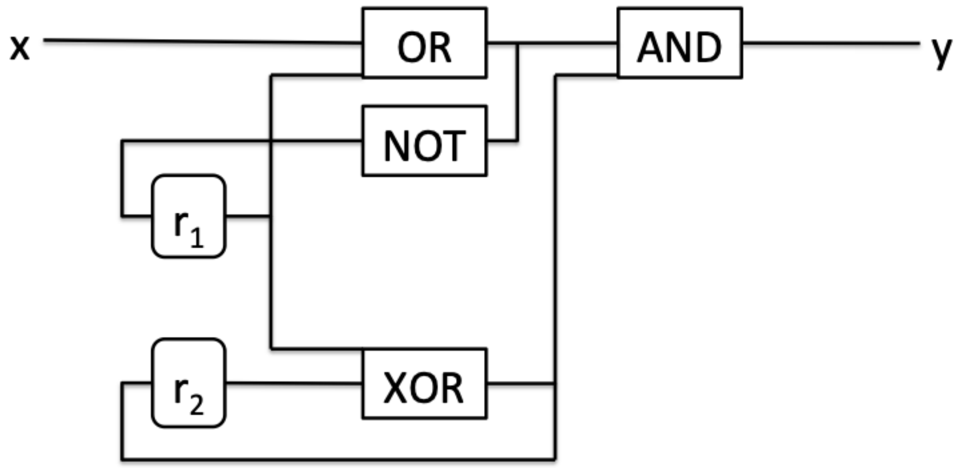
Master of Science in Computer Science - University of Camerino
Systems Verification Lab A. Y. 2018/2019
Written Test of 17th July 2019 (Appello V)
Teacher: Luca Tesei

## EXERCISE 1 (8 points)

Consider the following circuit.




Draw the transition system describing the behaviour of the circuit. Use $AP = \{y\}$ as set of atomic propositions to label states. Registers are initialised to 0.

## EXERCISE 2 (8 points)

Consider the atomic propositions $AP = \{P, Q, R\}$ and the following linear time properties:

**(a)** $P$ always holds the step before $Q$ holds unless $R$ holds together with $Q$, in which case $P$ may hold or not.

**(b)** $Q$ holds only finitely many times and whenever $Q$ holds also $R$ holds.

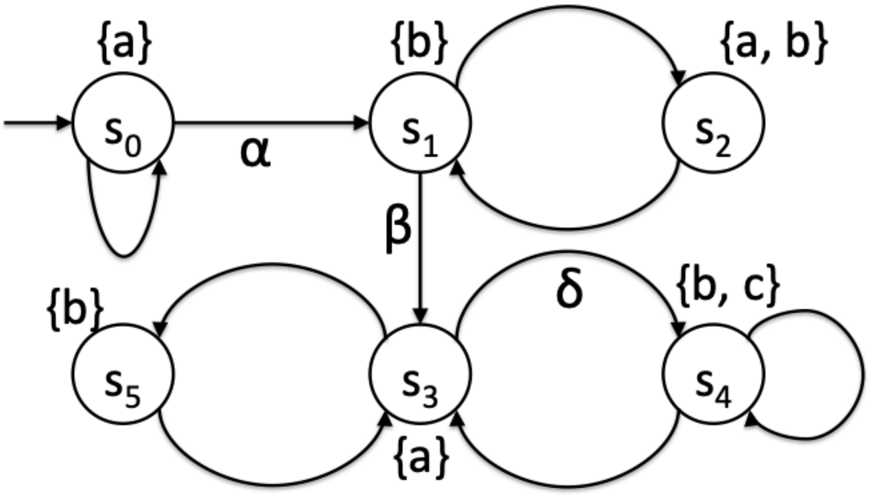
**(c)** Whenever $P$ holds then $Q$ and $R$ will hold together afterwards (or immediately).

