Introduction à la Logique

version du 26 octobre 2000 – 08 h 10

Quels sont les buts de la logique ?

- Pour tous
- Pour les mathématiciens
- Pour les informaticiens

Quels sont les buts de la logique ?

Pour tous

– Comprendre la nature intime du raisonnement mathématique [a]
– Faire du “raisonnement” une théorie mathématique comme les autres.
– Donner un sens précis à ce que peut-être le vrai

dès qu’il s’agit de raisonnement et d’argumentation.

[a] et du raisonnement non mathématique !

Quels sont les buts de la logique ?

Pour les mathématiciens

– S'assurer (se convaincre ?) que les mathématiques sont exemptes de contradictions et de paradoxes.

– Apprendre une branche des mathématiques.

Quels sont les buts de la logique ?

Pour les informaticiens

– Mécaniser les processus de raisonnement.
– Exhiber les liens entre *démonstrations* et *calculs*.
– Formaliser les objets informatiques.

Ce que la logique n'est pas

Point de vue personnel

– Le fondement ultime auquel se réduisent les mathématiques, (point de vue réductionniste)
– La discipline qui va faire remplacer les humains (en général) et les mathématiciens (en particulier) par des machines (point de vue mécaniste).

La logique, une théorie mathématique

La logique est une théorie mathématique[a],

– elle utilise les mathématiques comme le font les autres branches des mathématiques,

– elle étudie des sortes particuliers d'objets mathématiques : les propositions, les théorèmes, les jugements, les démonstrations, etc.

[a] comme les autres !

Un peu d'histoire

L'histoire montre que tout ce qui est susceptible de se mathématiser se mathématise.

Au début, seuls les entiers sont des êtres mathématiques.

Puis les Anciens acceptent les rationnels et les relatifs.

A la Renaissance, les complexes (ou imaginaires) deviennent eux-aussi des êtres mathématiques.

Un peu d'histoire

Au dix-neuf siècle

– les réels (Dedekind),
– puis les fonctions (en "extension")
– et les ensembles (Cantor) deviennent des êtres mathématiques.

Au début vingtième siècle, les fonctions (en "intention") (Church et Curry) et les théorèmes (Boole, Frege etc.) deviennent des êtres mathématiques.

Aujourd'hui (1980), les démonstrations (Curry et Howard) deviennent des êtres mathématiques.

Mécaniser la logique ?

Deux positions s'affrontent.

Le mathématicien ne sera jamais battu par une machine

Alain Connes (le triangle de la pensée)

Il existe un théorème qui ne peut être prouvé que par un ordinateur

Veroff and McCune

Les algèbres de Boole peuvent être axiomatisées par le seul axiome

$$((x \mid z) \mid y) \mid ((x \mid (x \mid y)) \mid x) = y$$

où est $\mid$ est le symbole de Sheffer qui peut être interprété comme

$$x \mid y \quad = \quad \bar{x} \,\&\, \bar{y}.$$

Les deux niveaux de la logique

En logique, il y a deux niveaux qui interfèrent et qu'il ne faut pas confondre.

– La théorie, (on dit aussi parfois la théorie objet, si l'on veut être plus précis).
– La méta-théorie, c'est une mathématique dans laquelle on va raisonner sur l'objet. C'est aussi un système logique !

Les deux niveaux de la logique

Le théorie objet est l'objet logique que l'on étudie et que l'on souhaite donc formaliser.

En général, on accepte dans la méta-théorie toute la puissance du raisonnement traditionnel. Si elle est mécanisée, cela peut-être par un système formel plus ou moins puissant.

Les deux niveaux de la logique

Dans la méta-théorie, on prouve des méta-théorèmes, c-à-d des théorèmes à propos de la théorie objet.

Quelques méta-théorèmes courants sont :

- la correction,
- la cohérence,
- la complétude.

Les ingrédients de la logique

Les aspects preuves

En logique on trouve :

– un langage d'expressions bien formées : les propositions (construites avec des *connecteurs*), les jugements, etc.
  On dit aussi que c'est la *syntaxe*.

– des axiomes,

– des règles.

Les ingrédients de la logique

Les axiomes affirment que certaines propositions sont des théorèmes : on définit un prédicat unaire dans la méta-théorie.

