

Devoir "Introduction à la Vérification"

M1

HOLLANDER Théo 26 Mars

EXERCICE 1

$$1.1. \quad \Phi = \underbrace{AF(b \wedge \neg a)}_{\phi_1} \rightarrow \underbrace{AFA(b \wedge (\neg a \wedge \neg b))}_{\phi_2}$$

$$\Phi = \phi_1 \rightarrow \phi_2$$

$$\Phi = \neg \phi_1 \vee \phi_2 = \neg(\phi_1 \wedge \neg \phi_2)$$

$$\phi_1 = AF(b \wedge \neg a)$$

$$= \neg EG \neg(b \wedge \neg a) \quad (\text{par règle de dualité})$$

$$\phi_2 = AFA(b \wedge (\neg a \wedge \neg b))$$

$$= AF \neg E \left((b \wedge \neg(\neg a \wedge \neg b)) \cup (\neg b \wedge \neg(\neg a \wedge \neg b)) \right) \quad (\text{par définition de l'opérateur dérivé 'until faible'})$$

$$= \neg EG \neg E \left(\underbrace{(b \wedge \neg(\neg a \wedge \neg b))}_{\phi_{22}} \cup \underbrace{(\neg b \wedge \neg(\neg a \wedge \neg b))}_{\phi_{23}} \right) \quad (\text{par règle de dualité})$$

$$\phi_{22} = b \wedge \neg(\neg a \wedge \neg b)$$

$$= b \wedge (a \vee b)$$

$$= (b \wedge a) \vee (b \wedge b)$$

$$= (b \wedge a) \vee b$$

$$= b$$

$$\phi_{23} = \neg b \wedge \neg(\neg a \wedge \neg b)$$

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

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

$$= (\neg b \wedge a) \vee (\text{false})$$

$$= \neg b \wedge a$$

On peut réécrire ϕ_2 ,

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

Φ en forme normale existentielle donne :

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

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

RAPPEL ENF :

$$\phi ::= \text{true}$$

$$| a$$

$$| \phi_1 \wedge \phi_2$$

$$| \neg \phi$$

$$| EX \phi$$

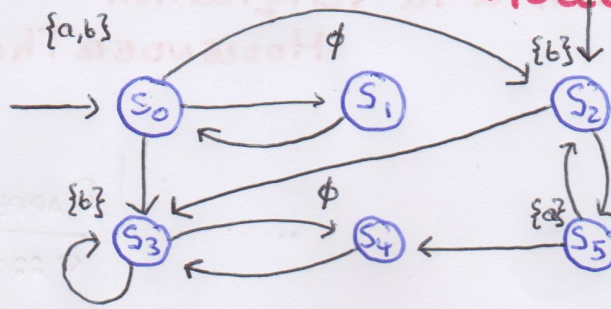
$$| E(\phi_1 \cup \phi_2)$$

$$| EG \phi$$

Devoir "Introduction à la Vérification"

HouENDER Theo 26 Mars M1

1.2



$$\Phi_1 = \neg EG \neg (b \wedge \neg a)$$

$$\bullet \text{Sat}(b \wedge \neg a) = \{S_2, S_3\} \quad \text{Sat}(\neg(b \wedge \neg a)) = S \setminus \{S_2, S_3\} = \{S_0, S_1, S_4, S_5\}$$

$$\bullet S' := S \setminus \{S_0, S_1, S_4, S_5\}$$

$(S_0, S_1)^\omega$ est composante ^{fortement} connexe non-triviale.

