<u>Correction</u> 1 : *Méthode du tableau*

Afin de vérifier qu'une formula LTL f est satisfaite par un modèle (structure de Kripke) $M = (S_M, R_M, L_M)$ dans l'état s ($M, s \models A\ f$), deux méthodes "tableau" existent. Le principe commun à ces méthodes est de construire à partir de la formule un graphe qui permettra d'extraire un modèle pour la formule ssi la formule est satisfaisable. Les deux méthodes diffèrent dans la manière dont elles composent le graphe "tableau" de la formule avec le modèle M.

1. méthode implicite : construit le graphe "tableau" et fait directement le produit avec M. La complexité en temps de cette méthode est $O((|S_M| + |R_M|)2^{O(|f|)})$.
2. méthode explicite (ou symbolique) : construit séparément le graphe "tableau" qu'elle compose ensuite avec le modèle M, en déterminant ainsi les exécutions communes à M et f. Déterminer si s satisfait f revient à déterminer s'il existe un chemin dans la composition qui satisfait f.

Dans les deux cas, on suppose que la formule f est une formule "restreinte sur les chemins", c'est-à-dire que les sous-formules de f sur les états sont des propositions atomiques.

Dans la suite, on présente sur les deux formules données les deux méthodes pour vérifier si $M, s \models A\ f$. Comme $M, s \models A\ f$ ssi $M, s \models \neg E \neg f$, il suffit de pouvoir vérifier des formules de type Ef avec f formule "restreinte sur les chemins", puis de montrer qu'il n'existe pas de chemin qui satisfait $\neg f$.

De plus, il suffit de considérer que les formules sont construites avec les operateurs X et U car les autres opérateurs sont dérivés ($F\ f = t\ U\ f$, $G\ f = \neg F\ \neg f$ et $f_1\ R\ f_2 = \neg(\neg f_1\ U\ \neg f_2)$).

Méthode implicite : étape 1 — calcul de la clôture La clôture de f, $CL(f)$, contient les formules dont la vérité peut influencer la vérité de f. Donc $CL(f)$ est le plus petit ensemble qui contient f et qui satisfait les propriétés suivantes :

- $\neg f_1 \in CL(f)$ ssi $f_1 \in CL(f)$
- si $f_1 \vee f_2 \in CL(f)$ alors $f_1, f_2 \in CL(f)$
- si $Xf_1 \in CL(f)$ alors $f_1 \in CL(f)$
- si $\neg X f_1 \in CL(f)$ alors $X \neg f_1 \in CL(f)$
- si $f_1\ U\ f_2 \in CL(f)$ alors $f_1, f_2, X(f_1\ U\ f_2) \in CL(f)$

Il est à remarquer que la taille de $CL(f)$ est linéaire dans la taille de f.

Exemples :

- Pour la formule $f = G\ (b \Rightarrow F\ b)$, on traduit les opérateurs dérivés comme suit :

$$\begin{aligned} f &\equiv \neg F\ \neg(\neg b \vee F\ b) \\ &\equiv \neg F\ \neg(\neg b \vee F\ b) \end{aligned}$$

$$\equiv \quad \neg(T\ U\ \neg(\neg b \vee (T\ U\ b)))$$

Alors la clôture de f on la construit en itérant la définition jusqu'à la stabilisation :

$$\begin{array}{rcl}
CL(\neg f) & = & \{f \equiv (\neg(T\ U\ \neg(\neg b \wedge \neg(T\ U\ b)))), \neg f\} \cup CL(\neg f) \\
& = & \{f, \neg f\} \cup CL(f_1 \equiv \neg(\neg b \vee (T\ U\ b))) \cup CL(f_2 \equiv X \neg f) \\
& = & \{f, \neg f, f_1, \neg f_1, f_2, \neg f_2 \equiv X f\} \cup \\
& & \{b, \neg b\} \cup CL(f_3 \equiv = (T\ U\ b)) \\
& = & \{f, \neg f, f_1, \neg f_1, f_2, \neg f_2, b, \neg b\} \cup \\
& & \{f_3, \neg f_3\} \cup CL(f_4 \equiv X f_3) \\
& = & \{f, \neg f, f_1, \neg f_1, f_2, \neg f_2, f_3, \neg f_3\} \cup \\
& & \{b, \neg b, f_4, \neg f_4, f_5\} \\
& where & \\
f & \equiv & \neg(T\ U\ f_1) \\
f_1 & \equiv & \neg(\neg b \vee f_3) \\
f_2 & \equiv & X\ (\neg f) \\
f_3 & \equiv & T\ U\ b \\
f_4 & \equiv & X\ f_3 \\
f_5 & \equiv & X\ \neg f_3
\end{array}$$

