10 Vérification de modèles pour le μ-calcul

Nous ne présentons ici qu'une version simple du μ-calcul propositionnel introduit par D. Kozen [Koz83]. On pourra consulter par exemple l'ouvrage de synthèse [AN01] pour une introduction plus systématique. Nous adoptons ici les idées et la présentation de [**?**].

10.1 Syntaxe

On suppose donné un ensemble de variables propositionnelles $\mathcal{P}$. Les négations sont supposées poussées jusqu'aux propositions. L'ensemble des formules du μ-calcul est le plus petit ensemble tel que, si ϕ, ϕ_1, ϕ_2 sont des formules et $P \in \mathcal{P}$ alors

$\mathbf{true}, \mathbf{false}, P, \neg P$

y (variable)

$\phi_1 \wedge \phi_2, \phi_1 \vee \phi_2$

$AX\phi, EX\phi$

$\mu y.\phi, \nu y.\phi$

sont des formules.

10.2 Sémantique

$\mathcal{K}$ est une structure de Kripke d'ensemble S de configurations, ϕ est une formule comportant n variables libres $y_1, \ldots, y_n$ σ est une substitution $\{y_i \mapsto S_i \mid i \in \{1, \ldots, n\},\ S_i \subseteq S\}$.

$[\![\phi]\!]_\sigma^{\mathcal{K}}$ est défini par :

$$[\![\mathbf{true}]\!]_\sigma^{\mathcal{K}} \stackrel{\text{def}}{=} S$$

$$[\![\mathbf{false}]\!]_\sigma^{\mathcal{K}} \stackrel{\text{def}}{=} \emptyset$$

$$[\![y]\!]_\sigma^{\mathcal{K}} \stackrel{\text{def}}{=} \sigma(y)$$

$$[\![\phi \wedge \psi]\!]_\sigma^{\mathcal{K}} \stackrel{\text{def}}{=} [\![\phi]\!]_\sigma^{\mathcal{K}} \cap [\![\phi]\!]_\sigma^{\mathcal{K}}$$

$$[\![\phi \vee \psi]\!]_\sigma^{\mathcal{K}} \stackrel{\text{def}}{=} [\![\phi]\!]_\sigma^{\mathcal{K}} \cup [\![\phi]\!]_\sigma^{\mathcal{K}}$$

$$[\![AX\phi]\!]_\sigma^{\mathcal{K}} \stackrel{\text{def}}{=} \{s \in S \mid \forall s \to s',\ s' \in [\![\phi]\!]_\sigma^{\mathcal{K}}\ \}$$

$$[\![EX\phi]\!]_\sigma^{\mathcal{K}} \stackrel{\text{def}}{=} \{s \in S \mid \exists s \to s',\ s' \in [\![\phi]\!]_\sigma^{\mathcal{K}}\ \}$$

$$[\![\mu y.\phi]\!]_\sigma^{\mathcal{K}} \stackrel{\text{def}}{=} \bigcap_{\substack{S_1 \subseteq S \\ [\![\phi]\!]_{\sigma \cup \{y \mapsto S_1\}}^{\mathcal{K}} \subseteq S_1}} S_1$$

$$[\![\nu y.\phi]\!]_\sigma^{\mathcal{K}} \stackrel{\text{def}}{=} \bigcup_{\substack{S_1 \subseteq S \\ [\![\phi]\!]_{\sigma \cup \{y \mapsto S_1\}}^{\mathcal{K}} \supseteq S_1}} S_1$$

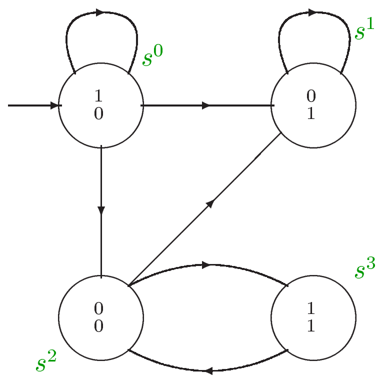

FIG. 23 – Une structure de Kripke

Si ϕ est une formule close, alors $\mathcal{K} \models \phi$ ssi $s^0 \in [\![\phi]\!]^{\mathcal{K}}_{\emptyset}$.

Exercice 34 Montrer que les définitions sémantiques de $\mu y.\phi$ et $\nu u.\phi$ correspondent bien (respectivement) au plus petit et au plus grand point fixe :

$$\begin{array}{ll} [\![\mu y.\phi]\!]^{\mathcal{K}}_{\sigma} & = [\![\phi\{y \mapsto \mu y.\phi\}]\!]^{\mathcal{K}}_{\sigma} \\ [\![\nu y.\phi]\!]^{\mathcal{K}}_{\sigma} & = [\![\phi\{y \mapsto \nu y.\phi\}]\!]^{\mathcal{K}}_{\sigma} \end{array}$$

L'exercice suivant montre comment effectivement construire les points fixes à partir des approximations successives. Elle se généralise aisément à des structures de Kripke arbitraires en définissant S_α et T_α pour un ordinal α au lieu de les définir seulement pour des entiers.

