Pouvoir expressif des logiques : séparation

Luigi Santocanale

5 octobre 2010

1 Rappels

Définition 1.1.

- Les formules de la logique multimodale :

$$\phi := x \mid \top \mid \phi \wedge \phi \mid \neg\phi \mid [a]\phi\,,$$

où $a \in act$.

- Les programmes de PDL (sans test)

$$p := a \mid \emptyset \mid p \cup p \mid 1 \mid p \cdot p \mid p^*\,,$$

où $a \in act$, et ses formules :

$$\phi := x \mid \top \mid \phi \wedge \phi \mid \neg\phi \mid [p]\phi\,,$$

où p est un programme PDL (sans test).

- Les programmes et les formules de PDL avec test, définies par induction mutuelle :

$$\begin{aligned} p &:= a \mid \emptyset \mid p \cup p \mid 1 \mid p \cdot p \mid p^* \mid ?\phi\,,\\ \phi &:= x \mid \top \mid \phi \wedge \phi \mid \neg\phi \mid [p]\phi\,, \end{aligned}$$

où $a \in act$.

2 Séparation entre PDL et la logique modale

Soit act le programme PDL

$$act := \bigcup_{a \in act} a$$

et considérons la formule PDL suivante :

$$\phi_0 := \langle\, act^* \,\rangle(\bigwedge_{a \in act} [\,a\,]\bot)$$

qui est satisfaite dans un état s ssi il existe un chemin de s qui amène à un blocage (deadlock). Nous montrerons que

Théorème 2.1. *Il n'existe aucune formule de la logique multimodale qui est équivalente à* ϕ_0.

A ce fin nous introduisons les notions de profondeur modale k et de k-bisimilarité.

Définition 2.2. La profondeur modale d'une formule dp est definie comme suit :

$$\begin{aligned} \mathrm{dp}(x) = \mathrm{dp}(\top) &= 0 \\ \mathrm{dp}(\phi \wedge \psi) &= \max(\mathrm{dp}(\phi), \mathrm{dp}(\psi)) \\ \mathrm{dp}(\neg\phi) &= \mathrm{dp}(\phi) \\ \mathrm{dp}([\,a\,]\phi) &= 1 + \mathrm{dp}(\phi)\,. \end{aligned}$$

Si $\langle S, \{ \xrightarrow{a} \}_{a\in act}\rangle$ est un modèle et $v : X \longrightarrow P(S)$ est une valuation, posons

$$\lambda(s) = \{\, x \in X \mid s \in v(x) \,\}\,.$$

Si $\langle T, \{ \xrightarrow{a} \}_{a\in act}\rangle$ est un autre modèle (avec une autre valuation v), définissons la notion de k-bisimilarité entre $s \in S$ et $t \in T$, notée $s \sim_k t$, par induction sur $k \geq 0$:

$$\begin{aligned} s \sim_0 t \;\; &\text{ssi} \;\; \lambda(s) = \lambda(t)\,, \\ s \sim_{k+1} t \;\; &\text{ssi} \;\; \lambda(s) = \lambda(t)\,, \text{ et} \\ &\quad s \xrightarrow{a} s' \implies \exists t' \text{ t.q. } t \xrightarrow{a} t' \text{ et } s' \sim_k t' \\ &\quad t \xrightarrow{a} t' \implies \exists s' \text{ t.q. } s \xrightarrow{a} s' \text{ et } s' \sim_k t'\,. \end{aligned}$$

Proposition 2.3. *Soient* s, t *tels que* $s \sim_k t$ *et soit* ϕ *une formule multimodale telle que* $\mathrm{dp}(\phi) \leq k$. *Alors*

$$s \models \phi \quad \textit{ssi} \quad t \models \phi\,. \tag{1}$$

Démonstration. La preuve et par induction sur la structure des formules.

Si $\phi = x$, alors $\mathrm{dp}(\phi) = 0$, et (1) suit de $\lambda(s) = \lambda(t)$.

Si $\phi = \top$, alors (1) est évidente.

Si $\phi = \psi \wedge \chi$, alors $\mathrm{dp}(\psi) \leq k$ et $\mathrm{dp}(\chi) \leq k$.

$$\begin{aligned} s \models \psi \wedge \chi \;\; &\text{ssi} \;\; s \models \psi \text{ et } s \models \chi \\ &\text{ssi} \;\; t \models \psi \text{ et } t \models \chi \qquad \text{par hypothèse d'induction sur } \psi \text{ et } \chi \\ &\text{ssi} \;\; t \models \psi \wedge \chi\,. \end{aligned}$$

Si $\phi = \neg\psi$, alors on raisonne de façon semblable en sachant que $\mathrm{dp}(\psi) = \mathrm{dp}(\phi) \leq k$ et en utilisant l'hypothèse d'induction pour ψ.

