

DM Introduction à la vérification

Ex 1

$$1) \phi = \underbrace{AF(b \wedge \neg a)}_{\phi_1} \rightarrow \underbrace{AFA(b \wedge (\neg a \wedge \neg b))}_{\phi_2}$$

Pour $\phi_1 = AF(b \wedge \neg a)$, on sait que $AF\psi = \neg EG \neg \psi$
 donc $\phi_1 = \neg EG \neg (b \wedge \neg a)$

Pour $\phi_2 = \underbrace{AFA(b \wedge (\neg a \wedge \neg b))}_{\phi_3}$

$$\text{on a } \phi_2 = AF \phi_3 = \neg EG \neg \phi_3$$

$$\begin{aligned} \phi_3 &= A(b \wedge (\neg a \wedge \neg b)) \\ &= \neg E((b \wedge \neg(\neg a \wedge \neg b)) \vee (\neg b \wedge \neg(\neg a \wedge \neg b))) \\ &= \neg E((b \wedge (a \vee b)) \vee (\neg b \wedge (a \vee b))) \end{aligned}$$

ici on a b et a ou b
 négatif a b alors on garde
 b

ici cela ne peut pas être b et ¬b
 donc on garde a

$$\phi_3 = \neg E(b \vee (\neg b \wedge a))$$

$$\phi_2 = \neg EG \neg (\neg E(b \vee (\neg b \wedge a)) = \neg EG E(b \vee (\neg b \wedge a))$$

On a donc $\phi_1 \rightarrow \phi_2$. Or on sait que $\phi_1 \rightarrow \phi_2 = \neg \phi_1 \vee \phi_2$

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

Ainsi $\phi = \neg(\neg EG \neg (b \wedge \neg a) \wedge EG E(b \vee (\neg b \wedge a)))$ ✓

$$2) \phi = \underbrace{\neg(\neg EG \neg(b \wedge \neg a))}_{(3)} \wedge \underbrace{EG E(b \vee (\neg b \wedge a))}_{(2)} \quad (1)$$

① On va d'abord utiliser l'algorithme du plus petit point fixe pour avoir $\text{sat}(\phi)$. ✓

~~Soit~~ soit $E(b \vee (\neg b \wedge a)) = \psi_1$

$\text{sat}(\neg b \wedge a) = S_5 = T_0$

$T_1 = T_0 \cup S_2$ car S_2 satisfait b

On a donc $T_1 = \{S_5, S_2\}$

$T_2 = T_1 \cup S_0$ car S_0 est prédécesseur de S_2 et satisfait b .

$T_3 = T_2 = \{S_5, S_2, S_0\}$ car S_0 n'a pas de pred. qui satisfait b .

② $EG(\psi_1)$. On va utiliser l'algo du point fixe. ✓

$T_0 = \text{sat}(\psi_1) = \{S_5, S_2, S_0\}$

S_0	S_1
S_2	S_3
S_5	S_4
T	V

$C_{S_0} = 3$

$C_{S_2} = 2$

$C_{S_5} = 2$

$V := V \setminus \{S_1\}$

$V := V \setminus \{S_3\}$

$V := V \setminus \{S_4\}$

$C_{S_0} \leftarrow 2$ car S_0 est pred de S_2

$C_{S_2} \leftarrow 1$ et $C_{S_0} \leftarrow 1$

$C_{S_5} \leftarrow 1$

$$V := V \setminus \{S_4\}$$

$$C_{S_2} = 1 \text{ et } C_{S_0} = 1 \text{ donc } C_{S_5} = 1$$

$\hookrightarrow$ Aucun ~~compteur~~ compteur = 0 donc l'algo est fini car V est vide
donc $\text{Sat}(EG(\varphi_1)) = \{S_0, S_2, S_5\}$ ✓

