11,5

RALISON
Mathieu

Devoir "Introduction à la vérification"

$\neg AF\phi = EG(\neg\phi)$

Exercice 1 :

$$\phi = AF(G \wedge \neg a) \rightarrow AFA(G \; W \; (\neg a \wedge \neg G))$$

1. Soit ϕ_1 et ϕ_2 des formules de ϕ tel que

$$\phi = \phi_1 \rightarrow \phi_2 \quad = \neg\phi_1 \vee \phi_2 = \neg(\phi_1 \wedge \neg\phi_2)$$

donc on va écrire ϕ_1 et ϕ_2 en forme normale existentielle pour obtenir ϕ en ENF.

$$\phi_1 = AF(G \wedge \neg a) = \neg EF \neg(G \wedge \neg a) = \neg EF(\neg G \vee a)$$

EG

f

$$\begin{aligned}\phi_2 &= AFA(G \; W \; (\neg a \wedge \neg G)) \\ &= AF \neg E((G \wedge (a \vee G)) \; U \; (\neg G \wedge (a \vee G)))\\ &= \neg EG \; E((G \wedge (a \vee G)) \; U \; (\neg G \wedge (a \vee G)))\\ &= \neg EG \; E(G \; U \; (\neg G \wedge a))\end{aligned}$$

✓

On note $\phi_2' = \neg\phi_2$

Donc on a $\phi = \neg(\phi_1 \wedge \phi_2')$

$$\boxed{\phi = \neg(\neg EF(\neg G \wedge a)) \wedge (EG \; E(G \; U \; (\neg G \wedge a)))}$$

2] $Sat(\phi) = S \setminus Sat(G\phi_1 \wedge \phi_2')$

$= S \setminus (Sat(\phi_1) \cap Sat(\phi_2'))$

Calculons $Sat(\phi_1)$ avec l'algo vu en cours ? pour G ?

- $T_0 = \{s_1, s_4, s_5, s_6\}$ $V_0 = \{s_2, s_3\}$

$pre(s_2) = \{s_5, s_6, s_1\} \Rightarrow pre(s_2) \cap T_0 = \{s_5, s_6\}$

- $T_1 = \{s_1, s_4, s_5, s_6\}$ $V_1 = \{s_3\}$?

$pre(s_3) = \{s_6, s_2, s_4\} \Rightarrow pre(s_3) \cap T$

- $T_2 = \{s_1, s_5, s_6\}$ $V_2 = \{s_4\}$

$pre(s_4) = \{s_3, s_5\} \Rightarrow pre\{s_4\} \cap T_2 = \{s_5\}$

- $T_3 = \{s_1, s_6\}$ $V_3 = \{s_5\}$

$pre(s_5) \cap T_3 = \emptyset$

- Donc $sat(G\phi_1) = \{s_1, s_6\}$

$sat(\phi_1) = S \setminus \{s_1, s_6\}$

Calculons maintenant $Sat\ \phi_2'$.
Avant cela, on aura besoin de calculer $sat(E(G \cup (\neg G \wedge a)))$.

- $V_0 = T_0 = \{s_5\} = sat(\neg G \wedge a)$

$pre\{s_5\} \setminus T_0 = \{s_2\}$

- $V_1 = \{s_2\}$ $T_2 = \{s_5, s_2\}$

pre(s_2) $\setminus T_1 = \{s_0\}$

- $V_2 = \{s_0\}$ $T_2 = \{s_5, s_2, s_0\}$

pre(s_2) $\cap T_2 = \emptyset$

Donc sat(EGU($\tau\beta \wedge \alpha$)) $= \{s_5, s_2, s_0\}$ ✓

Maintenant il faut calculer sat(ϕ_2')

- $T_0 = \{s_5, s_2, s_0\}$ $V_0 = \{s_1, s_3, s_4\}$

? pre(s_4) $\cap T_0 = \{s_0\}$? + compteur

- $T_1 = \{s_5, s_2, s_0\}$ $V_1 = \{s_3, s_4\}$

pre(s_3) $\cap T_1 = \{s_0, s_2\}$

- $T_2 = \{s_5, s_2, s_0\}$ $V_2 = \{s_4\}$

pre(s_4) $\cap T_2 = \{s_5\}$

Donc Sat $\phi_2' = \{s_5, s_2, s_0\}$ (✓)