Exercice 35 Soient S_n et T_n les suites d'ensembles de positions de la structure de Kripke finie $\mathcal{K}$ définies par récurrence par :

- $S_0 = \emptyset$ et $T_0 = S$
- $S_{n+1} = [\![\phi]\!]^{\mathcal{K}}_{\sigma \cup \{x \mapsto S_n\}}$, $T_{n+1} = [\![\phi]\!]^{\mathcal{K}}_{\sigma \cup \{x \mapsto T_n\}}$.

Montrer que $\displaystyle\bigcup_{n=1}^{+\infty} S_n = [\![\mu x.\phi]\!]^{\mathcal{K}}_{\sigma}$ et $\displaystyle\bigcap_{n=1}^{+\infty} T_n = [\![\nu x.\phi]\!]^{\mathcal{K}}_{\sigma}$.

Exercice 36 Soit $\mathcal{K}$ une structure de Kripke et S_1 un sous-ensemble des configurations de $\mathcal{K}$. Montrer que

$$S_1 \subseteq [\![\phi]\!]^{\mathcal{K}}_{\sigma \cup \{x \mapsto S_1\}} \quad \Rightarrow \quad S_1 \subseteq [\![\nu x.\phi]\!]^{\mathcal{K}}_{\sigma}$$

Montrer par un contre-exemple que l'on n'a pas nécessairement $S_1 \subseteq [\![\mu x.\phi]\!]^{kripke}_{\sigma}$.

Exemple 57 Soit ϕ la formule $\mu y.(Q \vee (P \wedge EXy))$ et $\mathcal{K}$ la structure de Kripke donnée dans la figure 23.

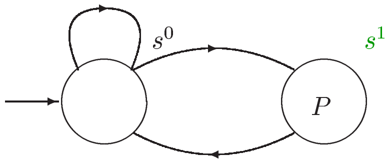

Fig. 24 – Une structure de Kripke

$[\![\phi_1]\!]^{\mathcal{K}}$ est calculé en dépliant les définitions de point fixe : calculer tout d'abord $V_1 \stackrel{\text{def}}{=} [\![Q \vee (P \wedge EXy)]\!]^{\mathcal{K}}_{y \mapsto \emptyset}$, puis $V_2 \stackrel{\text{def}}{=} [\![Q \vee (P \wedge EXy)]\!]^{\mathcal{K}}_{y \mapsto V_1}$, ...

En partant de l'ensemble vide, on obtient d'abord $\{s^1, s^3\}$, puis $\{s^0, s^1, s^3\}$ et ensuite on atteint un point fixe : $[\![\phi_1]\!]^{\mathcal{K}} = \{s^0, s^1, s^3\}$.

Soit ϕ_2 la formule $\nu y.(Q \wedge (P \vee AXy))$. Pour calculer l'interprétation de ϕ_2 sur la structure donnée dans la figure 23, on procède de la même manière que précédemment, excepté qu'on commence par l'affectation de y à S, parce qu'il s'agit d'un plus grand point fixe.

On trouve finalement $[\![\phi_2]\!]^{\mathcal{K}}_{\sigma} = \{s^1, s^3\}$.

Exercice 37 Soient $\phi_1 \stackrel{\text{def}}{=} \mu x.\nu y.((P \wedge EXy) \vee EXx)$ et $\phi_2 \stackrel{\text{def}}{=} \nu x.\mu y.((P \wedge EXy) \vee EXx)$. Calculer $[\![\phi_1]\!]^{\mathcal{K}}$ et $[\![\phi_2]\!]^{\mathcal{K}}$ sur la structure de Kripke $\mathcal{K}$ donnée dans la figure 24.

Exercice 38 A-t-on, pour toute formule ϕ et toute structure de Kripke $\mathcal{K}$, $[\![\mu x.\nu y.\phi]\!]^{\mathcal{K}} \subseteq [\![\nu y.\mu x.\phi]\!]^{\mathcal{K}}$? Justifier.

Remarquons que le μ-calcul est plus expressif que CTL*. Par exemple $EP\,\mathcal{U}Q$ s'exprime par $\mu y.Q \vee (EXy \wedge P)$. Dans l'autre sens, la propriété "P peut être atteint après un nombre pair de transitions" s'exprime en μ-calcul par $\mu y.P \vee EXEXy$ et n'a pas d'équivalent en CTL*.