– Pour la formule $f = a\ U\ b$, on obtient la clôture :

$$CL(\neg f) \quad = \quad \{\neg f, f, X\ f, \neg X\ f, X\ \neg f, a, \neg a, b, \neg b\}$$

Méthode implicite : étape 2 — calcul de l'intersection L'intersection est faite à la volée, en décorant les états du modèle avec des formules incluses dans la clôture de la formule, de manière à rester consistent (ne pas contredire) l'étiquetage déjà existant (par L_M) et à respecter la sémantique des formules.

Soit G le graphe intersection calculé. Les états de ce graphe on les appelle des atomes. Un atome $A = (s_A, K_A)$ est tel que $s_A \in S_M$ et $K_A \subseteq CL(f) \cup AP$ (AP est l'ensemble des propositions atomiques qui peuvent étiqueter les états de M) tel que :

- pour chaque $p \in AP$, $p \in K_A$ ssi $p \in L(s_A)$ (consistence avec l'étiquetage initial de M)
- pour chaque $f_1 \in CL(f)$, $f_1 \in K_A$ ssi $\neg f_1 \notin K_A$ (consitence avec la négation de formules)
- pour chaque $f_1 \vee f_2 \in CL(f)$, $f_1 \vee f_2 \in K_A$ ssi $f_1 \in K_A$ ou $f_2 \in K_A$ (sémantique du ou)

- pour chaque $\neg X\ f_1 \in CL(f)$, $\neg X\ f_1 \in K_A$ ssi $X\ \neg f_1 \in K_A$ (sémantique de la négation sur opérateur X)
- pour chaque $f_1\ U\ f_2 \in CL(f)$, $f_1\ U\ f_2 \in K_A$ ssi $f_2 \in K_A$ ou $f_1, X(f_1\ U\ f_2) \in K_A$ (sémantique de l'opérateur U)

Une paire d'atomes (A, B) est une arête de G ssi :

- $(s_A, s_B) \in R$ et
- pour toute formule $X\ f_1 \in CL(f)$, $X\ f_1 \in K_A$ ssi $f_1 \in K_B$ (consistence avec la sémantique de l'opérateur X).

Pour eviter l'explosion des exemples, on considère que la formule $f = a\ U\ b$ sur les deux graphes :

1. Formule $f = a\ U\ b$ et modèle M_1, le graphe G_1 est défini par :
   - Atomes :

$$
\begin{aligned}
A_1^1 &= (s_1, \{a, b, \neg c, f, X\ f\}) \\
A_2^1 &= (s_1, \{a, b, \neg c, f, \neg X\ f, X\ \neg f\}) \\
A_3^1 &= (s_2, \{b, c, \neg a, f, X\ f\}) \\
A_4^1 &= (s_2, \{b, c, \neg a, f, \neg X\ f, X\ \neg f\}) \\
A_5^1 &= (s_3, \{c, \neg a, \neg b, \neg f, X\ f\}) \\
A_6^1 &= (s_3, \{c, \neg a, \neg b, \neg f, \neg X\ f, X\ \neg f\})
\end{aligned}
$$