Enfin, soit $\phi = [\,a\,]\psi$, de façon que $\mathrm{dp}(\psi) \leq k - 1$. Supposons que $s \models [\,a\,]\psi$ et montrons que $t \models [\,a\,]\psi$. Si $t \xrightarrow{a} t'$ alors il existe s' tel que $s \xrightarrow{a} s'$ et $s' \sim_{k-1} t'$ (on utilise ici le fait que $s \sim_k t$). De $s \models [\,a\,]\psi$ il découle $s' \models \psi$. Car $s' \sim_{k-1} t'$, $\mathrm{dp}(\psi) \leq k-1$ et $s' \models \psi$, on déduit que $t' \models \psi$ par hypothèse d'induction sur ψ.

On montre que $t \models [\,a\,]\psi$ implique $s \models [\,a\,]\psi$ de façon semblable. □

Preuve du Théorème 2.1. Supposons que ϕ soit une formule modale telle que $s \models \phi$ ssi il existe un chemin de s qui amène à un blocage.

Soit $k = \mathrm{dp}(\phi)$, et considérons le modèle $\langle \mathbf{N}, \rightarrow \rangle$, où $n \rightarrow n+1$, pour tout $n \in \mathbf{N}$:

$$0 \rightarrow 1 \rightarrow 2 \rightarrow \ldots \rightarrow k \rightarrow k+1 \rightarrow \ldots$$

Considérons aussi le modèle suivant :

$$\hat{0} \rightarrow \hat{1} \rightarrow \hat{2} \rightarrow \ldots \rightarrow \hat{k}$$

où $\lambda(\hat{n}) = \lambda(n)$. Évidemment

$$0 \not\models \phi\,, \qquad\qquad \hat{0} \models \phi\,.$$

Aussi, $0 \sim_k \hat{0}$ et donc, par la Proposition,

$$0 \models \phi\,,$$

ce qui contredit $0 \not\models \phi$. □

3 Séparation entre PDL, avec et sans test

Rappelons qu'un sous-ensemble (ou langage) $L \subseteq \Sigma^*$ est *régulier* s'il existe un automate fini qui reconnaît cet ensemble. Observez que si $\Sigma = \{\, a \,\}$ alors Σ^*, l'ensemble des mots sur cet alphabet, est – à isomorphisme près – l'ensemble $\mathbf{N}$ des entiers positifs. Par exemple, le mot *aaaaa* codera l'entier 5 ; plus en général, on peut coder un entier n comme le seul mot de longueur n sur l'alphabet $\Sigma = \{\, a \,\}$. Avec ce codage, quels sont les sous-ensembles d'entiers qui sont réguliers ? La réponse à cette question est donnée par le Lemme suivant.

Lemme 3.1. *Un ensemble $I \subseteq \mathbf{N}$ d'entiers est régulier si et seulement si il est ultimement périodique :*

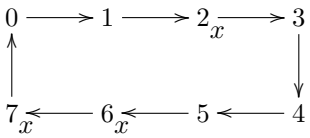
$$\exists n_0, k \geq 0 \quad \textit{t.q.} \quad x \geq n_0 \;\; \textit{implique} \;\; x \in I \;\; \textit{ssi} \;\; x + k \in I\,.$$

Démonstration. Considérez la forme d'un automate déterministe, reconnaissant l'ensemble I, sur l'alphabet $\Sigma = \{\, a \,\}$ avec une seule lettre. □

Poir $m \geq 2$, considérons le système de transition $\mathfrak{A}_m = \langle \{\, 0, \ldots, 2m-1 \,\}, \xrightarrow{a} \rangle$, avec $i \xrightarrow{a} j$ ssi $j = i + 1 \bmod 2m$. Soit aussi v_m la valuation telle que

$$v_m(y) = \begin{cases} \{\, m-2, 2m-2, 2m-1 \,\} & y = x\,, \\ \emptyset\,, & y \neq x\,. \end{cases}$$

Par exemple le couple $\mathfrak{A}_4, v_4$ est comme suit :



Considérez la formule de PDL (avec test)

$$\phi = \langle\, (?(\neg x) \cdot a)^* \cdot ?x \cdot a \,\rangle \neg x\,. \tag{2}$$

Clairement, si l'on considère $\mathfrak{A}_4$ et v_4, on a $0 \models \phi$, $1 \models \phi$, $2 \models \phi$, $4 \not\models \phi$, $5 \not\models \phi$, $6 \not\models \phi$.

Plus en général on aura :

$$\mathfrak{A}_m, v_m, k \models \phi\,, \qquad\qquad \mathfrak{A}_m, v_m, k+m \not\models \phi\,, \tag{3}$$

si $k \in \{\, 0, \ldots, m-2 \,\}$, pour tout $m \geq 4$.

