Indécidabilité de la validité d'une formule en logique du premier ordre

Leçons : 914 ; 924

Références : HUTH–RYAN, *Logic in computer science* (p.133) [?] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 812) [?]

Remarques :
La référence peut différer de la version que j'écris ci-dessous, car j'ai écris le développement en faisant la réduction moi-même (en m'appuyant tout de même sur le polycopié de François Schwarzentruber). Puis durant l'année, on a trouvé une référence, donc je la mets ici mais je ne m'en suis pas servi pour écrire le développement.

On utilise ici un schéma de preuve classique (la réduction) pour montrer l'indécidabilité de la validité en logique du premier ordre, ce qui permet d'illustrer la leçon 914. Ce problème s'intègre aussi dans la leçon 924 puisque d'une part, la preuve de la réduction met en jeu des manipulations de modèles et d'autre part, ce résultat montre l'indécidabilité de la théorie vide.

Prérequis :

- indécidabilité du problème Post
- bien différencier la syntaxe et la sémantique de la logique du premier ordre
- notions de modèles et théorie en logique du premier ordre

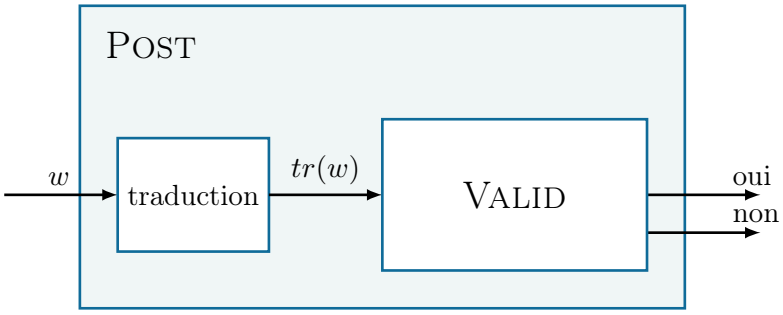
Introduction :
On va montrer que la validité d'une formule close en logique du premier ordre est un problème indécidable. Pour cela on va réduire Post à Valid.

Théorème 1. Le problème

Valid { entrée : une formule φ close en logique du premier ordre
sortie : oui si φ est valide, non sinon

est indécidable

Démonstration : On va réduire le problème Post au problème Valid. On sait que le problème Post est indécidable [1], donc si on réduit le problème Post au problème Valid, il sera lui aussi indécidable, car s'il était décidable, on rendrait le problème Post décidable, ce qui serait absurde.



1. voir appendice

On se place sur l'alphabet $\Sigma = \{a, b\}$. Soit w une instance du problème de Post, autrement dit un ensemble fini de N tuiles de la forme $\boxed{\begin{array}{|c|}\hline u_i \\ \hline v_i \\ \hline \end{array}}$, pour i allant de 1 à N avec u_i et v_i des mots sur l'alphabet Σ. On suppose que la tuile $\boxed{\begin{array}{|c|}\hline \varepsilon \\ \hline \varepsilon \\ \hline \end{array}}$ n'est pas dans w[2]. On rappelle que le problème de Post est de savoir s'il existe ou non une suite de tuiles telle qu'en les concaténant, les mots du haut et du bas formés par la concaténation des tuiles sont les deux mêmes.

On pose $tr(w) = (\varphi \to \psi)$ avec :

$$\varphi = p(\varepsilon, \varepsilon) \wedge \bigwedge_{i=1}^{N} \Big(\forall x \forall y \big(p(x, y) \to p(u_i(x), v_i(y)) \big) \Big)$$

$$\psi = \exists x \Big(p(a(x), a(x)) \vee p(b(x), b(x)) \Big)$$

Notation :

- pour chaque mot $m = m_1 m_2 \dots m_n$, on notera $m(.) = m_1 m_2 \dots m_n(.) = m_n(m_{n-1}(\dots m_1(.) \dots))$ (pour justifier l'écriture $u_i(x)$)
- on notera $\boxed{\boxed{\begin{array}{|c|}\hline x \\ \hline y \\ \hline \end{array}}}$ une succession de tuiles de w telle que le mot du haut soit x et celui du bas y. Cela sous entend qu'en écrivant $\boxed{\boxed{\begin{array}{|c|}\hline x \\ \hline y \\ \hline \end{array}}}$, il existe une succession de tuiles de w qui forme les mots x en haut et y en bas.

