Preuve:

Les états de l'automate sont les sous-formules de ϕ. Pour distinger formules et états de l'automate, ces derniers seront écrits $< \phi >$.

On suppose, sans perdre de généralité, que chaque variable est liée exactement une fois dans ϕ : pour tout x apparaissant liée dans ϕ, on note ϕ_x la sous-formule de ϕ de la forme $\mu x.\phi_1$ ou $\nu x.\phi_1$.

La relation de transition est définie par :

$$\delta(< \mathbf{true} >, a) \stackrel{\text{def}}{=} \mathbf{true},\ \delta(< \mathbf{false} >, a) \stackrel{\text{def}}{=} \mathbf{false}$$

$$\delta(< P >, a) \stackrel{\text{def}}{=} \begin{cases} \mathbf{true} & \text{Si } P \in a \\ \mathbf{false} & \text{Sinon} \end{cases}$$

$$\delta(< \neg P >, a) \stackrel{\text{def}}{=} \begin{cases} \mathbf{true} & \text{Si } P \notin a \\ \mathbf{false} & \text{Sinon} \end{cases}$$

$$\delta(< x >, \epsilon) \stackrel{\text{def}}{=} < \phi_x >$$

$$\delta(< \phi_1 \wedge \phi_2 >, \epsilon) \stackrel{\text{def}}{=} < \phi_1 > \wedge < \phi_2 >$$

$$\delta(< \phi_1 \vee \phi_2 >, \epsilon) \stackrel{\text{def}}{=} < \phi_1 > \vee < \phi_2 >$$

$$\delta(< AX\phi >, a) \stackrel{\text{def}}{=} (\square, \phi)$$

$$\delta(< EX\phi >, a) \stackrel{\text{def}}{=} (\Diamond, \phi)$$

$$\delta(< \mu y.\phi >, \epsilon) \stackrel{\text{def}}{=} < \phi >$$

$$\delta(< \nu y.\phi >, \epsilon) \stackrel{\text{def}}{=} < \phi >$$

On définit maintenant le *rang* d'un état de la façon suivante : (intuitivement, le rang correspond à la profondeur d'alternation dans ϕ) :

$$\begin{array}{rcll} r(< \mu x.\psi >) & \stackrel{\text{def}}{=} & 2 \times (a(\phi) - a(\mu x.\psi)) + 1 & \\ r(< \psi >) & \stackrel{\text{def}}{=} & 2 \times (a(\phi) - a(\psi)) & \text{Pour toutes les autres formules} \end{array}$$

La condition d'acceptance est la condition de parité (sur toute branche d'un calcul le rang minimal d'un état apparaissant infiniment souvent est pair).

Montrons que l'automate $\mathcal{A}_\phi$ accepte bien les modèles de ϕ.

Supposons d'abord que ρ est un calcul réussi de $\mathcal{A}_\phi$ sur $t_{\mathcal{K}}$.

Soit , pour toute sous-formule ψ de ϕ, $S(\psi, \rho)$ l'ensemble des $s \in S$ telles qu'il existe une position p de s dans $t_{\mathcal{K}}$ et une position de ρ étiquetée par (ψ, p).

On considère alors la substitution σ_ρ telle que $\sigma_\rho(x) = S(\phi_x, \rho)$, pour toute variable x.

On montre, par récurrence sur la taille de ψ que

$$S(\psi, \rho) \subseteq [\![\psi]\!]^{\mathcal{K}}_{\sigma_\rho}$$

Lorsque $\psi \in \{P, \neg P, \mathbf{true}, \mathbf{false}\}$, la propriété découle des définitions.

Si $\psi = \psi_1 \wedge \psi_2$, par construction de δ, pour toute position p telle que $\rho(p) = (<\psi_1 \wedge \psi_2>, w)$, il existe deux successeurs de p dans ρ étiquetés par $(<\psi_1>, w)$ et $(<\psi_2>, w)$ respectivement. Donc, si $s \in S(\psi, \rho)$, $s = t_{\mathcal{K}}\ (w)$, alors $s \in S(\psi_1, \rho) \cap S(\psi_2, \rho)$ et, par hypothèse de récurrence $S(\psi_i, \rho) \subseteq [\![\psi_i]\!]_{\sigma_\rho}$. Comme $[\![\psi_1 \wedge \psi_2]\!]^{\mathcal{K}}_{\sigma_{\rho'}}$ est, par définition, $[\![\psi_1]\!]^{\mathcal{K}}_{\sigma_{\rho'}} \cap [\![\psi_2]\!]^{\mathcal{K}}_{\sigma_{\rho'}}$, on obtient l'inclusion voulue.

Si $\psi = \psi_1 \vee \psi_2$, de la même manière que ci-dessus,

$$S(\psi_1 \vee \psi_2, \rho) \subseteq S(\psi_1, \rho) \cup S(\psi_2, \rho)$$

et, par hypothèse de récurrence $S(\psi_i, \rho) \subseteq [\![\psi_i]\!]_{\sigma_{\rho'}}$. Comme $[\![\psi_1 \vee \phi_2]\!]^{\mathcal{K}}_{\sigma_\rho}$ est, par définition, $[\![\psi_1]\!]^{\mathcal{K}}_{\sigma_\rho} \cup [\![\psi_2]\!]^{\mathcal{K}}_{\sigma_\rho}$, on obtient l'inclusion voulue.

