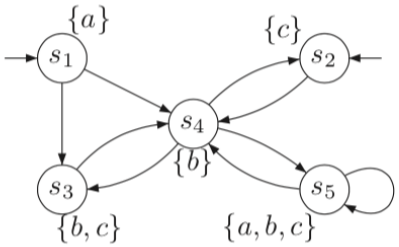
Verificação Formal de Software, 2019/20

FCUP

TP MC-2– LTL and CTL

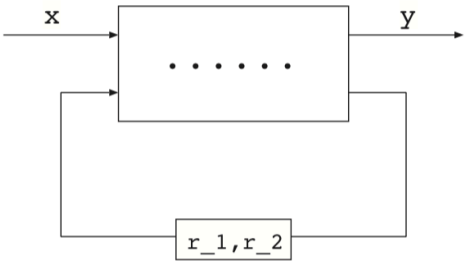
1. Consider the transition system over the set of atomic propositions $AP = \{a, b, c\}$:



Decide for each of the LTL formulae φ_i below whether $s_1 \models \varphi_i$ and $s_2 \models \varphi_i$. Justify your answers. If $s_j \not\models \varphi_i$ (for either $j = 0$ or $j = 1$, and $i \in \{1, 2, 3, 4, 5\}$) provide a path $\pi \in Paths(s_j)$ such that $\pi \not\models \varphi_i$.

$$
\begin{aligned}
\varphi_1 &= \mathrm{FG}c \\
\varphi_2 &= \mathrm{GF}c \\
\varphi_3 &= \mathrm{X}\neg c \rightarrow \mathrm{XX}c \\
\varphi_4 &= a\mathrm{UG}(a \vee c) \\
\varphi_5 &= \mathrm{XX}b\mathrm{U}(b \vee c)
\end{aligned}
$$

2. Consider the sequential circuit with one1 bit input x, two 1 bit registers (r_1,r_2) and one 1 bit output y, where $AP = \{ x, y, r_1, r_2 \}$.



Write LTL formulas for the following properties:

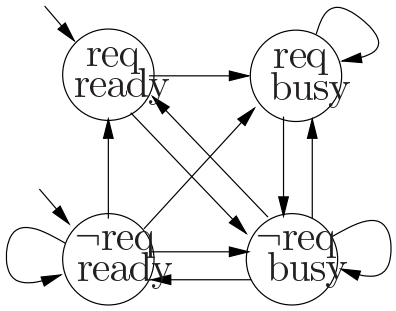
a) It is impossible that the circuit outputs two successive 1s.

b) Whenever the input bit is 1, in at most two steps the output bit will be 1

c) Whenever the input bit is 1, the register bits do not change in the next step.

d) Register r_1 has infinitely often the value 1.

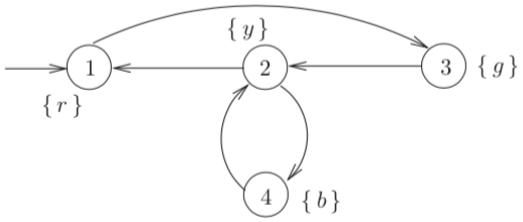
3. Consider the transition system T over the set of atomic propositions $AP = \{req, busy, ready\}$.



   (a) Check that for all initial states s, $s \models \mathrm{G}(req \rightarrow \mathrm{F}busy)$ (i.e $T \models \mathrm{G}(req \rightarrow \mathrm{F}busy)$.

   (b) It is true that $\neg(req\mathrm{U}\neg busy)$ is verified in all initial states of the system?

4. Consider the transition system over the set of atomic propositions $AP = \{\, b, g, r, y \,\}$. The model is intended to describe a traffic light that is able to blink yellow. The atomic proposition r is red, y is yellow, g is green and b is switched off.



   You are requested to indicate for each of the following CTL formulae the set of states for which these formulae hold and to informally indicate which property they express. Note: You may want to build some levels of the computation tree of the system from the initial state.

   (a) AFy

   (b) AGy

   (c) AGAFy

   (d) EFg

   (e) EG$\neg g$

   (f) A(bU$\neg b$)

   (g) E(bU$\neg b$)

   (h) A($\neg b$UEFb)

   (i) A($\neg b$Ub)

5. Express the following properties in CTL and in LTL whenever possible (atomic propositions in typewriter font).

   (a) For any state, if a `request` occurs then it will eventually be `acknowledged`.