En fait le μ-calcul est presque aussi expressif que SkS : si l'on ne s'autorise pas à distinguer entre les différents successeurs (i.e. on oublie leur numérotation), alors on obtient le théorème [?] : *les formules de SkS qui sont invariantes par bisimilarité sont expressibles en SkS.* Montrer ce résultat est en dehors de la portée de ces notes, mais nous pouvons préciser son énoncé et donner une traduction du μ-calcul en SkS.

10.3 Profondeur d'alternance

On suppose, par renommage, que chaque variable est liée au plus une fois dans la formule. $M(\phi)$ est alors l'ensemble des variables liées pas un μ et $N(\phi)$ est l'ensemble des variables liées par un ν. La *profondeur d'alternance* $a(\phi)$ d'une formule du μ-calcul est définie récursivement par :

– $a(\phi) = A(\phi, \emptyset, -1)$

- $A(\mathbf{true}, E, i) = A(\mathbf{false}, E, i) = A(P, E, i) = A(\neg P, E, i) = 0$
- $A(x, E, i) = E(x)$ si $E(x)$ est défini, $A(x, E, i) = 0$ sinon.
- $A(\phi_1 \wedge \phi_2, E, i) = A(\phi_1 \vee \phi_2, E, i) = \max(A(\phi_1, E, i), A(\phi_2, E, i))$
- $A(EX\phi_1, E, i) = A(AX\phi_1, E, i) = A(\phi_1, E, i)$
- $A(\mu x.\phi, E, i) = A(\phi, E \cup \{x \mapsto 0\}, 0)$ si $i = 0, -1$
- $A(\mu x.\phi, E, 1) = A(\phi, E', 0)$ où $E'(y) = E(y) + 1$ si $y \neq x$ et $E'(x) = 0$.
- $A(\nu x.\phi, E, i) = A(\phi, E \cup \{x \mapsto 0\}, 1)$ si $i = 0, -1$
- $A(\nu x.\phi, E, 0) = A(\phi, E', 1)$ où $E'(y) = E(y) + 1$ si $y \neq x$ et $E'(x) = 0$.

Dans cette définition, ϕ peut le cas échéant contenir des variables libres.
Le μ-calcul *sans alternance* est le fragment du μ-calcul pour lequel $a(\phi) = 0$.

Exercice 39 Donner la profondeur d'alternance des formules suivantes :

1. $\mu y.(Q \vee (P \wedge EXy))$
2. $\mu x.\nu y.((P \wedge EXy) \vee EXx)$
3. $\mu x.EXx \wedge (\mu z.P \vee AXz \vee (\nu y.AXy \vee Q))$
4. $\nu y.\mu x.(P \wedge y) \vee EXx$
5. $\nu x.\mu y.(Q \vee (P \wedge EXy))$

10.4 Traduction du μ-calcul en SmS

Soit $\phi(y_1, \ldots, y_n)$ une formule du μ-calcul de variables libres $y_1, \ldots, y_n$ et $\mathcal{K} = (s^0, S, \to, f)$ une structure de Kripke. Comme d'habitude la structure de Kripke est identifiée à son dépliage $t_{\mathcal{K}}$: $x_1, \ldots, x_k$ sont les ensembles de positions auxquelles $P_1, \ldots, P_k$ sont satisfaits respectivement. Z est l'ensemble des positions de $t_{\mathcal{K}}$. On suppose que le branchement de $\mathcal{K}$ est borné par m.

On définit une formule $\hat{\phi}(y_1, \ldots, y_n, y)$ telle que $[\![\phi]\!]_\sigma^{\mathcal{K}} = S$ si et seulement si $\sigma, S \models_{SmS} \hat{\phi}$, avec l'interprétation adéquate de $X_1, \ldots, X_n, Z$.

$\widehat{\mathbf{true}}(y) \stackrel{\text{def}}{=} \mathbf{true}$, $\widehat{\mathbf{false}}(y) \stackrel{\text{def}}{=} \mathbf{false}$,

$\widehat{P}(y) \stackrel{\text{def}}{=} y = x_P$, $\widehat{\neg P}(y) \stackrel{\text{def}}{=} \forall x.(x \in y \Leftrightarrow x \notin x_P)$

$\widehat{y_1}(y) \stackrel{\text{def}}{=} y = y_1$

$\widehat{\phi \wedge \psi}(y_1, \ldots, y_n, y) \stackrel{\text{def}}{=} \exists z_1, z_2.\hat{\phi}(y_1, \ldots, y_n, z_1) \wedge \hat{\phi}(y_1, \ldots, y_n, z_2) \wedge y = z_1 \cap z_2$

