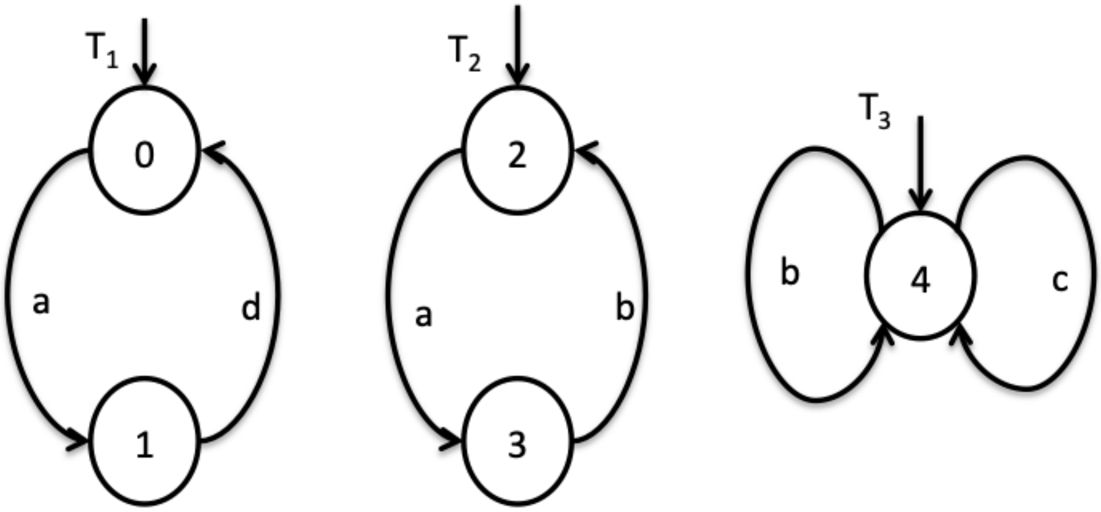
Master of Science in Computer Science - University of Camerino
Systems Verification Lab A. Y. 2018/2019
Written Test of 28th June 2019 (Appello IV)
Teacher: Luca Tesei

EXERCISE 1 (4 points)

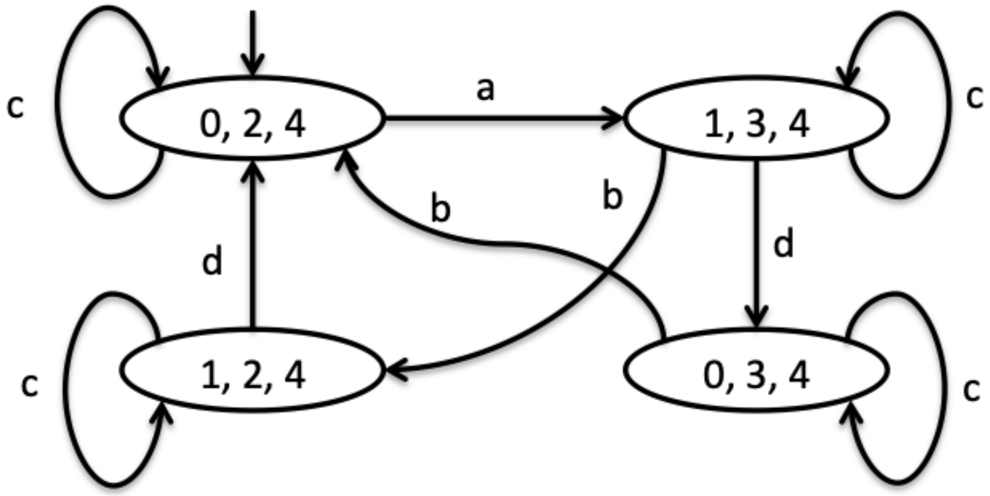
Consider the three following transition systems T_1, T_2 and T_3.



Draw the transition system resulting from their product using handshaking with the handshake action set $H = \{a, b\}$, i.e., $T_1\|_{\{a,b\}}T_2\|_{\{a,b\}}T_3$.

