10 Automates d'arbres alternants

La notion clef cette fois ci est celle des automates d'arbres alternants (ou plus exactement des sous-classes de celle-ci). Nous introduisons et étudions les automates d'arbres alternants faibles (WAA) et leur algorithmique. Nous présentons ensuite tout ou partie des algorithmes optimaux de model-checking qui en découle :
– - CTL (polynomial)
– - mu-calcul sans alternation (polynomial)
– - CTL* (PSPACE-complet)
– - mu-calcul (NP inter co-NP)
Pourquoi la complexité pourrait-elle être réduite par rapport au problème de vérification en LTL, alors que les automates sont plus complexes ? En bref, c'est parce qu'on teste l'appartenance et non l'inclusion.

10.1 Automates alternants d'arbres ; différentes conditions d'acceptance

Les arbres considérés ici sont infinis et leur branchement est variable (éventuellement infini), l'ordre des fils n'étant pas significatif. Pour être plus précis, on considère un ensemble D (par exemple l'ensemble des entiers naturels). Un arbre T (sous-entendu à branchements dans D) étiqueté par A est une application d'un ensemble $Pos(T) \subseteq D^*$ clos par préfixe (appelé *ensemble des positions de* T) dans A. Si $t \in Pos(t)$, on note $s_T(t)$ l'ensemble des successeurs de t dans T : $s_T(t) \stackrel{\text{def}}{=} \{d \mid d \in D, t \cdot d \in Pos(T)\}$.

Un automate d'arbres alternant $\mathcal{A}$ est un tuple (A, Q, δ, q_0, F) où Q est ensemble fini d'états, $q_0 \in Q$ est l'état initial, A est l'alphabet d'entrée, supposé fini. $\delta : Q \times A \to \mathcal{B}^+(\{A, E\} \times Q)$.

La taille d'un automate alternant est (comme pour les mots) égale au nombre d'états + taille de l'alphabet + taille du système de transition. Cette dernière est définie comme la somme, pour chaque transition qui ne va pas à **false**de la taille de la formule résultat.

Un *calcul* de l'automate sur un arbre T est un arbre T_r dont la racine est étiquetée par q_0 et tous les autres nœuds sont étiquetés par un élément de $Q \times Pos(T)$. De plus, si $T_r(u) = (q, t)$, $T(t) = a$, alors $\delta(q, a)$ est défini et, il existe un ensemble (éventuellement vide) $S = \{(A, q_1), \ldots, (A, q_k), (E, q'_1), \ldots, (E, q'_m)\}$ tel que S satisfait $\delta(q, a)$ et

– pour tout $d \in s_T(t)$, pour tout $i = 1, \ldots k$, il existe un $j \in s_{T_r}(u)$ tel que $T_r(u \cdot j) = (q_i, t \cdot d)$
– pour tout $i = 1, \ldots, m$, il exite un $d_i \in s_T(t)$, il existe un $j \in s_{T_r}(u)$ tel que $T_r(u \cdot j) = (q'_i, t \cdot d_i)$

Un calcul est *réussi* s'il satisfait les conditions définies par F (ce peut être des conditions de Büchi ou à parité par exemple).

Exemple 45 Soit δ la relation de transition définie par la table :

δ	0	1
q_1	**false**	**true**
q_0	**true**	$(A, q_1) \wedge (E, q_0)$

L'état initial étant q_0, un arbre et un calcul de l'automate sont représentés sur la figure 21.

Exercice 38
Soit l'automate d'arbres alternants dont les transitions sont données par la table :

	$\begin{smallmatrix}0\\0\end{smallmatrix}$	$\begin{smallmatrix}0\\1\end{smallmatrix}$	$\begin{smallmatrix}1\\0\end{smallmatrix}$	$\begin{smallmatrix}1\\1\end{smallmatrix}$
q_0	**true**	**true**	$((A, q_2) \vee (E, q_1)) \wedge (A, q_0)$	**true**
q_1	(A, q_2)	(A, q_2)	$(A, q_2) \vee (E, q_1)$	**true**
q_2	**false**	**true**	**false**	**true**

L'état initial est q_0. Donner un calcul de l'automate sur le dépliage de la structure de Kripke représentée sur la figure 22.