Il y a deux résultats à prouver :

— $tr(.)$ est une fonction calculable, c'est bien le cas car tr effectue un calcul fini pour toute instance de Post (il y a toujours un nombre fini de tuiles, et donc cela prend un temps fini pour créer la formule $\varphi \to \psi$).

— $tr(w)$ valide SSI w est une instance positive du problème de Post.

$\boxed{\Longrightarrow}$ Pour le sens direct :

La formule $\varphi \to \psi$ est valide donc pour tout modèle $\mathcal{M}$, on a $\mathcal{M} \vDash (\varphi \to \psi)$.

On choisit le modèle $\mathcal{M}$ suivant :

- le domaine est $\mathcal{D}_{\mathcal{M}} = \Sigma^*$
- $\varepsilon^{\mathcal{M}}$ correspond à ε_{Σ^*}
- $a^{\mathcal{M}}(.) : \begin{cases} \Sigma^* & \to & \Sigma^* \\ x & \mapsto & xa \end{cases}$
- $b^{\mathcal{M}}(.) : \begin{cases} \Sigma^* & \to & \Sigma^* \\ x & \mapsto & xb \end{cases}$
- $p^{\mathcal{M}}(.,.) : \begin{cases} (\Sigma^*)^2 & \to & \{0,1\} \\ (x, y) & \mapsto & \begin{cases} 1 & \text{si } \boxed{\boxed{\begin{array}{|c|}\hline x \\ \hline y \\ \hline \end{array}}} \text{ existe} \\ 0 & \text{sinon} \end{cases} \end{cases}$

2. Cela ne serait pas très interessant car toute instance du problème de Post qui contient $\boxed{\begin{array}{|c|}\hline \varepsilon \\ \hline \varepsilon \\ \hline \end{array}}$ est positive, il suffit de mettre la tuile $\boxed{\begin{array}{|c|}\hline \varepsilon \\ \hline \varepsilon \\ \hline \end{array}}$ pour avoir une solution. Il suffit alors de donner une formule valide comme traduction de cette instance de Post

Montrons que $\mathcal{M} \vDash \varphi$:

On a $\mathcal{M} \vDash p(\varepsilon, \varepsilon)$ [3].

Puis pour tout mot $u, v \in \Sigma^*$, on a si $\mathcal{M} \begin{bmatrix} x := u \\ y := v \end{bmatrix} \vDash p(x, y)$ cela veut dire que $\left\| \begin{array}{|c|} \hline u \\ \hline v \\ \hline \end{array} \right\|$ existe. Donc en concaténant $\left\| \begin{array}{|c|} \hline u \\ \hline v \\ \hline \end{array} \right\|$ et $\begin{array}{|c|} \hline u_i \\ \hline v_i \\ \hline \end{array}$, il existe bien $\left\| \begin{array}{|c|} \hline uu_i \\ \hline vv_i \\ \hline \end{array} \right\|$ pour tout $i \in \{1, \dots, N\}$, alors $\mathcal{M} \begin{bmatrix} x := u \\ y := v \end{bmatrix} \vDash p(u_i(x), v_i(y))$.
Donc pour tout $i \in \{1, \dots, N\}$, $\mathcal{M} \vDash \Big(\forall x \forall y \big(p(x, y) \to p(u_i(x), v_i(y))\big)\Big)$ Ainsi $\mathcal{M} \vDash \varphi$.

Or la formule $\varphi \to \psi$ est valide donc en particulier $\mathcal{M} \vDash (\varphi \to \psi)$ ainsi puisque $\mathcal{M} \vDash \varphi$ alors $\mathcal{M} \vDash \psi$. Sans perte de généralité, on peut dire que $\mathcal{M} \vDash \exists x \; p(a(x), a(x))$ (le cas pour b serait similaire). Donc il existe $\alpha \in \Sigma^*$ tel que $\mathcal{M} \big[x := \alpha\big] \vDash p(a(x), a(x))$. Donc $\left\| \begin{array}{|c|} \hline \alpha a \\ \hline \alpha a \\ \hline \end{array} \right\|$ existe. Ainsi par définition, il existe une succession de tuiles telle que le mot du haut et celui du bas soit le même. L'instance w est bien une instance positive du problème Post.

$\boxed{\Longleftarrow}$ Pour le sens indirect :

On suppose que w est une instance positive de Post donc il existe $m \geqslant 1$ tel qu'il existe $i_1, \dots, i_m \in \{1, \dots, N\}$ avec $u_{i_1} u_{i_2} \dots u_{i_m} = v_{i_1} v_{i_2} \dots v_{i_m}$.

