LOGIQUE
L3 Informatique

Salim Lardjane
Université Bretagne Sud

3. La logique propositionnelle (LP0)

3.5. Systèmes formels pour la LP0

Système $\mathcal{S}_1$

Nous allons définir un système formel $< \mathcal{L}, \mathcal{R}, \mathcal{A} >$ que nous appellerons $\mathcal{S}_1$.

1) $\mathcal{L}$

Nous nous restreignons aux fbf utilisant exclusivement comme connectifs $\Rightarrow$ et $\neg$, sachant que si l'on veut traiter d'autres connectifs on peut utiliser les trois définitions suivantes (A, B et C dénotent des fbf) :

D_1) $A \wedge B \overset{\text{def}}{:} \neg(A \Rightarrow B)$

D_2) $A \vee B \overset{\text{def}}{:} \neg A \Rightarrow B$

D_3) $A \Leftrightarrow B \overset{\text{def}}{:} (A \Rightarrow B) \wedge (B \Rightarrow A)$

Système $\mathcal{S}_1$

2) $\mathcal{R}$

Seule règle d'inférence : *modus ponens* ou *règle de détachement* (abrégée par la suite MP) :

$$MP : \frac{A \quad A \Rightarrow B}{B}$$

Comme A et B sont des (méta) variables dénotant des fbf quelconques, MP devrait être, à proprement parler, appelé *schéma de règle d'inférence*.

Système $\mathcal{S}_1$

3) $\mathcal{A}$

L'ensemble des trois schémas d'axiome suivant.

A, B et C dénotent des fbf, donc chacun des *schémas d'axiomes* ci-dessous dénote une infinité (dénombrable) de fbf.

A_1) $A \Rightarrow (B \Rightarrow A)$

A_2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

A_3) $(\neg B \Rightarrow \neg A) \Rightarrow ((\neg B \Rightarrow A) \Rightarrow B)$

De la définition de la notion de théorème il est clair que l'ensemble des théorèmes de $\mathcal{S}_1$ est *infini dénombrable*.

Exemple

Montrons que $\vdash_{\mathcal{S}_1} A \Rightarrow A$.

Première démonstration :

1) $A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$

Dans A_2, $B \leftarrow A \Rightarrow A$, $C \leftarrow A$.

2) $A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$

Dans A_1, $B \leftarrow A \Rightarrow A$.

3) $(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$

1, 2, MP.

4) $A \Rightarrow (A \Rightarrow A)$

Dans A_1, $B \leftarrow A$.

5) $A \Rightarrow A$

3, 4, MP.

Exemple

Deuxième démonstration :

1) $(A \Rightarrow (B \Rightarrow A) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow A))$

Dans A_2, $C \leftarrow A$.

2) $(A \Rightarrow B) \Rightarrow (A \Rightarrow A)$

A_1, *1 et MP*.

3) $(A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A)$

Dans 2) : $B \leftarrow B \Rightarrow A$.

4) $A \Rightarrow A$

A_1, *3 et MP.*

Méta-lemme 1

Soit Γ un ensemble de fbf de $\mathcal{S}_1$.

Si $\vdash_{\mathcal{S}_1} A$*, alors* $\Gamma \vdash_{\mathcal{S}_1} A$.

Preuve. Application de la définition de déduction.

Méta-théorème 4

Soit Γ un ensemble de fbf de $\mathcal{S}_1$ et A, B des fbf de $\mathcal{S}_1$. On note Γ, A pour $\Gamma \cup \{A\}$.

Théorème de la déduction.

$\Gamma, A \vdash_{\mathcal{S}_1} B$ *si et seulement si* $\Gamma \vdash_{\mathcal{S}_1} A \Rightarrow B$

En particulier (si $\Gamma = \emptyset$) :

$$A \vdash_{\mathcal{S}_1} B \textit{ si et seulement si } \vdash_{\mathcal{S}_1} A \Rightarrow B$$

Preuve

Seulement si)

Soit $B_1, B_2, \ldots, B_n$ une déduction à partir de $\Gamma \cup \{A\}$ $(B_n = B)$

Preuve par induction sur i de $\Gamma \vdash_{\mathcal{S}_1} A \Rightarrow B_i$ $(1 \leq i \leq n)$

1) $i = 1$

de la définition de déduction, on a trois cas :

$i)$ $B_1 \in \Gamma$

$ii)$ B_1 axiome de $\mathcal{S}_1$

$iii)$ B_1 est A ($B_1 \in (\Gamma \cup \{A\})$ et $B_1 \notin \Gamma$ (cas i))

Les trois cas sont démontrés comme suit.