Les règles montrent comment construire des théorèmes à partir d'autres théorèmes. On définit dans la méta-théorie,

– des fonctions des propositions vers les propositions (règles monadiques)
– ou des fonctions des couples de propositions vers les propositions (règles dyadiques)

Les ingrédients de la logique

Le but des axiomes et des règles est de former des expressions particulières, les théorèmes en construisant des objets mathématiques particuliers les démonstrations (ou preuves).

Les ingrédients de la logique

Il y a différentes sortes d'objets : propositions[a], théorèmes, etc.

Dans une logique, l'appartenance d'un objet à telle ou telle sorte se décrète par un jugement.

[a] qui ne sont pas théorèmes

Syntaxe concrète et syntaxe abstraite

Un ordinateur a besoin qu'on lui parle de la syntaxe à un bas niveau, c'est la syntaxe concrète, c-à-d les virgules, les parenthèses, les retours à la ligne, etc.

Un humain préfère une syntaxe lisible et flexible, il a besoin de la syntaxe abstraite, c-à-d plutôt la structure arborescente, donc il souhaite des opérateurs infixes, l'associativité.

Les ingrédients de la logique

Les aspects modèles

On interprète le langage dans un univers mathématique particulier : les modèles. On parle aussi de sémantique.

Les propositions qui sont “satisfaites” (dans un sens à préciser) par le modèle sont dites valides.

Correction, cohérence et complétude établissent des liens entre

– les théorèmes (propositions prouvables)

– et les tautologies (propositions valides),

c’est-à-dire entre la prouvabilité et la validité.

Les deux branches de la logique

La partie de la logique où l'on s'intéresse plutôt aux démonstrations s'appelle la la théorie de la démonstration ou théorie de la preuve (proof theory).

La partie de la logique où l'on s'intéresse plutôt à la validité s'appelle la théorie des modèles.

L'organisation du cours

Deux enseignants

– *Odile Millet-Botta*,

– *Pierre Lescanne*.

qui feront cours et TD.

Odile Millet-Botta

- La logique classique et les modèles de la logique classique,
- Le calcul des prédicats, (la logique avec quantificateurs),
- Le calcul des séquents
- PROLOG
- La théorie des ensembles.

Pierre Lescanne

– La logique intuitionniste,
– Le lien avec le calcul : le lambda calcul,
– Les modèles de la logique de la logique intuitionniste,
– D'autres logiques : logique modale, logique épistémique (ou logique de la connaissance).

Bibliographie

Un livre de base :

R. Lalement. Logique, Réduction, Résolution. Études et recherches en informatique. Masson, Paris, 1990.

Ma référence :

D. van Dalen. Logic and Structure. Springer Verlag, 1994.

Bibliographie (suite)

Un livre assez complet sur la logique de l'informatique en français :

P. Gochet, P. Gribomont. Logique. Volume 1 : méthodes pour l'informatique fondamentale, HERMES, 1990

Sur la logique épistémique :

R. Fagin, Y. Halpern, Y. Moses, and M. Y. Vardi. Reasoning about Knowledge. The MIT Press, 1995.

La logique propositionnelle
(approche à la Hilbert)

La logique propositionnelle minimale

La syntaxe

Il n'y a qu'un connecteur $\Rightarrow$

et des variables propositionnelles p, q, ..., p_1, p_2, ...

Par exemple, les expressions sont p, $p \Rightarrow q$, $(p \Rightarrow q) \Rightarrow p$.

On adopte la convention d'associativité à droite à savoir que

$$p_1 \Rightarrow (p_2 \Rightarrow \ldots \Rightarrow (p_{n-1} \Rightarrow p_n)\ldots))$$

s'écrit

$$p_1 \Rightarrow p_2 \Rightarrow \ldots \Rightarrow p_{n-1} \Rightarrow p_n$$

La méta-théorie

Je choisis comme une méta-théorie, un système logique très puissant : le Calcul des Constructions Inductifs, mécanisé dans l'assistant de preuve COQ.

A la fin du cours, on aura une meilleure idée de ce qu'est le Calcul des Constructions Inductifs

Un peu de “méta syntaxe”

$(p, q : proposition)$ signifie “pour tout p et tout q qui sont des propositions”

$Inductive$ signifie que l’on définit un concept : proposition, theorem par induction.