Dans S' , S_4 est état puit, de plus (toujours dans S') $\text{Post}(S_5) = \{S_4\}$.

$$\text{Donc } EG \neg (b \wedge \neg a) = \{S_0, S_3\}$$

$$\bullet \text{Donc } \text{Sat}(\Phi_1) = S \setminus \{S_0, S_1\} = \{S_2, S_3, S_4, S_5\}$$

$$\neg \Phi_2 = \neg \neg EG \neg E(b \vee (\neg b \wedge a))$$

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

$$T_1 = T_0 \cup \{S_2\} \quad \text{car } \{S_2\} \in \text{Pre}(S_5) \text{ et } S_2 \in \text{Sat}(a)$$

$$T_2 = T_1 \cup \{S_0\} \quad \text{car } \{S_0\} \in \text{Pre}(S_2) \text{ et } S_0 \in \text{Sat}(b) \quad | \text{Pre}(S_2) = \{S_0, S_5\}$$

$$T_3 = T_2 \quad \text{car } \text{Pre}(S_0) = \{S_1\} \text{ or } S_1 \notin \text{Sat}(b)$$

Donc

$$\text{Sat}(E(b \vee (\neg b \wedge a))) = T_3 = \{S_0, S_2, S_5\}$$

$$\bullet \text{Sat}(\neg E(b \vee (\neg b \wedge a))) = S \setminus \{S_0, S_2, S_5\} = \{S_1, S_3, S_4\}$$

$$\bullet S'' := S \setminus \{S_1, S_3, S_4\}$$

Dans S'' , S_5 est état puit.

Dans S'' , $(S_3 S_4)^\omega$ ~~est~~ ^{est} composante ^{fortement} connexe non-triviale.

$$\text{Donc } \text{Sat}(\Phi_2) = \{S_3, S_4\}$$

$$\text{Sat}(\neg \Phi_2) = S \setminus \{S_3, S_4\} = \{S_0, S_1, S_2, S_5\}$$

$$\Phi = \neg (\Phi_1 \wedge \neg \Phi_2)$$

$$\text{Sat}(\Phi_1) = \{S_2, S_3, S_4, S_5\}$$

$$\text{Sat}(\neg \Phi_2) = \{S_3, S_4\}$$

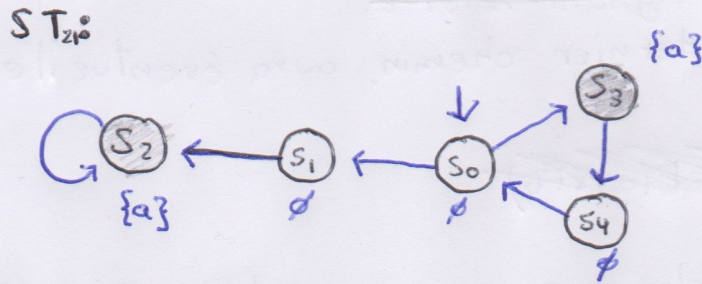
$$\text{Sat}(\Phi_1 \wedge \neg \Phi_2) = \text{Sat}(\Phi_1) \cap \text{Sat}(\neg \Phi_2) = \{S_3, S_4\}$$

$$\text{Sat}(\Phi) = S \setminus \{S_3, S_4\} = \{S_0, S_1, S_2, S_5\}$$

2

EXERCICE 2

2.1 AFAXa n'est pas équivalent à FXa



$ST_{21} \models FXa$

or

$ST_{21} \not\models AFAXa$

car le chemin $(s_0 s_3 s_4)^\omega$ ne satisfait pas $AFAXa$, s_1 reste un successeur possible pour s_0 .

FXa
formule de chemin

2.2 $AF(a \wedge AFb) \equiv A(\text{true} U (a \wedge AFb)) \equiv (\phi)$
est-il équivalent à:
 $F(a \wedge Fb) \equiv \text{true} U (a \wedge Fb) \equiv (\phi)$

($\Rightarrow$)

Prenons un système de transition TS, tel que $TS \models \phi$

Prenons π un chemin dans TS,

De part la sémantique de CTL, $\pi \models \text{true} U (a \wedge AFb)$

À un moment donné, $(a \wedge AFb)$ sera ~~éventuellement~~ satisfait.

C'est à dire π admettra un sous-chemin π' tel que:

$\pi = s_0 s_1 \dots \underbrace{s_i s_{i+1} \dots}_{\pi'} \dots$ (possiblement $s_0 = s_{i+1}$)

avec $\pi' \models (a \wedge AFb)$

Ainsi, donc s_{i+1} aura a comme label.

et identiquement, b sera ~~éventuellement~~ satisfait dans π' .

