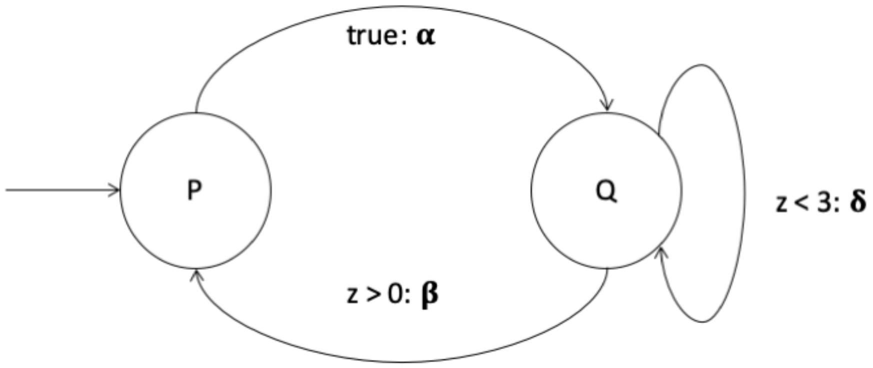
Master of Science in Computer Science - University of Camerino
Systems Verification Lab A. Y. 2018/2019
Written Test of 12th September 2019 (Appello VI)
Teacher: Luca Tesei

EXERCISE 1 (8 points)

Consider the following program graph



where z is a variable such that $\mathrm{dom}(z) = \{0, 1, 2, 3\}$, $g_0 \equiv (z = 1)$, $\mathrm{Loc}_0 = \{P\}$, $\mathit{Effect}(\alpha, \eta) = \eta[z := 0]$, $\mathit{Effect}(\beta, \eta) = \eta[z := \eta(z) - 1]$ and $\mathit{Effect}(\delta, \eta) = \eta[z := \eta(z) + 1]$.

1. Translate the given program graph into an equivalent transition system.

EXERCISE 2 (8 points)

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

(a) Whenever A holds then B holds after two steps

(b) A and B hold together infinitely many times

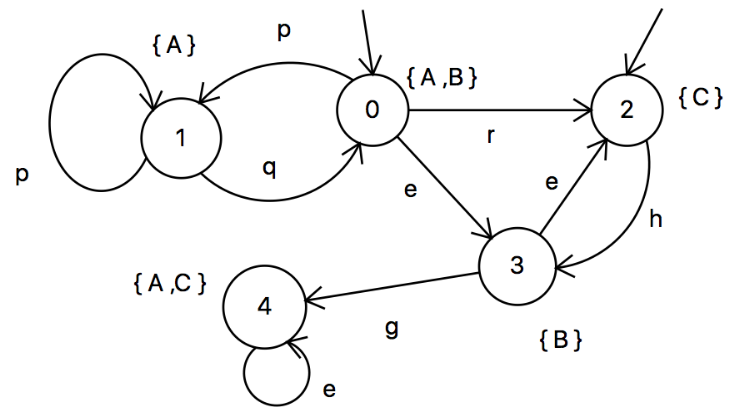
(c) A holds once and B never holds

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**.

EXERCISE 3 (8 points)

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



Decide whether or not the following LTL formulas:

$$\varphi_0 = \Box(C \to \Diamond A) \qquad \varphi_1 = \Diamond(B \wedge \bigcirc(B \vee C))$$
$$\varphi_2 = \Box\Diamond\neg B$$

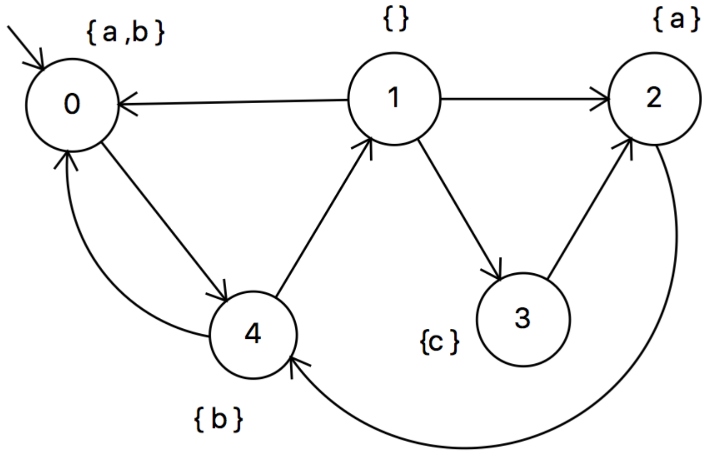
are satisfied by TS under the following fairness conditions (to be considered separately):