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:

$$\varphi_0 = \Box\Diamond b \qquad \varphi_1 = \Box(a \to \bigcirc(a \vee b))$$
$$\varphi_2 = \Box\Diamond c$$

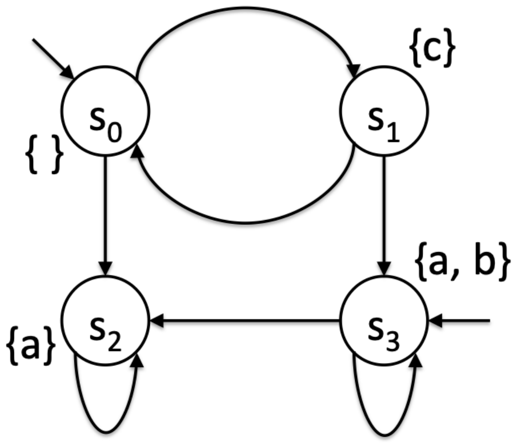
are satisfied by $TS$ under the following fairness conditions (to be considered separately):

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

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

**EXERCISE 4 (8 points)**

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

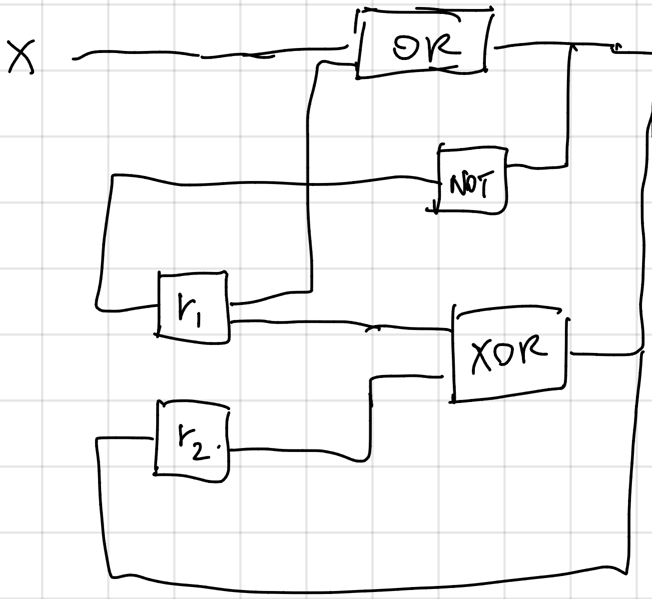



Decide whether or not the following CTL formulas:

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

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

$\boxed{\text{EX 1}}$



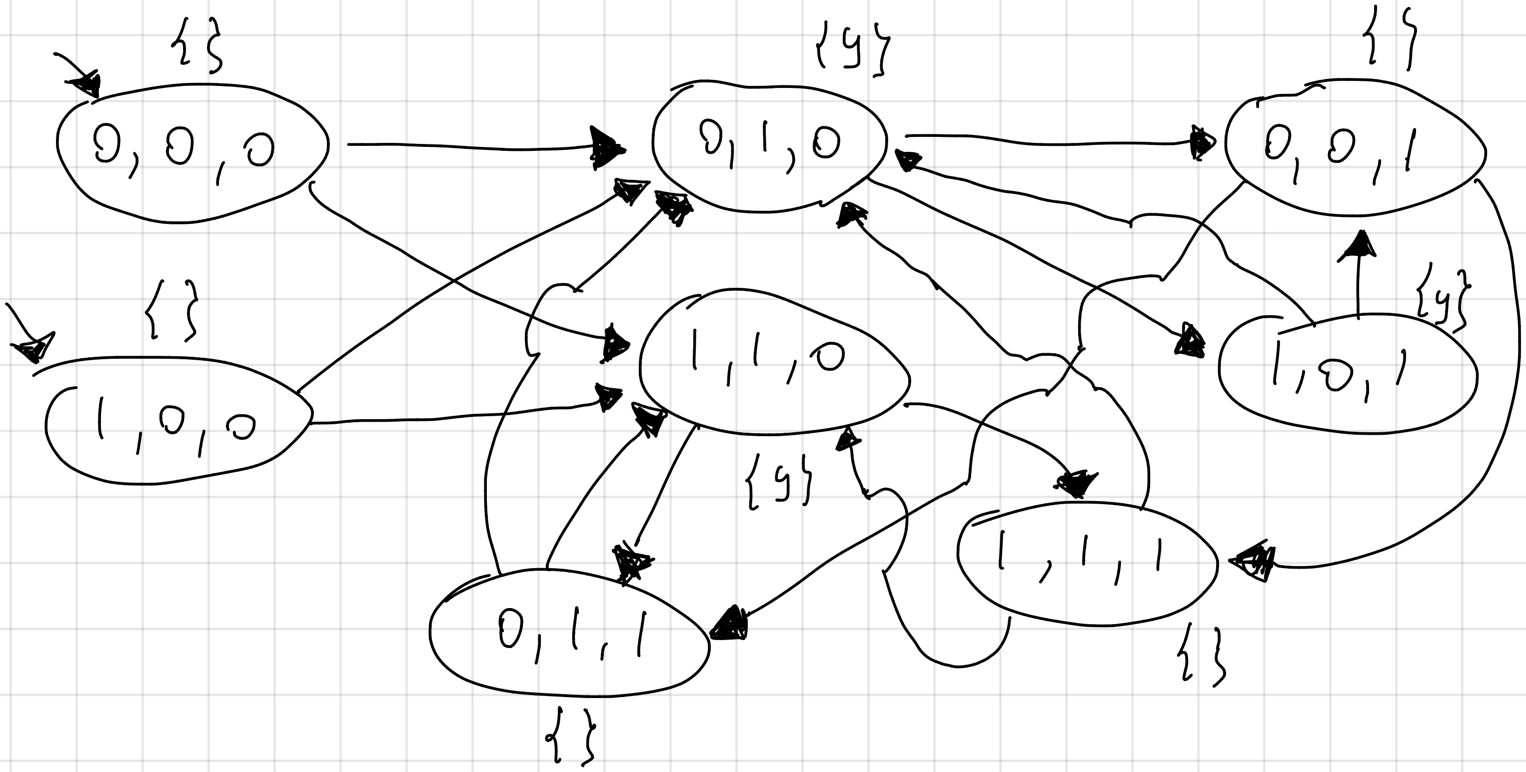

$(x, r_2, r_2)$ STATE

$AP = \{y\}$

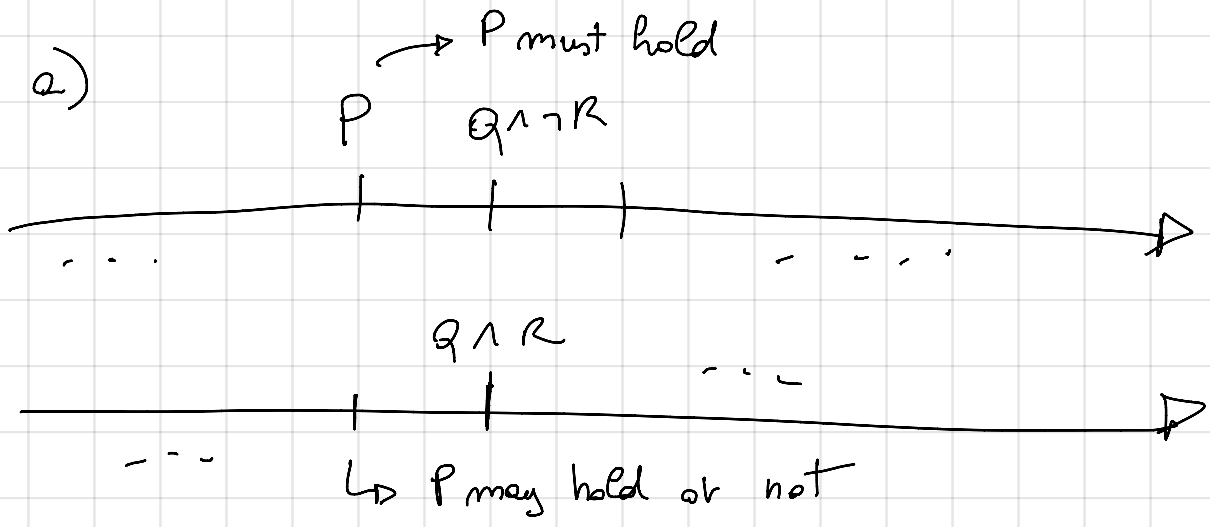
$r_1 = \text{NOT}(x \text{ xor } r_2)$

$r_2 = r_2 \text{ xor } r_2$

$y = (r_2 \text{ xor } r_2) \text{ AND } (x \text{ or } r_1)$




$\boxed{\text{EX 2}}$ a)