Alors on obtient Sat $\phi = S \setminus (S \setminus \{s_1, s_0\} \cap \{s_5, s_2, s_0\})$

Sat $\phi = S \setminus (\{s_2, s_3, s_4, s_5\} \cap \{s_5, s_2, s_0\})$

Sat $\phi = S \setminus \{s_2, s_5\}$

Exercice 2

1. Soit S le système de transition ci dessous

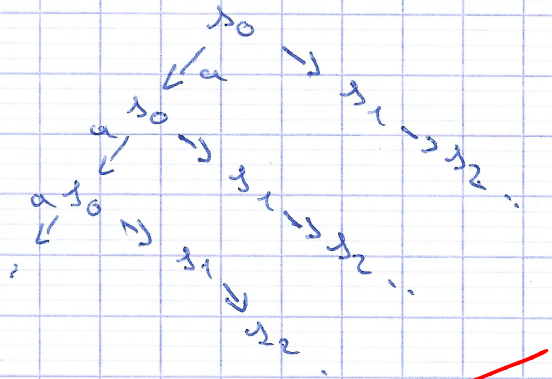
✓

exécutions

$S \models FXa$ en effet les ~~mots acceptant~~ des système sont ~~s_0^w s_1^w~~ s_2^w, et donc il satisfait bien la formule CTL

L'arbre d'exécution de S ressemble à ça :

$s_0^* s_1 s_2^w$ et s_0^w



F(AX)

On voit que l'exécution $s_0 \to s_0 \to \dots$ ne satisfait pas ~~AXa~~ donc

(✓)

$S \not\models AFAXa$

2. $AF(a \wedge AFG)$ et $F(a \wedge FG)$

On souhaite montrer que $S \models AF(a \wedge AFG) \Leftrightarrow S \models F(a \wedge FG)$

"$\Rightarrow$"

Soit S un système de transition tel que $S \models AF(a \wedge AFG) \Rightarrow$ Pour toute exécution à partir d'un état initial s_0, il existe un état qui satisfait $a \wedge AFG$. Soit $s_i \models a \wedge FG$, avec s_i un état de S

$s_i \models a \wedge AFG \Leftrightarrow s_i \models a$ et $s_i \models AFG$

⇒ Pour toute execution à partir de s_i ($s_i \to s_{i+1} \to \dots$ il y a un un état qui satisfait G. $\exists m \geq i$ tel que $s_m \models G$.

Donc pour toute execution à partir d'un état initial $(a \wedge FG)$ sera satisfait donc $S \models F(a \wedge FG)$

"⇐"

On suppose que S satisfait la formule LTL $S \models F(a \wedge FG)$ ⇒ à partir un etat initial s_0, il existe i tel que

$s_0 \to s_1 \to \dots \to s_i$

$s_i \models a \wedge FG$

⇒ $s_i \models a$ et $s_i \models FG$

$s_i \to s_{i+1} \to \dots \to s_m$

⇒ $s_m \models G$

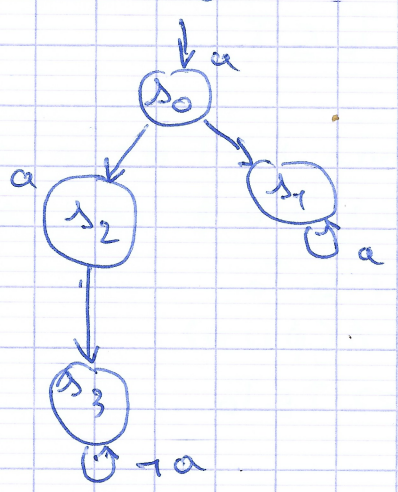
ne montre pas AFG

vu sur notes 9/4/21

Donc pour toute exécution, il existe un état qui satisfait a et à partir de ce dernier G sera toujours satisfait dans le futur.