$$\psi_0^{\text{fair}} = (\{\}, \{\}, \{\}) \qquad \psi_1^{\text{fair}} = (\{\}, \{\{g\}, \{e, r\}\}, \{\{q\}\})$$
$$\psi_2^{\text{fair}} = (\{\}, \{\}, \{\{g\}, \{e\}, \{q\}\})$$

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

EXERCISE 4 (8 points)

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



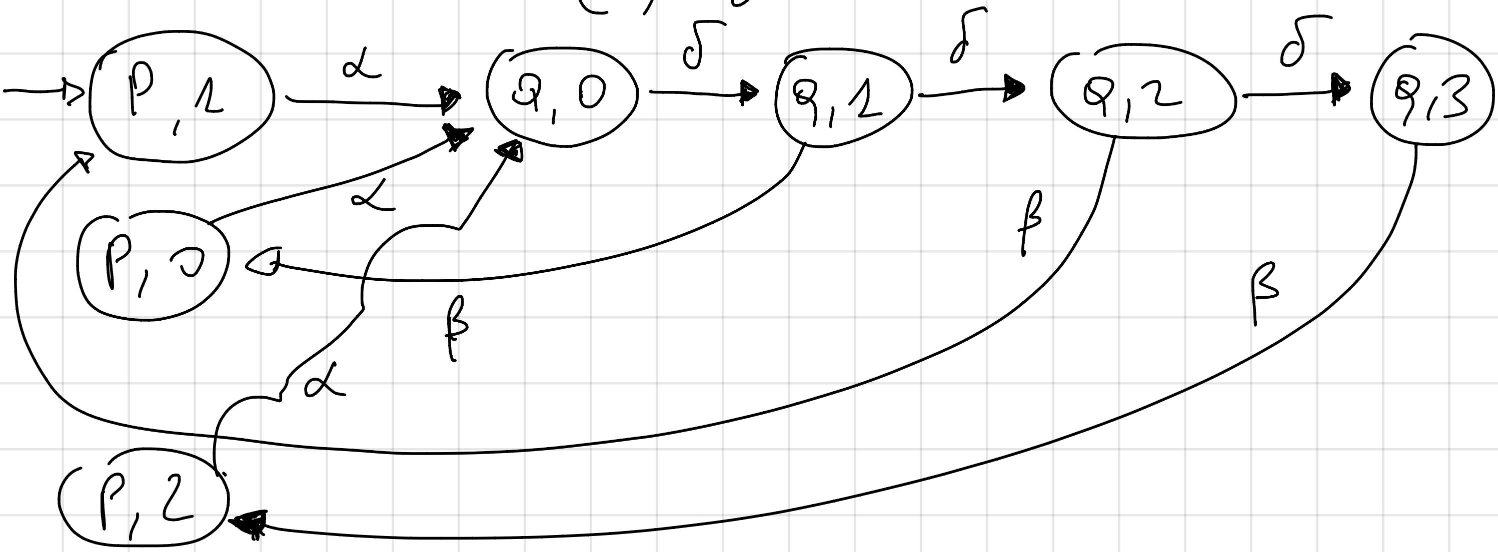
Decide whether or not the following CTL formulas:

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

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

EX1 The state space is $S = \{(loc, v) \mid loc \in \{P,Q\}, v \in \{0,1,2,3\}\}$