$$E_a = \{ A_0 A_1 \cdots \in (2^{AP})^\omega \mid \forall i \in \mathbb{N}:$$
$$((i>0) \land (Q \in A_i) \land (R \notin A_i)) \Rightarrow P \in A_{i-1} \}$$

in LTL the same property can be expressed using the next operator by reformulating the property as the equivalent set $\{ A_0 A_1 \ldots \in (2^{AP})^\omega \mid \forall i \in \mathbb{N}:$

$$i <= 0 \lor Q \notin A_i \lor R \in A_i \lor P \in A_{i-1} \}$$

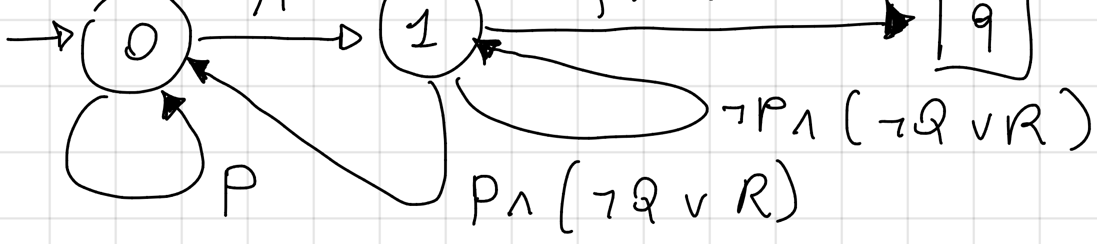
which, by substituting $J = i-1$, is equivalent to

$$\{ A_0 A_1 \cdots \in (2^{AP})^\omega \mid \forall J \in \mathbb{N}:$$
$$J \leq -1 \lor Q \notin A_{J+1} \lor R \in A_{J+1} \lor P \in A_J \}$$

since $J \leq -1$ is equivalent to false, it can be ignored in the disjunction. Then, the property is an invariant:

$$\Box(\bigcirc \neg Q \lor \bigcirc R \lor P) \quad \text{in LTL}$$

The property is SAFETY. To draw the NFA accepting the minimal bad prefixes, we refer to the original formulation:



b) $E_b = \{ A_0 A_1 \cdots \in (2^{AP})^\omega \mid \overset{\infty}{\forall} i : Q \notin A_i \wedge \forall J \in \mathbb{N} :$

$$Q \in A_i \Rightarrow R \in A_i \}$$

in LTL : $(\Diamond \Box \neg Q) \wedge \Box (Q \Rightarrow R)$

This is a MIXED property

c) $E_c = \{ A_0 A_1 \ldots \in (2^{AP})^\omega \mid \forall i \in \mathbb{N} : P \in A_i \Rightarrow ($