Soit $\mathcal{M}$ un modèle. On suppose que $\mathcal{M} \vDash \varphi$, montrons que $\mathcal{M} \vDash \psi$.

Prouvons par récurrence sur k que $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_k}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_k}(\varepsilon) \end{bmatrix} \vDash p(x, y)$.

Initialisation : pour $k = 0$, on a $\mathcal{M} \vDash p(\varepsilon, \varepsilon)$ car $\mathcal{M} \vDash \varphi$.

Hérédité : On suppose que l'on a $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_k}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_k}(\varepsilon) \end{bmatrix} \vDash p(x, y)$. On veut prouver que $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_{k+1}}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_{k+1}}(\varepsilon) \end{bmatrix} \vDash p(x, y)$.
On sait que $\mathcal{M} \vDash \forall x \forall y \big(p(x, y) \to p(u_i(x), v_i(y))\big)$ pour tout $i \in \{1, \dots, N\}$, en particulier, pour $i = i_{k+1}$, on a $\mathcal{M} \vDash \forall x \forall y \big(p(x, y) \to p(u_{i_{k+1}}(x), v_{i_{k+1}}(y))\big)$. Donc $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_k}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_k}(\varepsilon) \end{bmatrix} \vDash \big(p(x, y) \to p(u_{i_{k+1}}(x), v_{i_{k+1}}(y))\big)$.
Ainsi $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_{k+1}}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_{k+1}}(\varepsilon) \end{bmatrix} \vDash p(x, y)$.

Conclusion : On a, pour tout $k \in \{1, \dots, m\}$,

$$\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_k}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_k}(\varepsilon) \end{bmatrix} \vDash p(x, y).$$

Sans perte de généralité, on suppose que $u_{i_1} u_{i_2} \dots u_{i_m}$ finit par un a. On écrit $u_{i_1} u_{i_2} \dots u_{i_m} = \tilde{u}a$ et $v_{i_1} v_{i_2} \dots v_{i_m} = \tilde{v}a$. On veut prouver que $\mathcal{M} \vDash \psi$ et on a $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_m}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_m}(\varepsilon) \end{bmatrix} \vDash p(x, y)$, donc $\mathcal{M} \begin{bmatrix} x := \tilde{u}a(\varepsilon) \\ y := \tilde{v}a(\varepsilon) \end{bmatrix} \vDash p(x, y)$, d'où $\mathcal{M} \begin{bmatrix} x := \tilde{u}a(\varepsilon) \\ y := \tilde{u}a(\varepsilon) \end{bmatrix} \vDash p(x, y)$. De ce fait il existe $\tilde{u}$ tel que $\mathcal{M} \big[x := \tilde{u}(\varepsilon)\big] \vDash p(a(x), a(x))$. Donc $\mathcal{M} \vDash \psi$. Ainsi $\mathcal{M} \vDash (\varphi \to \psi)$. Ce qui prouve que $(\varphi \to \psi)$ est valide.

□

3. car si l'on ne met aucune tuile, par définition, on a $\left\| \begin{array}{|c|} \hline \varepsilon \\ \hline \varepsilon \\ \hline \end{array} \right\|$ (on rappelle que l'on a considéré que la tuile $\begin{array}{|c|} \hline \varepsilon \\ \hline \varepsilon \\ \hline \end{array}$ n'est pas dans notre instance w)

Remarques :

Le problème de savoir si une formule du calcul propositionnel est valide est décidable, c'est le dual du problème SAT que l'on étudie dans le Théorème de Cook.

Astuces de l'agrégatif :

Je présente ce développement dans la leçon 924, en disant que la théorie vide n'est pas décidable, en effet dire qu'une formule est satisfaite par la théorie vide est une autre formulation de la validité d'une formule

On rappelle qu'on dit qu'une théorie T satisfait une formule φ, que l'on note $T \vDash \varphi$, si, pour tout modèle $\mathcal{M}$, on a

$$\mathcal{M} \vDash T \text{ implique } \mathcal{M} \vDash \varphi$$

Comme tout modèle satisfait le vide, on a

$$\emptyset \vDash \varphi \text{ est équivalent à } \varphi \text{ est valide}$$

cela justifie le fait que la validité de φ est parfois notée $\vDash \varphi$

Questions possibles :

- VALID est-il dans RE ?

  Réponse : oui

- qu'en est-il de SATFO ?

  Réponse : il est aussi indécidable mais est dans co-RE

On a appelé SATFO le problème

SATFO
- entrée : un formule φ close en logique du premier ordre
- sortie : oui si φ est satisfiable, non sinon