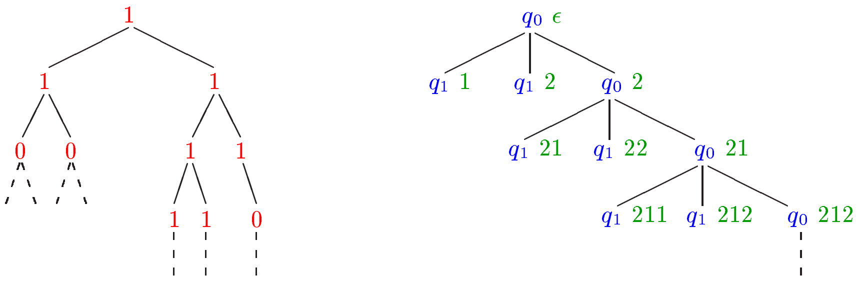

FIG. 21 – Un exemple de calcul d'un automate alternant d'arbres

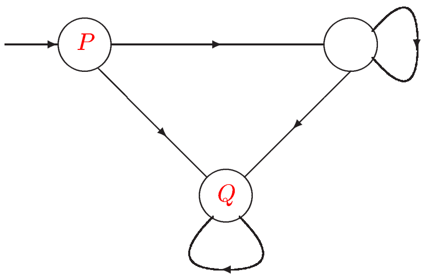

FIG. 22 – Une structure de Kripke

La *condition d'acceptance de Büchi* est donnée par un sous-ensemble Q_f de Q. Un calcul ρ est alors réussi si tout chemin infini de ρ contient une infinité d'éléments de Q_f.

La *condition d'acceptance à parité* est donnée par une application de rang r de l'ensemble des états dans $\mathbb{N}$: Un calcul ρ est alors réussi si, pour tout chemin infini π de ρ, le minimum des rangs des états apparaissant infiniment souvent dans π est pair.

10.1.1 Automates alternants faibles

Un automate alternant d'arbres de Büchi est *faible* s'il a une condition d'acceptance de Büchi $Q_f \subseteq Q$ et, de plus, il existe une partition de Q en ensembles $Q_1, \ldots, Q_n$ telle que, pour tout i, ou bien $Q_i \subseteq Q_f$ (et dans ce cas Q_i est un ensemble acceptant), ou bien $Q_i \cap Q_f = \emptyset$ (et dans ce cas c'est un ensemble de rejet). De plus, il existe un ordre partiel sur les ensembles Q_i tel que, si $q \in Q_i$ et $q' \in Q_j$ et q' apparait dans une des formules $\delta(q, a)$, alors $Q_j \leq Q_i$.

Exemple 46 Les automates des exemples 15, 18, 45 sont tous faibles. L'automate des exemples 38 et 39 n'est pas faible.

Exercice 39
Montrer que cette condition correspond à la condition d'acceptance des automates à parité faibles.

10.2 CTL et automates d'arbres alternants

Theorème 47 *Etant donnés une formule ϕ de CTL, on peut construire en temps linéaire un automate alternant faible qui accepte exactement l'ensemble des arbres qui satisfont ϕ.*

Preuve: On suppose tout d'abord, sans perte de généralité, que les négations sont poussées dans ϕ à l'intérieur des formules suivant les règles :

$$\begin{array}{rcl}
\neg\neg\psi & \rightarrow & \psi \\
\neg(\psi_1 \vee \psi_2) & \rightarrow & (\neg\psi_1) \wedge (\neg\psi_2) \\
\neg(\psi_1 \wedge \psi_2) & \rightarrow & (\neg\psi_1) \vee (\neg\psi_2) \\
\neg(A\mathbf{X}\psi) & \rightarrow & E\mathbf{X}(\neg\psi) \\
\neg(E\mathbf{X}\psi) & \rightarrow & A\mathbf{X}(\neg\psi) \\
\neg\mathbf{true} & \rightarrow & \mathbf{false} \\
\neg\mathbf{false} & \rightarrow & \mathbf{true}
\end{array}$$

Cette normalisation peut être effectuée en temps linéaire.

Si bien que les négations n'apparaissent que devant les variables propositionnelles et devant $A\,\mathcal{U}$ et $E\,\mathcal{U}$.

Les états de l'automate $\mathcal{A}_\phi$ sont alors les sous-formules de ϕ ainsi que les négations des sous-formules de la forme $A\,\mathcal{U}$ ou $E\,\mathcal{U}$. le nombre d'états est linéaire en la taille de ϕ. L'état initial est ϕ, les états finaux sont les formules de la forme $\neg A(\phi_1\,\mathcal{U}\phi_2)$ ou $\neg E(\phi_1\,\mathcal{U}\phi_2)$. La fonction de transition est définie par :