③ $EG \neg(b \wedge a)$. On prend $\neg(b \wedge a) = \varphi_2$ puis on fait tourner l'algorithme avec $EG(\varphi_2)$

$$T_0 := \text{Sat}(\varphi_2) = \{S_0, S_1, S_4, S_5\}$$

S_0	S_2
S_1	S_3
S_4	S_4
S_5	S_5
T	V

$$\begin{aligned} C_{S_0} &= \cancel{2} \\ C_{S_1} &= \cancel{1} \\ C_{S_4} &= \cancel{0} \\ C_{S_5} &= \cancel{0} \end{aligned}$$

$$\begin{aligned} V &:= V \setminus \{S_2\} \\ V &:= V \setminus \{S_3\} \end{aligned}$$

$$\begin{aligned} C_{S_2} &= 1 \text{ et } C_{S_5} = 1 \text{ donc } C_{S_1} = 1 \text{ et } C_{S_5} = 1 \\ C_{S_4} &= 0 \text{ et } C_{S_0} = \cancel{1} \end{aligned}$$

$C_{S_4} = 0$ donc on passe S_4 dans V
 $T := T \setminus \{S_4\}$ et $V := V \cup \{S_4\}$

$$\begin{aligned} V &:= V \setminus \{S_4\} \\ T &:= T \setminus \{S_5\} \text{ et } V := V \cup \{S_5\} \text{ car } C_{S_5} = 0 \end{aligned}$$

$$V := V \setminus \{S_5\} \text{ (ne change rien)}$$

V est vide donc l'algo est terminé. On a donc $\text{Sat}(EG \neg(b \wedge a)) = \{S_0, S_2\}$ ✓

De on veut $\neg(EG \rightarrow (b \wedge \neg a))$

$$\text{Sol: } \neg(EG \rightarrow (b \wedge \neg a)) = \text{l'ensemble des états de ST} \setminus \text{Sol}(EG \rightarrow (b \wedge \neg a))$$

$$= \{S_0, S_1, S_2, S_3, S_4, S_5\} \setminus \{S_0, S_4\}$$

$$= \{S_2, S_3, S_4, S_5\}$$

On fait ensuite l'intersection avec (2)

$$\text{Sol: } (3) \cap (2) = \{S_2, S_3, S_4, S_5\} \cap \{S_0, S_2, S_5\}$$

$$= \{S_2, S_5\}$$

Et pour finir, $\text{Sol}(\phi) = \text{l'ensemble des états de ST} \setminus \{S_2, S_5\}$
 car ϕ est la négation de cette intersection.

On a donc $\text{Sol}(\phi) = \{S_0, S_1, S_3, S_4\}$. ✓

Ex 2

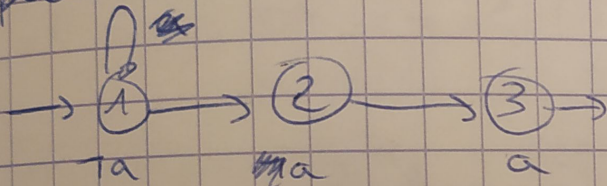
1) AFAX a $\neq$ FX a

cela utilise le système de transition

Ex 2

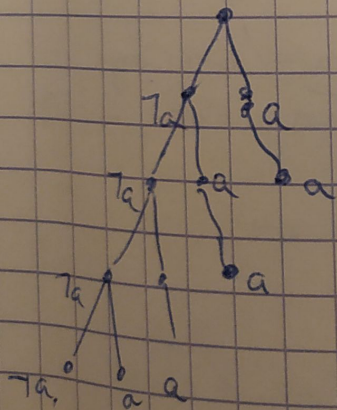
1) $AFAXa \neq FXa$

On peut notamment pour prouver cela utiliser le système de transition simple :



