

MSO

En logique du premier ordre (FO), les quantifications ne peuvent porter que sur les éléments de l'univers M . La logique du second ordre (SO) étend FO en introduisant la possibilité de quantifier sur les parties de M^k .

Formellement, en plus de la syntaxe de la logique du premier ordre, la logique du second ordre inclut :

- Une sorte de variable sur les ensembles d'individus : si S est une telle variable et t est un terme du premier ordre, alors $t \in S$ ou $S(t)$ est une formule atomique ;
- Pour tout nombre entier k il existe une sorte de variables sur les relations k -aires ;
- Pour tout entier k il existe une sorte de variables sur les fonctions de FO^k dans FO.

La logique monadique du second ordre se limite à la quantification sur les relations unaires, c'est-à-dire les propriétés booléennes sur les éléments.

Dans la suite, on considère l'alphabet $\Sigma = \{0, 1\}$. La σ -structure M_s associée au mot s contient l'intégralité des formules logiques vraies sur $\leq, P_0, P_1$ où $\leq$ est la relation d'ordre usuelle sur les entiers, P_t l'ensemble des i tels que $s_i = t$.

Si φ est une formule de MSO, s est reconnu par φ si $M_s \models \varphi$. Le langage défini par φ est l'ensemble des mots reconnus par φ .

Montrez le théorème de Büchi :

Théorème 0.1 — Büchi Un langage est MSO-définissable si et seulement si il est rationnel.

Arithmétique de Presburger

On considère dans cet exercice la logique de Presburger, c'est-à-dire la logique du premier ordre sur le langage $\{0, 1, +, =\}$. Un terme est défini par induction comme une constante, une variable, ou une addition entre deux termes. Une formule est définie par induction comme une égalité entre deux termes, ou la négation, conjonction disjonction, implication de formules, ou une quantification existentielle ou universelle par rapport à une variable d'une formules.

Par exemple, $\varphi_0 : \forall x \exists y (x = 0 \vee x = y + 1)$ et $\varphi_1 : \forall x \forall y \forall z (x + y) + z = x + (y + z)$ sont des formules en logique de Presburger.

Pour réaliser des démonstrations en arithmétique de Presburger, on considère les règles données en annexe, correspondant à la logique classique auxquelles on ajoute des axiomes et le raisonnement par récurrence.

1. Montrer que les règles suivantes sont dérivables (pour t, u, v des termes) à partir des règles d'introduction et d'élimination de l'égalité.
2. Montrer que la règle (R2) est dérivable à partir des règles de la logique classique et des autres règles de l'arithmétique de Presburger.
3. Montrer que φ_1 est démontrable.

On cherche à démontrer que l'arithmétique de Presburger est décidable. On introduit pour cela une sémantique : φ est vraie dans $\mathbb{N}$ notée $\mathbb{N} \models \varphi$ lorsque la formule est vraie en considérant les variables quantifiées comme appartenant à $\mathbb{N}$. On admet que la logique de Presburger est complète pour cette sémantique, c'est-à-dire que $\mathbb{N} \models \varphi$ implique que φ est démontrable.

A un n -uplet d'entiers $a_1, \dots, a_n$ on associe un mot $(a_1, \dots, a_n)$ de $(\Sigma = \{0, 1\}^n)^*$ qui correspond à

$$(a_1^{(0)}, \dots, a_n^{(0)})(a_1^{(1)}, \dots, a_n^{(1)}) \dots (a_1^{(m)}, \dots, a_n^{(m)})$$

où $a_i^{(0)} a_i^{(1)} \dots a_i^{(m)}$ est la décomposition binaire de a_i , en petit-boutiste avec des 0 rajoutés pour compléter à m .

Pour $x_1, \dots, x_n$, on appelle formule élémentaire une formule de la forme $x_i = 0$, $x_i = 1$, $x_i = x_j$ ou $x_i + x_j = x_k$. On dit qu'une formule $\varphi(x_1, \dots, x_n)$ est rationnelle si $L(\varphi) = \{(a_1, \dots, a_n) \in \Sigma^* \mid \mathbb{N} \models \varphi(a_1, \dots, a_n)\}$ est rationnel.