Donc $S \models AF(a \wedge AFG)$

3] Soit S le système de transition ci-dessous



(AX_a est prouvée d'état
GAX_a —— de deux)

$s_0 \to s_1 \to s_2 \to \dots \models AX a \Rightarrow s \models EGAX_a$

$s_0 s_2 \overset{\omega}{s_3} \not\models GX_a \Rightarrow s \not\models GX_a$

Donc $EGAX_a \not\equiv GX_a$

Exercice 3

1) Montrons que $\{s \in sat(\phi) : post(s) \subseteq T_0\} \subseteq T_0$ avec $T_0 = Sat(A\phi \cup \psi)$, et que pour $T \subseteq S$ et qui contient $Sat\psi$ et satisfait $\{s \in sat\phi : post(s) \subseteq T\} \subseteq T$ implique qu'il contient T_0] ②

- $Sat(\psi) \subseteq T_0$ par définition.
Soit $s \in \{s \in sat(\phi) : post(s) \subseteq T_0\} \subseteq T_0$
$\Rightarrow s \models \phi$ et $\forall s' \in post(s)$ $s' \in T_0$ ✓
$\Rightarrow s' \models \psi$ ou $s' \models \phi \wedge X(\phi \cup \psi)$ pas CTL
$\Rightarrow s' \in T_0 \Rightarrow s \in T_0$
$\Rightarrow \{s \in Sat(\phi) : post(s) \subseteq T_0) \subseteq T_0$

c'est la même dose, vous n'avez rien démontré pour ①

- Soit $T \subseteq S$ tel que $sat(\psi) \subseteq T$ et $\{s \in sat\phi : post(s) \subseteq T\} \subseteq T$
Montrons que $T_0 \subseteq T$
Soit $s \in T_0$:
• si $s \models \psi$ alors $s \in T$ car $sat(\psi) \subseteq T$
• si $s \not\models \psi$ alors $s \models \phi$ car $s \in T_0$, et
$\Rightarrow post(s) \subseteq T_0$
$\Rightarrow s \models AXA(\phi \cup \psi)$
$\Rightarrow s \in T$ $\Rightarrow T \subseteq T_0$

pourquoi ? ça vient de nul part 6/10

2] Montrons que :

$Sat(AG\phi) \subseteq \{s \in sat(\phi) : post(s) \subseteq sat(AG\phi)\}$

Soit $s_0 \in sat\ AG\phi$

$s_0 \models AG\phi \Rightarrow s_0 \to s_1 \to s_2 \to \dots$ (ϕ ϕ)

$\Rightarrow s_0 \in sat\ \phi$ et $\forall i\ \ s_i \models \phi$

$\Rightarrow post(s) \subseteq sat\ AG\phi$

$\Rightarrow sat\ AG\phi \subseteq \{s \in sat\ \phi : post(s) \subseteq sat\ AG\phi\}$ ✓

Maintenant montrons pour tout $T \subseteq s$:

$T \subseteq \{s \in sat\ \phi : post(s) \subseteq T\} \Rightarrow T \subseteq sat\ AG\phi$

Soit $s \in T$

$\Rightarrow s \in sat\ \phi$ et $post(s) \subseteq T$

$\Rightarrow \forall s' \in post(s) \quad s' \in T$

$\Rightarrow s' \in sat(\phi)$ et $post(s') \subseteq T$

Donc récursivement $s \in sat\ AG\phi$ donc $T \subseteq sat\ AG\phi$ ✓

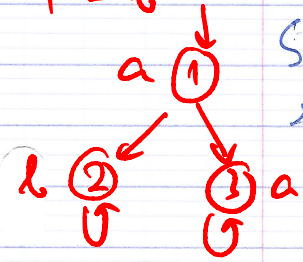
3] Montrons que :

$Sat\ A(\phi\ W\ \psi) \subseteq \{sat(\psi \cup ?)\ s \in sat\ \phi : post(s) \subseteq T\}$

ex :

$\phi = a$

$\psi = b$



$1 \not\models AG\,a$

$1 \not\models A(a\ U\ b)$

$A(\phi\ W\ \psi) = AG\phi \vee A(\phi\ U\ \psi)$ non, ce n'est pas vrai

Soit $\in s \in Sat\ A(\phi\ W\ \psi)$, montrons que $s \in sat\ \phi\ U) s \in sat\ \phi$: post $(s) \subseteq T$?

