$ 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}.

Solution

$TS \not\models \varphi_1$ - A path showing this is $0\ 2\ 3 \cdots$
$TS \not\models \varphi_2$ - A path showing this is $0\ (1)^\omega$
$TS \not\models \varphi_3$ - A path showing this is $0\ (2\ 3)^\omega$

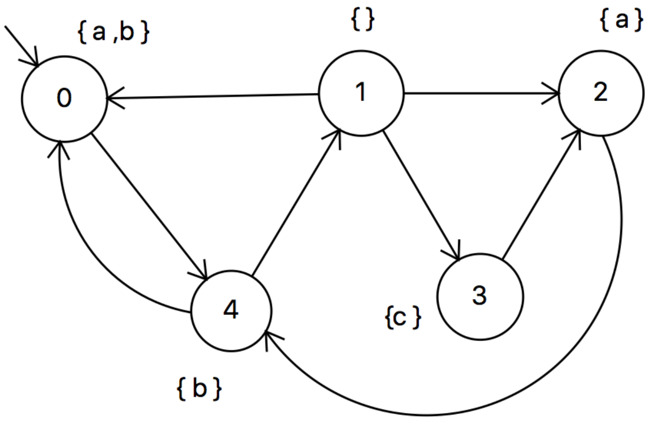
$TS \not\models_{\psi_1^{\text{fair}}} \varphi_2$ - Paths like $0\ (1)^\omega$ are no longer fair due to strong fairness on q, but the weak fairness on r does not rule out paths like $(0\ 1)^\omega$.
$TS \models_{\psi_2^{\text{fair}}} \varphi_2$ - Paths like $0\ (1)^\omega$ are no longer fair due to weak fairness on q and paths like $(0\ 1)^\omega$ are no longer fair due to strong fairness on r.

$TS \not\models_{\psi_3^{\text{fair}}} \varphi_2$ - Paths like $0\ (1)^\omega$ are still fair.
$TS \not\models_{\psi_4^{\text{fair}}} \varphi_2$ - Paths like $0\ (1)^\omega$ are still fair.

$TS \not\models_{\psi_1^{\text{fair}}} \varphi_3$ - Paths like $0\ (2\ 3)^\omega$ are still fair.
$TS \not\models_{\psi_2^{\text{fair}}} \varphi_3$ - Paths like $0\ (2\ 3)^\omega$ are still fair.
$TS \models_{\psi_3^{\text{fair}}} \varphi_3$ - Paths like $0\ (2\ 3)^\omega$ are no longer fair due to strong fairness on g.
$TS \not\models_{\psi_4^{\text{fair}}} \varphi_3$ - Paths like $0\ (2\ 3)^\omega$ are still fair because weak fairness on g or e does not rule out them.

EXERCISE 4 (8 points)

Consider the following transition system



1. Calculate $\text{Sat}(a \wedge (b \leftrightarrow c))$, $\text{Sat}(\exists(c \vee b)\mathcal{U}a)$ and $\text{Sat}(\exists\Box(b \vee c))$. Justify your answers by showing the steps of the algorithm used for the CTL formulas.

Solution

To calculate $\text{Sat}(a \wedge (b \leftrightarrow c))$:

- $\text{Sat}(a) = \{0, 2\}$
- $\text{Sat}(b)) = \{0, 4\}$
- $\text{Sat}(c) = \{3\}$
- $\text{Sat}(b \leftrightarrow c) = \{1, 2\}$
- $\text{Sat}(a \wedge (b \leftrightarrow c)) = \{0, 2\} \cap \{1, 2\} = \{2\}$

To calculate $\text{Sat}(\exists(c \vee b)\mathcal{U}a)$:

- $\text{Sat}(a) = \{0, 2\}$
- $\text{Sat}(b)) = \{0, 4\}$
- $\text{Sat}(c) = \{3\}$
- $\text{Sat}(c \vee b) = \{3\} \cup \{0, 4\} = \{0, 3, 4\}$
- $\text{Sat}(\exists(c \vee b)\mathcal{U}a)$:
  - $T_0 = \text{Sat}(a) = \{0, 2\}$
  - $T_1 = T_0 \cup (\text{Pred}(T_0) \cap \text{Sat}(c \vee b)) = \{0, 2\} \cup (\{1, 3, 4\} \cap \{0, 3, 4\}) = \{0, 2\} \cup \{3, 4\} = \{0, 2, 3, 4\}$

- $T_2 = T_1 \cup (\text{Pred}(T_1) \cap \text{Sat}(c \vee b)) = \{0,2,3,4\} \cup (\{0,1,2,3,4\} \cap \{0,3,4\}) = \{0,2,3,4\} \cup \{0,3,4\} = \{0,2,3,4\}$. The least fixpoint is $\{0,2,3,4\}$.

To calculate $\text{Sat}(\exists\Box(b \vee c))$:

- $\text{Sat}(b)) = \{0,4\}$
- $\text{Sat}(c) = \{3\}$
- $\text{Sat}(b \vee c) = \{0,4\} \cup \{3\} = \{0,3,4\}$
- $\text{Sat}(\exists\Box(b \vee c))$:
  - $T_0 = \text{Sat}(b \vee c) = \{0,3,4\}$
  - $T_1 = T_0 - \{s \in T_0 \mid \text{Succ}(T_0) \cap \text{Sat}(b \vee c) = \emptyset\} = \{0,3,4\} - \{3\} = \{0,4\}$
  - $T_2 = T_1 - \{s \in T_0 \mid \text{Succ}(T_1) \cap \text{Sat}(b \vee c) = \emptyset\} = \{0,4\} - \emptyset = \{0,4\}$. The greatest fixpoint is $\{0,4\}$.