The initial state is $(P, 1)$

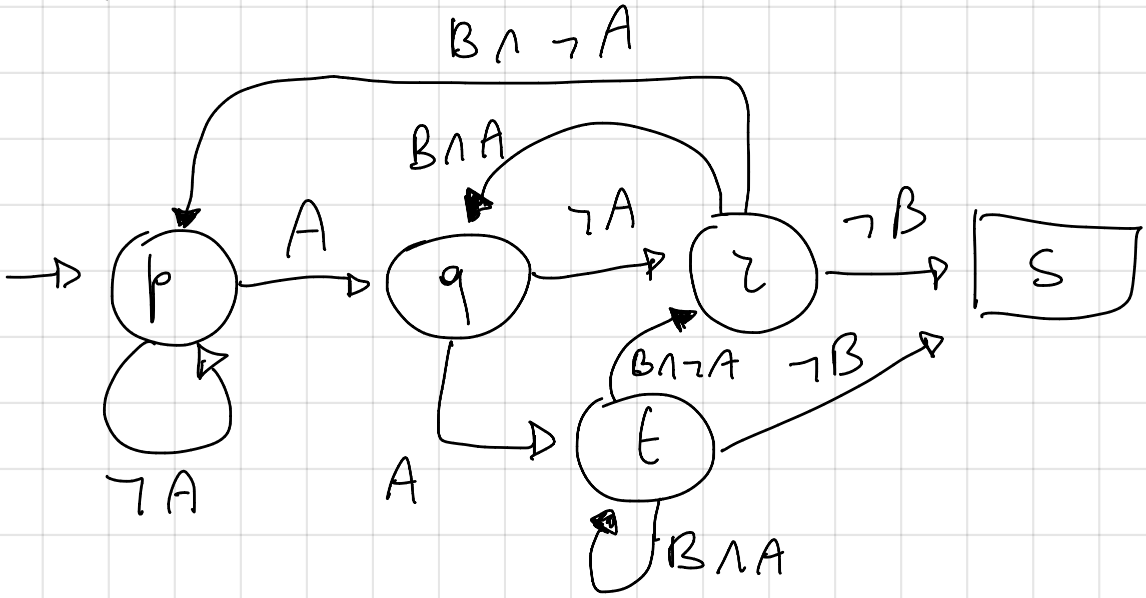


EX2

a) $E_a = \{X_0 X_1 \cdots \in (2^{AP})^\omega \mid \forall i \in \mathbb{N}.\ A \in X_i \Rightarrow B \in X_{i+2}\}$

in LTL: $\Box(A \to \bigcirc\bigcirc B)$

This is a SAFETY PROPERTY. An NFA accepting the language of minimal bad prefixes is the following one:



b) $E_{(b)} = \{ X_0 X_1 \ldots \in (2^{AP})^\omega \mid \overset{\infty}{\exists} i \in \mathbb{N} : A \in X_i \wedge B \in X_i \}$

in LTL: $\Box \Diamond (A \wedge B)$

This is a pure LIVENESS PROPERTY

c) $E_{(c)} = \{ X_0 X_1 \ldots \in (2^{AP})^\omega \mid (\forall i \in \mathbb{N} . \ B \notin X_i) \wedge$
$(\exists J \in \mathbb{N} : A \in X_J \wedge (\forall k \in \mathbb{N} . (k < J \Rightarrow A \notin X_k) \wedge$
$(k > J \Rightarrow A \notin X_k))) \}$

in LTL: $\Diamond (A \wedge \bigcirc (\Box \neg A)) \wedge \Box \neg B$

This is a MIXED property

EX3 The TS presents the following path schemes:

$\Pi_1 : (0\ 1^+)^* \, 0\ 1^\omega$

$\Pi_2 : (0\ 1^+)^\omega$

$\Pi_3 : (2\ 3)^\omega$

$\Pi_4 : (2\ 3)^+ \, 4^\omega$

$\Pi_5 : (0\ 1^+)^+ \, 0\ (2\ 3)^\omega$

$\Pi_6 : (0\ 1^+)^+ \, 0\ 3(2\ 3)^\omega$

$\Pi_7 : (0\ 1^+)^+ \, 0\ (2\ 3)^+ \, 4^\omega$

$\Pi_8 : (0\ 1^+)^+ \, 0\ 3(2\ 3)^+ \, 4^\omega$

- All the paths are fair with respect to φ_0^{fair}
- With respect to φ_2^{fair}, the fair paths are: Π_4, Π_7, Π_8, the others are all unfair
- With respect to φ_2^{fair}, the fair paths are: $\Pi_2, \Pi_3, \Pi_4, \Pi_5, \Pi_6, \Pi_7, \Pi_8$.
  The only unfair paths are Π_1.

