15/15

Introduction à la Vérification

DM

Exercice n°1 :

$$\Phi = \underbrace{AF(b \wedge \neg a)}_{\Phi_1} \rightarrow \underbrace{AFA(b \,W\, (\neg a \wedge \neg b))}_{\Phi_3 \;\; \Phi_2}$$

1. On pose
   1- $\Phi_1 = AF(b \wedge \neg a)$
   2- $\Phi_2 = A(b \,W\, (\neg a \wedge \neg b))$
   3- $\Phi_3 = AF\,\Phi_2$

Transformons en Forme Normale Existentielle

1- $\Phi_1 \equiv \neg E G \neg (b \wedge \neg a)$

$\equiv \neg E G (\neg b \vee a)$

2- $\Phi_2 \equiv \neg E ((b \wedge (a \vee b)) \cup (\neg b \wedge (a \vee b)))$

$\equiv \neg E (((b \wedge a) \vee b) \cup (\neg b \wedge a))$

3- $\Phi_3 \equiv \neg E G \neg \Phi_2$

De plus $\Phi = \Phi_1 \Rightarrow \Phi_3$

$\equiv \neg \Phi_1 \vee \Phi_3$

Donc

$$\Phi \equiv EG(\neg b \vee a) \vee \neg EG\, E((b \wedge a) \vee b)\, U\, (\neg b \wedge a))$$

$$\equiv \underbrace{EG(\neg b \vee a)}_{\Phi_1} \vee \neg EG \underbrace{E(b\, U\, (\neg b \wedge a))}_{\Phi_2}$$

Φ_3

2. On pose

- $\Phi_1 = EG(\neg b \vee a)$
- $\Phi_2 = E(b\, U\, (\neg b \wedge a))$
- $\Phi_3 = EG\, \Phi_2$

On cherche donc

$$Sat(\Phi) = Sat(\Phi_1 \vee \neg \Phi_3)$$

$$= Sat(\Phi_1) \cup S \setminus Sat(\Phi_3)$$

- Calculons $Sat(\Phi_1)$ (Algo de EG)

$T = \{ s_0\ s_1\ s_4\ s_5 \}$ $\quad V = \{ s_2\ s_3 \}$

$c_0 = 3\ \ c_1 = 2\ \ c_4 = 1\ \ c_5 = 2$

(avec c_i : compteur des successeurs de s_i)

① s_2 : $\quad V = \{ s_3 \}$

$c_1 = 1 \qquad c_5 = 1$

$c_0 = 2$

→ $T = \{ s_0\ s_1\ s_4\ s_5 \} \quad V = \{ s_3 \}$

② s_3 : $\quad V = \emptyset$

$c_0 = 1 \qquad c_4 = 0$

→ $T = \{ s_0\ s_1\ s_5 \} \quad V = \{ s_4 \}$

③ s_4 : $V = \emptyset$

$c_5 = 0$

→ $T = \{s_0\ s_1\}$ $V = \{s_5\}$ ✓

④ s_5 : $V = \emptyset$

→ $T = \{s_0, s_1\}$ $V = \emptyset$

$$Sat(\Phi_1) = \{s_0\ s_1\}$$ ✓

- Calculons $Sat(\Phi_2)$ (Algo de EU)