SOLUTION

The resulting transition system is the following one:



EXERCISE 2 (10 points)

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

(a) A holds at least twice

(b) B holds infinitely many times and whenever B holds then also C holds

(c) Whenever A holds then B does not hold in the next step and whenever B holds then A does not hold in the next step

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 pure safety property provide an NFA for the language of the **minimal bad prefixes**.

SOLUTION

EX 2

a) A holds at least twice

1- $E_a = \{ X_0 X_1 \dots \in (2^{AP})^\omega \mid \exists i \in \mathbb{N} \ \exists j \in \mathbb{N} : i \neq j \land A \in X_i \land A \in X_j \}$

2- LTL: $\Diamond (A \land \bigcirc \Diamond A)$

3- This is a pure liveness property

b) B holds infinitely many times and whenever B holds then also C holds.

1- $E_b = \{ X_0 X_1 \dots \in (2^{AP})^\omega \mid \overset{\infty}{\exists} i \in \mathbb{N} : B \in X_i \land (\forall j \in \mathbb{N}. \ B \in X_j \rightarrow C \in X_j) \}$

2- LTL: $\Box \Diamond B \land \Box (B \rightarrow C)$

3- This is a mixed property.

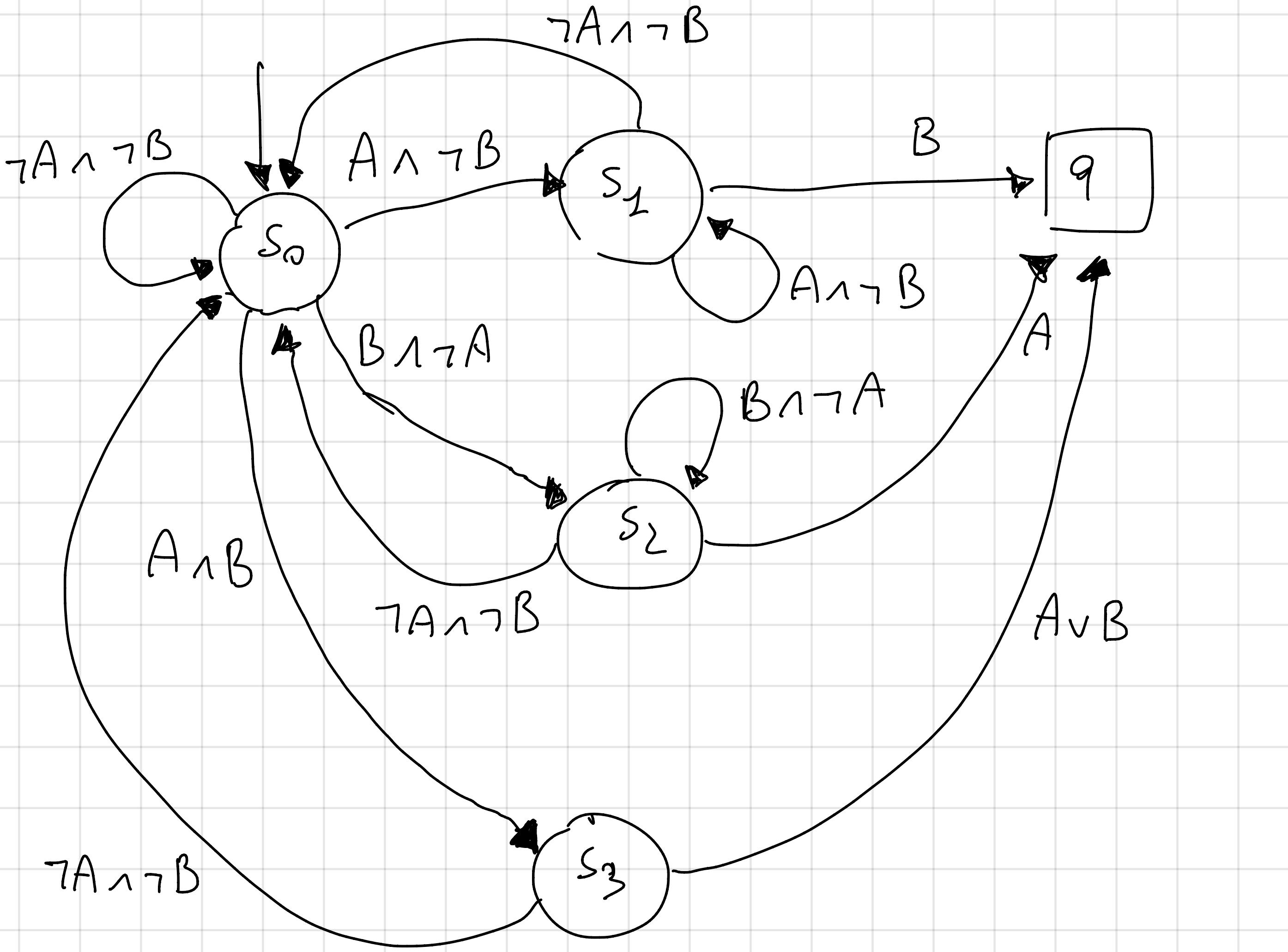
c) Whenever A holds then B does not hold in the next step and whenever B holds then A does not hold in the next step.

