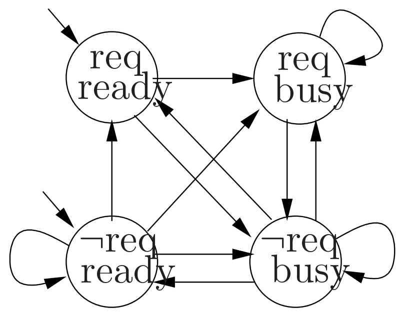
Verificação Formal de Software - Exercícios

Lógica Temporal Linear (LTL)

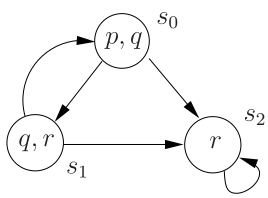
1. Considera o seguinte sistema de transições T



   (a) Verifica que $T \models \mathrm{G}(req \to \mathrm{F}busy)$.

   (b) É verdade que $\neg(req \mathrm{U} \neg busy)$ se verifica em todos os estados do sistema?

2. Considera o sistema $T = (S = \{s_0, s_1, s_2\}, \{s_0 \longrightarrow s_1, s_0 \longrightarrow s_2, s_1 \longrightarrow s_2, s_1 \longrightarrow s_0, s_2 \longrightarrow s_2\}, L(s_0) = \{p, q\}, L(s_1) = \{q, r\}, L(s_2) = \{r\})$.



   Determina quais destas relações são verdadeiras:

   1. $s_0 \models p \wedge q$
   2. $s_0 \models \mathrm{X}r$
   3. $s_0 \models \mathrm{X}(q \wedge r)$
   4. $s_0 \models \mathrm{G}\neg(p \wedge r)$
   5. $s_0 \models \mathrm{GF}p$
   6. $s_0 \models \mathrm{GF}p \to \mathrm{GF}r$

3. Considera o sistema $\mathcal{M} = (S = \{q_1, q_2, q_3, q_4\}, \{q_1 \to q_2, q_2 \to q_2, q_3 \to q_1, q_3 \to q_2, q_3 \to q_4, q_4 \to q_3\}, L(q_1) = \{\}, L(q_2) = \{b\}, L(q_3) = \{a\}, L(q_4) = \{a, b\})$.

   Para cada uma das fórmulas seguintes:

   a) Ga;

   b) aUb;

   c) $aUX(a \wedge \neg b)$;

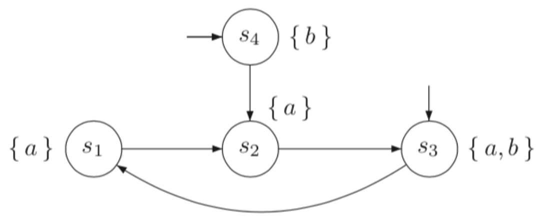
   d) $X\neg b \wedge G(\neg a \vee \neg b)$;

   e) $X(a \wedge b) \wedge F(\neg a \wedge \neg b)$;

   (a) encontra um caminho a partir do estado q_3 que satisfaz φ;

(b) determina se $q_3 \models \varphi$.

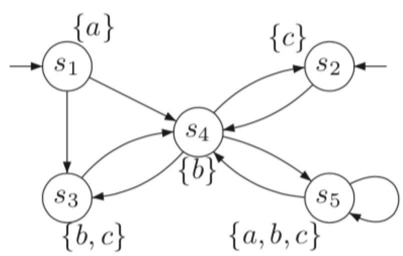
4. Considera o sistema de transições abaixo com $AP = \{a, b\}$.



Indica para cada fórmula abaixo quais os estados em que elas são satisfeitas:

a) Xa
b) XXXa
c) Gb
d) GFa
e) G(bUa)
f) F(aUb)

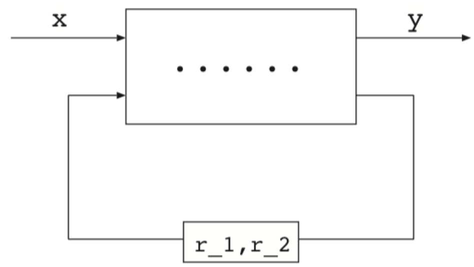
5. Considera o sistema de transições abaixo com $AP = \{a, b, c\}$.



Decide para cada fórmula LTL φ_i se $T \models \varphi_i$, justificando a tua resposta.

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

6. Considera o circuito sequencial com uma entrada de 1 bit x com dois registos de um bit (r_1,r_2) e uma saída de um bit y, e $AP = \{x, y, r_1, r_2\}$.