non, car $11 \dots = 1^{\omega}$
ne satisfait jamais a

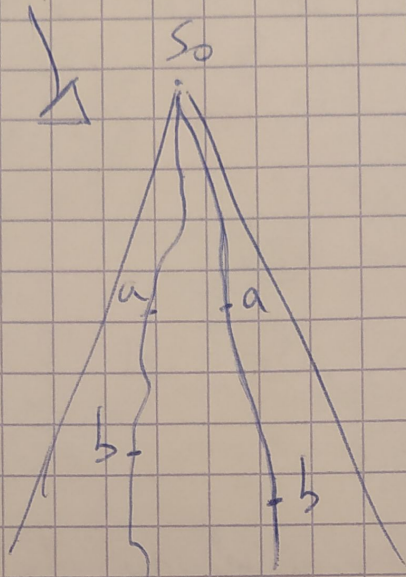
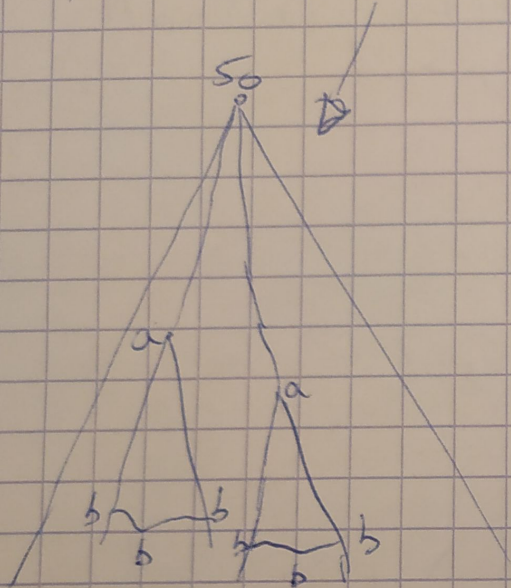
Le dernier satisfait FXa . En effet, Par contre, en prenant l'arbre représentant le système de transition on a :



=) On voit bien que le chemin tout à gauche ne satisfait pas ~~AF~~ car c'est une boucle sur a jamais AXa , car $11^{\omega} a$

Donc ce système ~~ne~~ satisfait FXa mais pas $AFAXa$.

$$2) AF(a \wedge AFb) = F(a \wedge Fb)$$



⊛ Vous avez juste expliqué ce que signifie que un chemin π sat. $F(a \wedge Fb)$, ce ne dit rien sur $AF(a \wedge AFb)$

Soit ST , un système de transition

Pour toute exécution on a $S_0 \rightarrow S_1 \rightarrow S_2 \dots$ Satisfait Fa

Donc $S_0 \rightarrow S_1 \rightarrow S_2 \dots \exists n$ tel que $0 \leq n$ et $S_n \neq a$

De plus avec l'intersection on a aussi $\forall$ exécution à partir de S_n sat. Fb

Ainsi $S_n \rightarrow S_{n+1} \rightarrow S_{n+2} \dots \exists m$ tel que $n \geq m$ et $S_m \neq b$

Au final on se retrouve avec

$\pi: S_0 \rightarrow S_1 \rightarrow S_2 \dots \rightarrow S_n \rightarrow S_{n+1} \dots S_m$

$\exists n, m, 0 \leq n \leq m$ et $S_n \neq a$ tout comme $S_m \neq b$

π satisfait donc $F(a \wedge Fb)$

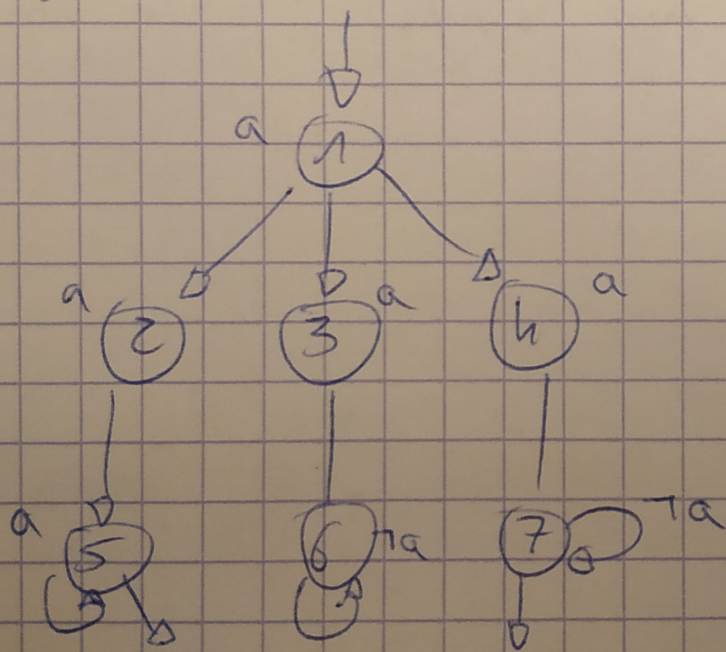
Donc la formule CTL et LTL sont donc équivalentes