Si $\psi = AX\psi_1$ et $p \in S(\psi, \rho)$, $\rho(p) = (<\psi>, w)$, alors, par définition, pour tout successeur $s_i = t_{\mathcal{K}}\ (w \cdot i)$ de $s = t_{\mathcal{K}}\ (w)$ dans $\mathcal{K}$, il existe un successeur p_{j_i} de p dans ρ tel que $\rho(p \cdot j_i) = (<\psi_1>, w \cdot i)$. Par hypothèse de récurrence $S(\psi_1, \rho) \subseteq [\![\psi_1]\!]^{\mathcal{K}}_{\sigma_\rho}$ et donc, pour tout i, $s_i \in [\![\psi_1]\!]^{\mathcal{K}}_{\sigma_\rho}$. Alors, par définition de $[\![AX\psi_1]\!]^{\mathcal{K}}_i\ on \sigma_\rho$, $s \in [\![AX\psi_1]\!]^{\mathcal{K}}_{\sigma_\rho}$, ce qui permet de conclure.

Si $\psi = EX\psi_1$, le raisonnement est analogue au précédent.

Si ψ est une variable x, alors $[\![x]\!]^{\mathcal{K}}_{\sigma_\rho} = S(\phi_x, \rho)$ par définition. Or, par construction de l'automate, $S(x, \rho) \subseteq S(\phi_x, \rho)$.

Si $\psi = \mu x.\phi$ et $s \in S(\psi, \rho)$, $\rho(p) = (<\psi>, w)$, $t_{\mathcal{K}}\ (w) = s$, considérons alors l'arbre $\rho|_p$ dans lequel les branches sont coupées aux variables libres de ψ. Formellement, soit E le plus grand sous-ensemble des positions de $\rho|_p$ qui soit clos par préfixe et tel que, pour tout $\pi \in E$, il existe une sous-formule θ de ψ et un mot w' tels que $\rho(p \cdot \pi) = (<\theta>, w')$. Soit t le sous-arbre de $\rho|_p$ dont les positions sont l'ensemble E. Par construction, les feuilles de t sont étiquetées par des variables z qui sont libres dans ψ.

Le calcul ρ étant réussi et le rang de ψ étant impair et minimal dans les étiquettes de t, t ne contient pas de chemin infini.

Soit encore E_ψ l'ensemble des noeuds de t étiquetés par $(<\psi>, w')$ pour un certain w'. On définit alors E_α, où α est un ordinal, par récurrence bien fondée :

- $E_0 = \emptyset$
- $E_{\alpha+1}$ est l'ensemble des positions π de E_ψ dont tous les descendants ou bien sont dans $\bigcup_{\alpha' \leq \alpha} E_{\alpha'}$ ou bien n'appartiennent pas à E_ψ
- $E_\alpha = \bigcup_{\alpha' < \alpha} E_{\alpha'}$ si α est un ordinal limite.

Montrons que p est dans l'un des ensembles E_α (pour un certain ordinal α). ** to be completed **

On montre maintenant le résultat par récurrence sur l'ordinal α : si σ est la restriction de σ_ρ aux variables libres de ψ, par récurrence sur α, p est dans l'ensemble S_α défini dans le paragraphe 10.3.

Si $\psi = \nu x.\theta$, comme, par hypothèse de récurrence, $S(\theta, \rho) \subseteq [\![\theta]\!]^{\mathcal{K}}_{\sigma_\rho}$ et que, par définition, $[\![\psi]\!]^{\mathcal{K}}_{\sigma_\rho}$ contient tous les ensembles S_1 tels que $S_1 \subseteq [\![\theta]\!]^{\mathcal{K}}_{\sigma' \cup \{x \mapsto S_1\}}$, $S(\theta, \rho) \subseteq [\![\psi]\!]^{\mathcal{K}}_{\sigma_\rho}$ et l'inclusion voulue découle de la définition des calculs.

En conclusion, on a toujours $S(\psi,\rho) \subseteq [\![\psi]\!]^{\mathcal{K}}_{\sigma_\rho}$. En particulier, si on considère la formule ϕ elle-même, $s^0 \in S(\phi,\rho) \subseteq [\![\phi]\!]^{\mathcal{K}}$ et donc $\mathcal{K} \models \phi$.

Réciproquement, supposons que $\mathcal{K} \models \phi$.