   (b) For any state, if a `request` occurs then it will be `acknowledged`.

(c) A lift can remain on a `floor` with its door `closed`.

(d) An upwards lift at the `floor2` and with `buttonpressed5` goes `up` until it reaches the `floor5`

(e) The door is not `open` if the lift is not in a `floor`.

6. Which of the following pairs of formulae are equivalent? For those which are not, exhibit a model of one of the pair which is not a model of the other. In the affirmative case, give a justification.

   (a) $\mathrm{G}\varphi \wedge \mathrm{XF}\varphi$ and $\mathrm{G}\varphi$

   (b) $\mathrm{AGAF}\psi$ and $\mathrm{AFAG}\psi$

   (c) $\mathrm{AF}\varphi \vee \mathrm{AF}\psi$ and $\mathrm{AF}(\varphi \vee \psi)$

   (d) $\mathrm{EF}\varphi \vee \mathrm{EF}\psi$ and $\mathrm{EF}(\varphi \vee \psi)$.

   (e) $\mathrm{AG}(\varphi \rightarrow \psi)$ and $\mathrm{EF}\varphi \rightarrow \mathrm{EF}\psi$

   (f) $\neg\mathrm{A}(\varphi \mathrm{U} \psi)$ and $\mathrm{E}(\varphi \mathrm{U} \neg\psi)$

(g) E(bU$\neg b$)

(h) A($\neg b$UEFb)

(i) A($\neg b$Ub)

Solution:

(a) $\{1, 2, 3, 4\}$; "It is inevitable that the traffic light is yellow"

(b) $\emptyset$, "Invariantly the traffic light is yellow"

(c) $\{1, 2, 3, 4\}$, "The traffic light is infinitely often yellow"

(d) $\{1, 2, 3, 4\}$, "Potentially the traffic light is green"

(e) $\{2, 4\}$, "Potentially always the traffic light is not green"

(f) $\{1, 2, 3, 4\}$, "It is inevitable that the traffic light is not switched off"

(g) $\{1, 2, 3, 4\}$, "Potentially the traffic light is not switched off"

(h) $\{1, 2, 3, 4\}$,

(i) $\{4\}$, "It is inevitable that the traffic light is switched off"

5. Express the following properties in CTL and in LTL whenever possible (atomic propositions in typewriter font).
   (a) For any state, if a `request` occurs then it will eventually be `acknowledged`.
   (b) For any state, if a `request` occurs then it will be `acknowledged`.
   (c) A lift can remain on a `floor` with its door `closed`.
   (d) An upwards lift at the `floor2` and with `buttonpressed5` goes `up` until it reaches the `floor5`
   (e) The door is not `open` if the lift is not in a `floor`.

Solution: If possible we write a CTL formula; LTL formula, in each case.

a) AG(`request` $\rightarrow$ AF`acknowledged`); G(`request` $\rightarrow$ F`acknowledged`)

b) AG(`requested` $\rightarrow$ EF`acknowledge`); Not possible

c) AG((`floor` $\wedge$ `closed`) $\rightarrow$ EG(`floor` $\wedge$ `closed`)); Not possible

d) AG((`floor2` $\wedge$ `buttonpressed5`) $\rightarrow$ A(`upUfloor5`)); G((`floor2` $\wedge$ `buttonpressed5`) $\rightarrow$ (`upUfloor5`))

e) AG($\neg$`floor` $\rightarrow$ $\neg$`open`);G($\neg$`floor` $\rightarrow$ $\neg$`open`)

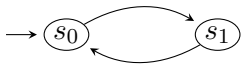
6. Which of the following pairs of formulae are equivalent? For those which are not, exhibit a model of one of the pair which is not a model of the other. In the affirmative case, give a justification.

   (a) $\mathrm{G}\varphi \wedge \mathrm{XF}\varphi$ and $\mathrm{G}\varphi$

   Solution: Are equivalent because for all π, if $\pi \models \mathrm{G}\varphi$ then $\pi \models \mathrm{XF}\varphi$.