Proposition 3.2. Pour toute formule ϕ de PDL, *sans test*, il existe m_ϕ, k_ϕ, avec $0 \leq k_\phi \leq m_\phi$, tels que, si m est un multiple de m_ϕ et $0 \leq k \leq m - k_\phi$, alors

$$\mathfrak{A}_m, v_m, k \models \phi \;\text{ ssi }\; \mathfrak{A}_m, v_m, k+m \models \phi\,.$$

Par cette Proposition et la relation (3), la formule ϕ de (2) ne peut pas être équivalente à une formule du PDL sans test. Nous reformulons cette observation en un théorème :

Théorème 3.3. *PDL avec test est strictement plus expressif que PDL sans test.*

Démonstration de la Proposition 3.2. Si ϕ est une variable propositionnelle distinguée de x, ou si ϕ est $\top$, alors le résultat est évidemment vrai : $m_\phi = 2$ et $k_\phi = 2$.

Le résultat est aussi vrai si ϕ est la variable x, car encore on peut poser $m_\phi = 2$ et $k_\phi = 2$.

Si $\phi = \neg\psi$, alors on peut poser $m_\phi = m_\psi$ et $k_\phi = k_\psi$.

Considérons le cas $\phi = \psi_0 \wedge \psi_1$: soit $k_\phi = \max(k_{\psi_0}, k_{\psi_1})$ et choisissons m_ϕ un multiple de m_{ψ_0}, m_{ψ_1} tel que $m_\phi \geq > k_\phi$.

Donc si m est un multiple de m_ϕ alors il est aussi un multiple de m_{ψ_0}, m_{ψ_1}. De façon semblable, si $k \leq m - k_\phi$, alors $k \leq m - k_{\psi_0}, m - k_{\psi_1}$. On a donc que

$$\begin{aligned}
&\mathfrak{A}_m, v_m, k \models \psi_0 \wedge \psi_1 \\
&\qquad\qquad \text{ssi}\;\; \mathfrak{A}_m, v_m, k \models \psi_0 \;\text{ et }\; \mathfrak{A}_m, v_m, k \models \psi_1 \\
&\qquad\qquad \text{ssi}\;\; \mathfrak{A}_m, v_m, k+m \models \psi_0 \;\text{ et }\; \mathfrak{A}_m, v_m, k+m \models \psi_1 \\
&\qquad\qquad \text{ssi}\;\; \mathfrak{A}_m, v_m, k+m \models \psi_0 \wedge \psi_1\,.
\end{aligned}$$

Considérons maintenant une formule ϕ de la forme $\langle\, r \,\rangle\psi$. Soit J_r l'ensemble d'entiers dénoté par l'expression régulière r. Rappelons que :

$$\mathfrak{A}_m, v, k \models \langle\, r \,\rangle\psi \;\text{ ssi }\; \exists j \in J_r \text{ t.q. } (k+j) \bmod 2m \models \psi\,.$$

Soit n, p tels que $n' \geq n$ implique $n' \in J_r$ ssi $n' + p \in J_r$.

Étudions d'abord l'image de J_r modulo $2m$, où m est un multiple de p. Cette image est de la forme $A \cup B$ où $A \subseteq \{\, 0, \ldots, n \,\}$ et $B \subseteq \{\, 0, \ldots, 2m-1 \,\}$ est tel que $j \in B$ ssi $j + p \mod 2m \in B$. On a donc

$$\begin{aligned}\mathfrak{A}_m, v, k \models \langle\, r \,\rangle\psi \;\text{ ssi }\; & \exists j \in A \cup B \text{ t.q. } (k+a) \bmod 2m \models \psi \\ \text{ssi }\; & \exists a \in A \,\text{t.q. } (k+a) \bmod 2m \models \psi \\ \text{ou }\; & \exists b \in B \,\text{t.q. } (k+b) \bmod 2m \models \psi\,.\end{aligned}$$

Observons que, si m est un multiple de p, alors, pour tout k,

$$\exists b \in B.\, k + b \bmod 2m \models \psi \;\text{ ssi }\; \exists b' \in B,\, k + m + b' \bmod 2m \models \psi\,,$$

car m est un multiple of p. Pour vérifier cela, choisissons $b' = b - m \mod 2m$ et $b = m + b' \mod 2m$.

En plus, si k tel que $k \leq m - k_\psi - n$ et m est un multiple de m_ψ, alors

$$\begin{aligned}\exists a \in A.\, (k+a) \bmod 2m \models \psi \;\text{ ssi }\; & \exists a \in A.\, k + a \models \psi \\ \text{ssi }\; & \exists a \in A.\, k + m + a \models \psi\,, \\ \text{ssi }\; & \exists a \in A.\, (k + m + a) \bmod 2m \models \psi\,,\end{aligned}$$

car $k + a \leq k + n \leq m - k_\psi$.

Il suffit alors de poser m_ϕ multiple de m et p, et $k_\phi = k_\psi + n$. □