$$\begin{array}{rcll}
\delta(P, a) & \stackrel{\text{def}}{=} & \mathbf{true} & \text{Si } P \in a \\
 & & \mathbf{false} & \text{Sinon} \\
\delta(\neg\phi, a) & \stackrel{\text{def}}{=} & \overline{\neg\delta(\phi, a)} & \\
\delta(\phi_1 \wedge \phi_2, a) & \stackrel{\text{def}}{=} & \delta(\phi_1, a) \wedge \delta(\phi_2, a) & \\
\delta(\phi_1 \vee \phi_2, a) & \stackrel{\text{def}}{=} & \delta(\phi_1, a) \vee \delta(\phi_2, a) & \\
\delta(A\mathbf{X}\phi_1, a) & \stackrel{\text{def}}{=} & (A, \phi_1) & \\
\delta(E\mathbf{X}\phi_1, a) & \stackrel{\text{def}}{=} & (E, \phi_1) & \\
\delta(A\phi_1\,\mathcal{U}\phi_2, a) & \stackrel{\text{def}}{=} & \delta(\phi_2, a) \vee (\delta(\phi_1, a) \wedge (A, A\phi_1\,\mathcal{U}\phi_2)) & \\
\delta(E\phi_1\,\mathcal{U}\phi_2, a) & \stackrel{\text{def}}{=} & \delta(\phi_2, a) \vee (\delta(\phi_1, a) \wedge (E, E\phi_1\,\mathcal{U}\phi_2)) &
\end{array}$$

où $\overline{\phi}$ est la normalisation en poussant les négations : on utilise le système ci-dessus ainsi que les règles

$$\begin{array}{rcl}
\neg(A, \psi) & \rightarrow & (E, \overline{\psi}) \\
\neg(E, \psi) & \rightarrow & (A, \overline{\psi})
\end{array}$$

La preuve que cet automate accepte bien les arbres qui satisfont ϕ est laissée au lecteur ; il s'agit d'une double récurrence, comme dans la preuve du théorème 17. L'automate est faible : il suffit de choisir pour partition l'ensemble des singletons $\{q\}$ et pour ordre $\phi_1 \geq \phi_2$ si ϕ_2 est une sous-formule de ϕ_1 ou bien la négation d'une sous-formule stricte de ϕ_1. On peut vérifier qu'il s'agit bien d'une relation d'ordre sur les états. □

Exemple 48 Soit ϕ la formule $\neg A(P\,\mathcal{U}(A\mathbf{X}\neg P))$. La fonction de transition associée est donnée par la table :

δ	0	1
ϕ	(E, P)	$((E, P)) \wedge ((E, \phi))$
P	**false**	**true**

Exercice 40
Calculer la relation de transition de l'automate correspondant à la formule $A[(E(P\,\mathcal{U}A\mathbf{X}Q))\,\mathcal{U}\neg P]$.

10.3 Satisfaisabilité de formules CTL

On peut tout d'abord se ramener aux structures à branchement borné :

Lemme 49 ([ES84]) *Soit ϕ une formule de CTL. Soit d le nombre d'occurrences de E, A dans la formule ϕ. ϕ est satisfaisable ssi il existe une structure de Kripke $\mathcal{K}$ dont le branchement maximal est $max(d, 1)$ et telle que $\mathcal{K} \models \phi$.*

Preuve: Supposons que $\mathcal{K} = (S, R, s^0, f, \mathcal{P})$ est une structure de Kripke arbitraire qui satisfait ϕ. Soient $\phi_1, \ldots, \phi_d$ les sous-formules de ϕ de la forme $E\psi$ ou $A\psi$. On construit une structure de Kripke de branchement d (ou 1 si $d = 0$) qui satisfait ϕ comme suit : pour chaque $s \in S$, on notera $\mathcal{K}_s$ la structure $(S, R, s, f, \mathcal{P})$.

- Si $\phi_i = E\mathbf{X}\psi_i$ et $\mathcal{K}_s \models \phi_i$, on choisit $s_i \in S$ tel que $\mathcal{K}_{s_i} \models \psi_i$ et $(s, s_i) \in R$
- Si $\phi_i = A\mathbf{X}\psi_i$ et $\mathcal{K}_s \not\models \phi_i$, on choisit $s_i \in S$ tel que $\mathcal{K}_{s_i} \not\models \psi_i$ et $(s, s_i) \in R$
- Si $\phi_i = E(\psi_i \,\mathcal{U} \psi'_i)$ et $\mathcal{K}_s \models \phi_i$, alors il existe une suite $s = t_0, \ldots, t_n$ de sommets de S telle que $(t_j, t_{j+1}) \in R$ et $\mathcal{K}_{t_j} \models \psi_i$ pour $j < n$ et $\mathcal{K}_{t_n} \models \psi'_i$. On suppose de plus que cette séquence est de longueur minimale. On choisit alors $s_i = t_1$ si $n \geq 1$ et s_i arbitraire tel que $(s, s_i) \in R$ si $n = 0$.
- Si $\phi = A(\psi_i \,\mathcal{U} \psi'_i)$ et $\mathcal{K}_s \not\models \phi_i$, alors ou bien il existe une suite infinie $s = t_0, t_1, \ldots, t_n, \ldots$ telle que $(t_j, t_{j+1}) \in R$ et $\mathcal{K}_{t_j} \models \psi_i \wedge \neg\psi'_i$ et dans ce cas on choisit $s_i = t_1$, ou bien il existe une suite finie $s = t_0, t_1, \ldots, t_n$ telle que $(t_j, t_{j+1}) \in R$ et $\mathcal{K}_{t_j} \models \psi_i$ pour $j < n$ et $\mathcal{K}_{t_n} \models \neg\psi_i \wedge \neg\psi'_i$. On choisit alors cette suite de longueur minimale. Dans ce cas, si $n > 0$, on choisit $s_i = t_1$ et si $n = 0$, s_i est un sommet arbitraire tel que $(s, s_i) \in R$.