$T = \{s_5\}$

$V = \{s_5\}$

④ s_5 : $V = \emptyset$

$s_2 \models b$ et $s_2 \notin T$

→ $T = \{s_2\ s_5\}$ $V = \{s_2\}$

② s_2 : $V = \emptyset$

$s_0 \models b$ et $s_0 \notin T$

→ $T = \{s_0\ s_2\ s_5\}$ $V = \{s_0\}$

① s_0 : $V = \emptyset$

→ $T = \{s_0\ s_2\ s_5\}$ $V = \emptyset$

$$Sat(\Phi_2) = \{s_0\ s_2\ s_5\}$$ ✓

- Calculons $Sat(\Phi_3)$

$T = \{s_0\ s_2\ s_5\}$ $V = \{s_1\ s_3\ s_4\}$

$c_0 = 3$ $c_2 = 2$ $c_5 = 2$

① s_1 : $V = \{s_3\ s_4\}$

$c_0 = 2$

→ $T = \{s_0\ s_2\ s_5\}$ $V = \{s_3\ s_4\}$

② s_3 : $V = \{s_4\}$

$c_0 = 1$ $c_2 = 1$

→ $T = \{s_0\ s_2\ s_5\}$ $V = \{s_4\}$

③ s_4 : $V = \emptyset$

$c_5 = 1$

→ $T = \{s_0\ s_2\ s_5\}$ $V = \emptyset$

$$\boxed{Sat\ \Phi_3 = \{s_0\ s_2\ s_5\}}$$ ✓

Donc

$$Sat\ \phi = Sat(\Phi_1) \cup S \setminus Sat(\Phi_3)$$

$$= \{s_0\ s_1\} \cup \{s_1\ s_3\ s_4\}$$

$$\boxed{Sat\ \phi = \{s_0\ s_1\ s_3\ s_4\}}$$ ✓

Remarque :

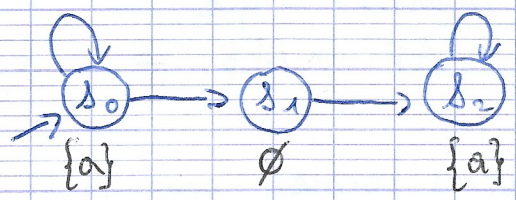
Le système de transition ne satisfait pas ϕ car car tous ses état initiaux ne sont pas dans $Sat(\phi)$.

$s_2 \notin Sat(\phi)$

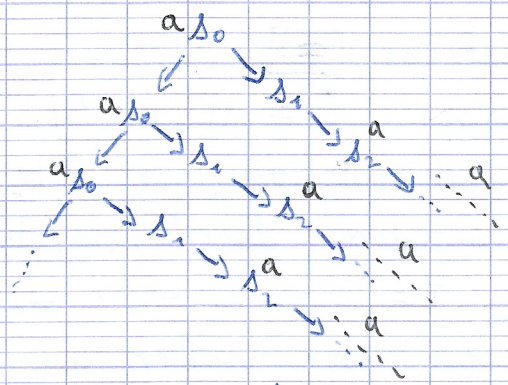
Exercice n°2

1. AFAX a / FX a

Soit le système de transition $\mathcal{S}$:



Arbre d'exécutions :



① On voit que $\mathcal{S}$ satisfait FX a car, pour chaque exécution, on remarque que l'on trouvera toujours un état dont le successeur satisfait a. $\mathcal{S} \models FX\,a$

② On remarque dans $\mathcal{S}$ que le sommet s_0 ne satisfait pas AX a, c'est-à-dire $s_0 \models \neg AX\,a$.

On remarque aussi dans l'arbre d'exécution, qu'il existe un chemin infini où l'on reste sur s_0. On peut donc écrire que $\mathcal{S} \models EG\,\neg AX\,a$

$\Leftrightarrow \mathcal{S} \models \neg AFAX\,a$

Donc

$$\mathcal{S} \not\models AFAX\,a$$ ✓

Conclusion

$$AFAX\,a \not\equiv FX\,a$$

2. $AF(a \wedge AFb)$ / $F(a \wedge Fb)$

Soit un Système de Transition noté $\mathcal{S}$.

On veut montrer que

$$AF(a \wedge AFb) \equiv F(a \wedge Fb)$$

En d'autres termes, pour tout système de transition $\mathcal{S}$, on a l'équivalence :

$$\mathcal{S} \models AF(a \wedge AFb) \iff \mathcal{S} \models F(a \wedge Fb)$$

- Montrons $\boxed{\Rightarrow}$

Supposons $\mathcal{S} \models AF(a \wedge AFb)$:

On veut montrer que $\mathcal{S} \models F(a \wedge Fb)$

On considère donc une exécution

$\pi := s_0 \to s_1 \to s_2 \to \dots$ de $\mathcal{S}$ avec $s_0 \in I$

On veut donc vérifier que :

$$\exists n, m \ ; \ m \geq n \text{ et } s_m \models a \text{ et } s_m \models b.$$