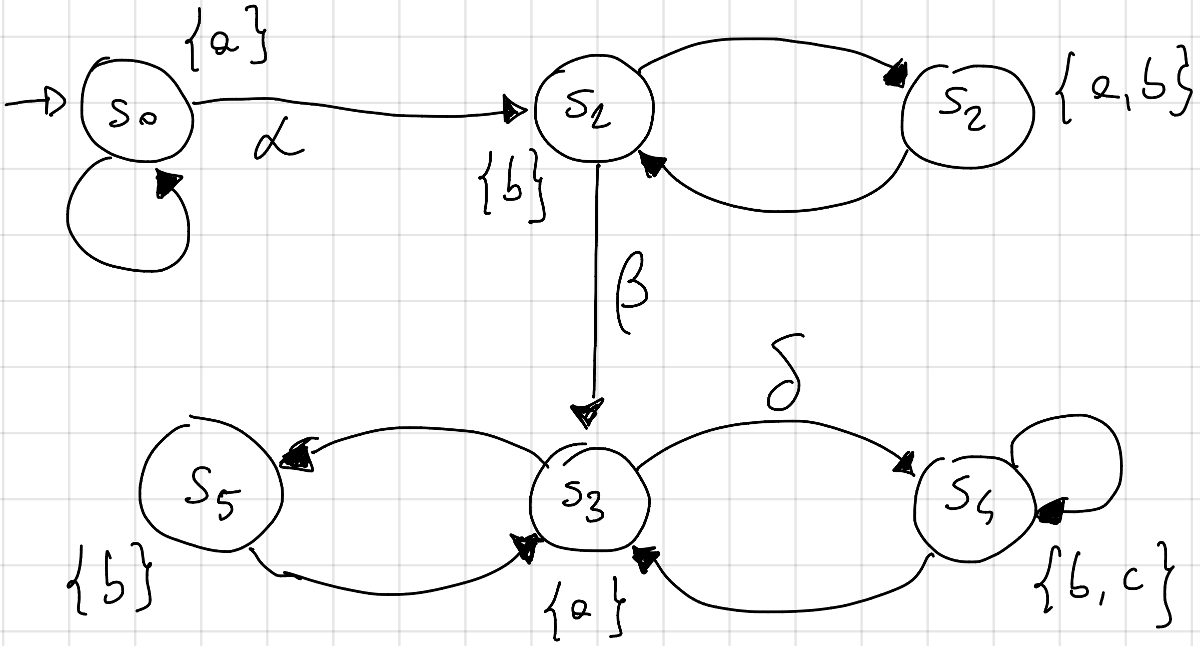
$$\exists J \in \mathbb{N} : J \geq i \wedge Q \in A_J \wedge R \in A_J ) \}$$

In LTL : $\Box (P \rightarrow \Diamond (Q \wedge R))$

This is a LIVENESS property

---

EX 3




$\varphi_0 = \Box \Diamond b$ $\qquad$ $\psi_0^{fair} = ( \{\}, \{\}, \{\} )$

$TS \not\models_{\psi_0^{fair}} \varphi_0$ because path $s_0^\omega$ is fair and is a counterexample

$\varphi_0 = \Box \Diamond b$ $\qquad\qquad$ $\psi_1^{fair} = (\{\ \}, \{\alpha, \beta, \delta\}, \{\ \})$

$TS \models_{\psi_1^{fair}} \varphi_0$ because path $s_0^\omega$ is not fair

Any other fair path visit a state labelled with $b$ infinitely many times.

$\varphi_0 = \Box \Diamond b$ $\qquad\qquad$ $\psi_2^{fair} = (\{\ \}, \{\ \}, \{\alpha, \beta, \delta\})$

$TS \models_{\psi_2^{fair}} \varphi_0$ because path $s_0^\omega$ is not fair as well.

$\varphi_1 = \Box(a \rightarrow \bigcirc(a \vee b))$

This is a safety property, thus it is not influenced by fairness conditions.

$TS \models_{\psi_i^{fair}} \varphi_1$ for $i = 0, 1, 2$. The safety property is satisfied:

$\{a\}\, s_0 \rightarrow s_0\, \{a\}$ $\qquad$ $\{a,b\}\, s_2 \rightarrow s_1\, \{a\}$

$\{a\}\, s_0 \rightarrow s_2\, \{b\}$ $\qquad$ $\{a\}\, s_3 \rightarrow s_4\, \{b,c\}$

$\{a\}\, s_3 \rightarrow s_5\, \{b\}$

$\varphi_2 = \Box\Diamond c$

$TS \not\models_{\psi_0 fair} \varphi_2$ because path $s_0^\omega$ is fair.

$TS \models_{\psi_1 fair} \varphi_2$ because paths $s_0^\omega$, $s_0^+(s_1 s_2)^\omega$,

$s_0^+(s_1 s_2)^+ s_3 \left[ (s_4^+ s_3)^+ (s_5 s_3)^+ \mid (s_5 s_3)^+ (s_4^+ s_3)^+ \right]^+ (s_5 s_3)^\omega$

are all unfair due to strong fairness of $\alpha, \beta, \delta$.