On a dans tous les cas :

(A_1) $A \Rightarrow (B \Rightarrow A)$ $A \leftarrow B_1$

$B \leftarrow A$

$B_1 \Rightarrow (A \Rightarrow B_1)$

A présent :

$ii)$ et MP : $\vdash_{\mathcal{S}_1} A \Rightarrow B_1$, donc (méta-lemme précédent) $\Gamma \vdash_{\mathcal{S}_1} A \Rightarrow B_1$

$i)$ et MP : $\Gamma \vdash_{\mathcal{S}_1} A \Rightarrow B_1$

$iii)$ On a montré précédemment que $\vdash A \Rightarrow A$ (exemple), donc $\vdash_{\mathcal{S}_1} A \Rightarrow B_1$, donc (méta-lemme ci-dessus) $\Gamma \vdash_{\mathcal{S}_1} A \Rightarrow B_1$

Preuve

2) Induction

Supposons $\Gamma \vdash_{\mathcal{S}_1} A \Rightarrow B_k$ $(k < i)$
de la définition de déduction, on a quatre cas :
$i)$ B_i est un axiome de $\mathcal{S}_1$
$ii)$ $B_i \in \Gamma$
$iii)$ B_i est A
$ii)$ ou $iii)$: $B_i \in \Gamma \cup \{A\}$
$iv)$ B_i peut être déduite à partir de B_j, B_k $(1 \leq j < i)$
par MP, donc B_k a la forme $B_j \Rightarrow B_i$
$i)$, $ii)$, $iii)$ comme dans le cas 1)
par hypothèse d'induction :
$iv)$
$(*)$ $\Gamma \vdash_{\mathcal{S}_1} A \Rightarrow B_j$
$(**)$ $\Gamma \vdash_{\mathcal{S}_1} A \Rightarrow (B_j \Rightarrow B_i)$
(A_2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
$B \leftarrow B_j$
$C \leftarrow B_i$
en appliquant MP :
$\Gamma \vdash_{\mathcal{S}_1} (A \Rightarrow B_j) \Rightarrow (A \Rightarrow B_i)$ $(**)$
$\Gamma \vdash_{\mathcal{S}_1} (A \Rightarrow B_i)$ $(*)$
avec $i = n$ on a la preuve cherchée.

Si) : cf. TD.

Remarques

1. Pour la preuve de la première partie du théorème de la déduction nous avons eu besoin seulement des schémas d'axiomes A_1 et A_2.

2. La technique de preuve utilisée (et qui est une technique générale) pour prouver une propriété d'un système formel a été la suivante :

– prouver la propriété pour les (schémas) d'axiomes ;
– prouver que la(les) règle(s) d'inférence préserve(nt) cette propriété ;
– utiliser l'induction mathématique sur la longueur de la démonstration (déduction) .

Remarques

3. L'utilisation du théorème de la déduction dans les preuves est appelé *méthode de l'hypothèse supplémentaire*.

Cette méthode est très puissante ; il suffit pour s'en convaincre de montrer $\vdash_{\mathcal{S}_1} A \Rightarrow A$ en l'utilisant et de comparer la preuve avec celles données en exemple précédemment :

On a $A \vdash_{\mathcal{S}_1} A$ par définition de déduction. On obtient immédiatement $\vdash_{\mathcal{S}_1} A \Rightarrow A$ par application du théorème de la déduction.

Remarques

4. D'autres systèmes formels pour la LP0 seront vus en TD.

5. Le (méta)théorème de la déduction n'en est pas un pour toute logique.

Propriétés des Systèmes Formels

Soit $\mathcal{S} =< \mathcal{L}, \mathcal{R}, \mathcal{A} >$ un système formel.

Une règle d'inférence est dite **correcte** (ang. *sound*) si et seulement si la conclusion est une conséquence logique des prémisses.