$\widehat{\phi \vee \psi}(y_1, \ldots, y_n, y) \stackrel{\text{def}}{=} \exists z_1, z_2.\hat{\phi}(y_1, \ldots, y_n, z_1) \wedge \hat{\phi}(y_1, \ldots, y_n, z_2) \wedge y = z_1 \cup z_2$

$$\widehat{EX\phi}(y_1, \ldots, y_n, y) \stackrel{\text{def}}{=} \exists z.\hat{\phi}(y_1, \ldots, y_n, z) \wedge \forall x(x \in y \Leftrightarrow (x \in Z \wedge \bigvee_{i=1}^{m} x \cdot i \in z))$$

$$\widehat{AX\phi}(y_1, \ldots, y_n, y) \stackrel{\text{def}}{=}$$
$$\exists z.\hat{\phi}(y_1, \ldots, y_n, z) \wedge \forall x(x \in y \Leftrightarrow (x \in Z \wedge \bigwedge_{i=1}^{m} (x \cdot i \in Z \Rightarrow x \cdot i \in z)))$$

$$\widehat{\mu x.\phi}(y_1, \ldots, y_n, y) \stackrel{\text{def}}{=}$$
$$\hat{\phi}(y_1, \ldots, y_n, y, y) \wedge y \subseteq Z \wedge \forall z.(z \subseteq Z \wedge \hat{\phi}(y_1, \ldots, y_n, z, z) \Rightarrow y \subseteq z)$$

$\widehat{\nu x.\phi}(y_1, \ldots, y_n, y) \stackrel{\text{def}}{=}$
$\hat{\phi}(y_1, \ldots, y_n, y, y) \wedge y \subseteq Z \wedge \forall z.(z \subseteq Z \wedge \hat{\phi}(y_1, \ldots, y_n, z, z) \Rightarrow z \subseteq y)$

10.5 μ-calcul et automates alternants

Tout d'abord, on étend légèrement la définition des automates alternants en autorisant les ϵ-transitions : en plus des transitions habituelles, on peut désormais avoir des transitions $\delta(q, \epsilon) \in \mathcal{B}^+(Q)$. Dans le cas où il existe une ϵ-transition à partir de q, on fait l'hypothèse qu'il n'existe aucune autre transition à partir de q.

La définition d'un calcul de l'automate est alors légèrement modifiée également : si $T_r(p) = (q, w)$ et que l'automate effectue une ϵ-transition à partir de q, alors il existe un ensemble $S = \{q_1, \ldots, q_n\}$ d'états tels que $S \models \delta(q, \epsilon)$ et p a $|S|$ successeurs $p \cdot 1, \ldots, p \cdot n$ dans T_r, et $T_r(p \cdot i) = (q_i, w)$ (le même w : on ne progresse pas dans la lecture de l'arbre).

On peut éviter cette modification de définition, mais au prix d'une part d'une réduction aux formules gardées du μ-calcul et d'autre part d'une étape supplémentaire dans la construction des automates.

Theorème 58 *Etant donnée une formule ϕ du μ-calcul, on peut calculer en temps $O(|\phi|)$ un automate alternant d'arbres avec condition de parité $\mathcal{A}_\phi$ qui accepte les modèles de ϕ.*

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 :

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

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

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

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

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

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

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

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

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

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

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 $t_{\mathcal{K}}$. On peut supposer sans perdre de généralité qu'il est minimal dans le sens suivant : pour toute position p de ρ telle que $\rho(p)=(<\psi>,w)$ et $t_{\mathcal{K}}\ (w)=s$

- Ou bien l'automate effectue une ϵ-transition sur $<\psi>$ et il existe un ensemble $E=\{q_1,\ldots,q_n\}$ d'états *minimal* tel que $E\models\delta(<\psi>,\epsilon)$ et p a exactement n fils étiquetés respectivement par $(q_1,w),\ldots,(q_n,w)$
- Ou bien l'automate n'effectue pas de ϵ-transition et il existe un ensemble $E=\{(\Box,q_1),\ldots,(\Box,q_n),(\Diamond,q'_1),\ldots,(\Diamond,q'_m)\}$ *minimal* tel que $E\models\delta(q,s)$ et p a pour fils, exactement $\{p\cdot j_{d,i}\mid d\in s_{t_{\mathcal{K}}}\ (s),1\le i\le n\}\cup\{p\cdot k_i\mid 1\le i\le m\}$ avec $\rho(p\cdot j_{d,i})=(q_i,w\cdot d)$ et $\rho(p\cdot k_i)=(q'_i,w\cdot d_i)$.

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 $[\![AX\psi_1]\!]^{\mathcal{K}}_{\sigma_\rho}$, $s\in[\![AX\psi_1]\!]^{\mathcal{K}}_{\sigma_\rho}$, ce qui permet de conclure.