ALBA
Vincent

18/5

DM Intro Vérif

Exercice 1

1) $\phi = AF(b \wedge \neg a) \rightarrow AFA(b \, W (\neg a \wedge \neg b))$

$\equiv (\neg AF(b \wedge \neg a)) \vee AFA(b \, W (\neg a \wedge \neg b))$

$\equiv \neg(\underbrace{AF(b \wedge \neg a)}_{\phi_1} \wedge \neg \underbrace{AFA(b \, W (\neg a \wedge \neg b))}_{\phi_2})$

$\phi_1 \equiv \neg EG \neg (b \wedge \neg a)$ ✓

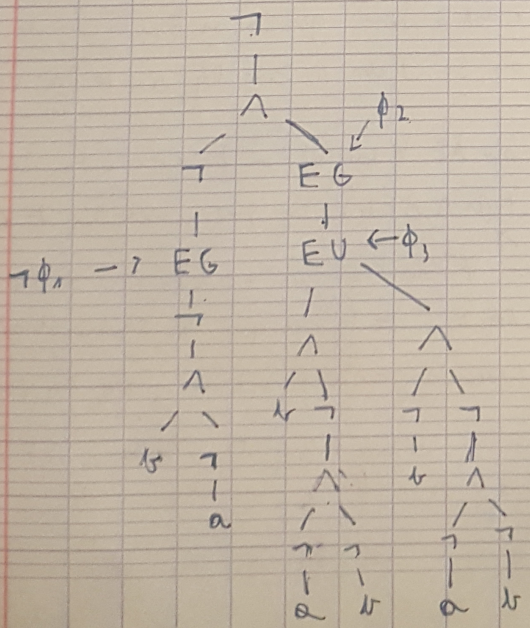
$\phi_2 \equiv E b \, \neg \phi_3$ avec $\phi_3 = A(b \, W (\neg a \wedge \neg b))$

$\phi_3 \equiv \neg E((b \wedge \neg(\neg a \wedge \neg b)) \, U \, (\neg b \wedge \neg(\neg a \wedge \neg b)))$

donc $\phi_2 = EG E((\underbrace{b \wedge \neg(\neg a \wedge \neg b)}_{= b}) U (\underbrace{\neg b \wedge \neg(\neg a \wedge \neg b)}_{= \neg b \wedge a}))$ ✓

$\phi = \neg(\phi_1 \wedge \phi_2)$

2) On peut représenter ϕ par l'arbre :



- Pour trouver les états de S tq $Sat(\neg\phi_1)$ on met dans T les états qui satisfont $\neg(b \wedge \neg a)$ et dans V le reste

T				V
s0,	s1,	s4,	s5	s2, s3, s4, s5
b	a	a	a	
a	1	0	a	
1			0	

$Sat(\neg\phi_1) = \{s0, s1\}$ ✓

$Sat(\phi_1) = \{s2, s3, s4, s5\}$

pour trouver $Sat(\phi_3)$ on met dans V les états qui satisfont $(\neg b \wedge \neg(\neg a \wedge \neg b))$ puis on copie V dans T, puis on check les prédécesseurs qui satisfont $b \wedge \neg(\neg a \wedge \neg b)$

V	T
~~s_5~~	s_5
~~s_2~~	s_2
~~s_0~~	s_0

pas de prédécesseur qui satisfait $b \wedge \neg(\neg a \wedge \neg b)$ →

$Sat(\phi_3) = \{s_5, s_2, s_0\}$

Enfin pour $Sat(\phi_2)$ même calcul que pour $Sat(\neg\phi_1)$ mais avec ϕ_3

T			→ V
s_5	s_2	s_0	s_1, s_3, s_4,
~~x~~	~~x~~	~~x~~	
~~1~~	~~1~~	~~x~~	
		~~1~~	

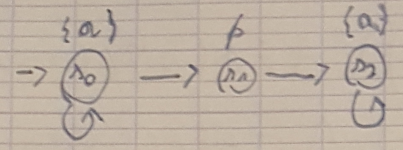
$Sat(\phi_2) = \{s_5, s_2, s_0\}$ ✓

$Sat(\phi) = S \setminus (Sat(\phi_1) \cap Sat(\phi_2)) = \{s_0, s_1, s_3, s_4\}$