   - Transitions :
     - (A_1^1, A_3^1), (A_1^1, A_4^1),
     - (A_2^1, A_5^1), (A_2^1, A_6^1),
     - (A_3^1, A_1^1),
     - (A_4^1, A_5^1), (A_3^1, A_6^1),
     - (A_6^1, A_6^1)
2. Formule $f = a\ U\ b$ et modèle M_2, le graphe G_2 est définit par :
   - Atomes :

$$
\begin{aligned}
A_1^2 &= (s_{1'}, \{a, \neg b, f, X\ f\}) \\
A_2^2 &= (s_{1'}, \{a, \neg b, \neg f, \neg X\ f, X\ \neg f\}) \\
A_3^2 &= (s_{2'}, \{a, b, f, X\ f\}) \\
A_4^2 &= (s_{2'}, \{a, b, f, \neg X\ f, X\ \neg f\}) \\
A_5^2 &= (s_{3'}, \{\neg a, \neg b, \neg f, X\ f\}) \\
A_6^2 &= (s_{3'}, \{\neg a, \neg b, \neg f, \neg X\ f, X\ \neg f\}) \\
A_7^2 &= (s_{4'}, \{\neg a, b, f, X\ f\}) \\
A_8^2 &= (s_{4'}, \{\neg a, b, f, \neg X\ f, X\ \neg f\})
\end{aligned}
$$

   - Transitions :
     - (A_1^2, A_3^2), (A_1^2, A_4^2), (A_1^2, A_7^2), (A_1^2, A_8^2),
     - (A_2^2, A_5^2), (A_2^2, A_6^2),
     - (A_3^2, A_1^2),

- (A^2_4, A^2_2),
- (A^2_5, A^2_7), (A^2_5, A^2_8),
- (A^2_7, A^2_7), (A^2_7, A^2_8)

Méthode implicite : étape 3 — calcul de chemin Une composante fortement connexe non-triviale C de G est auto-suffisante ssi pour chaque atome A en C et pour chaque formule $f_1\ U\ f_2 \in K_A$ il existe un atome B en C tel que $f_2 \in K_B$.

Alors $M, s \vdash E\ f$ ssi il existe un atome $A = (s, K)$ en G tel que $f \in K$ et il existe un chemin en G à partir de A vers une composante fortement connexe auto-suffisante.

Pour nos exemples, un état s satisfait $\neg f$ s'il existe un atome (s, K) tel que $\neg f \in K$ et un chemin de (s, K) en G vers une composante auto-suffisante.

1. Graphe G_1 pour tester $M_1, s_1 \models E\ \neg f$ donc $M_1, s_1 \not\models A\ f$.
2. Graphe G_2 pour tester $M_2, s_{4'} \not\models E\ \neg f$ (toutefois $M_2, s_{1'} \models E\ \neg f$), donc $M_2, s_{1'} \not\models A\ f$.

Méthode explicite : étape 1 — calcul de sous-formules élémentaires Pour tester la vérité d'une formule $E\ f$ sur un modèle M, on construit un graphe “tableau” T (structure de Kripke) qui inclut tout chemin qui satisfait f.

$T = (S_T, R_T, L_T)$ où chaque état de S_T est un ensemble de formules élémentaire, $el(f)$, obtenues à partir de f comme suit :
- $el(p) = \{p\}$ si $p \in AP_f$ ($AP_f \subseteq AP$ les propositions atomiques de f)
- $el(\neg g) = el(g)$
- $el(g \vee h) = el(g) \cup el(h)$
- $el(X\ g) = \{X\ g\} \cup el(g)$
- $el(g\ U\ h) = \{X\ (g\ U\ h)\} \cup el(g) \cup el(h)$

Exemple :
- Pour la formule $\neg f = (T\ U\ \neg(\neg b \vee (T\ U\ b))$, on a :

$$\begin{aligned} el(\neg f) &= \{X\ \neg f\} \cup el(\not(\neg b \vee (T\ U\ b))) \\ &= \{X\ \neg f\} \cup el(\neg b \vee (T\ U\ b)) \\ &= \{X\ \neg f, b\} \cup el(T\ U\ b) \\ &= \{X\ \neg f, b, X\ (T\ U\ b)\} \end{aligned}$$

- Pour la formule $\neg f = \neg(a\ U\ b)$, on a :

$$el(\neg f) = el(f) = \{X\ f, a, b\}$$

Alors $S_T = P(el(f))$ et L_T est définit pour un état tel qu'il renvoit les propositions élémentaires contenues dans l'état.