Donc que toute exécution est de la forme :

$$s_0 \to \dots \to s_n \to \dots \to s_m \to \dots$$
$$\models a \qquad \models b$$

$\mathcal{S} \models AF(a \wedge AFb)$

$\Rightarrow \forall \pi$ de $\mathcal{S}$, $\exists n \geq 0$; $s_n \models (a \wedge AFb)$

$\Rightarrow \forall \pi$ de $\mathcal{S}$, $\exists n \geq 0$; $s_n \models a \wedge s_n \models AFb$

Pour une exécution quelconque de $\mathcal{S}$:

$$s_0 \xrightarrow{*} s_n \to \dots$$

On prend $s_n \models AFb$

$\Rightarrow$ Pour toute exécution partant de s_n,

$\exists m \geq n$; $s_m \models b$

Et donc, pour toute exécution de S :

$$\exists n \geq m \; ; \; s_n \models a \wedge s_m \models b$$

Donc toutes ces exécutions sont de la forme :

$$s_0 \xrightarrow{*} s_n \; (\models a) \xrightarrow{*} s_m \; (\models b) \longrightarrow \ldots$$

Ce qui est bien ce que l'on voulait vérifier.

$$\boxed{S \models AF(a \wedge AFb) \Rightarrow S \models F(a \wedge Fb)}$$

- Montrons $\boxed{\Leftarrow}$

Supposons $S \models F(a \wedge Fb)$ (1)

Ça veut dire que pour toute exécution depuis un état initial s_0, on arrive à un état où a est vrai et où, depuis cet état, on arrive un jour à un état où b est vrai

Toute exécution de ce système peut donc se représenter comme ci-dessous :

$$\exists m \geq n \; ; \; s_0 \; (\in I) \longrightarrow \ldots \longrightarrow s_n \; (\models a) \longrightarrow \ldots \longrightarrow s_m \; (\models b) \longrightarrow \ldots$$

Supposons maintenant

$$S \not\models AF(a \wedge AFb)$$
$$\Leftrightarrow S \models \neg AF(a \wedge AFb)$$
$$\Leftrightarrow S \models EG(\neg a \vee EG\neg b) \quad (2)$$

L'hypothèse (2) nous dit qu'il existe une exécution où :

① On ne trouve JAMAIS "a est vrai".

OU

② À partir d'un certain état s_n qui satisfait a, il existe une exécution où on ne trouve JAMAIS "b est vrai"

$\exists n$?

Or, d'après (1)

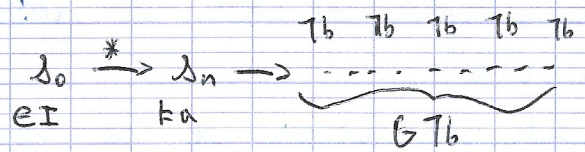
① Impossible car par définition, pour toute exécution de S' : $\exists n$; $s_n \models (a \wedge Fb)$

$\Leftrightarrow \exists n$; $s_n \models a$ et $s_n \models Fb$.

En particulier on aura toujours, pour chaque exécution, un état où a est vrai.

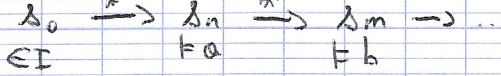
② Soit $s_n \models a$ avec $n \geq 0$, lorsque il existe une exécution depuis cet état où l'on ne trouve JAMAIS "b est vrai".

Cela veut dire qu'il existe une exécution de la forme :



Ça marche seulement si n est la première position qui sat. a

Or d'après (1) toute exécution sans exception doit être de la forme



(V)

Donc ② est absurde.