Let us analyse the formulas:

$\varphi_0 = \Box(C \rightarrow \Diamond A)$

- $TS \not\models_{\varphi_0^{fair}} \varphi_0$, counterexample $\Pi_3 : (\{C\}\{B\})^\omega$
- $TS \models_{\varphi_1^{fair}} \varphi_0$, all fair paths Π_4, Π_7, Π_8 lead to state 4 which satisfies A
- $TS \not\models_{\varphi_2^{fair}} \varphi_0$, counterexample Π_3 as above

$\varphi_1: \Diamond (B \wedge \bigcirc (B \vee C))$

$TS \not\models_{\psi_0 \, fair} \varphi_1$ counterexample π_1 (case 01^{ω}): $(\{A,B\}\{A\})^{\omega}$

$TS \models_{\psi_1 \, fair} \varphi_1$ all fair paths contains the subtrace

$$\ldots \underset{\substack{\downarrow \\ \text{state} \\ 3}}{\{B\}} \; \underset{\substack{\downarrow \\ \text{state} \\ 4}}{\{A, C\}} \ldots$$

$TS \not\models \psi_2^{fair} \; \varphi_1$ counterexample π_2 as above

$\varphi_2: \Box \Diamond \neg B$

$TS \models \psi_0^{fair} \; \varphi_2$ all paths contain A or C infinitely many times

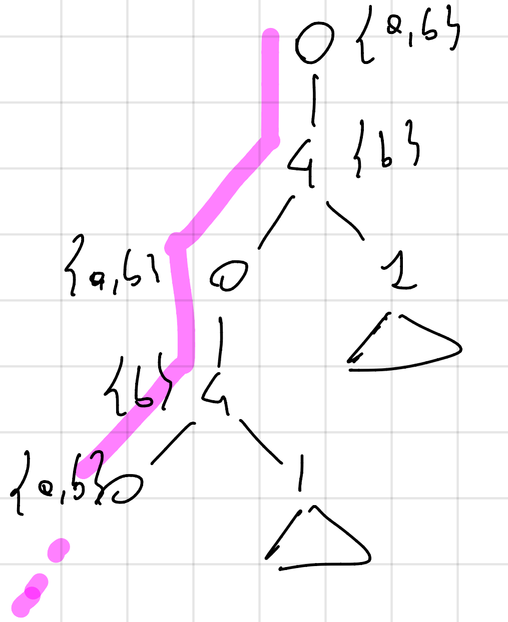
$TS \models \psi_1^{fair} \; \varphi_2$ as above

$TS \models \psi_2^{fair} \; \varphi_2$ as above

Ex 4

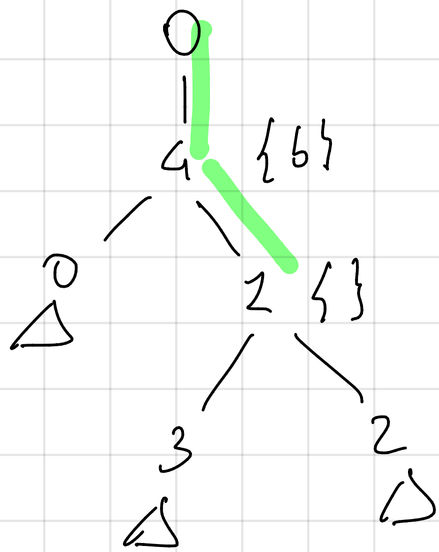
$TS \not\models \forall \Diamond c$ counterexample

ϕ_0



$TS \models \exists \Diamond (b \wedge \exists \bigcirc \neg b)$ witness

ϕ_1



ϕ_2: $TS \models \forall \Box (a \rightarrow \forall \Diamond b)$ state 0 satisfies a and $0 \rightarrow 4$ {b}

state 2 satisfies a and $2 \rightarrow 4$ {b}

ϕ_3 : $TS \not\models \forall\square(\neg b \rightarrow \forall\bigcirc(a \vee b))$

counterexample