C'est à dire π' admettra un état $s_{i'}$ tel que $s_{i'}$ aura b comme label, avec $i' \geq 0$.

Ainsi donc $\pi \models F(a \wedge Fb)$

Devoir "Introduction à la Vérification"

HOLLENDER Théo

26 Mars

M1

($\Leftarrow$)

Prenons un système de transition TS tel que $TS \models \Phi$.

le par définition $\forall \pi$ un chemin de TS, $\pi \models \Phi$

Prenons π , un chemin quelconque de TS

À un moment donné, π aura un état s_b étiqueté b à ~~un état~~ s_b .

Comme

Identiquement, tous les chemins de TS ~~seront~~ → issus de s_b ont à un moment donné un état étiqueté a . En particulier π à lui aussi un état s_a étiqueté a , avec $a \leq b$.

Donc l'état s_a satisfait $a \wedge A \wedge Fb$.

Comme π a été pris quelconque nous avons bien $TS \models A \wedge Fb$ ($a \wedge A \wedge Fb$)

Donc, $TS \models \Phi$.

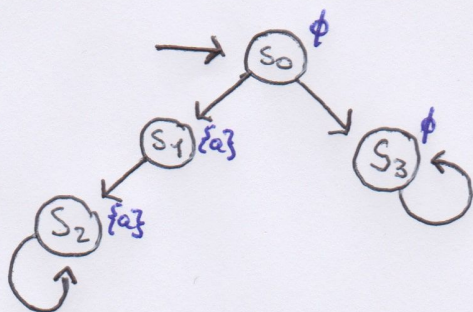
(✓)

2.3

~~AXa~~

~~$EGXa$~~ n'est pas équivalent à GXa .

ST_{23} :



$ST_{23} \models EGXa$.

$\hookrightarrow s_0 s_1(s_2)^\omega$

or,

$ST_{23} \not\models GXa$.

en effet $s_0 s_3(s_3)^\omega$

ne satisfait pas GXa .

✓

4

EXERCICE 3

3.1 MONTRER QUE: $\text{Sat}(A(\phi \cup \psi))$ EST LE PLUS PETIT $T \subseteq S$
 TEL QUE: $\left| \begin{array}{l} \text{Sat}(\psi) \subseteq T \quad (1) \\ \& \{s \in \text{Sat}(\phi) \mid \text{post}(s) \subseteq T\} \subseteq T \quad (2) \end{array} \right.$

(i) Montrons que $\forall T = \text{Sat}(A(\phi \cup \psi))$, T satisfait (1) & (2).

Par la loi d'expansion: $A(\phi \cup \psi) \equiv \psi \vee (\phi \wedge A X A(\phi \cup \psi))$ ✓
 on en déduit trivialement que T satisfait bien (1) & (2).

(ii) Montrons que $\forall T$ qui satisfait (1) & (2), on a $\text{Sat}(A(\phi \cup \psi)) \subseteq T$.
 Soit $s \in \text{Sat}(A(\phi \cup \psi))$

• Si $s \in \text{Sat}(\psi)$, par (1) on a que $s \in T$. ✓

• sinon,

□ par définition, les chemins $\pi = s_0 s_1 s_2 \dots$ partants de $s = s_0$ satisfont: $\pi \models \phi \cup \psi$

□ Soit $n > 0$ tel que $s_n \models \psi$ & si $\models \phi$ ~~pour tout~~ $\forall i \in [0; n]$

□ On a $s_n \in T$, ~~car~~ (car $s_n \in \text{Sat}(\psi)$).

et $s_n \in \text{Post}(s_{n-1})$ et $s_{n-1} \in \text{Sat}(\phi)$

- Si $\text{Post}(s_{n-1}) = \{s_n\}$, on a $\text{Post}(s_{n-1}) \subseteq T$

Donc, par (2) $s_{n-1} \in T$.

- Sinon, tous les $p_s \in \text{Post}(s_{n-1}) \setminus \{s_n\}$, par définition, sont membre d'un autre chemin π (comme définit plus haut)

Et ainsi, par récurrence $p_s \in T$. $\forall p_s$.

