Alexandre DIKOVSKY
Université de Nantes

Logique Mathématique pour l'Informatique

Cours 10. Expressivité de $\mathcal{L}^1$.

10.1. Paradoxes. Théories élémentaires.

Les interprétations du premier ordre n'imposent pas de contraintes sur la nature des domaines. Ceci peut conduire à des paradoxes.

Exemple 1. *Considérons une interprétation I_0 dont le domaine est constitué des ensembles qui ne sont pas ses propres éléments :*
(1) $D_{I_0} =_{df} \{A \text{ (un ensemble)} \mid A \notin A\}$.
$\in /2$, *le seul prédicat de sa signature Σ_0, est interprété par l'appartenance : $x \in^{I_0} y$: x est un élément de y.*
On se pose la question : est-ce-que $D_{I_0} \in D_{I_0}$?
(2) Si $D_{I_0} \in D_{I_0}$, alors selon (1), $D_{I_0} \notin D_{I_0}$.
(3) Si $D_{I_0} \notin D_{I_0}$, alors selon la même définition (1), $D_{I_0} \in D_{I_0}$.

Les paradoxes informels sont connus depuis le $IV^{ème}$ siècle avant J.C. :

Exemple 2. *Epiménidos (un poète crétois) : $\ll$ Tous les crétois sont menteurs $\gg$.*
Cet énoncé ne peut être ni vrai, ni faux, de même que celui-ci :
$\ll$ La phrase que je lis à cet instant est fausse $\gg$.

Les paradoxes logiques mettent en question les fondements mathématiques des sciences.

Pour échapper à ce problème, D. Hilbert a avancé son programme célèbre de formalisation de la mathématique. Le programme de Hilbert devait montrer que toute classe importante de modèles $\mathcal{M}$ est axiomatisable.

Définition 1. *Une classe de modèles est* axiomatisable *si elle dispose d'une théorie élémentaire A : $Th^1(A) = Tm^1(\mathcal{M})$ avec l'ensemble des axiomes A énuméré par un algorithme.*

Par exemple, $Tm^1(\mathcal{G})$, la théorie des groupes, est axiomatisable dans ce sens : $Th^1(EQ_{gr} \cup \mathbf{Gr}) = Tm^1(\mathcal{G})$ parce que l'axiomatique $EQ_{gr} \cup \mathbf{Gr}$ est finie.

Mais le programme d'Hilbert a échoué, même pour le modèle standard **Ar** de l'arithmétique. K. Gödel a montré que $Tm^1(\mathbf{Ar})$ n'est pas axiomatisable. Voici les idées majeures qui se trouvent à la base de ce résultat fondamental.

Remarque. Soit $\Sigma_1 \subseteq \Sigma_2$ une restriction de la signature Σ_2 (Σ_1 contient au moins un prédicat). Alors

$$Th^1(\mathcal{A}, \Sigma_1) = Th^1(\mathcal{A}, \Sigma_2)|_{\Sigma_1}$$

($T|_\Sigma$ est la partie de T limitée aux symboles de Σ). Par exemple, pour prouver les théorèmes arithmétiques par le calcul naturel N, il suffit d'utiliser dans les preuves seulement les formules dans la signature Σ_{ar}.

10.2. Numéraux, preuves par induction.

Pour coder les nombres dans **S**, on utilise les *numéraux* : les termes composés de la constante **0** à l'aide du foncteur $'/1$:

$$\ulcorner\ \mathbf{0}\ \urcorner \hat{=} \mathbf{0}$$
$$\ulcorner\ n\ \urcorner \hat{=} (...(\mathbf{0}')'...)'\ (n \text{ fois})$$

Par exemple : $\ulcorner\ 3\ \urcorner = \mathbf{0}'''$. $\ulcorner\ n\ \urcorner$ est un *numéral*.

En utilisant l'axiome d'induction (si), on peut prouver les théorèmes arithmétiques par l'induction sur les numéraux : soit $\Phi(x)$ une formule arithmétique avec une variable x libre. Pour prouver la formule $\forall x\ \Phi(x)$, il suffit de prouver la formule $\Phi(\mathbf{0})$ (*base*) et la formule $\forall x\ (\Phi(x) \to \Phi(x'))$ (*pas d'induction*). C'est de cette manière, que la formule $\forall t, s\ ((t + s = \mathbf{0}) \to (t = \mathbf{0}) \wedge (s = \mathbf{0}))$ a été prouvée à partir des axiomes de **S**.

10.3. Arithmétisation.

L'idée due à Gödel de l'arithmétisation provient du fait que chaque entier positif n a une représentation *unique* sous la forme :

$$(4) \qquad n = p_1^{i_1} p_2^{i_2} ... p_k^{i_k},$$

où $p_1 = 2, p_2 = 3, p_3 = 5, ...$ (entiers premiers). Alors on peut coder les expressions finies (les mots, les formules, les arbres de démonstration, etc.) par les nombres naturels.

Exemple 3. *Codes de Gödel des formules de* $\mathcal{L}^1$ *:*

$$(5) \quad g('(') = 3,\ g(')') = 5,\ g(',') = 7,\ g('\neg') = 11,\ g('\wedge') = 13,\ g('\forall') = 17$$
$$g(x_k) = 13 + 8k \quad (k = 1, 2, ...)$$
$$g(c_k) = 7 + 8k \quad (k = 1, 2, ...)$$
$$g(f_k/n) = 1 + 8(2^n * 3^k) \quad (k, n \geq 1)$$
$$g(p_k/n) = 3 + 8(2^n * 3^k) \quad (k, n \geq 1)$$

Pour $s_1, s_2 \in \Sigma,\ s_1 \neq s_2$ *ssi* $g(s_1) \neq g(s_2)$ *(unicité de codes).*

Finalement, pour une expression $u_0...u_r$ *dans* Σ *:*

$$(6) \quad CG(u_0...u_r) =_{df} 2^{g(u_0)} 3^{g(u_1)} ... p_r^{g(u_r)}$$

est le code de Gödel (CG) de $u_0...u_r$.

En utilisant les diviseurs et les restes correspondants aux types des expressions, on peut coder et décoder les expressions par des fonctions calculables.

10.4. Calculabilité.

Définition 2. *Les fonctions sur les nombres naturels :*

(7) $z(x) = \mathbf{0},\ s(x) = x',\ u_i^n(x_1, ..., x_n) = x_i$

sont récursives primitives.

Si $f/n,\ h_1/k,\ ...,\ h_n/k$ sont récursives primitives, alors la composition

(8) $f(h_1(x_1, ..., x_k), ..., h_n(x_1, ..., x_k))$

l'est aussi.

Si g/n et $h/(n+2)$ sont récursives primitives, alors la fonction

$$(9)\quad \begin{cases} f(x_1, ..., x_n, \mathbf{0}) = g(x_1, ..., x_n) \\ f(x_1, ..., x_n, s(y)) = h(x_1, ..., x_n, y, f(x_1, ..., x_n, y)) \end{cases}$$

l'est aussi.

Exemple 4.
(10) La fonction $pre(x)$ qui calcule le prédécesseur d'un entier est récursive primitive [1] *:*

$$\begin{cases} pre(\mathbf{0}) & = \mathbf{0} & (\mathbf{0} = z(x)) \\ pre(s(y)) & = y & (y = I_1^1(y)) \end{cases}$$

(11) $x + y$ est récursive primitive :

$$\begin{cases} x + \mathbf{0} = u_1^1(x) \\ x + s(y) = s(x + y) \end{cases}$$

(12) Soustraction réduite définie à partir de prédécesseur :

$$\begin{cases} x \dot{-} \mathbf{0} & = & x \\ x \dot{-} s(y) & = & pre(x \dot{-} y) \end{cases}$$

(13) $x * y$ est récursive primitive :

$$\begin{cases} x * \mathbf{0} = z(x) \\ x * s(y) = u_1^1(x) + x * y \end{cases}$$

(14) Exponentiation définie à partir de multiplication :

$$\begin{cases} x^{\mathbf{0}} & = & s(z(x)) \\ x^{s(y)} & = & x^y * x \end{cases}$$

[1] Dans la deuxième équation, $h(x, y) =_{df} I_2^2(x, y)$. C'est-à-dire, $pre(s(y)) = h(pre(y), y) = y$.

(15) Les fonctions :

$$\begin{cases} sg(\mathbf{0}) &= \mathbf{0} \\ sg(s(x)) &= \mathbf{1} \end{cases}$$

et

$$\begin{cases} \bar{sg}(\mathbf{0}) &= \mathbf{1} \\ \bar{sg}(s(x)) &= \mathbf{0}, \end{cases}$$

où $\mathbf{1}=_{df} \mathbf{0}'$, *sont récursive primitives. Ainsi les connecteurs* $\wedge, \vee, \rightarrow, \neg$ *sont aussi récursive primitifs.*
(16) Les relations $x < y$, $x = y$, $x \leq y$ *sont récursive primitives :*

$$x < y =_{df} sg(y \dot{-} x),\ x = y =_{df} \neg(x < y) \wedge \neg(y < x),\ \ x \leq y =_{df} x = y \vee x < y.$$

(17) La disjonction de longueur k *d'une fonction booléenne récursive primitive* f *est aussi récursive primitive :*

$$\begin{cases} \bigvee\limits_{i=l}^{\mathbf{0}}(f(i)) &= \mathbf{0} \\ \bigvee\limits_{i=l}^{k+1}(f(i)) &= sg(f(k+1) + \bigvee\limits_{i=l}^{k} f(i)) \end{cases}$$

(18) La relation d'être diviseur $div(x, y)$ *est récursive primitive :*

$$div(x, y) =_{df} \bigvee_{i=2}^{y-1}(i * x = y).$$

Il est clair que toute fonction récursive primitive est calculable.

Corollaire 1. *Les fonctions de codage et décodage de Gödel* $CG(x)$ *et* $CG^{-1}(x)$ *sont calculables.*

Définition 3. *Toute fonction récursive primitive est récursive partielle (RP).*
Si $g/(n+1)$ *est RP, alors* $f(x_1, ..., x_n) =_{df} \mu y\ (g(x_1, ..., x_n, y) = 0)$ *est aussi RP. Une fonction RP totale est récursive.*

La classe des fonctions calculable est très large :

Exemple 5. *La fonction carrée par excés* $sqr(x)$ *est récursive :*

$$\textit{(19)}\ sqr(x)\ =\ \mu y\ (x \leq y * y)$$

parce qu'elle est définie pour tout x.

Les fonctions récursives sont calculables ; les fonctions RP sont semi-calculables.

Théorème 1.
(i) [Ackerman] Il existe une fonction (relation) récursive non-récursive primitive.
(ii) [Church] Il existe une fonction (relation) récursive partielle non-récursive.

10.5. Expressivité.

Il s'avère que toute fonction (ou relation) calculable est exprimée en **S** et même en **R** :

Définition 4. *Une relation arithmétique R/k exprimée en* **S** *par une formule $\phi(x_1, ..., x_k)$:*
(20) *si $R(n_1, ..., n_k) = 1$, alors $\phi(\lceil n_1 \rceil, ..., \lceil n_k \rceil) \in Th^1(\mathbf{S})$,*
(21) *si $R(n_1, ..., n_k) = 0$, alors $\neg\phi(\lceil n_1 \rceil, ..., \lceil n_k \rceil) \in Th^1(\mathbf{S})$,*
Une fonction arithmétique f/k exprimée en **S** *par une formule $\psi(x_1, ..., x_k, y)$:*
(22) *si $f(n_1, ..., n_k) = n$, alors $\psi(\lceil n_1 \rceil, ..., \lceil n_k \rceil, \lceil n \rceil) \in Th^1(\mathbf{S})$,*
(23) $\forall x, y\ (\psi(\lceil n_1 \rceil, ..., \lceil n_k \rceil, x) \wedge \psi(\lceil n_1 \rceil, ..., \lceil n_k \rceil, y) \rightarrow x = y) \in Th^1(\mathbf{S})$ *pour tous numeraux $n_1, ..., n_k$.*

Théorème 2. *Les fonctions et les relations récursives partielles sont exprimées en* **R** *et en* **S**.

Exemple 6. *On peut prouver la récursivité des fonctions/relations suivantes :*
Fonction $D(u)$: si u est le CG d'une formule $\phi(x)$, alors
(24) $D(u) = \lceil CG(\phi(\lceil u \rceil)) \rceil$ *(ϕ appliquée à son propre code).*
Relation $Neg(x, y)$: x est le CG de la formule $\neg\phi$ telle que y est le CG de ϕ.
Relation $Pf(y, x)$: y est le CG d'une preuve $\Gamma \vdash_N \phi, \Gamma \subset Th^1(\mathbf{S}), x = CG(\phi)$.

10.6. Points fixes.

Un des moyens les plus puissants de Gödel est le théorème suivant de récursion. Notons $\lceil\psi\rceil$ le numéral $\lceil CG(\psi) \rceil$ (le numéral qui représente le code de ψ).

Théorème 3. *Soit $\phi(x)$ une formule arithmétique à une variable libre. Alors il existe une proposition arithmétique ψ telle que*

$$(25) \qquad \Gamma \vdash_N \ (\psi \leftrightarrow \phi(\lceil\psi\rceil))$$

pour un $\Gamma \subset Th^1(\mathbf{S})$ fini.

10.7. Théorème de Gödel de non-complétude de S.

Théorème 4. *(variante de Rosser)*
Il existe une proposition arithmétique $G_{\mathbf{S}}$ telle que : si **S** *est N-cohérent, alors*
(26) $\mathbf{Ar} \models G_{\mathbf{S}}$ *(une vérité arithmétique) et*
(27) $G_{\mathbf{S}} \notin Th^1(\mathbf{S})$ *(n'est pas prouvable dans* **S***).*

10.8. Méta-théorème de non-complétude de Gödel.

Remarquez qu'on peut exprimer la N-cohérence de **S** dans **S** :

$$(28) \qquad CONS_{\mathbf{S}} =_{df} \forall x, y, z, v\ (\mathcal{N}eg(x, z) \rightarrow \neg(\mathcal{P}f(y, x) \wedge \mathcal{P}f(v, z))).$$

Dans l'interprétation standard **Ar**, $CONS_{\mathbf{S}}$ dit qu'il n'y a pas de preuve de formules ϕ et $\neg\phi$ (N-cohérence de **S**).

Théorème 5. *(méta-théorème de non-complétude)[Gödel]*
$CONS_{\mathbf{S}} \rightarrow G_{\mathbf{S}} \in Th^1(\mathbf{S})$.

Corollaire 2. *Si* **S** *est N-cohérent, alors* $\mathbf{Ar} \models CONS_{\mathbf{S}}$ *et* $CONS_{\mathbf{S}} \notin Th^1(\mathbf{S})$.

(On ne peut pas prouver dans **S** la propriété de N-cohérence de **S** lui-même.)

Corollaire 3. *Si* **S** *est N-cohérent, alors* $Tm^1(\mathbf{Ar}) \not\subseteq Th^1(\mathbf{S})$.

10.9. Non-décidabilité de $\mathcal{L}^1$.

Il s'avère que l'ensemble des tautologies du 1^{er} ordre est non-décidable.

Remarque. Soit $\mathcal{A}$ un système d'axiomes. Alors

$$(29) \qquad \phi \in Th^1(\mathcal{A}) \ \ ssi \ \ (\wedge_{\psi\in\Delta}\psi \rightarrow \phi) \in Th^1(\emptyset)$$

pour un ensemble fini $\Delta \subseteq \mathcal{A}$.

Théorème 6. *[Church]* $Th^1(\emptyset)$ *est non-décidable.*