LOGIQUE

L3 Informatique

Salim Lardjane

Université Bretagne Sud

3. La logique propositionnelle (LP0)

3.4. Systèmes formels : généralités

Introduction

La notion de *système formel* est intimement liée à la notion de *preuve*.

Cette dernière est extrêmement importante et subtile.

Il est difficile de saisir sa signification à l'aide, uniquement, d'une définition formelle.

Elle est présente dans beaucoup de domaines, dans les sciences exactes (mathématiques, physique, biologie, chimie, etc.), dans les sciences humaines (histoire, paléontologie, sociologie, etc.) ainsi que dans beaucoup d'activités inhérentes aux sociétés organisées (justice, police, vente, assurances, etc.) et a une longue histoire.

Notion de preuve

A notre niveau, nous pouvons essayer de nous baser sur notre expérience directe des mathématiques pour mieux comprendre le sujet et nous demander, par exemple :

Peut-on abstraire des caractéristiques communes des preuves que l'on a découvertes, lues, étudiées, etc. ?

Notion de preuve

Les preuves se présentent comme des *suites finies de formules*, parfois avec des dessins (correspondant à des cas particuliers : exemples (modèles), contre-exemples (contre-modèles)) intercalés, combinés avec des phrases en langue naturelle (en général un sous-ensemble très restreint de notre langage quotidien) justifiant l'introduction des nouvelles formules et. . . c'est tout !

Notion de preuve

– *Par quelles formules commence-t-on ?* : par des formules réputées "indiscutables" ou que l'on admet.

– *Comment passe-t-on de certaines formules à d'autres ?* : par des *règles*, en général pas très nombreuses, implicitement correctes et supposées être "naturelles", et dont on ne prend pas la peine de déclarer qu'elles seront celles, et seulement celles, que l'on s'autorise à utiliser.

On a ainsi identifié les idées de base de ce que nous définirons plus loin comme *système formel*.

Terminologie

Les formules réputées "indiscutables" sont appelées *axiomes*.

Les "règles de passage" sont appelées *règles d'inférence*.

Pour éviter les ambiguïtés, on se donnera dans la suite un *langage formel*.

Pour commencer, donnons *quelques exemples de règles d'inférence*.

Modus Ponens

Cette règle est également appelée *modus ponendo ponens* ou *syllogisme hypothétique*.

Elle est la suivante :

de A et *si* A *alors* B déduire B.

Récurrence

Elle consiste en une *infinité* de syllogismes hypothétiques :

Le théorème est vrai du nombre 1.

(*) Or, s'il est vrai de 1, il est vrai de 2.

Donc, il est vrai de 2.

(*) Or, s'il est vrai de 2, il est vrai de 3.

Donc, il est vrai de 3.

...

De plus, il y a une formule unique pour exprimer toutes les formules (*) : *si le théorème est vrai de $n-1$, alors il l'est de n.*

Conclusion : *le théorème est vrai pour tout entier naturel non nul n.*

Modus Tollens

Cette règle est également appelée *modus tollendo tollens*.

Elle est la suivante :

de *si* A *alors* B et $\neg B$ déduire $\neg A$.

Elle peut être considérée comme un cas particulier de *la réduction à l'absurde*.

Réduction à l'absurde

Elle figure parmi les règles les plus anciennes.

On distingue deux cas.

1. Quand elle est utilisée pour prouver **l'existence** d'un objet mathématique, elle est intimement liée au *principe du tiers exclu*. Pour prouver P, on prouve que $\neg P$ mène à contradiction. Comme, en vertu du principe du tiers exclu, $P \vee \neg P$ est toujours vrai, on conclut à P. A cause de l'utilisation du tiers exclu, les intuitionnistes n'acceptent pas toujours ce type de preuves.

2. Quand elle est utilisée pour prouver **la non-existence** d'un objet mathématique, elle est acceptée par toutes les écoles. Si P mène à une contradiction, l'objet avec la propriété P ne peut pas exister (sans aucune autre considération).

Système formel

Un **système formel** ou **théorie formelle** ou **système axiomatico-déductif** $\mathcal{S}$ est un triplet :

$$\mathcal{S} =< \mathcal{L}, \mathcal{R}, \mathcal{A} >$$

où :

– $\mathcal{L}$ est un **langage formel** sur un vocabulaire fini : on peut toujours décider de façon mécanique si une suite de symbole est un mot du langage (c'est-à-dire une fbf) ou non.

– $\mathcal{R} = \{RI_k | k \geq 1\}$ est une ensemble fini de **règles d'inférence**, c'est-à-dire des *relations* dans $\mathcal{L}^n$ ($n \geq 2$).
Elles sont notées en général :

$$RI_k : \frac{\mathcal{A}_1, \ldots, \mathcal{A}_{n-1}}{\mathcal{A}_n}$$

Système formel

Les $\mathcal{A}_i$ $(1 \leq i \leq n-1)$ sont appelées les *prémisses* et $\mathcal{A}_n$ la *conclusion* ou la *conséquence directe* des $\mathcal{A}_i$ $(1 \leq i \leq n-1)$.

On peut décider de façon mécanique si une fbf est conséquence directe d'autres fbf.

– $\mathcal{A} \subset \mathcal{L}$ sont les **axiomes**.

On peut accepter le cas des règles d'inférence sans prémisse, c'est-à-dire des relations dans $\mathcal{L}^n$ $(n \geq 1)$.

Les axiomes sont dans ce cas, aussi des règles d'inférence.

Les axiomes et règles d'inférence ont été aussi appelés *règles de transformation*.