✓

Exercice 2

1) Soit le système de Transition suivant :



ici $S \models FX a$ car toutes les exécution de S commence soit par $s_0 \to s_0 \cdots$ soit par $s_0 \to s_1 \to s_2 \cdots$ ici Xa est satisfait dès le début donc $s_0 \to s_0$ soit il est satisfait au deuxième état donc $s_0 \to s_1 \to s_2$

donc $\forall$ exécution de S on a bien FXa ✓

Contre exemple

$S \not\models AFAXa$ car comme $s_0 \not\models AXa$

l'exécution $s_0 - s_0 - s_0 - s_0 \cdots$ ne satisfait jamais AXa donc on ne satisfait pas AF ✓

donc $AFAXa \neq FXa$

2) - Soit S un ST tq $S \models AF(A \wedge AF b)$ on veut prouver $S \models F(A \wedge Fb)$ c'est à dire que pour toute exécution $s_0 - s_1 - s_2 \cdots$ de S $\exists$ un $n \geq 0$ tq $s_n \models (a \wedge F b)$ ① ②

① par définition de AF $\forall$ exécution $s_0 - s_1 - s_2 \cdots$ de S $\exists$ un tq $s_m \models (a \wedge AF b)$ en particulier $s_m \models a$

② comme $s_n \models AF b$ $\forall$ exécution $s_m - s_{m+1} \cdots$ à partir de s_m $\exists$ un $m \geq n$ tq $s_m \models b$ ce qui est équivalent à $s_n \models Fb$ ($\forall$ exec $s_m - s_{m+1} \cdots \exists$ un $m \geq n$ tq $s_m \models b$)

donc $\forall$ exec $s_0 - s_1 \cdots \exists$ un $n \geq 0$ tq $s_n \models a \wedge Fb$

donc $s \models F(a \wedge Fb)$

✓

- Soit S un ST tq $S \models F(a \wedge F b)$ on veut montrer $S \models AF(a \wedge AF b)$
c'est à dire que $\forall$ exec $s_0 - s_1 - s_2 \cdots$ de S, $\exists$ un $n \geq 0$ tq
$s_n \models (a \wedge AF b)$
① ②

① $S \models F(a \wedge F b)$ donc autrement dit, $\forall$ exec $s_0 - s_1 - s_2 \cdots$ de S
$\exists n \geq 0$ tq $s_n \models (a \wedge F b)$ ce qui veut dire $s_n \models a$

② d'après ① on a aussi $s_n \models F b$ on veut montrer
$s_n \models AF b$, comme $s_n \models F b$ donc $\forall$ exec $s_n - s_{n+1} \cdots$
$\exists$ un $m \geq n$ tq $s_m \models b$ ce qui est équivalent à la
définition de $AF b$ (voir la preuve ② précédente).
donc $s_n \models AF b$

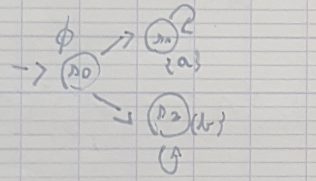
l'erreur est ici

par rapport à une exécution

$s_n \models Fb \not\Rightarrow s_n \models AFb$

donc $\exists$ bien un $n \geq 0$ tq $s_n \models (a \wedge AF b)$ $\forall$ exec partant de S
donc $F(a \wedge Fb) \equiv AF(a \wedge AF b)$

3) On considère le système de transition suivant :



$s_1 \models AX a$ car son seul successeur
est s_1 qui satisfait A
En particulier l'exec $s_1 - s_1 - s_1 \cdots$
satisfait $EGAX a$
donc $s_0 - s_1 - s_1 - s_1 \cdots$ aussi

donc $S \models EGAX a$
pourtant comme $\exists$ une exec depuis un état initial
de S qui ne satisfait pas GXa ($s_2 \not\models Xa$ donc $s_0 - s_2 - s_2 - s_2 \cdots$
ne satisfait pas GXa) alors $S \not\models GXA$ (qui veut dire $\forall$ exec
de S on satisfait GXa) ✓

donc $EGAXa \not\equiv GXa$

Exercice 3

1) $SAT(A(\phi U \psi))$ est le plus petit $T \subseteq S$ qui satisfait :

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

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

On doit prouver : (i) $Sat(A(\phi U \psi))$ satisfait (1) et (2)

(ii) tout T qui satisfait (1) et (2) contient $Sat(A(\phi U \psi))$

(i) : (1) $Sat(\psi) \subseteq Sat(A(\phi U \psi))$ par définition de AN

(2) $s \in$ ② alors $s \models \phi$ et $\forall s' \in Post(s)$ alors $s' \models A(\phi U \psi)$, ce qui correspond à dire que $s \models AX A(\phi U \psi)$ donc pour tout exec partant de s on a $s \xrightarrow{\phi} s_1 \xrightarrow{\phi} s_2 \xrightarrow{\phi} \dots \xrightarrow{\psi} s_n$ avec $n \geq 0$ donc $s \subseteq Sat(A(\phi U \psi))$ ✓

donc $Sat(A(\phi U \psi))$ satisfait (1) et (2)