En conclusion $S' \not\models EG(\neg a \vee EG \neg b)$

$\Leftrightarrow S' \not\models \neg AF(a \wedge AFb)$

$\Leftrightarrow S' \models AF(a \wedge AFb)$

On a bien

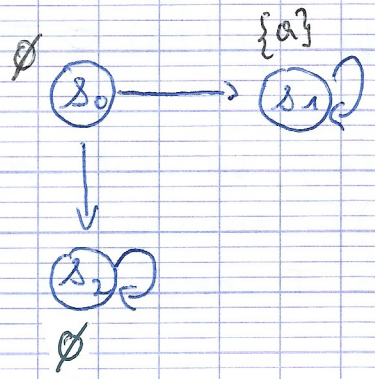
$$\boxed{S \models F(a \wedge Fb) \Rightarrow S' \models AF(a \wedge AFb)}$$ ✓

Au final :

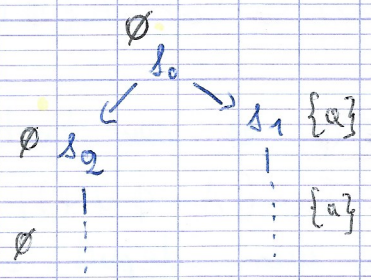
$$F(a \wedge Fb) \equiv AF(a \wedge AFb)$$

3. $EGAXa \;/\; GXa$

Soit le système de transition S :



Arbre d'exécutions :



On remarque bien que :

$$S \models \neg EGAXa$$

par l'exécution $s_0 \to s_1 \to s_1 \to \dots$

Mais on a aussi

$$S \not\models GXa$$

car on peut avoir une exécution où a n'est jamais satisfait. ✓

Exercice n° 3 :

1. $Sat(A(\phi \cup \psi))$ est le plus petit ensemble $T \subseteq S$ tel que :
   (1) $Sat(\psi) \subseteq T$
   (2) $\{s \in Sat(\phi) ; post(s) \subseteq T\} \subseteq T$

Pour montrer cela, on doit montrer que
(i) $Sat(A(\phi \cup \psi))$ satisfait (1) et (2)
(ii) Tout ensemble T satisfaisant (1) et (2) contient $Sat(A(\phi \cup \psi))$.

(i) (1) Par définition de $Sat(A(\phi \cup \psi))$:
$$Sat(\psi) \subseteq Sat(A(\phi \cup \psi))$$
$s \not\models \psi \Rightarrow$

(2) Si ($s \models \phi$ et) pour tout s' successeur de s on a $s' \in Sat(A(\phi \cup \psi))$

Toute exécution depuis s sera de la forme

$$s \to s' \to s_0 \to s_1 \to \cdots \to s_n$$
$\models \phi \quad \models \phi \quad \models \phi \quad \models \phi \qquad \models \psi$

Donc $s \in Sat(A(\phi \cup \psi))$

(ii) Soit T un ensemble satisfaisant (1) et (2)
On veut montrer que $Sat(A(\phi \cup \psi)) \subseteq T$.
Soit $s \models A(\phi \cup \psi)$
On a donc
- $s \models \psi$, dans ce cas on a aussi $s \in T$ d'après (1)

OU
- Pour tout états successeurs s' de s, on a $s' \models A(\phi \cup \psi)$ et $s \models \phi$.

pas tout à fait, il faudrait avoir $post(s_{n-1}) \subseteq T$ pour ça.

Prenons l'exécution

$$s = s_0 \to s' = s_1 \to s_2 \to s_3 \to \dots \to s_n \to \dots$$
$$\models \phi \quad \models \phi \quad \models \phi \quad \models \phi \quad \models \psi$$

tel que $s \models A(\phi \cup \psi)$

On voit que si $s_{n-1} \models \phi$ alors, puisque $s_n \in T$, $s_{n-1} \in T$ d'après (2).

Et donc, supposons qu'en remontant jusqu'à un certain s_i avec $1 \leq i \leq n-1$, on ait $s_i \in T$

Montrons que $s_{i-1} \in T$:

En effet $s_{i-1} \models A(\phi \cup \psi)$. Prenons le cas où $s_{i-1} \models \phi$.

Comme $s_i \in T$ et $s_{i-1} \models \phi$ alors d'après (2).

$$s_{i-1} \in T$$

(+)

Par ce raisonnement par induction, on montre en particulier que $s \in T$ (✓)

Donc en conclusion.

$$Sat(A(\phi \cup \psi)) \subseteq T.$$

2. $Sat(AG\phi)$ est le <u>plus grand ensemble</u> $T \subseteq S$ tel que

(1) $T \subseteq Sat(\phi)$

(2) $T \subseteq \{ s \in Sat(\phi) : Post(s) \subseteq T \}$

Pour montrer cela, on doit montrer que :

(i) $Sat(AG\phi)$ satisfait (1) et (2)

(ii) Tout ensemble T satisfaisant (1) et (2) <u>est contenu</u> dans $Sat(AG\phi)$.