1- $E_c = \{ X_0 X_1 \dots \in (2^{AP})^\omega \mid (\forall i \in \mathbb{N}. \ A \in X_i \rightarrow B \notin X_{i+1}) \land (\forall j \in \mathbb{N}. \ B \in X_j \rightarrow A \notin X_{j+1}) \}$

2- LTL $\square((B \rightarrow \bigcirc \neg A) \wedge (A \rightarrow \bigcirc \neg B))$

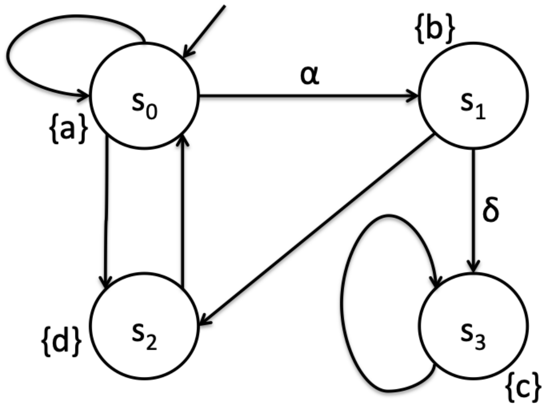
3- This is a pure safety property, actually an invariant.

An NFA accepting the language of minimal bad prefixes is the following:



EXERCISE 3 (10 points)

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



Decide whether or not the following LTL formulas:

$$\varphi_0 = \Box\Diamond(a \vee c) \qquad \varphi_1 = (a \vee d)\,\mathcal{U}\,b$$
$$\varphi_2 = \Box(a \rightarrow \bigcirc(b \vee d)) \qquad \varphi_3 = \Diamond c$$

are satisfied by TS under the following fairness conditions (to be considered separately):

$$\psi_0^{\text{fair}} = (\{\}, \{\}, \{\}) \qquad \psi_1^{\text{fair}} = (\{\}, \{\{\alpha\}, \{\delta\}\}, \{\})$$
$$\psi_2^{\text{fair}} = (\{\}, \{\}, \{\{\alpha\}, \{\delta\}\}) \qquad \psi_3^{\text{fair}} = (\{\}, \{\{\alpha, \delta\}\}, \{\})$$

Justify your answers! In case the answer is no, provide a counterexample.

SOLUTION

EX3 | Possible path <u>SCHEMES</u> are:

Π_1: $\dots s_0^\omega \mapsto$ trace $\dots \{a\}^\omega$

Π_2: $\dots (s_0^+ s_2 s_0^+)^\omega \mapsto$ trace $\dots (\{a\}^+ \{d\} \{a\}^+)^\omega$

Π_3: $\dots (s_0^+ s_2 s_0^+ s_1 s_2)^\omega \mapsto$ trace

$\dots (\{a\}^+ \{d\} \{a\}^+ \{b\} \{d\})^\omega$

Π_4: $\dots s_3^\omega \mapsto$ trace $\dots \{c\}^\omega$

Let us consider the different fairness conditions.

