La logique propositionnelle de Hilbert

1 La logique propositionnelle minimale

1.1 La syntaxe

Il n'y a qu'un connecteur $\Rightarrow$ et des variables propositionnelles p, q, $\ldots$, p_1, p_2, $\ldots$

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

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

s'écrit

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

1.2 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

1.3 Un peu de "méta syntaxe"

$(p, q : \mathit{proposition})$ signifie "pour tout p et tout q qui sont des propositions"

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

1.4 Le jugement *theorem*

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

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

On omet $\vdash$ dans les règles.

1.5 Une règle

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

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

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!

1.6 Deux axiomes

Il y a deux axiomes appelés K et S :

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

et

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

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

1.7 Exercice

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

1.8 Une règle dérivée : la règle C

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

$$rule\_C \quad \frac{p \Rightarrow q \Rightarrow r}{q \Rightarrow p \Rightarrow r}$$

1.9 Exercice

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

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

1.10 La règle Cut

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

$$rule\_Cut \quad \frac{q \Rightarrow r \qquad p \Rightarrow q}{p \Rightarrow r}$$

1.11 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.

1.12 Exercices

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 $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$ est valide classiquement.

1.13 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 !

2 La logique propositionnelle intuitionniste

2.1 La syntaxe

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

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

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

Il y a six axiomes.

$Or0$: $\vdash (p \Rightarrow r) \Rightarrow (q \Rightarrow r) \Rightarrow (p \vee q) \Rightarrow r$
$Or1$: $\vdash p \Rightarrow (p \vee q)$
$Or2$: $\vdash q \Rightarrow (p \vee q)$

$And0$: $\vdash p \Rightarrow q \Rightarrow (p\&q)$
$And1$: $\vdash (p\&q) \Rightarrow p$
$And2$: $\vdash (p\&q) \Rightarrow q$

2.3 Quelques conséquences

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

Et des règles :

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

2.4 Le connecteur False

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

F : $\vdash False \Rightarrow p$

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

2.5 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).

2.6 La logique intuitionniste et la logique classique

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

- $\neg\neg p \Rightarrow p$
- $p \vee \neg p$
- $(\neg p \Rightarrow \neg q) \Rightarrow q \Rightarrow p$

2.7 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”[1].
Sa négation est “La variable x n'est pas nulle”[2].
A-t-on $Null \vee \neg Null$?
A-t-on une seule manière d'interpréter la négation ?

2.8 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 $\neg p$ [3].

C'est comme construire une maison sur un terrain situé
à Vaise ou à Vénissieux !

2.9 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 [4] des preuves de $p \Rightarrow q$.

[1] On devrait préciser “La variable x vaut toujours zéro”
[2] “La variable x ne vaut jamais zéro”
[3] qu'on ne possède pas quand on affirme $p \vee \neg p$
[4] plutôt que l'ensemble