(ii) $\forall T$ qui satisfait ① et ② $\forall s \in T$ on a bien $s \models \psi$ donc comme montré dans $s \models \phi$ et $Post(s) \subseteq T$

Si $s \models \psi$ alors $s \in Sat(A(\phi U \psi))$ (②) ✓

si $s \models \phi$ alors $\forall s' \in Post(s)$, $s' \in T$, (②)

tout $s \models \phi$ a un voisin qui satisfait (2) ou (1)

autrement dit toute exécution partant de s peut être construite par induction comme $s_0 \xrightarrow{\phi} s_1 \xrightarrow{\phi} s_2 \xrightarrow{\phi} s_3 \dots s_n \xrightarrow{\psi}$ avec $n \geq 0$

donc $s \in Sat(A(\phi U \psi))$

(i) et (ii) vrais donc hypothèse vraie

Vous avez compté le nombre $T \subseteq Sat(A \phi U \psi))$, mais ce n'est pas correct (ex : $T = S$ satisfait (2))

2) $Sat(A G \phi)$ est le + grand ensemble $T \subseteq S$ qui satisfait

① $T \subseteq \{ s \in Sat(\phi) : post(s) \subseteq T \}$

On veut prouver : (i) $Sat(A G \phi)$ satisfait ①

(ii) Tout $T \subseteq S$ qui satisfait ① est contenu dans $Sat(A G \phi)$

(i) si $s \in Sat(A G \phi)$ par définition de $A G$

$s \models \phi$ et toutes les exécutions à partir de s doivent satisfaire $A G \phi \rightarrow s \models A X A G \phi$

autrement dit $A G \phi$ peut être décomposé en

$\phi \wedge A X A G \phi$

$s \models \phi$ donc $s \in \{ s \mid s \models \phi \}$ et comme $s \models A X A G \phi$

$\forall s' \in post(s)$, $s' \in Sat(A G \phi)$

donc $s \subseteq$ ① donc $Sat(A G \phi) \subseteq$ ① car c'est vrai $\forall s \in Sat(A G \phi)$ ✓

(ii) Soit T satisfait ① alors $\forall s \in T$, $s \models \phi$ et $\forall s' \in post(s)$, $s' \subseteq T$

On veut montrer que $T \subseteq Sat(A G \phi)$ autrement dit $\forall s$ atteignable depuis un état de T, $s \models \phi$

on peut le prouver par induction sur n la distance de l'état s_n d'un état initial de l'exécution :

$n = 0$

$s_0 \models \phi$ car $s_0 \in$ ①

$n = 1$

$s_0 \in$ ① donc $s_1 \in post(s_0) \subseteq T \subseteq$ ①

donc $s_1 \models \phi$

On suppose vrai jusqu'à n on veut prouver pour $n+1$

$s_n \subseteq$ ① donc $s_{n+1} \in post(s_n) \subseteq T \subseteq$ ①

donc s_{n+1} → hypothèse vraie

donc $Sat(A G \phi)$ est le + grand ensemble $T \subseteq S$ qui satisfait ① ✓

3) $Sat(A(\phi W \psi))$ est le plus grand ensemble $T \subseteq S$ qui satisfait :

① $T \subseteq Sat(\psi) \cup \{ s \in Sat(\phi) : post(s) \subseteq T \}$

On veut prouver :

(i) $Sat(A(\phi W \psi))$ satisfait ①

$\forall s \in Sat(A(\phi W \psi))$ sais $s \models \psi$ (car par déf de AW $Sat(\psi) \subseteq Sat(A(\phi W \psi))$ donc $s \in$ ①

Sais $s \models \phi$ donc quel cas $\forall s'$ in $post(s)$, $s' \models A(\phi W \psi)$ car sinon il existe une exec $s - s' \cdots$ depuis s qui ne satisfait pas $\phi W \psi$, ce qui est impossible par définition de AW donc $s \models \phi$ et $post(s) \subseteq Sat(A(\phi W \psi))$

$s \in$ ① oui, $A(\phi W \psi) = \psi \vee (AX A(\phi W \psi) \wedge \phi)$

dans les deux cas on a donc $s \in$ ① ✓

(ii) Sais T satisfait ① on veut prouvé $T \subseteq Sat(A(\phi W \psi))$

autrement on veut prouvé que $\forall$ exec $s_0 - s_1 \to s_2 \cdots$ où T sais $\forall n$, $s_n \models \phi$

sais $\exists m \geq 0$ tq $s_m \models \psi$ et $\forall n < m$, $s_n \models \phi$

