Approche à la Hilbert

version du 9 octobre 2002 – 09 h 13

La logique propositionnelle
(approche à la Hilbert)

Les jugements (1/2)

Le concept de base de la théorie de la démonstration est le jugement.

Un jugement s'écrit $\Gamma \vdash \Delta$ et est constitué de regroupement de propositions.

– Si Γ est vide et Δ ne contient qu'une proposition, c'est l'approche à la Hilbert.
– Quand Γ est un multiensemble (une structure de données où l'ordre ne compte pas, mais où les éléments peuvent être répétés) et Δ ne contient qu'une proposition, on a affaire à la déduction naturelle.

Les jugements (2/2)

– Quand Γ et Δ sont des multiensembles de propositions, on parle de calcul des séquents.
– Si Γ et Δ sont des multi-ensembles, mais si l'on contrôle très strictement l'emploi des duplications dans les preuves, – une proposition ne sert qu'une fois dans chaque preuve – on parle de logique linéaire.
– Si les propositions déclarent le type d'un élément, on parle de jugements de typage.

La logique propositionnelle minimale

La syntaxe 1/2

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

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

Par exemple, les propositions sont

– p,

– $p \Rightarrow q$,

– $(p \Rightarrow q) \Rightarrow p$.

La syntaxe 2/2

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

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

Les jugements de logique à la Hilbert

Les jugements sont de la forme $\vdash \varphi$ où φ est une proposition.

Ainsi on distingue certaines propositions des autres.

Les jugements de logique à la Hilbert

Les jugements sont de la forme $\vdash \varphi$ où φ est une proposition.

Ainsi on distingue certaines propositions des autres.

Question : Quelles sont en logique les propositions que l'on veut distinguer des autres ?

Les constituents de la logique propositionnelle à la Hilbert

C’est une logique de presque rien :

– des jugements rudimentaires,
– une règle,
– deux axiomes.

Du coup, elle est difficile d’emploi, il va falloir s’aider d’un logiciel pour la manipuler.

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].

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

[a] Ces notes de cours vont de paire avec un script en COQ.

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”.

Une règle

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

le Modus Ponens :

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

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 $B : (p \Rightarrow q) \Rightarrow (r \Rightarrow p) \Rightarrow r \Rightarrow q)$.

Preuve de KS

$$\mathcal{D} = \dfrac{\vdash (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p \qquad \dfrac{\mathcal{D}' \qquad \vdash p \Rightarrow p \Rightarrow p}{\vdash p \Rightarrow p}}{\vdash q \Rightarrow p \Rightarrow p}$$

où $\mathcal{D}'$ est

$$\dfrac{\vdash (p \Rightarrow (p \Rightarrow p) \Rightarrow p) \Rightarrow (p \Rightarrow p \Rightarrow p) \Rightarrow p \Rightarrow p \qquad \vdash p \Rightarrow (p \Rightarrow p) \Rightarrow p}{\vdash (p \Rightarrow p \Rightarrow p) \Rightarrow p \Rightarrow p}$$

Preuve de KS

$$\mathcal{D} = \dfrac{\vdash (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p \qquad \dfrac{\mathcal{D}' \qquad \vdash p \Rightarrow p \Rightarrow p}{\vdash p \Rightarrow p}}{\vdash q \Rightarrow p \Rightarrow p}$$

où $\mathcal{D}'$ est

$$\dfrac{\vdash (p \Rightarrow (p \Rightarrow p) \Rightarrow p) \Rightarrow (p \Rightarrow p \Rightarrow p) \Rightarrow p \Rightarrow p \qquad \vdash p \Rightarrow (p \Rightarrow p) \Rightarrow p}{\vdash (p \Rightarrow p \Rightarrow p) \Rightarrow p \Rightarrow p}$$

$\mathcal{D}$ et $\mathcal{D}'$ sont des arbres de preuve.

$\mathcal{D}$ est l'arbre de preuve ou la preuve de $q \Rightarrow p \Rightarrow p$.

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.

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

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 $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$ 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.

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 ! Par exemple en ajoutant l'axiome de Pierce

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.

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

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

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

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

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

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

Quelques conséquences

- $p \vee q \Leftarrow b \wedge d$
- $(p \vee q) \wedge r \Leftarrow (b \wedge d) \wedge r$
- $p \vee q \Leftarrow d \wedge d$
- $(p \vee r) \Leftarrow (b \wedge d) \Leftarrow (b \Leftarrow d)$
- $p \parr q \Leftarrow b \parr d$
- $(p \parr q) \parr r \Leftarrow (b \parr d) \parr r$
- $p \parr q \Leftarrow d \parr d$
- $(p \Leftarrow d) \Leftarrow (b \Leftarrow d) \Leftarrow r \parr d \Leftarrow r \parr b \Leftarrow q \parr r$

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 :

$$\frac{\vdash p \qquad \vdash q}{\vdash p \,\&\, q} \qquad \frac{\vdash p \Rightarrow q \qquad \vdash p \Rightarrow r}{\vdash p \Rightarrow q \,\&\, r}$$

$$\frac{\vdash p1 \Rightarrow q1 \qquad \vdash p2 \Rightarrow q2}{\vdash p1 \,\&\, p2 \;\Rightarrow\; q1 \,\&\, q2}$$

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.

– $\neg\neg p \Rightarrow p$

– $p \vee \neg p$

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

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

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