⊛

3) $EGAXa \neq GXa$

En effet, la formule CTL indique qu'il existe un chemin/exécution tel que chaque successeur de chaque état composant l'exécution satisfait a .

Dans ce système de transition, on peut trouver un chemin qui satisfait cette formule CTL : $(1 \rightarrow 2 \rightarrow 5)$



$\Rightarrow$ chaque successeur de l'état 1 satisfait a , chaque succ. de l'état 2, $sat. a$ et chaque succ. de l'état 5 $sat. a$

$\uparrow$ il faut écrire :

$136^w \neq GXa$

$147^w \neq GXa$

Cependant, ce ST ne satisfait pas la formule LTL donc les deux formules ne sont pas équivalentes. Les états 3 et 4 ne $\neq GXa$

Dans LTL les états ne satisfont pas, c'est les chemins

E 3

1. Soit $T_0 = \text{sat}(\phi \cup \psi)$
 on cherche d'abord à montrer que T_0 satisfait la propriété suivante:
 $\{s \in \text{sat}(\phi) : \text{post}(s) \subseteq T_0\} \subseteq T_0$ avec $\text{sat}(\psi) \subseteq T_0$.

on sait que $A(\phi \cup \psi) = \frac{\psi}{(1)} \vee \frac{(\phi \wedge AX A(\phi \cup \psi))}{(2)}$ (cases)

① ~~pour~~ ~~sat~~ ~~(\phi)~~ on est sûr que $\text{sat}(\psi) \subseteq T_0$ grâce à ce qu'on a dit plus haut

② À l'inverse, un état $\text{sat}(A(\phi \cup \psi))$ s'il satisfait ϕ dans un premier temps tout en ayant ses successeurs — qui $\text{sat}(\psi)$ ①
 ou qui $\text{sat}(\phi)$ jusqu'à arriver à un état satisfaisant ψ (où l'appel récursif $A(\phi \cup \psi)$ pour arriver à un état déjà dans T_0).

① correspond donc à $\text{sat}(\psi) \subseteq T_0$ et ② correspond à la propriété voulue. On a bien T_0 satisfait $\{s \in \text{sat}(\phi) : \text{post}(s) \subseteq T_0\} \subseteq T_0$ avec $\text{sat}(\psi) \subseteq T_0$.

• Soit T , le plus petit ensemble, avec $\text{sat}(\psi) \subseteq T$ et satisfaisant $\{s \in \text{sat}(\phi) : \text{post}(s) \subseteq T\} \subseteq T$

Tous les états de T_0 qui ~~satis~~ $\text{sat}(\psi) \subseteq T$ car $\text{sat}(\psi) \subseteq T$
 Pour les autres états de T_0 , qui ne satisfont pas directement ψ on a :

$s \in A(\phi \cup \psi)$ car $s \in T_0$
 mais $s \notin \psi$
 alors $s \in \phi \wedge \text{post}(s) \subseteq \text{sat}(A(\phi \cup \psi)) = T_0$
 $L_s = AX A(\phi \cup \psi)$

Donc on retrouve $(\phi \wedge AX A(\phi \cup \psi))$ satisfait $\exists \text{ sat}(T)$ et

Donc T , le plus petit ensemble

Assi $\phi \wedge AX A(\phi \cup \psi)$ pourquoi? $\text{sat}(\psi) \cup \text{sat}(\phi \wedge AX A(\phi \cup \psi)) = \text{sat}(A(\phi \cup \psi))$

et est donc le plus petit ensemble.