Donc $\text{Post}(s_{n-1}) \subseteq T$

Donc, par (2) $s_{n-1} \in T$

□ &c...

□ Par récurrence, avec les mêmes argument on obtient que $s_0 \in T$.

□ Or $s_0 = s$, donc, $s \in T$. ✓

ça va, mais ça aurait
 mieux de raisonner
 du bas vers le haut

3.2 MONTRER QUE $\text{Sat}(\text{AG}\phi)$ EST LE PLUS GRAND ENSEMBLE TES
TEL QUE $T \subseteq \{s \in \text{Sat}(\phi) \mid \text{Post}(s) \subseteq T\}$ (3).

(i) Soit $T = \text{Sat}(\text{AG}\phi)$

Par la loi d'expansion: $\text{AG}\phi \equiv \phi \wedge \text{AXAG}\phi$ ✓

Il vient trivialement que T satisfait (3).

(ii) Montrons que $\forall T$ satisfaisant (3) on a $T \subseteq \text{Sat}(\text{AG}\phi)$

□ Soit $T \subseteq \text{Sat}(\text{AG}\phi)$ qui satisfait (3)

□ Soit $s \in T$.

- construisons les chemins $\pi = s_0 s_1 s_2 \dots$ partants de $s = s_0$.

- comme $s_0 \in T$, par (3), nous avons $s_0 \in \text{Sat}(\phi)$

& tous les $s_1 \in \text{Post}(s_0)$ sont dans T .

- par récurrence: [pour $i \geq 0$]

comme $s_i \in T$, par (3), nous avons $s_i \in \text{Sat}(\phi)$

& tous les $s_{i+1} \in \text{Post}(s_i)$ sont dans T

- &c...

□ Ainsi, $\forall i \geq 0, s_i \in \text{Sat}(\phi)$

□ Donc les chemins $\pi = s_0 s_1 s_2 \dots$ partants de $s = s_0$ satisfont $G\phi$

□ Comme s a été pris quelconque nous avons: ~~$s \in \text{Sat}(\text{AG}\phi)$~~

$\forall s \in T, s \in \text{Sat}(G\phi) \Rightarrow T \subseteq \text{Sat}(\text{AG}\phi)$. ✓

3.2 MONTRER QUE $\text{Sat}(\text{AG}\phi)$ EST LE PLUS GRAND ENSEMBLE TES
TEL QUE $T \subseteq \{s \in \text{Sat}(\phi) \mid \text{Post}(s) \subseteq T\}$ (3).

(i) Soit $T = \text{Sat}(\text{AG}\phi)$

Par la loi d'expansion: $\text{AG}\phi \equiv \phi \wedge \text{AXAG}\phi$

Il vient trivialement que T satisfait (3).

(ii) Montrons que $\forall T$ satisfaisant (3) on a $T \subseteq \text{Sat}(\text{AG}\phi)$

□ Soit $T \subseteq \text{Sat}(\text{AG}\phi)$ qui satisfait (3)

□ Soit $s \in T$.

- construisons les chemins $\pi = s_0 s_1 s_2 \dots$ partants de $s = s_0$.

- comme $s_0 \in T$, par (3), nous avons $s_0 \in \text{Sat}(\phi)$

& tous les $s_1 \in \text{Post}(s_0)$ sont dans T .

- par récurrence: [pour $i \geq 0$]

comme $s_i \in T$, par (3), nous avons $s_i \in \text{Sat}(\phi)$

& tous les $s_{i+1} \in \text{Post}(s_i)$ sont dans T

- &c...

□ Ainsi, $\forall i \geq 0, s_i \in \text{Sat}(\phi)$

□ Donc les chemins $\pi = s_0 s_1 s_2 \dots$ partants de $s = s_0$ satisfont $G\phi$

□ Comme s a été pris quelconque nous avons: ~~$T \subseteq \text{Sat}(\text{AG}\phi)$~~

$\forall s \in T, s \in \text{Sat}(G\phi) \Rightarrow T \subseteq \text{Sat}(\text{AG}\phi)$.