φ_0^{fair} is empty so all paths of schemes Π_{1-4} are fair

φ_1^{fair} has strong fairness on both α and δ so:

- paths Π_1 are not fair (fails strong fairness on α)
- paths Π_2 are not fair (fails strong fairness on α)
- paths Π_3 are not fair (fails strong fairness on δ)
- paths Π_4 are fair

φ_2^{fair} has weak fairness on both α and δ

- paths Π_1 are not fair (fails weak fairness on α)
- paths Π_2 are fair (weak fairness on α is not violated because α is not

Continuously enabled

- paths Π_3 are fair (weak fairness on δ does not fail because δ is not continuously enabled)
- paths Π_4 are fair

φ_3^{fair} has strong fairness on the set $\{\alpha, \delta\}$

- paths Π_1 are not fair (fails sf. on $\{\alpha, \delta\}$)
- paths Π_2 are not fair (fails sf on $\{\alpha, \delta\}$)
- paths Π_3 are fair (sf on $\{\alpha, \delta\}$ does not fail because α is executed infinitely many times)
- paths Π_4 are fair

Let us consider now the formulas.

φ_0 : $TS \models_{\varphi_0^{fair}} \Box\Diamond(a \vee c)$ because all the paths of TS have a or c infinitely many times.

$TS \models_{\varphi_1^{fair}} \varphi_0$ because the paths Π_4 all have c infinitely many times

We have also $TS \models_{\varphi_3^{fair}} \varphi_0$

$TS \models_{\varphi_2}^{fair} \varphi_0$ because paths π_{2-4} have all a or c infinitely many times.

$\varphi_1 : (a \vee d) \, \mathcal{U} \, b$

$TS \not\models_{\varphi_0}^{fair} \varphi_1$ counterexample π_1, which are fair

$TS \models_{\varphi_1}^{fair} \varphi_2$ because all the fair paths π_4 have reached $\{b\}$ (state s_1) starting from state s_0 and possibly passing through s_2; in both cases $a \vee d$ is satisfied

We have also $TS \models_{\varphi_3}^{fair} \varphi_2$ because paths π_3 reach s_1

$TS \not\models_{\varphi_2}^{fair} \varphi_1$ because paths π_2 are fair counterexamples: $(s_0^{+} s_2 s_0^{+})^{\omega}$

$\varphi_2 = \Box(a \rightarrow \bigcirc(b \vee d))$ is a SAFETY property, therefore it is not affected by fairness

$TS \not\models \varphi_2$ under <u>any</u> of the four fairness assumptions.

a Counter example is

$s_0 s_0 \ldots \mapsto \{a\}\{a\}\ldots$

is a bad prefix

$\varphi_3 = \Diamond c$

$TS \not\models_{\psi_0^{fair}} \varphi_3$ because, for instance, paths π_1 are fair: $s_0^\omega \mapsto \{a\}^\omega$ is a counterexample

$TS \models_{\psi_1^{fair}} \varphi_3$ because the only fair paths are π_3 and all of them sooner or later have 'c'

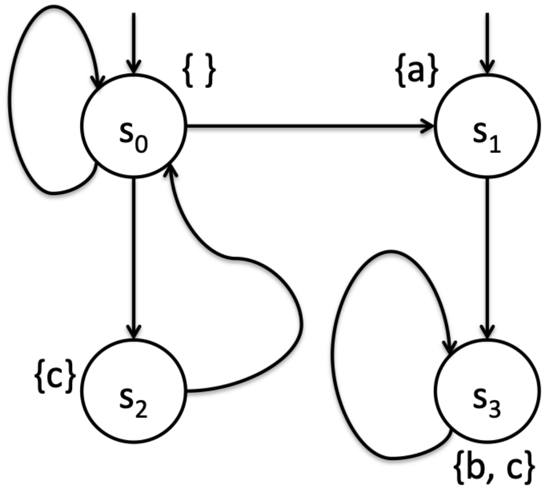
$TS \not\models_{\psi_3^{fair}} \varphi_3$ because paths π_3 are fair and so they are counterexamples.

