Logiques du second ordre

Lionel Vaux Auclair

I2M, université d'Aix-Marseille

M2 IMD

Quantifier sur les relations

- Dans le calcul des prédicats, on quantifie sur les individus (= les éléments de l'ensemble d'interprétation $|\mathcal{I}|$).
- Comment faire de la topologie, raisonner sur l'inclusion, les fonctions, les relations, *etc.* ?

Quantifier sur les relations

- Dans le calcul des prédicats, on quantifie sur les individus
  (= les éléments de l'ensemble d'interprétation $|\mathcal{I}|$).
- Comment faire de la topologie, raisonner sur l'inclusion, les fonctions, les relations, *etc.* ?
  - $\rightsquigarrow$ la théorie des ensembles : $|\mathcal{I}| =$ un *univers* d'ensembles ;

Quantifier sur les relations

- Dans le calcul des prédicats, on quantifie sur les individus (= les éléments de l'ensemble d'interprétation $|\mathcal{I}|$).
- Comment faire de la topologie, raisonner sur l'inclusion, les fonctions, les relations, *etc.* ?
  - $\rightsquigarrow$ la théorie des ensembles : $|\mathcal{I}|$ = un *univers* d'ensembles ;
  - $\rightsquigarrow$ les logiques d'ordre supérieur : on étend la quantification.

Quantifier sur les relations

- Dans le calcul des prédicats, on quantifie sur les individus (= les éléments de l'ensemble d'interprétation $|\mathcal{I}|$).
- Comment faire de la topologie, raisonner sur l'inclusion, les fonctions, les relations, *etc.* ?
  - $\rightsquigarrow$ la théorie des ensembles : $|\mathcal{I}| =$ un *univers* d'ensembles ;
  - $\rightsquigarrow$ les logiques d'ordre supérieur : on étend la quantification.

On va s'intéresser au *second ordre*.

Calcul des prédicats

- On fixe un ensemble $\mathcal{V}$ (infini, dénombrable) de variables d'individus, notées $x, y, \ldots$.
- Une signature Σ est donnée par $\mathcal{F}_\Sigma$ et $\mathcal{R}_\Sigma$ (avec les arités).
- Une formule atomique (sur la signature Σ) est une expression de la forme $R(t_1, \ldots, t_n)$ avec : $\quad R \in \mathcal{R}_\Sigma \quad t_1, \ldots, t_n \in \mathcal{T}_\Sigma \quad n = a(R)$

Définition

L'ensemble $\mathcal{F}_\Sigma$ des formules sur la signature Σ est l'ensemble des expressions de la forme :

$$A, B, \ldots \ ::= \ R(t_1, \ldots, t_n) \mid A \Rightarrow B \mid \cdots \mid \forall x A \mid \exists x A$$

Calcul des prédicats *du second ordre*

- On fixe un ensemble $\mathcal{P}$ (infini, dénombrable) de variables de prédicats notées $X, Y, \ldots$, chacune munie d'une arité.

  On pourra écrire X^n au lieu de X, pour signaler que $a(X) = n$.
- On fixe un ensemble $\mathcal{V}$ (infini, dénombrable) de variables d'individus, notées $x, y, \ldots$.
- Une signature Σ est donnée par $\mathcal{F}_\Sigma$ et $\mathcal{R}_\Sigma$ (avec les arités).
- Une formule atomique (sur la signature Σ) est une expression de la forme $R(t_1, \ldots, t_n)$ avec : $R \in \mathcal{R}_\Sigma \cup \mathcal{P}$ $\quad t_1, \ldots, t_n \in \mathcal{T}_\Sigma$ $\quad n = a(R)$

Définition

L'ensemble $\mathcal{F}_\Sigma$ des formules sur la signature Σ est l'ensemble des expressions de la forme :

$$A, B, \ldots \ ::= \ R(t_1, \ldots, t_n) \mid A \Rightarrow B \mid \cdots \mid \forall x A \mid \exists x A \mid \forall X A \mid \exists X A$$

Interprétation

- Pour interpréter une formule, on doit fixer la valeur des variables du second ordre : $E(X^n) \subset |\mathcal{I}|^n$.
- $\mathcal{I}, e, E \models X(t_1, \ldots, t_n)$ ssi $(\llbracket t_1 \rrbracket_{\mathcal{I},e}, \ldots, \llbracket t_n \rrbracket_{\mathcal{I},e}) \in E(X)$.
- $\mathcal{I}, e, E \models \forall X A$ si, pour tout $U \subset |\mathcal{I}|^n$, $\mathcal{I}, e, E[X \mapsto U] \models A$
- $\mathcal{I}, e, E \models \exists X A$ s'il existe un $U \subset |\mathcal{I}|^n$ tel que $\mathcal{I}, e, E[X \mapsto U] \models A$