   (b) $\mathrm{AGAF}\psi$ and $\mathrm{AFAG}\psi$

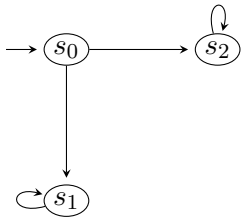
   Solution: Not equivalent. Consider the transition system $(S = \{s_0, s_1\}, \longrightarrow = \{(s_0, s_1), (s_1, s_0)\}, I = \{s_0\}, AP = \{p, r\}, L)$

   where $L(s_0) = \{p\}$ and $L(s_1) = \{r\}$ (where actions are omitted). We have that $s_0 \models \mathrm{AGAF}r$ but $s_0 \not\models \mathrm{AFAG}r$. There is only one path $\pi = s_0 s_1 s_0 s_1 \cdots$ from s_0. Because $s_0 \models \mathrm{AF}r$ and $s_1 \models \mathrm{AF}r$, we have $s_0 \models \mathrm{AGAF}r$. But $s_0 \not\models \mathrm{AG}r$ neither $s_1 \models \mathrm{AF}r$ as $s_0 \not\models r$. Thus $s_0 \not\models \mathrm{AFAG}r$.

   (c) $\mathrm{AF}\varphi \vee \mathrm{AF}\psi$ and $\mathrm{AF}(\varphi \vee \psi)$

   Solution: Not equivalent. Consider the transition system $(S = \{s_0, s_1, s_2\}, \longrightarrow = \{(s_0, s_1), (s_0, s_2), (s_1, s_1), (s_2, s_2)\}, I = \{s_0\}, AP = \{p, r\}, L)$

   where $L(s_0) = \{\}$, $L(s_1) = \{r\}$ and $L(s_2) = \{p\}$ (where actions are omitted). Consider $\mathrm{AF}(r \vee p)$. The paths from s_0 are $pi_1 = s_0 s_1 s_s \cdots$ and $\pi_2 = s_0 s_2 s_s \cdots$. We have that $\pi_1[2] = (r \vee p)$ and $\pi_2[2] = (r \vee p)$. So we have $\mathrm{AF}(r \vee p)$. But $s_0 \not\models \mathrm{AF}r$, because for π_2 for all $i \geq 1$, $\pi_2[i] \neq r$, and similarly $s_0 \not\models \mathrm{AF}p$. Thus $s_0 \not\models \mathrm{AF}r \vee \mathrm{AF}p$.

   (d) $\mathrm{EF}\varphi \vee \mathrm{EF}\psi$ and $\mathrm{EF}(\varphi \vee \psi)$.

   Solution: Are equivalent. Suppose that $s \models \mathrm{EF}(\varphi \vee)$ then exists one path $\pi \in Paths(s)$ such that exists $i \geq 1$ such that $\pi[i] \models (\varphi \vee \psi)$. Let $\pi[i] \models \varphi$, then also $s \models \mathrm{EF}(\varphi)$ and so $s| \models \mathrm{EF}\varphi \vee \mathrm{EF}\psi$. We conclude the same if $\pi[i] \models \psi$. If $s \models \mathrm{EF}\varphi \vee \mathrm{EF}\psi$, and suppose, without lost of generality, that $s \models \mathrm{EF}\psi$. Again there exists a path $\pi \in Paths(s)$ such that exists $i \geq 1$ such that $\pi[i] \models \varphi$. But then $\pi[i] \models \varphi \vee \psi$. So we also have $s \models \mathrm{EF}(\varphi \vee \psi)$.

   (e) $\mathrm{AG}(\varphi \rightarrow \psi)$ and $\mathrm{EF}\varphi \rightarrow \mathrm{EF}\psi$

Solution: Not equivalent. Consider the model of case (c). We have $s0 \models \mathrm{EF}p \rightarrow \mathrm{EF}r$ (because $s0 \models \mathrm{EF}r$). But $s0 \not\models \mathrm{AG}(p \rightarrow r)$ as $s2 \not\models (p \rightarrow r)$.

(f) $\neg\mathrm{A}(\varphi \mathrm{U} \psi)$ and $\mathrm{E}(\varphi \mathrm{U} \neg\psi)$

Solution: Not equivalent. Use the fact that $\mathrm{A}[\varphi \mathrm{U} \psi] \equiv \neg\mathrm{E}[\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)] \wedge \neg\mathrm{EG}\neg\psi$