On peut le prouvé par recurrence sur n où on est le numéro de l'étape dans l'exec

$n = 0$

Sais $s_0 \models \psi$ donc quel cas $s \subseteq Sat(A(\phi W \psi))$

sais $s_0 \models \phi$ OK

on suppose vrais jusqu'à n on veut prouvé $n+1$

Sais $s_{n+1} \models \psi$ donc $s_0 \xrightarrow[\phi]{} s_1 \cdots s_{n+1} \xrightarrow[\psi]{}$ satisfait $A(\phi W \psi)$

Sais $s_{n+1} \models \phi$ donc on a bien une exec où tous les états sont dans $Sat(\phi)$ ✓

donc vrais

(i) et (ii) vrais donc l'hypothèse de départ est vrais ✓

Exercice 4

1) Soit S_1 un ST et S_2 un ST tq $S_1 \subseteq S_2$ et $S_1 \models \phi$

① si $S_1 \models a$ alors $a \in L_1(s)$ $\forall s \in I_1$ et comme $I_1 = I_2$ et $L_2(s) = L_1(s)$ $\forall s \in S_1$, comme $I_1 \subseteq S_1 \to I_2 \subseteq S_1$ donc $a \in L_2(s)$ $\forall s \in I_2 \to S_2 \models a$ ✓

② même raisonnement pour $\neg a$ ✓

③ si $S_1 \models E\psi$ alors $\pi \models \psi$ pour certain chemin π qui commence par $s \in I_1$, comme $I_1 = I_2$ et que les état et transition de S_1 existe dans S_2 alors $\pi \models \psi$ pour ce même chemin qui commence par $s \in I_2$ dans S_2, $S_2 \models E\psi$ ✓

④ si $S_1 \models \phi_1 \wedge \phi_2$ on va prouvé par induction sur n le nombre de $\wedge$ imbriqué dans la formule E CTL que $S_1 \models \phi_1 \wedge \phi_2$ alors $S_2 \models \phi_1 \wedge \phi_2$

$S_1 \models \phi_1 \to S_2 \models \phi_1$, $S_1 \models \phi_2 \Rightarrow S_2 \Rightarrow \phi_2$, etc ✓

$n = 1$

$S_1 \models \phi_1 \wedge \phi_2 \to S_1 \models \phi_1$ ET $S_1 \models \phi_2$

ici $n = 1$ donc ϕ_1 est soit de la forme a, $\neg a$, $E\psi$ donc d'après ①, ②, ③ $S_2 \models \phi_1$, idem pour ϕ_2

On suppose l'hypothèse vraie jusqu'à n on veut prouvé $n+1$

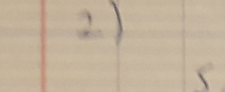
$S_1 \models \phi_1 \wedge \phi_2 \to S_1 \models \phi_1$ ET $S_1 \models \phi_2$

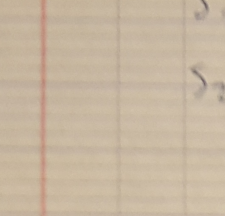
si ϕ_1 est de la forme a, $\neg a$, $E\psi$ même chose que pour $n = 1$

si ϕ_1 est construit à partir de n ou moins $\wedge$ imbriqué alors d'après l'hypothèse d'induction $S_2 \models \phi_1$ (avait pour ϕ_2

donc vrai $\forall n \to S_1 \models \phi_1 \wedge \phi_2 \to S_2 \models \phi_1 \wedge \phi_2$

2)

$S_1 =$ 

$S_2 =$ 

on a bien $I_1 = I_2$

$\{s_0\} \subseteq \{s_0, s_1\}$ donc $S_1 \subseteq S_2$

et $\rightarrow_1 \subseteq \rightarrow_2$ car les deux seuls transitions possibles $s_0 \rightarrow s_0$ (s_1 est bien dans $\rightarrow_1$)

et comme $L_1(s_0) = L_2(s_0)$ on a donc bien $S_1 \subseteq S_2$

$S_1 \models AG a$ car la seule exécution possible est $s_0 - s_0 - s_0 \cdots$ et $s_0 \models a$

mais $S_2 \not\models AG a$ à cause de $s_0 - s_1 - s_1 \cdots$ (a, $\neg a$, $\neg a$)

donc comme toute formule ECTL nécessite $S_1 \models \phi \rightarrow S_2 \models \phi$ si $S_1 \subseteq S_2$, donc aucune formule ECTL n'est équivalente à $AG a$

✓ super