Escreve fórmulas LTL para cada uma das seguintes propriedades.

a) É impossível que o circuito tenha como saída dois 1's consecutivos
b) Sempre que o bit de entrada é 1, no máximo em dois passos o bit de saída é 1.
c) Sempre que o bit entrada é 1, os registos não são alterados no passo seguinte
d) O registo r_1 tem um n.i.d.v o valor 1.

7. Mostra que

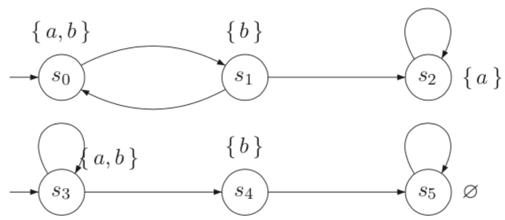
$$
\begin{aligned}
\neg(\varphi \mathrm{U} \psi) &\equiv \neg\varphi \mathrm{R} \neg\psi \\
\neg(\varphi \mathrm{R} \psi) &\equiv \neg\varphi \mathrm{U} \neg\psi \\
\mathrm{X}(\varphi \mathrm{U} \psi) &\equiv (\mathrm{X}\varphi)\mathrm{U}(\mathrm{X}\psi) \\
\varphi \mathrm{U} \psi &\equiv \varphi \mathrm{W} \psi \wedge \mathrm{F}\psi \\
\varphi \mathrm{W} \psi &\equiv \varphi \mathrm{U} \psi \vee \mathrm{G}\varphi \\
\varphi \mathrm{W} \psi &\equiv \psi \mathrm{R}(\varphi \vee \psi) \\
\varphi \mathrm{R} \psi &\equiv \psi \mathrm{W}(\varphi \wedge \psi) \\
\varphi \mathrm{U} \psi &\equiv \psi \vee (\varphi \wedge \mathrm{X}(\varphi \mathrm{U} \psi)) \\
\mathrm{F}\varphi &\equiv \varphi \vee \mathrm{XF}\varphi \\
\mathrm{G}\varphi &\equiv \varphi \wedge \mathrm{XG}\varphi
\end{aligned}
$$

8. Mostre que os seguintes conjuntos de connectivas temporais são completos par a LTL: $\{\mathrm{U}, \mathrm{X}\}$, $\{\mathrm{R}, \mathrm{X}\}$ e $\{\mathrm{W}, \mathrm{X}\}$.

9. Para as equivalências seguintes indica as que são verdadeiras (provando) e as que são falsas (indicando um contra-exemplo).

$$
\begin{aligned}
\mathrm{G}\varphi \rightarrow \mathrm{F}\psi &\equiv \varphi \mathrm{U}(\psi \vee \neg\varphi) \\
\mathrm{FG}\varphi \rightarrow \mathrm{GF}\psi &\equiv \mathrm{G}(\varphi \mathrm{U}(\psi \vee \neg\varphi)) \\
\mathrm{GG}(\varphi \vee \neg\psi) &\equiv \neg\mathrm{F}(\neg\varphi \wedge \psi) \\
\mathrm{F}\varphi \wedge \mathrm{XG}\varphi &\equiv \mathrm{F}\varphi \\
\mathrm{G}\varphi \wedge \mathrm{XF}\varphi &\equiv \mathrm{G}\varphi
\end{aligned}
$$

10. Considera o sistema de transições T seguinte, com $AP = \{\, a, b, c \,\}$.



Considera a assunção de justeza (*fairness*):

$$fair = (\mathrm{GF}(a \wedge b) \rightarrow \mathrm{GF}\neg c) \wedge (\mathrm{FG} \rightarrow \mathrm{GF}\neg b)$$

(a) Determina os caminhos justos em T i.e. os caminhos iniciais infinito que verifica, a fórmula $fair$

(b) Para cada uma das fórmulas LTL seguintes indica se $T \models_{fair} \varphi_i$. No caso $T \not\models_{fair} \varphi_i$, indica um caminho $\pi \in Paths(T)$ tal que $\pi \not\models \varphi_i$.

$$\begin{array}{rcl} \varphi_1 & = & \mathrm{FG}a \\ \varphi_2 & = & \mathrm{X}\neg a \rightarrow \mathrm{FG}a \\ \varphi_3 & = & \mathrm{X}a \\ \varphi_4 & = & b\mathrm{U}\mathrm{G}\neg b \end{array}$$

11. Seja $\varphi = (a \rightarrow \mathrm{X}\neg b)\mathrm{W}(a \wedge b)$ e $P = Words(\varphi)$ onde AP={ a,b }.
    (a) Mostra que P é uma propriedade de segurança.
    (b) Define um NFA A tal que $L(A) = BadPref(P)$.