$s \not\models A(\phi\ W\ \psi) \Rightarrow s \not\models AG\phi$ ou $s \not\models A(\phi\ U\ \psi)$

$\Rightarrow s \not\models AG\phi$ ou $s \not\models A\psi \vee AXA(\phi\ U\ \psi)$

$\Rightarrow s \not\models AG\phi \vee A\psi$ ou $\forall s' \in post(s)\ \ s' \not\models A(\phi\ U\ \psi)$

Donc d'après la question 1, tout successeur appartient $sat(A(\phi \cup \psi))$ si $s \not\models AG\phi \vee A\psi$

Donc $s \in \{s \in sat\ \phi : post(s) \subseteq Sat(\phi\ w\ \psi)\}$

Or $sat(AG\phi) \subseteq \{s \in sat\ \phi : post(s) \subseteq sat(\phi\ w\ \psi)\}$

Donc en a bien $s \in Sat\ \psi \cup \{s \in sat\ \phi : post(s) \subseteq sat(\phi\ w\ \psi)$

$\Rightarrow$ $Sat(\phi\ w\ \psi) \subseteq \{s \in sat\ \phi : post(s) \subseteq sat\ \phi\ w\ \psi\}$

Montrons que pour $T \subseteq S$:

$T \subseteq Sat(\psi) \cup \{s \in sat\ \phi : post(s) \subseteq T\} \Rightarrow T \subseteq sat\ \phi\ w\ \psi$

Soit $s \in T$, montrons que $s \in sat\ \phi\ w\ \psi$

$s \in T \Rightarrow s \models \psi$ ou, $s \in sat\ \phi$ et $post(s) \subseteq T$

$\Rightarrow s \models \psi$ ou, $s \models \phi$ et $\forall s' \in post(s)$ $s' \in T$

$\Rightarrow$ " " " " " $s' \models \psi$ ou

$s' \in \{s \in sat\ \phi \mid post(s) \subseteq T\}$

S: $s \not\models \psi$ alors $s \in Sat(AG\phi) \cup Sat(A(\phi \cup \psi))$

alors $s \in sat(A(\phi\ w\ \psi))$

Donc $T \subseteq sat(\phi\ w\ \psi)$

Exercice 4

I] Montrons que pour toute formules $\in CTL$ ϕ et S_1, S_2 tel que $S_1 \subseteq S_2$:

$$S_1 \models \phi \Rightarrow S_2 \models \phi$$

- $\phi = a$ ou $\phi = \neg a$

  $L_1(s) = L_2(s) \quad \forall s \in S_1$ car $S_1 \subseteq S_2$

  donc $S_1 \models \phi \Rightarrow S_2 \models \phi$ pour $\phi = a$ ou $\phi = \neg a$

  ↳ car $I_1 = I_2$ aussi !

- $\phi = \phi_1 \wedge \phi_2$

  $S_1 \models \phi_1 \wedge \phi_2 \Leftrightarrow$ pour tout chemin π commençant par un état initiaux $\pi \models \phi_1 \wedge \phi_2$

  $(I_1 = I_2)$

  $\Rightarrow S_1 \models \phi_1$ et $S_1 \models \phi_2$

  $\Rightarrow S_2 \models \phi_1$ et $S_2 \models \phi_2$

  $\Rightarrow S_2 \models \phi_1 \wedge \phi_2$ ✓

- $\phi = E\varphi$ $\quad (\varphi = X\phi \mid G\phi \mid \phi U \phi)$

  $S_1 \models E\varphi \Rightarrow$ il existe un chemin π tel que $\pi \models \varphi$

  Or ce chemin existe aussi dans S_2 donc $S_2 \models E\varphi$ ✓

Donc $S_1 \models \phi \Rightarrow S_2 \models \phi$

✓

2] Algorithme pas d'équivalence ECTL

$\varphi ::= X\phi \mid G\phi \mid \phi U \phi$

En effet le "pour tout" et le "ou" ne sont pas retranscrible en ECTL.

pas démontré