$\mathcal{S}$ est dit **correct** (ang. *sound*) si et seulement si **tout théorème est une fbf valide**.

$\mathcal{S}$ est dit **complet** (ou adéquat) si et seulement si **toute fbf valide est un théorème**.

Remarque

Les notions de correction et complétude ont une application naturelle en informatique.

Étant donné une spécification d'un problème à résoudre, le programme qui est sensé donner la(les) solution(s) du problème est dit *correct* s'il calcule des solutions correctes du problème (autrement dit s'il calcule ce qui est spécifié).

Il est dit *complet* s'il calcule toutes les solutions (autrement dit, il calcule tout ce qui est spécifié).

Propriétés des Systèmes Formels

$\mathcal{S}$ est dit **consistant** (ou cohérent) ou, plus précisément, **consistant pour la négation**, si et seulement s'il n'y a pas de fbf $A \in \mathcal{L}$ telle que $\vdash_{\mathcal{S}} A$ et $\vdash_{\mathcal{S}} \neg A$.

$\mathcal{S}$ est dit **absolument consistant** si et seulement si l'ensemble $\tau \subseteq \mathcal{L}$ des théorèmes de $\mathcal{S}$ est tel que $\tau \neq \mathcal{L}$ (c'est-à-dire que $\mathcal{L}$ contient au moins une fbf qui *n'est pas* un théorème).

$\mathcal{S}$ est dit **décidable** si et seulement s'il existe une procédure mécanique (algorithme) qui pour *toute* fbf $A \in \mathcal{L}$ permet de répondre à la question : $\vdash_{\mathcal{S}} A$?. Un tel algorithme est appelé **une procédure de décision**

Les limites : Théorèmes de Gödel

Les systèmes formels ont, en plus de leur élégance, un côté rassurant.

Puisqu'ils sont indépendants de toute interprétation particulière, on peut se dire, concernant ses formules et théorèmes, que « rien ne leur échappe ».

Cette caractéristique est reflétée dans l'école dite formaliste, qui insistait sur le côté purement formel des mathématiques (c'est-à-dire une activité entièrement gérée par des règles de jeu) et dont le grand mathématicien D. Hilbert était l'un des principaux représentants.

Les limites : Théorèmes de Gödel

Dans ce qui est appelé « programme de Hilbert », Hilbert, qui voulait obtenir des fondements sûrs pour les mathématiques, posa le problème de trouver un système formel (incluant l'arithmétique et l'analyse) capable de trouver toutes les vérités mathématiques et seulement celles-ci et ne contenant donc pas de contradiction (c'est-à-dire un système formel *consistant*).

Les limites : Théorèmes de Gödel

Un tel résultat parlerait des preuves, il serait donc un résultat de *métamathématique* (parfois on parle de *théorie de la preuve*).

Les espoirs du programme de Hilbert furent anéantis par les deux théorèmes d'incomplétude de Gödel.

Kurt Gödel (1906-1978), considéré comme l'un des plus grands logiciens de tous les temps, montra la distinction entre *vrai* et *prouvable*.

Les limites : Théorèmes de Gödel

Dans son *premier théorème d'incomplétude*, il montra que dans une théorie $\mathcal{T}$ contenant l'arithmétique et supposée consistante, dans laquelle les axiomes et règles d'inférence sont en nombre fini ou spécifiés de façon récursive, on peut construire des formules G (du langage de $\mathcal{T}$) **indécidables**, c'est-à-dire que $\nvdash_{\mathcal{T}} G$ et $\nvdash_{\mathcal{T}} \neg G$.

Parfois, ce théorème est énoncé en disant qu'il existe dans $\mathcal{T}$ des formules vraies non démontrables.

Les limites : Théorèmes de Gödel

L'arithmétique permet de coder les formules et les preuves comme des nombres et de parler de leurs propriétés comme des propriétés des entiers.

Dans le système $\mathcal{T}$ on peut coder une formule $C_{\mathcal{T}}$ dont l'interprétation est « $\mathcal{T}$ est consistante ».

Le *deuxième théorème d'incomplétude* de Gödel dit que $\nvdash_{\mathcal{T}} C_{\mathcal{T}}$, autrement dit : on ne peut pas prouver la consistance de $\mathcal{T}$ dans $\mathcal{T}$.