$TS \not\models_{\psi_2^{fair}} \varphi_3$ because paths π_2 are fair. Counterexample:

$(s_0^+ s_2 s_0^+)^\omega \mapsto (\{a\}^+\{d\}\{a\}^+)^\omega$

EXERCISE 4 (8 points)

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



Decide whether or not the following CTL formulas:

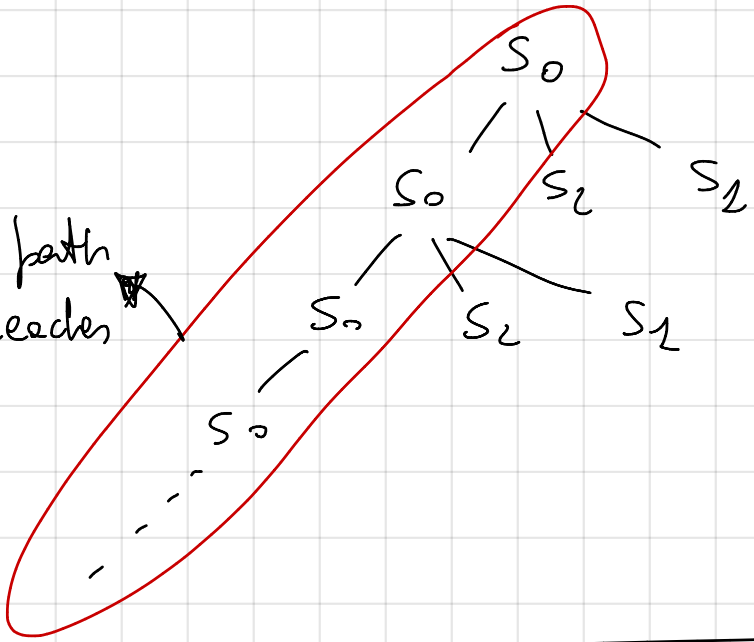
$$\phi_0 = \forall\Diamond c \qquad \phi_1 = \exists\Box(\exists \bigcirc a)$$
$$\phi_2 = \forall\Box(c \to \exists\Diamond b) \qquad \phi_3 = \forall\Box(c \to \forall\Diamond b)$$

are satisfied by TS. Justify your answers! When possible, provide a counterexample or a witness.

SOLUTION

EX 4 | $\phi_0 = \forall\Diamond c$

TS $\not\models \forall\Diamond c$ a counterexample is:



this path never reaches 'c'

$\phi_1 = \exists\Box(\exists\bigcirc a)$

TS $\models \phi_1$ a witness is path s_0^ω

$$\begin{tikzcd} s_0 \arrow[r] \arrow[d] & s_0 \arrow[r] \arrow[d] & s_0 \arrow[r] \arrow[d] & s_0 \arrow[r] \arrow[d] & \cdots \arrow[d] \\ s_1\{a\} & s_1\{a\} & s_1\{a\} & s_1\{a\} & \vdots \end{tikzcd}$$

$\phi_2 = \forall\Box(c \to \exists\Diamond b)$

TS $\models \phi_2$ This is an invariant.

c holds in state s_2 and in state s_3

- in state s_3 b is reached immediately.
- from state s_2 there is the path

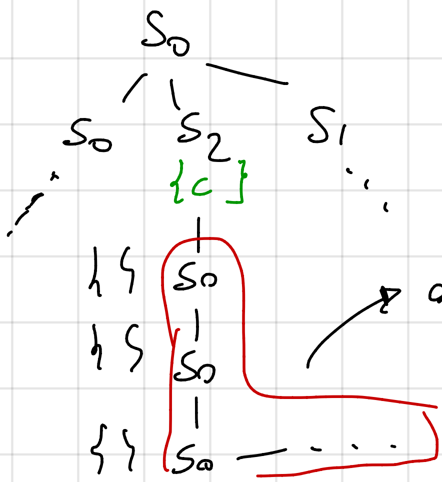
$$\underset{\{c\}}{s_2} \to s_0 \to s_1 \to \underset{\{b\}}{s_3} \; ---$$

From initial state s_0 both s_2 and s_3 can be reached; if they are not reached the implication $c \to \exists\Diamond b$ is trivially satisfied; if they are reached a path to 'b' can always be found.

From initial state s_1 only state s_3 can be reached and similar considerations apply.

$$\phi_3 = \forall\Box(c \to \forall\Diamond b)$$

$TS \not\models \phi_3$ a counterexample is



along this path b is never reached