Interprétation

- Pour interpréter une formule, on doit fixer la valeur des variables du second ordre : $E(X^n) \subset |\mathcal{I}|^n$.
- $\mathcal{I}, e, E \models X(t_1, \ldots, t_n)$ ssi $(\llbracket t_1 \rrbracket_{\mathcal{I},e}, \ldots, \llbracket t_n \rrbracket_{\mathcal{I},e}) \in E(X)$.
- $\mathcal{I}, e, E \models \forall X A$ si, pour tout $U \subset |\mathcal{I}|^n$, $\mathcal{I}, e, E[X \mapsto U] \models A$
- $\mathcal{I}, e, E \models \exists X A$ s'il existe un $U \subset |\mathcal{I}|^n$ tel que $\mathcal{I}, e, E[X \mapsto U] \models A$

Si on veut la complétude, il faut être un peu plus subtil. . .

Déduction au second ordre

On ajoute les règles :

$$\frac{\Gamma \vdash A \quad (X \notin \mathrm{VL}(\Gamma))}{\Gamma \vdash \forall X A}\ (\forall_i) \qquad \frac{\Gamma \vdash \forall X^n A}{\Gamma \vdash A[F/Xx_1 \cdots x_n]}\ (\forall_e)$$

$$\frac{\Gamma \vdash A[F/Xx_1 \cdots x_n]}{\Gamma \vdash \exists X A}\ (\exists_i) \qquad \frac{\Gamma \vdash \exists X A \quad \Gamma, A \vdash B \quad (X \notin \mathrm{VL}(\Gamma) \cup \mathrm{VL}(B))}{\Gamma \vdash B}\ (\exists_e)$$

Substitution

- Comme précédemment on peut substituer un terme t à une variable (d'individu) x dans une expression *en évitant les captures par les quantificateurs, quitte à renommer les variables liées* (par α-équivalence).
- Mais on peut aussi substituer une formule F à une variable du second ordre :

Définition

Si A et F sont des formules, $x_1, \ldots, x_n \in \mathcal{V}$ et $X^n \in \mathcal{P}$ alors

$$A[F/Xx_1 \cdots x_n]$$

est obtenue en remplaçant dans A chaque formule atomique de la forme

$$X(t_1, \ldots, t_n) \text{ par } F[t_1/x_1, \ldots, t_n/x_n]$$

(en évitant les captures).

Exemples niveau 0

$$\dfrac{\dfrac{\dfrac{}{X \vdash X}\;(ax)}{\vdash X \Rightarrow X}\;(\Rightarrow_i)}{\vdash \forall X\, X \Rightarrow X}\;(\forall_i)$$

$$\dfrac{\dfrac{}{\forall X\, X \vdash \forall X\, X}\;(ax)}{\forall X\, X \vdash X[A/X]}\;(\forall_e)$$

$$\shortparallel$$

$$\dfrac{\forall X\, X \vdash A}{\vdash (\forall X\, X) \Rightarrow A}\;(\Rightarrow_i)$$

Codage des connecteurs

On caractérise les constructeurs de formules par ce qu'ils impliquent :

$$
\begin{aligned}
\bot &\Leftrightarrow \forall X\, X \\
A \vee B &\Leftrightarrow \forall X (A \Rightarrow X) \Rightarrow (B \Rightarrow X) \Rightarrow X \\
A \wedge B &\Leftrightarrow \forall X (A \Rightarrow B \Rightarrow X) \Rightarrow X \\
\exists x A &\Leftrightarrow \forall Y (\forall x A \Rightarrow Y) \Rightarrow Y \\
\exists X A &\Leftrightarrow \forall Y (\forall X A \Rightarrow Y) \Rightarrow Y
\end{aligned}
$$

Codage des connecteurs

On caractérise les constructeurs de formules par ce qu'ils impliquent :

$$
\begin{aligned}
\bot &\Leftrightarrow \forall X\, X \\
A \vee B &\Leftrightarrow \forall X (A \Rightarrow X) \Rightarrow (B \Rightarrow X) \Rightarrow X \\
A \wedge B &\Leftrightarrow \forall X (A \Rightarrow B \Rightarrow X) \Rightarrow X \\
\exists x A &\Leftrightarrow \forall Y (\forall x A \Rightarrow Y) \Rightarrow Y \\
\exists X A &\Leftrightarrow \forall Y (\forall X A \Rightarrow Y) \Rightarrow Y
\end{aligned}
$$