(i) (1) Par définition :

$$s \models AG\phi \Rightarrow s \models \phi$$

Donc $Sat(AG\phi) \subseteq Sat(\phi)$

(2) Prenons $s \models AG\phi$

Cela veut dire que pour toute execution partant de s, ϕ est TOUJOURS vrai.

Donc $s \models \phi$ et $Post(s) \subseteq Sat(AG\phi)$

Donc $s \in \{ s \in Sat(AG\phi) : Post(s) \subseteq Sat(AG\phi) \}$

Ainsi

$$Sat(AG\phi) \subseteq \{ s \in Sat(\phi) : Post(s) \subseteq Sat(AG\phi) \}.$$ ✓

(ii) Soit T un ensemble satisfaisant (1) et (2).

Montrons que $T \subseteq Sat(AG\phi)$

Prenons $s \in T$

$\Rightarrow s \models \phi$ et $\forall s' \in Post(s)$, $s' \in T$ d'après (1) et (2)

$\Rightarrow s' \models \phi \wedge Post(s') \subseteq T$.

Maintenant, raisonnant par récurrence.

Prenons une exécution

$$s_0 \to s_1 \to s_2 \to \cdots \to s_n \to \cdots$$

tel que $s = s_0$ et $s' = s_1$.

On sait maintenant que

$$s_0 \in T \Rightarrow s_0 \models \phi \wedge s_1 \in T$$

Montrons que pour toute exécution à partir de s_n,

$$s_n \in T \Rightarrow s_{n+1} \models \phi \wedge s_{n+1} \in T \quad \forall n \geq 0$$ ✓

Donc, soit $s_n \in T$

$\Rightarrow s_n \in Sat(\phi)$ d'après (1)

$\Rightarrow s_{n+1} \in T$ d'après (2)
$\Rightarrow s_{n+1} \models \phi$ d'après (1)
$\Rightarrow s_{n+2} \in T$ d'après (2)

On a donc montré que pour toutes exécutions à partir de s_n, tous les états atteint satisfont ϕ si $s_n \in T$. ✓

En particulier, si $s_0 \in T$, alors tout états accessibles depuis ce dernier satisfont ϕ

Donc $s_0 = s \in T \Rightarrow s \in Sat(AG\phi)$ ✓

Donc $T \subseteq Sat(AG\phi)$. ✓

3. $Sat(A(\phi W \psi))$ est le plus grand ensemble $T \subseteq S$ tel que
(~~(1) $T \subseteq Sat(\psi) \cup Sat(\phi)$~~) n'était pas demandé
(2) $T \subseteq Sat(\psi) \cup \{s \in Sat(\phi) : post(s) \subseteq T\}$

Pour montrer cela, on doit montrer que :
(i) $Sat(A(\phi W \psi))$ satisfait (1) et (2)
(ii) Pour tout T satisfaisant (1) et (2), $Sat(A(\phi W \psi))$ contient cet ensemble.

(i) (1) Par définition de $A(\phi W \psi)$
$Sat(\psi) \subseteq Sat(A(\phi W \psi))$
et $Sat(A(\phi U \psi)) \subseteq Sat(\phi)$ → non, on peut avoir $s \models \psi$, mais $s \not\models \phi$

On peut donc écrire $Sat(A(\phi U \psi)) \subseteq Sat(\psi) \cup Sat(\phi)$ (✓)

(2) Soit $s \in Sat(A(\phi \, W \, \psi))$

Ce qui veut dire

- Toute exécution issue de s doit satisfaire
  $G\phi$
  ou $\phi \, U \, \psi$

mais aussi :

- Toute exécution issue d'un successeur s' de s doit satisfaire
  $G\phi$
  ou $\phi U \psi$