Le jugement *theorem*

En COQ, le jugement *theorem* appliqué à p se note $(theorem\ p)$.

Nous le noterons $\vdash p$ qui signifie que “p est un théorème”.

On omet $\vdash$ dans les règles.

Une règle

En logique propositionnelle minimale, il n'y a qu'une règle :

le Modus Ponens :

$$MP \quad \frac{p \Rightarrow q \qquad p}{q}$$

Le Modus Ponens

En COQ, MP est une fonction

$$(theorem\ p \Rightarrow q) \rightarrow (theorem\ p) \rightarrow (theorem\ q)$$

qui prend un objet du type $theorem\ p \Rightarrow q$ où $p \Rightarrow q$ est une proposition et un objet du type $theorem\ p$ où p est une proposition et fournit un objet du type $theorem\ q$.

Plus précisément, c'est une fonction qui prend quelque chose du type $p \Rightarrow q$ et rend une fonction qui à quelque chose de type p associe quelque chose de type q.

Mais c'est à peu près la même chose, à une curryfication prés !

Deux axiomes

Il y a deux axiomes appelés K et S :

K : $\quad \vdash p \Rightarrow q \Rightarrow p$

---

et

S : $\quad \vdash (p \Rightarrow q \Rightarrow r) \Rightarrow (p \Rightarrow q) \Rightarrow p \Rightarrow r$

Ne me demandez pas pour l'instant pourquoi ils s'appellent K et S !

Exercice

Prouver le lemme $B : (p \Rightarrow q) \Rightarrow (r \Rightarrow p) \Rightarrow r \Rightarrow q)$.

Une règle dérivée : la règle C

Notre but est de prouver une nouvelle règle applicable qui va nous simplifier la vie :

$$rule_C \quad \frac{p \Rightarrow q \Rightarrow r}{q \Rightarrow p \Rightarrow r}$$

Exercice

Prouver, en utilisant le lemme B, le lemme (la règle dérivée)

$$L : (theorem\ q \Rightarrow r) \rightarrow (theorem\ p \Rightarrow q) \rightarrow (theorem\ p \Rightarrow r).$$

La règle Cut

La règle Cut ou règle de coupure permet d'utiliser des théorèmes intermédiaires (des lemmes !) ici q.

$$rule_Cut \quad \frac{q \Rightarrow r \qquad p \Rightarrow q}{p \Rightarrow r}$$

Le modèle $\{0, 1\}$

Une formule est valide classiquement si elle prend la valeur 1 pour l'interprétation de $\Rightarrow$ suivante :

$\Rightarrow$	0	1
0	1	1
1	0	1

et quelles que soient les valeurs prises par les variables propositionnelles.

Exercice

1. Montrer que les axiomes $Hilbert_K$ et $Hilbert_S$ sont valides classiquement.
2. Montrer que la règle MP “préserve” les propositions valides classiquement.

   En déduire que tous les théorèmes sont valides classiquement.
3. Montrer que la formule de Pierce $\big((p \Rightarrow q) \Rightarrow p\big) \Rightarrow p$ est valide classiquement.

Incomplétude

La formule de Pierce n'est pas un théorème de la logique minimale.

La logique minimale est incomplète pour le modèle $\{0, 1\}$.

Il faut

– soit changer de logique,

– soit changer de modèles.

On fera les deux !

Incomplétude

La formule de Pierce n'est pas un théorème de la logique minimale.

La logique minimale est incomplète pour le modèle $\{0, 1\}$.

Il faut

– soit changer de logique, logique classique

– soit changer de modèles, modèles de Kripke

On fera les deux !

La logique propositionnelle intuitionniste

(approche à la Hilbert)

La syntaxe

Il y a deux nouveaux connecteurs $\&$ et $\vee$.

– $\&$ et $\vee$ représentent la conjonction et la disjonction.

Les axiomes pour $\&$ et $\vee$

Il y a six axiomes.