4. Montrer que les formules élémentaires sont rationnelles.
5. Montrer que les formules sans quantificateurs sont rationnelles.
6. On suppose $\varphi(x_1, \dots, x_n)$ rationnelle. Montrer que $\exists x_1 \varphi(x_1, \dots, x_n)$ est rationnelle.
7. En déduire que toute formule de la logique de Presburger est rationnelle, puis que la logique de Presburger est décidable.

Annexe : règles d'inférence de la logique de Presburger

$$\begin{array}{c}
\overline{\Gamma, \varphi \vdash \varphi} \text{ (Ax)} \quad \overline{\Gamma \vdash \top} \text{ (T)} \quad \frac{\Gamma, \psi \vdash \varphi}{\Gamma \vdash \varphi} \text{ (Aff)} \\
\\
\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi} (\rightarrow_i) \quad \frac{\Gamma \vdash \varphi \rightarrow \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi} (\rightarrow_e) \\
\\
\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi} (\wedge_i) \quad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi} (\wedge_e^g) \quad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi} (\wedge_e^d) \\
\\
\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi} (\vee_i^g) \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi} (\vee_i^d) \quad \frac{\Gamma \vdash \varphi \vee \psi \quad \Gamma, \varphi \vdash \theta \quad \Gamma, \psi \vdash \theta}{\Gamma \vdash \theta} (\vee_e) \\
\\
\frac{\Gamma, \varphi \vdash \perp}{\Gamma \vdash \neg \varphi} (\neg_i) \quad \frac{\Gamma \vdash \varphi \quad \Gamma \vdash \neg \varphi}{\Gamma \vdash \perp} (\neg_e) \\
\\
\frac{\Gamma, \neg \varphi \vdash \perp}{\Gamma \vdash \varphi} \text{ (Abs)} \\
\\
\frac{\Gamma \vdash \varphi \quad x \notin FV(\Gamma)}{\Gamma \vdash \forall x \varphi} (\forall_i) \quad \frac{\Gamma \vdash \forall x \varphi \quad FV(t) \cap BV(\varphi) = \emptyset}{\Gamma \vdash \varphi[x := t]} (\forall_e) \\
\\
\frac{\Gamma \vdash \varphi[x := t]}{\Gamma \vdash \exists x \varphi} (\exists_i) \quad \frac{\Gamma \vdash \exists x \varphi \quad \Gamma, \varphi[x := y] \vdash \psi \quad y \notin FV(\Gamma \cup \{\varphi, \psi\})}{\Gamma \vdash \psi} (\exists_e) \\
\\
\overline{\Gamma \vdash t = t} (=i) \quad \frac{\Gamma \vdash \varphi[x := t] \quad \Gamma \vdash t = u}{\Gamma \vdash \varphi[x := u]} (=e)
\end{array}$$

On ajoute les axiomes suivants :

— 0 n'est pas un successeur :

$$\vdash \forall x \neg(0 = x + 1) \quad (R_1)$$

— Tout entier non nul est un successeur :

$$\vdash \forall x (x = 0 \vee \exists y x = y + 1) \quad (R_2)$$

— L'incrémentement est inversible :

$$\vdash \forall x \forall y (x + 1 = y + 1) \rightarrow (x = y) \quad (R_3)$$

— 0 est l'élément neutre pour l'addition :

$$\vdash \forall x (x + 0 = x) \quad (R_4)$$

— L'incrémentement est associative :

$$\vdash \forall x \forall y ((x + y) + 1 = x + (y + 1)) \quad (R_5)$$

Enfin, on ajoute une infinité dénombrable de règles exprimant le principe de récurrence : pour toute formule $\varphi(x, y_1, \dots, y_n)$ ayant pour variables libres $x, y_1, \dots, y_n$:

$$\frac{\Gamma \vdash \varphi(0, y_1, \dots, y_n) \quad \Gamma \vdash \forall x (\varphi(x, y_1, \dots, y_n) \rightarrow \varphi(x + 1, y_1, \dots, y_n))}{\Gamma \vdash \forall x \varphi(x, y_1, \dots, y_n)} \text{ (rec)}$$