Système formel

Si on considère uniquement la paire

$$\mathcal{S} = < \mathcal{L}, \mathcal{R} >$$

on parle de **système déductif** ou **système de preuve** ou **de calcul**.

Si on considère uniquement la paire

$$\mathcal{S} = < \mathcal{L}, \mathcal{A} >$$

on parle de **système axiomatique** ou **structure axiomatique**.

Système formel

Ce dernier cas est le cas le plus fréquent en mathématiques, sans spécifier $\mathcal{L}$ formellement (l'humain est supposé reconnaître les fbf).

On ne restreint pas les règles d'inférence que l'on se permet d'utiliser.

On parle de *théories axiomatiques informelles* et on peut y obtenir des *preuves informelles*.

Système formel

En fait, on peut par exemple démontrer des théorèmes dans la théorie des groupes, des ensembles, etc. sans avoir étudié la LP1.

Ces preuves peuvent être qualifiées de correctes mais informelles (tenir compte de ce genre de preuves est particulièrement important dans les *mathématiques constructives*).

Ceci dit, on ne saurait surestimer l'importance des preuves formelles (et donc indiscutables), qui elles, peuvent être vérifiées par ordinateur, par ce que l'on appelle les *assistants de preuve* (*logical frameworks*).

Remarques

1. Un système formel s'occupe exclusivement de la *syntaxe*. A cette syntaxe on peut associer une pluralité de sens ou interprétations. On reconnaît ici l'importance de la *forme* en logique.

2. Le principe de *non-contradiction* et du *tiers exclu* ne sont pas des règles d'inférence. Ce sont des *propriétés* valables pour toute fbf considérée.

Exemple : Axiomatique de Peano

L'ensemble des entiers naturels $\mathbb{N}$ a les propriétés suivantes (axiomatique de l'arithmétique de Peano) :

1. $0 \in \mathbb{N}$

2. Si $n \in \mathbb{N}$ alors $s(n) \in \mathbb{N}$

3. $0 \neq s(n)$

4. Si $s(n) = s(m)$ alors $n = m$

L'axiome d'induction :

5. Si $P(0)$ et (si $P(n)$ alors $P(s(n))$) alors $P(x)$ pour tout $x \in \mathbb{N}$

Formulation alternative :

5$'$. Si $S \subseteq \mathbb{N}$ et $0 \in S$ et (si $n \in S$ alors $s(n) \in S$) alors $S = \mathbb{N}$

Remarques : Axiomatique de Peano

a. $s(n)$ désigne le *successeur* de n.

b. La version 5 de l'axiome d'induction est *plus faible* que la version 5'.

En effet, comme une *propriété* peut être spécifiée avec une liste finie de mots d'un langage (défini avec une grammaire), on peut spécifier une *infinité dénombrable* de propriétés des naturels. . . mais l'ensemble de tous les sous-ensembles de $\mathbb{N}$ est *infini non dénombrable*.

Il existe donc des théorèmes sur les naturels qui *ne peuvent pas être prouvés* en utilisant la forme 5 de l'axiome d'induction.

Formules démontrables (prouvables)

L'ensemble des **formules démontrables** (prouvables) dans un système formel est le *plus petit ensemble* tel que :

i) si A est un axiome, alors A est démontrable ;

ii) si A est démontrable et B est une conséquence directe de A, alors B est démontrable ;

iii) si A et B sont démontrables et C est une conséquence directe de A et B, alors C est démontrable.

La définition suivante formalise la même notion, à travers celles bien connues de *démonstration* et de *théorème*.

Formules démontrables (prouvables)

Dans la définition suivante, si l'on inclut les lignes précédées par ($\sharp$) et on exclut celles précédées par ($\flat$) (respectivement on inclut les lignes précédées par ($\flat$) et on exclut celles précédées par ($\sharp$)) on a la définition de démonstration (preuve) (respectivement de déduction) .

Formules démontrables (prouvables)

Définition (démonstration, déduction, preuve)

Soient $\mathcal{S}$ un système formel et $\mathcal{A}_i, C$ des fbf de $\mathcal{S}$.

($\flat$) Γ : ensemble des fbf de $\mathcal{S}$;

Une

($\sharp$) démonstration (ou preuve) de C

($\flat$) déduction de (ou preuve de) C **à partir de Γ**

dans $\mathcal{S}$ est une suite finie $A_1, \ldots, A_n$ de fbf telle que :

Formules démontrables (prouvables)

1) $C = A_n$

2) Pour $1 \leq i \leq n$, soit

a) A_i est un axiome

(♭) ou $A_i \in \Gamma$

soit :

b) A_i est une conséquence directe par une règle d'inférence à partir de $A_{i_1}, \ldots, A_{i_k}$, $i_j < i$ $(1 \leq j \leq k)$

Formules démontrables (prouvables)

($\sharp$) C est appelé un *théorème* et on le note

($\sharp$) $\vdash_{\mathcal{S}} C$ ou, si l'on sous-entend la théorie $\vdash C$

($\flat$) Γ est appelé *ensemble des hypothèses* ou des *prémisses* de la conclusion

($\flat$) On note : $\Gamma \vdash_{\mathcal{S}} C$

($\flat$) On dit que C est une *conséquence* de Γ.

Remarques

1. Le méta-théorème *de la déduction* mettra en rapport les deux notions définies ci-dessus.

2. Noter qu'un système formel $\mathcal{S}$ peut être considéré comme un *algorithme* dont la sortie est l'ensemble des théorèmes de $\mathcal{S}$.