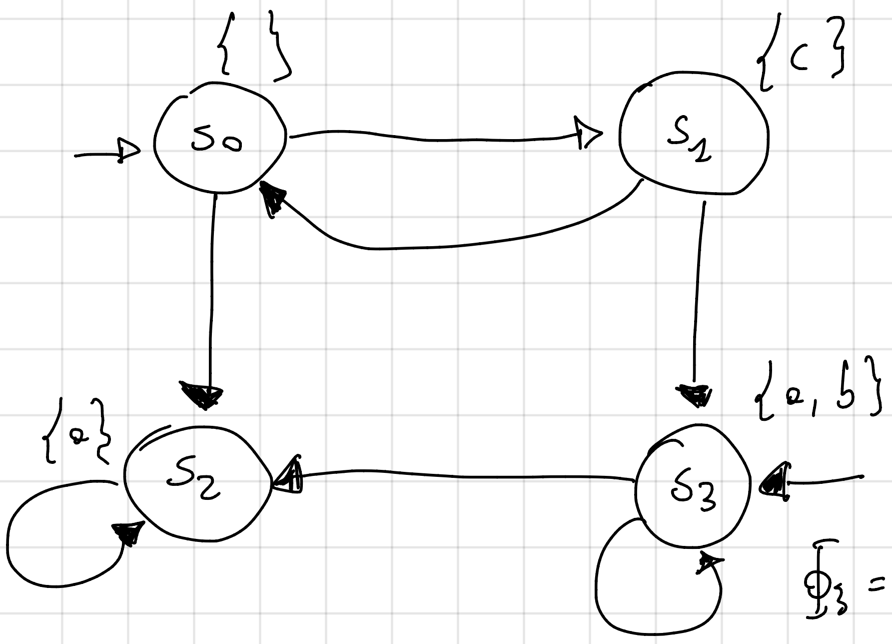
This means that state $s_4$ is always visited infinitely many times.

$TS \not\models_{\psi_2 fair} \varphi_2$ because weak fairness is not sufficient to exclude, e.g.,

paths $s_0^+(s_1 s_2)^\omega$.

---

EX 4




$\Phi_0 = \forall\Diamond b$

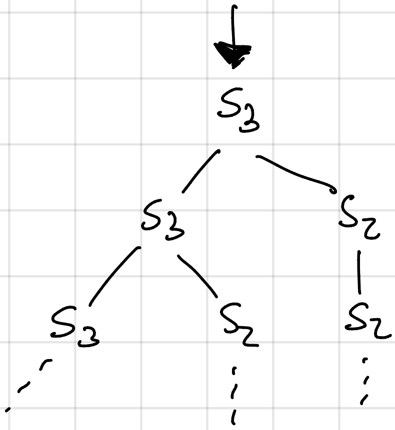
$\Phi_1 = \exists\Diamond c$

$\Phi_2 = \forall\Box c \to \exists\Diamond a$

$\Phi_3 = \forall\Box\forall\Diamond(a \vee c)$

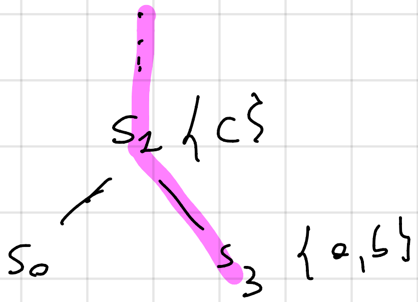
$TS \not\models \Phi_0$ Counterexample $(s_0 s_1)^\omega$

$TS \not\models \Phi_1$




there is no path leading to $c$ from initial state $s_3$, so the property is not satisfied by the TS, even if $s_0 \models \Phi_1$.

$TS \models \Phi_2$




$s_1$ is the only path in which $c$ is true. From there there is always one path leading to $a$, e.g. $s_2 \to s_3 \ldots$

$TS \models \Phi_3$ every path contains $a$ or $c$ infinitely many times: