Alexandre DIKOVSKY
Université de Nantes Faculté des Sciences et des Techniques Master Informatique

Épistémologie : HISTOIRE DE LA LOGIQUE

COURS II. Logique formelle

1 Les sources

Gottfried Wilheim Leibniz [1646–1716] a avancé l'idée de symbolisation et de mathématisation de la logique.
Augustus De Morgan [1806–1871] et **George Bool** [1815–1864] ont introduit les premières algèbres des propositions.

Voici une définition abstraite de l'algèbre de Boole.

Définition 1. $A = (0, 1, \neg, \wedge, \vee)$ *est une algèbre de Boole si :*

$$\begin{array}{ccc}
\neg 0 = 1 & 0 \wedge x = 0 & 0 \vee x = x \\
\neg 1 = 0 & 1 \wedge x = x & 1 \vee x = 1 \\
\neg\neg x = x & \neg(x \wedge y) = \neg x \vee \neg y & \neg(x \vee y) = \neg x \wedge \neg y \\
x \wedge x = x & x \wedge y = y \wedge x & (x \wedge y) \wedge z = x \wedge (y \wedge z) \\
x \vee x = x & x \vee y = y \vee x & (x \vee y) \vee z = x \vee (y \vee z) \\
(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z) & & (x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z) \\
x \wedge \neg x = 0 & & x \vee \neg x = 1
\end{array}$$

Hugh MacColl [1838–?] définit la syntaxe de la logique propositionnelle $\mathcal{L}^p$.
Gottlob Frége [1848–1925] est le créateur de la logique contemporaine. Il était le premier a utiliser les tables de vérité pour calculer les valeurs des formules propositionnelles.
Charles Sanders Peirce [1839–1914] définie la sémantique de la logique propositionnelle en utilisant les tables de vérité.
Dans son article *Begriffschrift* [1879], **Gottlob Frége** introduit le language de la logique des prédicats $\mathcal{L}$ et utilise les quantificateurs (plus tard et indépendamment le même a été fait par C. Peirce). **Frége** avance l'idée d'un système formel (des axiomes et des règles formelles pour déduire les formules valides)[1]. Cette idée fondamentale a été appréciée seulement au début du XX^e sciècle.
Guiseppe Péano [1858–1932] introduit les systèmes axiomatiques. L'idée d'un axiome est due au géomètre grec Euclide.
Euclide [450–380 avant JC]. Dans son œuvre ≪Les Éléments≫ Euclide traite le postulat (axiome) d'unicité d'une parallèle comme une proposition dont la vérité est évidente et qui est utilisée pour prouver des théorèmes.

Définition 2. Modèle d'un système d'axiomes :

$$M \models \mathcal{A} \; : \quad M \models \phi \;\; \textit{pour tout axiome } \phi \in \mathcal{A}.$$

EX : (i) Axiomes d'égalité :

$$\mathbf{EQ} = \{x = x,\; x = y \rightarrow y = x,\; x = y \;\wedge\; y = z \rightarrow x = z\}$$

[1] Cette idée a été avancée plus tôt (sous une forme peu précise) par **Bernhard Bolzano** [1781–1848].

(ii) Axiomes des groupes :

$$\mathbf{GR} = \{x * (y * z) = (x * y) * z,\ x * x^{-1} = 1, x * 1 = x\}$$

Par exemple, le groupe additif des entiers est un modèle de $\mathbf{EQ} \cup \mathbf{GR}$:

$$(Z; +, -(\ ), 0) \models \mathbf{EQ} \cup \mathbf{GR}.$$

Définition 3. Conséquence, théorie :

$$\Gamma \Rightarrow \phi \ : \quad si\ M \models \Gamma\ ,\ alors\ M \models \phi.$$
$$Th(\mathcal{A}) = \{\phi \mid \mathcal{A} \Rightarrow \phi\}.$$

EX :

$$x^{-1} * x = 1, 1 * x = x * 1, (x * y)^{-1} = y^{-1} * x^{-1} \in Th(\mathbf{GR} \cup \mathbf{EQ}),$$

c'est-à-dire,

$$\mathbf{GR} \cup \mathbf{EQ} \Rightarrow x^{-1} * x = 1, 1 * x = x * 1, (x * y)^{-1} = y^{-1} * x^{-1}.$$

Axiomatisation en 1826 de la géométrie sans postulat d'unicité de parallèle par N. Lobatchevski [1792–1856], et plus tard par J. Bolyai [1802–1860] et par K. Gauss [1777–1855] a changé le sens du concept d'axiome : désormais ils sont vus simplement comme des propositions prises pour prémisses (sans aucun rapport avec leur validité).

Pourtant, pour assurer qu'une théorie axiomatique $Th(\mathcal{A})$ est cohérente il suffit d'en trouver un modèle : $M \models \mathcal{A}$ parce que s'il existait une contradiction $\phi, \neg\phi \in Th(\mathcal{A})$, alors elle existerait dans le modèle M lui-même : $M \models \phi, \neg\phi$. C'est en trouvant un modèle que finamement F. Klein [1849–1925] et H. Poincaré [1854–1912] ont prouvé la cohérence de la géométrie de Lobatchevski.

Ainsi on arrive à un autre genre de théories logiques : *théorie d'un modèle ou d'une classe de modèles.*

Définition 4. *$\mathcal{M}$ ètant une classe de modèles,*

$$Th(\mathcal{M}) = \{\phi \mid M \models \phi \text{ pour tout } M \in \mathcal{M}\}.$$

Parfois $Th(\mathcal{M}) = Th(\mathcal{A})$ pour une axiomatique $\mathcal{A}$. Dans ce cas on dit que $\mathcal{A}$ est une théorie élémentaire *du modèle $\mathcal{M}$. Si de plus l'axiomatique $\mathcal{A}$ est represntée par un algorithme (par exemple, si elle est finie), alors on dit que la classe $\mathcal{M}$ est* axiomatisable.

EX : La classe des groupes est axiomatisable par $\mathbf{GR} \cup \mathbf{EQ}$.

Dans son œuvre *Die Grundlagen den Arithmetik* [1893], **Gottlob Frége** expose son programme de formalisation de la mathématique en utilisant sa logique des prédicats et son système déductif *Begriffschrift.* Mais **Bertrand Russel** [1872–1970] découvre un *paradoxe* dans ce programme.

Les paradoxes informels sont connus depuis le IV^e siècle avant J.C. :

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*$\gg$.

La source des paradoxes informels est l'ambiguïté des langues naturelles. Un paradoxe dans une théorie mathématique la détruit.
Le paradoxe de **Russel** est du au fait que dans la logique de Frége sont autorisés les variables qui portent sur les prédicats. Soit $w(p)$ le prédicat $\ll p(p) \equiv 0 \gg$. Si $w(w) \equiv 1$, alors $w(w) \equiv 0$. Si $w(w) \equiv 0$, alors $w(w) \equiv 1$.
En 1910–1913, enfluencés par les travaux de **Frége**, **Alfred North Whitehead** [1861–1947] et **Bertrand Russel** publient leur œuvre capitale $\ll$*Principia Mathematica*$\gg$ où ils lancent leur programme de formalisation de la mathématique en termes logiques et systématisent les moyens de preuve formelle de manière que les paradoxes soient évités.
David Hilbert [1862–1943] a, pour la première fois, développé ce programme en termes symboliques logiques dans le livre *D. Hilbert, W. Ackermann, Grundzüge der theoretischen Logik* [1928]. Le noyau de son programme consiste en l'idée de fonder toute théorie mathématique (et la mathématique entière) comme un système axiomatique utilisant un ensemble simple de règles de déduction (c.-à-d., un système formel). Ce livre a donné naissance à la théorie de démonstrations. Voici le système $\mathcal{H}$ de Hilbert formalisant la logique des prédicats du 1^{er} ordre (c'est-à-dire sans variables sur les prédicats).
Règles de déduction :
(r_1) $\phi, \phi{\to}\psi \vdash_H \psi$ (*modus ponens*)
(r_2) $\phi \vdash_H \forall x\ \phi$ (*généralisation*)
Axiomes :
(h_1) $\phi{\to}(\psi{\to}\phi)$
(h_2) $(\phi{\to}(\psi{\to}\eta)){\to}((\phi{\to}\psi){\to}(\phi{\to}\eta))$
(h_3) $\phi \wedge \psi{\to}\phi$
(h_4) $\phi \wedge \psi{\to}\psi$
(h_5) $(\phi{\to}(\psi{\to}\phi \wedge \psi))$
(h_6) $\phi{\to}(\phi \vee \psi)$
(h_7) $\psi{\to}(\phi \vee \psi)$
(h_8) $(\phi{\to}\eta){\to}((\psi{\to}\eta){\to}((\phi \vee \psi){\to}\eta))$
(h_9) $(\phi{\to}\psi){\to}((\phi{\to}\neg\psi){\to}\neg\phi)$
(h_{10}) $\neg\neg\phi{\to}\phi$
(h_{11}) $\forall x\ \phi{\to}\phi(t)$ (*x libre pour t*)
(h_{10}) $\forall x\ (\phi{\to}\psi){\to}(\phi{\to}\forall x\ \psi)$ (*ϕ sans x libre*)
$\mathcal{H}$ est *correct* dans le sens où il déduit seulement des tautologies de $\mathcal{L}^1$. Ce système a servi de base pour la logique formelle contemporaine.

EX : Un fragment d'une preuve dans $\mathcal{H}$:

$$\dfrac{\dfrac{\dfrac{\boxed{sous\ preuve_1}}{\neg(A \ \vee\ \neg A) \to A} \qquad \dfrac{\boxed{sous\ preuve_2}}{\neg(A \ \vee\ \neg A) \to \neg A} \qquad \boxed{ax_9}}{\neg\neg(A \ \vee\ \neg A)} \qquad \boxed{ax_{10}}}{A \ \vee\ \neg A}$$

2 Crise de la logique

Kurt Gödel [1906–1979] a prouvé en 1928 que le système $\mathcal{H}$ est complet dans le sens où il dérive toute tautologie de $\mathcal{L}^1$. Ainsi, $\mathcal{H}$ est une formalisation complète de $\mathcal{L}^1$.

Il semblerait que ce résultat fonde le programme de Hilbert : pour formaliser une théorie mathématique $\mathcal{T}$, il reste à ajouter au système $\mathcal{H}$ les axiomes formalisant $\mathcal{T}$ pour en obtenir

toutes les conséquences à l'aide de $\mathcal{H}$. Par exemple, pour formaliser l'arithmétique élémentaire, il suffirait de rajouter les axiomes suivants (*l'arithmétique de Péano*) :
$\mathcal{S}$:

$(S1)$ $\neg(\mathbf{0} = x')$
$(S2)$ $x' = y' \to x = y$
$(S3)$ $x + \mathbf{0} = x$
$(S4)$ $x + y' = (x + y)'$
$(S5)$ $x * \mathbf{0} = \mathbf{0}$
$(S6)$ $x * y' = (x * y + x)$
(Si) $\phi(\mathbf{0}) \to (\forall x\ (\phi(x) \to \phi(x')) \to \forall x\ \phi(x))$

((Si) est l'axiome d'induction, ϕ est une métavariable qui porte sur les formules dans la signature de l'arithmétique ; ainsi, ce système est infini et énumérable par un algorithme simple).

Un coup de tonnerre éclata en 1932, quand Kurt Gödel a prouvé que le programme de Hilbert n'était pas réalisable. Le sens approximatif de son résultat est que la supposition de complétude de l'arithmétique $\mathcal{S}$ amène aux paradoxes mathématiques.

Définition 5. *Soit un système formel $\mathcal{F}$ (e.g. $\mathcal{H}$). Une théorie $\mathcal{T}$ est $\mathcal{F}$-cohérente s'il existe au moins une formule ϕ qui n'est pas dérivée dans $\mathcal{F} + \mathcal{T}$ ($\mathcal{T} \nvdash_F \phi$).*

La non-$\mathcal{F}$-cohérence est équivalente à l'existence d'un paradoxe : $\mathcal{T} \vdash_F \phi$ et $\mathcal{T} \vdash_F \neg\phi$ pour une formule ϕ. Pourtant, la $\mathcal{F}$-cohérence de la théorie $\mathcal{T}$ est équivalente à sa *cohérence*, c.-à-d., à l'existence d'un modèle M de $\mathcal{T}$ ($M \models \mathcal{T}$) [**Gödel, Lindenbaum**]. Plus précisement, le théorème célèbre de Gödel est le suivant.

Théorème 1. *Il existe une proposition arithmétique G_S telle que si $\mathcal{S}$ est $\mathcal{H}$-cohérente, alors*
(i) $\mathcal{S} \Rightarrow G_S$ *et*
(ii) $\mathcal{S} \nvdash_H G_S$.

Bien plus, Gödel a défini une formule arithmétique $CONS_S$, qui dans le modèle standard d'arithmétique exprime la non-existence de paradoxes prouvables dans $\mathcal{H}+\mathcal{T}$. Et il a prouvé le méta-théorème suivant de non-complétude de l'arithmétique.

Théorème 2. *Si $\mathcal{S}$ est $\mathcal{H}$-cohérente, alors une preuve*

$$\mathcal{S} \vdash_H CONS_S \to G_S$$

existe pour la formule $CONS_S$ et ainsi pour la proposition G_S du théorème 1.

Ce théorème implique qu'on ne peut pas prouver dans l'arithmetique l'énoncé de sa cohérence, si cet énoncé est vrai :

Corollaire 1. *Si $\mathcal{S}$ est $\mathcal{H}$-cohérente, alors $\mathcal{S} \Rightarrow CONS_S$ et $\mathcal{S} \nvdash_H CONS_S$.*

Une autre conséquence : on ne peut pas axiomatiser l'arithmétique standarde par une axiomatique finie, ni même énumérable par un algorithme.

3 Logique post-Gödel

La première leçon des résultats de Gödel est qu'il faut faire attention aux moyens de formalisation. Pour fonder une théorie $\mathcal{T}$, il faut utiliser une méta-théorie fondée a priori ou prendre les risques d'utiliser une théorie non-fondée à laquelle on fait confiance. Par exemple, **Gerhard Gentzen** [1936] a finalement prouvé la cohérence de l'arithmétique S, mais en utilisant une méta-théorie plus forte, qui utilise l'induction transfinie. Cette dernière doit être fondée à son tour.

Un moyen de développement de méta-théories toujours plus expressives est d'établir un classement des formules par leurs types et de décrire les propriétés des formules d'un type τ en utilisant les formules des types superieur à τ. Cette approche, dont l'idée a été proposée par A. Whitehead et B. Russel dans ≪*Principia Mathematica*≫ , exclut les paradoxes.

La deuxième leçon des résultats de Gödel provient des moyens techniques qu'il a utilisé dans les preuves de ses théorèmes. En fait, il a donné une définition des fonctions arithmétiques dont un calcul est exprimé en arithmétique. Cette idée a amené dans les années 40 **Alonso Church**, **Stephen Cole Kleene** et **Alan Turing** aux définitions différentes mais équivalentes des fonctions calculables (dites *récursives*).

Fonctions récursives Ce sont les fonctions arithmétiques définies par substitution et par récurrence à partir des fonctions primitives.

Définition 6.
0. $\mathbf{0}$ *est une constante (elle est unique).*
1. **Fonctions primitives**
(1) $s(x) = x + 1$ *% successeur*
(2) $\mathbf{Z}(x) = 0$ *% zéro*
(3) $I_n^k(x_1, ...x_k, ..., x_n) = x_k$ *% projection*
2. **Substitution**
$f(\overline{x}) = h(\overline{x}, g(\overline{x}))$
3. **Récursion primitive**
$f(\overline{x}, 0) = g(\overline{x})$
$f(\overline{x}, s(y)) = h(\overline{x}, y, f(\overline{x}, y))$
% f est définie par récurrence sur y à partir de g, h.
4. **Minimisation**
$f(\overline{x}) = \mu\ y(t(y, \overline{x}) = \mathbf{0})$
% $\mu\ y$ est la solution minimale de l'équation $t(y, \overline{x}) = 0$ (si elle existe).
La classe des fonctions récursives primitives $\mathcal{FR}^{prim}$ (récursives partielles $\mathcal{FRP}$) *est l'ensemble minimal des fonctions contenant les fonctions primitives et fermé par la substitution et la récursion primitive (et aussi par la minimisation).*

Exemple 1. *(1)* **Prédécesseur** [2]

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

(2) **Addition à partir de successeur et projection**

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

(3) **Soustraction réduite à partir de prédécesseur**

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

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

(4) **Multiplication à partir d'addition et zéro**

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

(5) **Exponentiation à partir de multiplication**

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

(6) **Carré par exces à partir de multiplication et non-égalité**
Supposons que $x \geq y$ soit exprimé. Alors, la fonction

$$sqrt_{\geq}(x) = \mu y(y * y \geq x)$$

est définie pour tout x.

Définition 7. *Une fonction récursive partielle est* récursive *si elle est totale. La classe des fonctions récursives est notée $\mathcal{FR}$.*

Toute fonction récursive primitive est totale, par conséquent récursive. La majorité des fonctions calculables utilisées dans les applications réelles sont récursives primitives. Toutes les fonctions (1)-(6) le sont.

Il est clair que toute fonction récursive est calculée par un algorithme. Par ailleurs, toute fonction récursive n'est pas récursive primitive : $\mathcal{FR}^{prim} \subsetneq \mathcal{FR} \subsetneq \mathcal{FRP}$. Les résultats de Gödel, Kleene, Turing et de nombreux autres logiciens impliquent le théorème fondamental suivant.

Théorème 3. *La classe $\mathcal{FRP}$ des fonctions récursives partielles coïncide avec la classe des fonctions exprimées en arithmétique ou calculables en utilisant un langage de programmation (Machines de Turing, Pascal, C, etc...).*

Ce fait fondamental a amené à la notion suivante de décidabilité de problèmes.

Définition 8. *Un problème algorithmique (c'est-à-dire, une propriété) P est décidable, si la fonction*

$$f_P(n) \;=\; \begin{cases} 1 & , & n \in P, \\ 0 & , & n \notin P. \end{cases}$$

est récursive.

La majorité des problèmes importants qui concernent la validité des formules ou la ≪sémantique≫ des calculs s'avèrent non-décidables. Par exemple,

Théorème 4 (Church). *Le problème de validité d'une formule du 1^{er} ordre est non-décidable.*

L'évolution postérieure de la logique mathématique à donné l'origine à l'informatique contemporaine.

Références

[1] Scholz H. : *Geschichte der Logik.* Berlin : Junker u. Dunnhaupt, 1931.

[2] Kleene S. : *Mathematical logic.* N-Y, John Wiley & Sons, 1967.

[3] Cori R., Lascar D. : *Logique mathématique.* Paris, Masson, 1994.