Dans le cas où ~~$s \models \phi$~~ $s \not\models \psi$

(cas où $s \models \psi$ a été traité dans (1))

Or, si on est dans ce cas de figure, on $s \models \phi \wedge \neg\psi$

a

$$\forall s' \in Post(s), \quad \cancel{s' \models A(G\phi \vee (\phi U \psi))}$$
$$\Rightarrow s' \models A(\phi \, W \, \psi)$$
$$\Rightarrow s' \in Sat(A(\phi \, W \, \psi)) \quad \checkmark$$

Et donc

$$s \in \{ s \in Sat(\phi) : Post(s) \subseteq Sat(A(\phi W \psi)) \}$$

$$\cancel{\Rightarrow Sat(A(\phi W \psi)) \subseteq \{ s \in Sat(\phi) : Post(s) \subseteq Sat(A(\phi W \psi)) \}}$$

Or d'après (1) on sait que

$$Sat(\psi) \subseteq Sat(\phi W \psi)$$

On peut donc écrire :

$$Sat(A(\phi W \psi)) \subseteq Sat(\psi) \cup \{ s \in Sat(\phi) : Post(s) \subseteq Sat(A(\phi W \psi)) \} \quad \checkmark$$

(ii) Soit T satisfaisant (1) et (2)

Montrons que $T \subseteq Sat(\phi \mathcal{W} \psi)$

Soit $s \in T$; alors on a deux cas possible :

- $s \in Sat(\psi)$

Dans ce cas on a bien par définition

$s \in Sat(\phi \mathcal{W} \psi)$ (A)

- $s \in \{ s \in Sat(\phi) \ ; \ post(s) \subseteq T \} = T'$

Ce qui veut dire que

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

On prend donc une exécution

$\pi : s \to s' \to s_1 \to s_2 \to \cdots$

On peut montrer par récurrence que $\forall s_i \in T'$ (réc. ✓)

$\forall i \in [\![0, +\infty]\!], \ s_i \in T' \Rightarrow s_i \models \phi \wedge (s_{i+1} \models \phi \vee s_{i+1} \models \psi)$

Il faut montrer par réc. que $\pi \models \phi \mathcal{W} \psi$

On a vu que

$s_0 = s \in T' \Rightarrow s_0 \models \phi \wedge (s_{i+1} \in T)$

$\Rightarrow s_0 \models \phi \wedge (s_{i+1} \models \phi \vee s_{i+1} \models \psi)$

car $s_{i+1} \in Post(s)$ et $Post(s) \subseteq T'$

Donc supposons que cette propriété soit vraie jusqu'à i ; Montrons qu'elle est vraie pour $i+1$.

On a donc

$s_i \in T' \Rightarrow s_i \models \phi \wedge (s_{i+1} \models \phi \vee s_{i+1} \models \psi)$

Prenons le cas où

$s_{i+1} \models \phi$.

Et comme $s_i \in T'$ alors $s_{i+1} \in T$. Et dans notre cas, $s_{i+1} \models \phi$ donc $s_{i+1} \in T$. pas clair pourquoi,

(N) il manque $post(s_{i+1}) \in T$

15/21

Ce qui nous donne

$$s_{i+1} \in T' \Rightarrow s_{i+1} \models \phi \wedge s_{i+2} \in T$$

$$\Rightarrow s_{i+1} \models \phi \wedge (s_{i+2} \models \phi \vee s_{i+2} \models \psi)$$

On vient donc de montrer que pour toute execution partant de l'état $s_0 \in T'$, on a :

- ϕ est TOUJOURS vrai $(G\phi)$

OU

- ϕ est toujours vrai jusqu'à ce qu'on atteigne un état où ψ est vrai. $(\phi \, U \, \psi)$

Remarque :

En effet, dans la preuve, si $s_{i+1} \models \psi$, alors on a pas l'obligation $Post(s_{i+1}) \subseteq T$. Donc s_{i+2} peut très bien satisfaire $\neg\phi$ et $\neg\psi$.