L'argument pour $T_0 \subseteq T$ n'est pas très clair

2). Soit $T_0 = \text{Sat}(AG\phi)$

On va prouver que T_0 satisfait la propriété suivante:
 $T_0 \subseteq \{s \in \text{Sat}(\phi) : \text{post}(s) \subseteq T_0\}$

Pour qu'un état $s \models AG\phi$, il faut:

- ① ~~soit~~ ~~soit~~ $s \models \phi$
- ② ~~soit~~ ~~soit~~ ~~soit~~ états s' , accessible à partir de s , $s' \models \phi \wedge AG\phi$

C'est exactement ce que signifie la propriété, avec
 $s \in \text{Sat}(\phi) \Rightarrow$ ① et $\text{post}(s) \subseteq T_0 \Rightarrow$ ②

Or comme dit plus haut, on a $T_0 = \text{Sat}(AG\phi)$ donc T_0 vérifie bien la propriété ~~car l'ensemble contient bien~~

• Soit T , le plus grand ensemble d'états, satisfaisant
 $T \subseteq \{s' \in \text{Sat}(\phi) : \text{post}(s') \subseteq T\}$

On sait que $AG(\phi) = \phi \wedge AXAG\phi$
 $T \subseteq T_0$

Donc pour avoir $\text{Sat}(AG\phi)$ on va d'abord prendre tous les sommets $s \models \text{Sat}(\phi)$ puis on va vérifier que chaque successeur ~~de~~ ~~est~~ satisfait $(AG\phi)$ (va vérifier ϕ + tous les successeurs $\dots \Rightarrow$ appel récursif)

Or, c'est exactement ce que fait la propriété $\{s \in \text{Sat}(\phi) : \text{post}(s) \subseteq T\}$

~~Donc sachant que~~ ~~$\text{Sat}(AG\phi)$ est l'ensemble~~ ~~T , et que~~ $(\checkmark)$
En sachant que $T_0 = \text{Sat}(AG\phi)$, vérifie également la propriété,
on a donc $T \subseteq T_0$ avec T plus grand ensemble.

3) On sait que $\varphi \sqcup \varphi' = \varphi \cup \varphi' \vee G\varphi$
 Par conséquent $A(\phi \sqcup \psi) = A(\phi \cup \psi \vee G\phi)$
 Soit $T_0 = \text{sat}(A(\phi \cup \psi \vee G\phi))$

$$A(\phi \sqcup \psi)$$

$$\equiv A(\phi \cup \psi) \cup AG\phi$$

Les états satisfaisant $A(\phi \cup \psi \vee G\phi)$ sont donc soit :

- les états dont tous les descendants sont successeurs de ϕ et qui sat ϕ ex-nèces les états ns à la question 2 avec $AG\phi$
- les états ns à la question 1 avec $A(\phi \cup \psi)$ qui sat ψ ou qui sat ϕ jusqu'à avoir un successeur qui sat ψ .

Grâce aux deux précédentes questions, on peut facilement conclure que $T_0 \subseteq \text{sat}(\psi) \cup \{s \in \text{sat}(\phi) : \text{post}(s) \subseteq T_0\}$

En effet, on a ^{déjà} vu que $s \in \text{sat}(\phi) : \text{post}(s) \subseteq T_0$ avec $AG\phi$. Cela correspond également au cas de $A(\phi \cup \psi)$ lorsque qu'il y a une succession d'état $\text{sat}(\phi)$ en attendant d'arriver sur un état $\text{sat}(\psi)$.

Pour compléter ça, on a vu à la question 1 qu'il était impératif d'intégrer les états $\text{sat}(\psi)$ à la solution de $\text{sat}(\phi \cup \psi)$.