Pour notre exemple, S_T a les états :

- $s_1 = \{a, b, X\ f\}$
- $s_2 = \{a, b\}$
- $s_3 = \{a, \neg b, X\ f\}$
- $s_4 = \{a, \neg b\}$
- $s_5 = \{\neg a, b, X\ f\}$
- $s_6 = \{\neg a, b\}$
- $s_7 = \{\neg a, \neg b, X\ f\}$
- $s_8 = \{\neg a, \neg b\}$

Méthode explicite : étape 2 — calcul du graphe tableau La relation de transition R_T doit avoir la propriété que chaque formule élémentaire d'un état est vraie dans cet état. Par exemple, si Xf est vraie dans un état s, dans tous les états successeurs de s doit être vraie la formule f. De plus, si Xf n'est pas dans un état s, alors s doit satisfaire $\neg Xf$, donc tous ses successeurs ne doivent pas contenir f.

Donc la relation de transition est définie par :

$$R_t(s, s') = \wedge_{Xg \in el(f)} s \in sat(Xg) \Leftrightarrow s' \in sat(g)$$

où :
- $sat(g) = \{s \mid g \in s\}$ avec $g \in el(f)$
- $sat(\neg g) = \{s \mid s \notin sat(g)\}$
- $sat(g \vee h) = sat(g) \cup sat(h)$
- $sat(g\ U\ h) = sat(h) \cup (sat(g) \cap sat(X\ (g\ U\ h)))$

Le définition de R_T dit qu'il y a des transitions de tout état de $sat(X\ f)$ dans un état de $sat(f)$ et de tout état du complément de $sat(X\ f)$ dans un état du complément de $sat(f)$.

Pour notre exemple, le sat est definit par :
- $sat(a) = \{s_1, s_2, s_3, s_4\}$
- $sat(b) = \{s_1, s_2, s_5, s_6\}$
- $sat(X\ f) = \{s_1, s_3, s_5, s_7\}$
- $sat(f) = sat(a) \cup (sat(b) \cap sat(X\ f)) = \{s_1, s_2, s_3, s_4, s_5\}$

Donc la relation de transition est l'ensemble suivant de paires :
- (s_1, s_1), (s_1, s_2), (s_1, s_3), (s_1, s_4), (s_1, s_5)
- (s_2, s_6), (s_2, s_7), (s_2, s_8)
- (s_3, s_1), (s_3, s_2), (s_3, s_3), (s_3, s_4), (s_3, s_5)
- (s_4, s_6), (s_4, s_7), (s_4, s_8)
- (s_5, s_1), (s_5, s_2), (s_5, s_3), (s_5, s_4), (s_5, s_5)
- (s_6, s_6), (s_6, s_7), (s_6, s_8)
- (s_7, s_1), (s_7, s_2), (s_7, s_3), (s_7, s_4), (s_7, s_5)
- (s_8, s_6), (s_8, s_7), (s_8, s_8)

Méthode explicite : étape 3 — calcul du produit Le produit $P = (S, R, L)$ du tableau T et du modèle $M = (S_M, R_M, L_M)$ est définit par :

- $S = \{(s, s') \mid s \in S_T, s' \in S_M \wedge L_M(s') \cap AP_f = L_T(s)\}$
- $R((s, s'), (t, t'))$ ssi $R_T(s, t)$ et $R_M(s', t')$
- $L((s, s')) = L_T(s)$

Si la relation de transition R n'est pas totale pour des états du produit, on enlève ces états.

Puis, sur ce produit, on vérifie qu'il existe un chemin infini dans les états de $sat(\neg f)$ qui passe infiniment souvent dans les états de $sat(\neg(a\ U\ b) \vee b)$. Dans ce ca, $E\neg f$ est vérifié.

Dans nos exemples, on trouve toujours ce chemin, donc Af n'est pas satisfaisable.