Donc en conclusion

$$s_0 = s \in T' \Rightarrow s \in Sat(A(G\phi \vee (\phi U \psi)))$$
$$\Rightarrow s \in Sat(A(\phi W \psi))$$

Donc en conclusion on a.

$$s \in Sat(\psi) \cup T' \Rightarrow s \in Sat(A(\phi W \psi))$$

Donc

$$\boxed{Sat(\psi) \cup T' \subseteq Sat(A(\phi W \psi))}$$

Exercice n°4 :

ECTL :

$$\phi := a \mid \neg a \mid \phi \wedge \phi \mid E\varphi$$

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

1. • $\phi = a$

Si $S_1 \subseteq S_2$

alors $S_1 \models a \Rightarrow \forall s \in I_1, s \models a$.

$\Rightarrow \forall s \in I_2, s \models a$ car $I_1 = I_2$ et $\forall s \in S_1, \lambda_1(s) = \lambda_2(s)$

$\Rightarrow S_2 \models a$ ✓

• $\phi = \neg a$

Si $S_1 \subseteq S_2$

alors $S_1 \models \neg a \Rightarrow \forall s \in I_1, s \models \neg a$

$\Rightarrow \forall s \in I_2, s \models \neg a$ car $I_1 = I_2$ et $\forall s \in S_1, \lambda_1(s) = \lambda_2(s)$

$\Rightarrow S_2 \models \neg a$ ✓

• $\phi = \phi_1 \wedge \phi_2$

Si $S_1 \subseteq S_2$

alors $S_1 \models \phi_1 \wedge \phi_2 \Rightarrow S_1 \models \phi_1 \wedge S_2 \models \phi_2$

$\Rightarrow S_2 \models \phi_1 \wedge S_2 \models \phi_2$ d'après les deux premiers points

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

• $\phi = EX\phi_1$

Si $S_1 \subseteq S_2$

alors comme $\rightarrow_1 \subseteq \rightarrow_2$, $I_1 = I_2$ et $\forall s \in S_1, \lambda_1(s) = \lambda_2(s)$

$S_1 \models EX\phi_1 \Rightarrow S_2 \models EX\phi_2$

En d'autres termes :

$S_1 \models EX\phi_1 \Rightarrow \exists s_0 \rightarrow s_1 \rightarrow \dots ; s_1 \models \phi_1$ avec $s_0 \in I_1$ ✓

Or $\rightarrow_1 \subseteq \rightarrow_2$ et $S_1 \subseteq S_2$

Donc cette execution $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \dots$ est aussi dans S_2

Et comme $I_1 = I_2$ et $\mathcal{L}_1(s) = \mathcal{L}_2(s)$ $\forall s \in S_1$, on a bien $s_0 \in I_2$ et $s_1 \not\models \phi_1$

Donc

$S_2 \not\models EX\phi_1$

- $\phi = EG\phi_1$

Soit $S_1 \models EG\phi_1$ avec $S_1 \subseteq S_2$

Donc il existe une execution depuis $s_0 \in I_1$ tel que ϕ_1 est toujours satisfait.

On représente cette execution par

$\pi := s_0 \rightarrow s_1 \rightarrow s_2 \dots$

avec $\forall i \geq 0$, $s_i \models \phi_1$.

Comme $I_1 \supseteq I_2$ et $\forall s \in S_1$, $\mathcal{L}_1(s) = \mathcal{L}_2(s)$, on a

$s_0 \in I_2$ et $\forall i \geq 0$, $\mathcal{L}_2(s_i) \doteq \phi_1$

Comme $\rightarrow_1 \subseteq \rightarrow_2$ et $S_1 \subseteq S_2$, l'execution π existe aussi dans S_2 avec le même étiquetage que dans S_1 ✓