On tombe donc bien sur $T_0 \subseteq \text{sat}(\psi) \cup \{s \in \text{sat}(\phi) : \text{post}(s) \subseteq T_0\}$

~~On va poser~~ Soit T , le plus grand ensemble satisfaisant

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

On va d'abord ajouter les sommets ~~sat~~ qui satisfont ψ comme dans la première question. De cette manière, on pourra s'occuper du cas ~~$A/\phi \cup \psi$~~ .

Après cela, on va regarder tous les sommets qui ~~sat~~ ϕ . De manière récursive, on va vérifier si tous les ~~sommets~~ états accessibles à partir de ce ~~de~~ $\text{Sat}(\phi) \cup \text{Sat}(\psi)$ (les états satisfaisant ψ sont déjà dans T).

Avec le raisonnement récursif, on a bien dans T , tous les sommets qui ~~sat~~ ψ ou les états ~~ϕ~~ $\text{Sat}(\phi)$ ~~$\text{post}(s) \subseteq T$~~ avec des successeurs eux aussi inclus dans T .

$$\text{d'où } T \subseteq \text{Sat}(\psi) \cup \{s \in \text{Sat}(\phi) : \text{post}(s) \subseteq T\}$$

Donc $T \subseteq T_0$. Vu que $T_0 = \text{Sat}(A/\phi \cup \psi)$, alors ~~$\text{Sat}(A/\phi \cup \psi)$~~ est bien le plus grand ensemble.

Ex 4

Ex 4

→ et $I_1 = I_2$!

1) Les états de S_1 étant inclus dans S_2 , il est évident de dire que
 $S_1 \models \alpha \Rightarrow S_2 \models \alpha$ et $S_1 \models \neg \alpha \Rightarrow S_2 \models \neg \alpha$
car $L_1(s) = L_2(s)$ pour chaque état de S_1 .

• Pour $\phi_1 \wedge \phi_2$: $S_1 \models \phi_1 \Rightarrow S_2 \models \phi_1$
 $S_1 \models \phi_2 \Rightarrow S_2 \models \phi_2$

Avec ces hypothèses, on peut en déduire $S_1 \models \phi_1 \wedge \phi_2 \Rightarrow S_2 \models \phi_1 \wedge \phi_2$

• Pour EQ , il suffit de regarder la définition :
" $S \models EQ$ si $\forall \pi \models \varphi$ pour un chemin π qui ~~com~~ part de s "

En sachant que les états de S_1 sont inclus dans S_2 , tout comme les ~~mêmes~~ transitions et $L_1 = L_2$ pour ces états de S_1 .

Par conséquent, si ~~on~~ $S_1 \models EQ$, alors $S_2 \models EQ$ en partant
du sommet s venant de S_1 qui vérifie ~~$s \models EQ$~~
car les chemins de S_1 sont inclus dans les chemins de S_2

• Dans la même logique, il n'est pas nécessaire de prouver
 X, G et V . En effet, $EX/EG/EU$ parle de l'existence d'un
chemin ~~so~~ avec certaines spécifications. Comme dit plus haut, si
un tel chemin est satisfait dans S_1 alors il le sera aussi dans S_2 .

2) On peut remarquer 2 différences majeures entre ECTL et CTL.

En effet, en CTL on peut utiliser $A\psi$ mais aussi la négation de formule : $\neg\psi$.

De fait, on peut remplacer les formules $A\psi$ en CTL par $\neg E\psi$. Cependant, en ECTL on ne peut pas utiliser $A\psi$, mais combler cela on ne peut pas utiliser la négation de formule (car cela ne fait pas partie de la grammaire ECTL définie).

Par logique, il y aura forcément des formules CTL qui ne seront équivalentes à aucune formule ECTL.

De plus, on a juste le E disponible avec l'ECTL et pas le OU , ce qui empêche l'équivalence de certaines formules (notamment AF et EF en CTL).

Vous parler seulement de la syntaxe ici.

Or on peut parfois exprimer la même propriété de façons différentes (avec d'autres opérateurs)