Nous allons construire un calcul réussi de l'automate, en gardant l'invariant suivant : si $\rho(p) = (<\psi>, w)$, alors $\mathcal{K}, t_{\mathcal{K}}(w), \sigma_\phi \models \psi$. ** to be completed ** $\square$

Exemple 59 Reprenons l'exemple 57 : ϕ est la formule $\mu y.(Q \vee (P \wedge EXy))$. On note encore ψ la sous-formule $Q \vee (P \wedge EXy)$ L'automate associé est défini par :

$$
\begin{array}{lclllcl}
<\phi> & \rightarrow & <\psi> & \quad & <\psi> & \rightarrow & <Q> \vee (<P> \wedge <EXy>) \\
<Q> & \xrightarrow{\substack{0\\1},\substack{1\\1}} & \textbf{true} & & <Q> & \xrightarrow{\substack{1\\0},\substack{0\\0}} & \textbf{false} \\
<P> & \xrightarrow{\substack{1\\0},\substack{1\\1}} & \textbf{true} & & <P> & \xrightarrow{\substack{0\\1},\substack{0\\0}} & \textbf{false} \\
<EXy> & \xrightarrow{\substack{0\\0},\substack{0\\1},\substack{1\\0},\substack{1\\1}} & (\Diamond, <y>) & & <y> & \rightarrow & <\psi>
\end{array}
$$

Le rang de toutes les formules sauf ϕ est 0. $r(\phi) = 1$.

Exercice 39 Soit $\mathcal{K}$ la structure de Kripke donnée dans la figure 23. Construire deux calculs de l'automate de l'exemple ci-dessus sur $t_{\mathcal{K}}$, l'un réussi, l'autre non.

Exercice 40 Calculer l'automate correspondant à la formule $\mu x.x$. Quels sont les arbres acceptés par cet automate ?

Exercice 41 Soit $\mathcal{K}$ la structure de Kripke dont les positions sont $\{s^0\} \cup \{t_i, i \in \mathbb{N}\}$ et les transitions : $s^0 \rightarrow t_i$ pour tout i et $t_{i+1} \rightarrow t_i$ pour tout i. Soit enfin f définie par : $f(s^0) = \emptyset$, $f(t_0) = \{P, Q\}$ et $f(t_i) = \{Q\}$ pour $i \geq 1$.

Calculer $[\![\mu x.((P \vee EXx) \wedge (Q \vee AXx))]\!]^{\mathcal{K}}$. S'il existe un calcul réussi de l'automate $\mathcal{A}_\phi$ sur $\mathcal{K}$, l'exhiber.

10.8 Vérification de modèles en μ-calcul

Theorème 60 *Etant donnés $\mathcal{K}$ et ϕ, décider si $\mathcal{K} \models \phi$ est dans NP∩co-NP.*

Preuve: On peut tout d'abord calculer l'automate $\mathcal{A}_\phi$ en temps linéaire (théorème 58).

On construit ensuite l'automate produit comme suit :
- l'ensemble des états est $Q \times S$
- l'état initial est $<q_0, s^0>$
- le rang est défini par $r(<q,s>) = r_\phi(q)$
- $\delta(<q,s>) = \delta_\phi\{q' \mapsto <q',s>\}$ si δ_ϕ effectue une ϵ-transition à partir de q
- $\delta(<q,s>) = \delta_\phi(q, f(s))\{(\square, q') \mapsto \bigwedge_{s \rightarrow s'} <q',s'>, \ (\Diamond, q') \mapsto \bigvee_{s\rightarrow s'} <q',s'>\}$

$\mathcal{K} \models \phi$ si et seulement si l'automate produit (un automate alternant de mots sur un alphabet à une lettre) accepte au moins un mot.

Or, d'après le corollaire 35, ce problème est dans NP$\cap$ co-NP. (C'est le problème de déterminer si le joueur 1 a une stratégie gagnante dans un jeu à parité fini).

Exercice 42 Soit ϕ une formule du μ-calcul sans alternance, montrer par un exemple que l'automate à parité construit comme dans le théorème 58 n'est pas nécessairement un automate faible.

Montrer qu'on peut associer à toute formule ϕ du μ-calcul sans alternance un automate à parité *faible* qui accepte les dépliages des structures de Kripke qui satisfont ϕ.

En déduire que la vérification de modèles pour le μ-calcul sans alternance est PTIME-complète.

10.9 Satisfaisabilité du μ-calcul

La satisfaisabilité des formules du μ-calcul se ramène au problème du vide des automates alternants d'arbres (avec condition de parité), d'après le théorème 58.

A nouveau, ce problème se ramène à la recherche du joueur ayant une stratégie gagnante dans un jeu à parité. Un tel jeu peut être construit en temps exponentiel et comporte $O(2^{P(|A|)})$ positions où P est un polynôme et le rang maximal d'une position est $Q(|A|)$ où Q est un polynôme (voir par exemple [Wil01]). Il reste à regarder plus finement les algorithmes de décision de l'existence de stratégies gagnantes dans le cas des jeux à parité finis. On peut en fait décider qui a une stratégie gagnante en temps $O(|G|^p)$ où p est le rang maximal d'une position (voir par exemple [Jur00] pour des bornes plus fines). Il en résulte un algorithme de décision en $O(2^{P(|A|)\times Q(|A|)})$:

Theorème 61 *La satisfaisabilité du μ-calcul est dans DEXPTIME.*