Donc $S_2 \models EG\phi_1$

Ainsi

$S_1 \models EG\phi_1 \Rightarrow S_2 \models EG\phi_1$

- $\$ = E(\phi_1 \cup \phi_2)$

Soit $S_1 \models E(\phi_1 \cup \phi_2)$ et $S_1 \subseteq S_2$

Il existe donc une execution π de la forme

$$\underset{\phi_1}{s_0} \rightarrow \underset{\phi_1}{s_1} \rightarrow \underset{\phi_1}{s_2} \rightarrow \dots \rightarrow \underset{\phi_2}{s_n} \rightarrow \underset{\emptyset}{s_{n+1}} \rightarrow \dots$$

avec $s_0 \in I_1$

Or

→ $I_1 = I_2$

donc $s_0 \in I_2$

→ $\forall s \in S_1$, $\mathcal{L}_1(s) = \mathcal{L}_2(s)$

donc $\mathcal{L}_2(s) = \phi_1$

→ $\rightarrow_1 \subseteq \rightarrow_2$ et $S_1 \subseteq S_2$

donc π existe aussi dans S_2 avec le même étiquetage que dans S_1.

✓

Donc

$$S_1 \models E(\phi_1 \cup \phi_2) \Rightarrow S_2 \models E(\phi_1 \cup \phi_2)$$

2. Si on prend les formule CTL du type

$$\phi_{CTL} = \phi_1 \vee \phi_2$$

Donc $Sat(\phi_1 \vee \phi_2) = Sat(\phi_1) \cup Sat(\phi_2)$

Prenons maintenant

$$S_1 \models \phi_1 \qquad S_2 \models \phi_2 \qquad S \models \phi_1 \wedge \phi_2$$

On a donc

$S_1 \in Sat(\phi_1 \vee \phi_2)$

et $S_2 \in Sat(\phi_1 \vee \phi_2)$

et $S_3 \in Sat(\phi_1 \vee \phi_2)$

Donc, si Il existe une formule ϕ_{ECTL} tel que

$$\phi_{ECTL} \equiv \phi_{CTL}$$

alors

$S_1 \in Sat(\phi_{ECTL})$ et $S_2 \in Sat(\phi_{ECTL})$ et $S_3 \in Sat(\phi_{ECTL})$

Faisons au cas par cas pour trouver une formule ϕ_{ECTL} correspondant à ces propriétés

Désolé, mais le raisonnement pour la partie 2. n'est vraiment pas convaincant. 19/21

Si $\phi_1 = \phi_2 =$ true, ça donne quoi?

- $\phi_{ECTL} = \phi_1$

On a $S_2 \not\models \phi_1$ donc $S_2 \notin Sat(\phi_{ECTL})$

donc $\phi_{ECTL} \neq \phi_1$

- $\phi_{ECTL} = \phi_2$

De même que précédement avec S_1 donc

$\phi_{ECTL} \neq \phi_2$

- $\phi_{ECTL} = \phi_1 \wedge \phi_2$

On a $S_1 \not\models \phi_1 \wedge \phi_2$ donc $S \notin Sat(\phi_{ECTL})$

$\phi \neq \phi_1 \wedge \phi_2$

- $\phi_{ECTL} = E G \phi_1$

$S_2 \not\models \phi_1$ donc $S_2 \notin Sat(\phi_{ECTL})$

$\phi_{ECTL} \neq E G \phi_1$

- $\phi_{ECTL} = \tilde{E} G \phi_2$

Même argument que précédement mais avec S_1.

Donc $\phi_{ECTL} \neq \tilde{E} G \phi_2$

Prenons maintenant pour tout $i \in [\![1, 2]\!]$,

$S_i \models AX(\neg\phi_1 \wedge \neg\phi_2) \wedge \phi_i$

On a toujours

$S_i \in Sat(\phi_{ETL})$

Or

- $\phi_{ECTL} = \tilde{E} X \phi_1$

Pour tout $i \in [\![1, 2]\!]$, $S_i \not\models \tilde{E} X \phi_1$

- De même pour $\phi_{ECTL} = \tilde{E} X \phi_2$

Donc $\phi_{ECTL} \neq \tilde{E} X \phi_i$

- $\phi_{ECTL} = \tilde{E} G \phi_1$

Pour tout $i \in [\![1, 2]\!]$, $S_i \not\models \tilde{E} G \phi_1$

- De même pour $\phi_{ECTL} = E G \phi_2$

Donc $\phi_{ECTL} \neq E G \phi_i$

Et donc on ne trouve à ϕ_{CTL} aucune formule ECTL équivalente.