$Or0 :$ $\quad \vdash (p \Rightarrow r) \Rightarrow (q \Rightarrow r) \Rightarrow (p \vee q) \Rightarrow r$

$Or1 :$ $\quad \vdash p \Rightarrow (p \vee q)$

$Or2 :$ $\quad \vdash q \Rightarrow (p \vee q)$

$And0 :$ $\quad \vdash p \Rightarrow q \Rightarrow (p \& q)$

$And1 :$ $\quad \vdash (p \& q) \Rightarrow p$

$And2 :$ $\quad \vdash (p \& q) \Rightarrow q$

Quelques conséquences

- $p \vee q \;\Rightarrow\; q \vee p$
- $p \vee (q \vee r) \;\Rightarrow\; (p \vee q) \vee r$
- $p \vee p \;\Rightarrow\; p$
- $(p \Rightarrow q) \;\Rightarrow\; (p \vee r) \;\Rightarrow\; (q \vee r)$
- $p \,\&\, q \;\Rightarrow\; q \,\&\, p$
- $p \,\&(q \,\&\, r) \;\Rightarrow\; (p \,\&\, q) \,\&\, r$
- $p \,\&\, p \;\Rightarrow\; p$
- $(p \Rightarrow q) \;\Rightarrow\; p \,\&\, r \;\Rightarrow\; q \,\&\, r$

Quelques conséquences (suite)

- $(p \,\&\, q) \vee (p \,\&\, r) \;\Rightarrow\; p \,\&\, (q \vee r)$
- $p \,\&\, (q \vee r) \;\Rightarrow\; (p \,\&\, q) \vee (p \,\&\, r))$
- $(p \vee q) \,\&\, (p \vee r) \;\Rightarrow\; p \vee (q \,\&\, r)$
- $p \vee (q \,\&\, r) \;\Rightarrow\; (p \vee q) \,\&\, (p \vee r)$

Et des règles :

$$\frac{p \qquad q}{p \,\&\, q} \qquad \frac{p \Rightarrow q \qquad p \Rightarrow r}{p \Rightarrow q \,\&\, r} \qquad \frac{p1 \Rightarrow q1 \qquad p2 \Rightarrow q2}{p1 \,\&\, p2 \;\Rightarrow\; q1 \,\&\, q2}$$

Le connecteur False

Le connecteur $False$ est régi par l'axiome :

F : $\quad \vdash False \Rightarrow p$

La négation est $\neg p \equiv p \Rightarrow False$.

Réduire les connecteurs ?

En logique intuitionniste, on ne peut pas réduire les connecteurs les uns par rapport aux autres.

Chaque connecteur a sa vie propre.

Il faut donc des axiomes spécifiques pour chaque connecteur (voir exercice ... dans le livre de van Dalen).

La logique intuitionniste et la logique classique

En logique intuitionniste les formules suivantes ne sont pas des théorèmes.

– $\neg\neg p \Rightarrow p$

– $p \vee \neg p$

– $(\neg p \Rightarrow \neg q) \Rightarrow q \Rightarrow p$

Le tiers exclus

Le tiers exclus est la proposition $p \vee \neg p$.

En informatique, considérons la proposition $Null$ à savoir

"La variable x est nulle"[a].

Sa négation est "La variable x n'est pas nulle"[b].

A-t-on $Null \vee \neg Null$?

A-t-on une seule manière d'interpréter la négation ?

---

[a] On devrait préciser "La variable x vaut toujours zéro"

[b] "La variable x ne vaut jamais zéro"

La logique intuitionniste et les preuves

En logique intuitionniste les preuves sont des citoyens de première classe.

Une proposition est un théorème si on peut en exhiber une preuve.

Ainsi

– d'une preuve de $\neg\neg p$ on ne peut pas extraire une preuve de p.

– on ne peut pas construire une preuve de $p \vee \neg p$, car cet objet est construit à partir d'une preuve de p ou d'une preuve de $\neg p$ [a].

[a] qu'on ne possède pas quand on affirme $p \vee \neg p$

C’est comme construire une maison sur un terrain situé

à Vaise ou à Vénissieux !

La logique intuitionniste et les preuves

Retournons à MP.

En fait, dans

$$(theorem\ p \Rightarrow q) \rightarrow (theorem\ p) \rightarrow (theorem\ q)$$

MP prend une preuve de $p \Rightarrow q$ et retourne une fonction qui prend une preuve de p et retourne une preuve de q.

Donc $(theorem\ p \Rightarrow q)$ représente le type [a] des preuves de $p \Rightarrow q$.

[a] plutôt que l'ensemble