$\rightsquigarrow$ Faites les preuves

Codage des connecteurs

On caractérise les constructeurs de formules par ce qu'ils impliquent :

$$
\begin{aligned}
\bot &\Leftrightarrow \forall X\, X \\
A \vee B &\Leftrightarrow \forall X (A \Rightarrow X) \Rightarrow (B \Rightarrow X) \Rightarrow X \\
A \wedge B &\Leftrightarrow \forall X (A \Rightarrow B \Rightarrow X) \Rightarrow X \\
\exists x A &\Leftrightarrow \forall Y (\forall x A \Rightarrow Y) \Rightarrow Y \\
\exists X A &\Leftrightarrow \forall Y (\forall X A \Rightarrow Y) \Rightarrow Y
\end{aligned}
$$

$\rightsquigarrow$ Faites les preuves

Modulo ce codage + les lois de De Morgan, on se réduit à $\Rightarrow$ et $\forall$ (au premier et second ordre) : à partir de (ax), $(\Rightarrow_i)$, $(\Rightarrow_e)$, $(\forall_i)$, $(\forall_e)$, (abs) les règles des autres connecteurs deviennent admissibles.

Égalité de Leibniz

On pose $t = u \coloneqq \forall X^1\, X(t) \Rightarrow X(u)$.

- C'est réflexif, transitif et symétrique.

Égalité de Leibniz

On pose $t = u \coloneqq \forall X^1\, X(t) \Rightarrow X(u)$.

- C'est réflexif, transitif et symétrique.

$\rightsquigarrow$ Faites les preuves

L'arithmétique du second ordre

On garde un symbole de constante 0 et un symbole de fonction unaire s, et seulement deux axiomes :

$$\forall x \neg(0 = s(x)) \qquad \forall x \forall y\, s(x) = s(y) \Rightarrow x = y$$

Le reste se définit :

- « x est un entier » s'écrit $Nat(x)$: $\forall X^1\, X(0) \Rightarrow \big(\forall y\, X(y) \Rightarrow X(s(y))\big) \Rightarrow X(x)$
- « $z = x + y$ » s'écrit $Add(x, y, z)$:
  $\forall X^3 \big(\forall x' X(x', 0, x')\big) \Rightarrow \big(\forall x' \forall y' \forall z' X(x', y', z') \Rightarrow X(x', s(y'), s(z'))\big) \Rightarrow X(x, y, z)$
- « $z = x \times y$ » s'écrit $Mul(x, y, z)$: $\forall X^3 \big(\forall x' X(x', 0, 0)\big) \Rightarrow$
  $\big(\forall x' \forall y' \forall z' \forall w' X(x', y', z') \Rightarrow Add(x', z', w') \Rightarrow X(x', s(y'), w')\big) \Rightarrow X(x, y, z)$

On prouve par exemple $\forall x \forall y\, Nat(x) \Rightarrow Nat(y) \Rightarrow \exists! z\, Nat(z) \wedge Add(x, y, z)$.

L'arithmétique du second ordre = l'analyse

On garde un symbole de constante 0 et un symbole de fonction unaire s, et seulement deux axiomes :

$$\forall x \neg(0 = s(x)) \qquad \forall x \forall y\, s(x) = s(y) \Rightarrow x = y$$

Le reste se définit :

- « x est un entier » s'écrit $Nat(x)$: $\forall X^1\, X(0) \Rightarrow \big(\forall y\, X(y) \Rightarrow X(s(y))\big) \Rightarrow X(x)$
- « $z = x + y$ » s'écrit $Add(x, y, z)$: $\forall X^3 \big(\forall x' X(x', 0, x')\big) \Rightarrow \big(\forall x' \forall y' \forall z' X(x', y', z') \Rightarrow X(x', s(y'), s(z'))\big) \Rightarrow X(x, y, z)$
- « $z = x \times y$ » s'écrit $Mul(x, y, z)$: $\forall X^3 \big(\forall x' X(x', 0, 0)\big) \Rightarrow \big(\forall x' \forall y' \forall z' \forall w' X(x', y', z') \Rightarrow Add(x', z', w') \Rightarrow X(x', s(y'), w')\big) \Rightarrow X(x, y, z)$

On prouve par exemple $\forall x \forall y\, Nat(x) \Rightarrow Nat(y) \Rightarrow \exists! z\, Nat(z) \wedge Add(x, y, z)$.
Bonus : on peut quantifier sur les relations entre entiers (et donc les réels).

Références

- Le chapitre 9 de *Lambda-calcul, types et modèles* de Krivine.
- Le chapitre 6 du David–Nour–Raffalli (surtout le développement de PA2).