On définit alors R' par $(s, s') \in R'$ si et seulement si $s' = s_i$ pour au moins un indice i. La structure de Kriple $\mathcal{K}'$ est, par définition $(S, R', s^0, f, \mathcal{P})$

Par construction $\mathcal{K}'$ est de branchement au plus d. De plus, par récurrence sur la taille de ψ, sous-formule de ϕ, pour tout $s \in S$, $\mathcal{K}'_s \models \psi$ si et seulement si $\mathcal{K}_s \models \psi$:

- Si $\psi = \mathbf{true}, \mathbf{false}$ c'est immédiat
- Si $\psi = P \in \mathcal{P}$, $(S, R', s, f, \mathcal{P}) \models \psi$ ssi $P \in f(s)$ ssi $(S, R, s, f, \mathcal{P}) \models \psi$.
- Si ψ est une conjonction, une disjonction ou une négation, il suffit d'appliquer l'hypothèse de récurrence
- Si $\psi = E\mathbf{X}\psi_i$, alors $(S, R, s, f, \mathcal{P}) \models \psi$ entraine que $(S, R, s_i, f, \mathcal{P}) \models \psi_i$ pour s_i défini comme ci-dessus. Comme $(s, s_i) \in R'$ par définition, on en déduit $(S, R', s, f, \mathcal{P}) \models \psi$ par hypothèse de récurrence. La réciproque vient de $R' \subseteq R$
- Si $\psi = A\mathbf{X}\psi_i$ et $\mathcal{K}_s \not\models \psi$, alors, par construction, $\mathcal{K}_{s_i} \not\models \psi_i$ et donc, par hypothèse de récurrence, $\mathcal{K}'_{s_i} \not\models \psi_i$ et ainsi $\mathcal{K}'_s \not\models \psi$ puisque $(s, s_i) \in R'$. Il en résulte que, si $\mathcal{K}'_s \models \psi$, alors $\mathcal{K}_s \models \psi$. La réciproque est une conséquence de l'inclusion $R' \subseteq R$.
- Si $\psi = E(\psi_i \,\mathcal{U} \psi'_i)$ et $(S, R, s, f, \mathcal{P}) \models \psi$, il existe une suite $s = t_0, \ldots, t_n$ de sommets de S tels que $(t_j, t_{j+1}) \in R$, $\mathcal{K}_{t_j} \models \psi_i$ pour $j < n$ et $\mathcal{K}_{t_n} \models \psi'_i$. On raisonne alors par récurrence sur la longueur n minimale d'une telle suite. Si $n = 0$, alors $\mathcal{K}_s \models \psi'_i$ et on utilise l'hypothèse de récurrence sur les sous-formules. Sinon, par construction, on peut choisir $t_1 = s_i$ et $\mathcal{K}_{s_i} \models \psi$. Alors, par hypothèse de récurrence sur la longueur de la suite et puisque $(s, s_i) \in R'$, on obtient $\mathcal{K}'_s \models \psi$.
- Si $\psi = A(\psi_i \,\mathcal{U} \psi'_i)$ et $\mathcal{K}_s \not\models \psi$, on distingue les deux cas : ou bien il existe une suite de sommets, que l'on suppose de longueur minimale, $t_0, \ldots, t_n$ telle que $\mathcal{K}_{t_j} \models \psi_i$ pour $j < n$ et $\mathcal{K}_{t_n} \not\models \psi_i$ et $\mathcal{K}_{t_n} \not\models \psi'_i$. Ou bien il existe une suite infinie t_j telle que $(t_j, t_{j+1}) \in R$ et $\mathcal{K}_{t_j} \models \psi_i \wedge \neg\psi'_i$. Dans ce dernier cas, on montre par récurrence sur j que l'on peut choisir t_{j+1} de manière à ce que $\mathcal{K}'_{t_j} \models \psi_i \wedge \neg\psi'_i$ pour tout j. Dans le premier cas, on procède comme pour le cas $E\phi \,\mathcal{U} \psi$. Dans tous les cas, on montre que $\mathcal{K}'_s \not\models \psi$. Il en résulte que, si $\mathcal{K}'_s \models \psi$, alors $\mathcal{K}_s \models \phi$. La réciproque est une conséquence de $R' \subseteq R$.

$\square$

Exercice 41
Généraliser le lemme précédent à CTL*.