Calcul à la Hilbert

Pierre Lescanne

3 octobre 2005 – 13 : 11

Les séquents

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

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

Les séquents

- 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 séquents

- Quand Γ et Δ sont des multiensembles de propositions, on parle de calcul des séquents.
- Si Γ et Δ sont des multiensembles, 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 jugement de typage.

La syntaxe

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

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

Example

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

sont des propositions.

La syntaxe

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 séquents de logique à la Hilbert

Les séquents sont de la forme $\vdash \varphi$ où φ est une proposition.
Ainsi on distingue certaines propositions des autres.

Les séquents de logique à la Hilbert

Les séquents 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 propositions et les théorèmes

Les propositions sont des formules constituées de variables et de l'opérateur (du connecteur) $\Rightarrow$.
Elles n'ont pas de «contenu» utilisable pour raisonner.

Les théorèmes sont acceptables pour raisonner.

Example

$p \Rightarrow q \Rightarrow p$ *est un théorème de la logique minimale*
et on accepte parfaitement le raisonnement
Si p alors si q alors p.

Mais toutes les propositions ne sont pas acceptables.

Example

$p \Rightarrow p \Rightarrow q$.
Va-t-on accepter «Si p alors si p alors q ?».

Les propositions et les théorèmes dans les groupes

Dans les groupes, les propositions sont de la forme $exp \equiv exp'$

où exp et exp' sont formées

- de variables
- du symbole binaire $*$,
- du symbole unaire $^{-1}$
- et de la constante e.

Les théorèmes sont dérivés à partir des axiomes bien connus des groupes et des règles de remplacement des égaux par des égaux.

$(x * x^{-1}) * y \equiv (y * x^{-1}) * x$ est un théorème.

$(x * x^{-1}) * y^{-1} \equiv (y * x) * x$ est une proposition qui n'est pas un théorème.

Les propositions valides dans les groupes

Une proposition $e(x, y, z) \equiv e'(x, y, z)$ est valide si

- pour tous les groupes (groupe additif des entiers, groupe multiplicatif des entiers, groupe additif des espaces vectoriels, groupe des déplacements de l'espace, groupe de permutations, etc.)
- pour toute valeur $\bar{x}$ de x, $\bar{y}$ de y, $\bar{z}$ de z, on a

$$e(\bar{x}, \bar{y}, \bar{z}) \equiv e'(\bar{x}, \bar{y}, \bar{z})$$

Les constituants de la logique propositionnelle à la Hilbert

La logique propositionnelle à la Hilbert est une logique de presque rien :

- des séquents 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

Comme méta-théorie, je choisis, un système logique très puissant : le Calcul des Constructions Inductifs, mécanisé dans l'assistant de preuve COQ[1].

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

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

Un peu de «méta syntaxe»

forall 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 méta-prédicat theorem

En COQ, le méta-prédicat *theorem* appliqué à p se note

($theorem\ p$).

Mais plus tard, COQ nous permet d'utiliser le symbole de séquent $\vdash p$ qui doit se lire «p est un théorème».

Une règle

En logique propositionnelle minimale à la Hilbert, 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 $theorem\ q$.

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.

Le Modus Ponens

En COQ, MP est une fonction

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

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 :

Axiome (K)

$\vdash p \Rightarrow q \Rightarrow p$

Axiome (S)

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

Deux axiomes

Il y a deux axiomes appelés K et S :

Axiome (K)

$\vdash p \Rightarrow q \Rightarrow p$

Axiome (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 !

Preuve de KI

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

où $\mathcal{D}'$ est

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

Preuve de KI

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

où $\mathcal{D}'$ est

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

$\mathcal{D}$ 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 le lemme

Lemme

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

Exercice

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

Lemme

$$L \; : \; \vdash \; q \Rightarrow r \longrightarrow \; \vdash \; p \Rightarrow q \longrightarrow \; \vdash \; p \Rightarrow r.$$

La règle Cut

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

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

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.

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.

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 $\{0, 1\}$.

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,

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

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,
- soit changer de modèles, modèles de Kripke

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 l'un et l'autre !

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 l'un et l'autre !
On peut obtenir la logique classique en ajoutant l'axiome de Pierce.

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 l'un et l'autre !

On peut obtenir la logique classique en ajoutant l'axiome de Pierce. Mais ça serait un peu ah hoc !

La syntaxe

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

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

Les axiomes pour $\wedge$ et $\vee$

Il y a six axiomes :

$$
\begin{array}{lcl}
Or0 & : & \vdash (p \Rightarrow r) \Rightarrow (q \Rightarrow r) \Rightarrow (p \vee q) \Rightarrow r \\
Or1 & : & \vdash p \Rightarrow (p \vee q) \\
Or2 & : & \vdash q \Rightarrow (p \vee q) \\
\\
And0 & : & \vdash p \Rightarrow q \Rightarrow (p \wedge q) \\
And1 & : & \vdash (p \wedge q) \Rightarrow p \\
And2 & : & \vdash (p \wedge q) \Rightarrow q
\end{array}
$$

Quelques conséquences

- $\vdash \quad p \vee q \;\Rightarrow\; q \vee p$
- $\vdash \quad p \vee (q \vee r) \;\Rightarrow\; (p \vee q) \vee r$
- $\vdash \quad p \vee p \;\Rightarrow\; p$
- $\vdash \quad (p \Rightarrow q) \;\Rightarrow\; (p \vee r) \;\Rightarrow\; (q \vee r)$
- $\vdash \quad p \wedge q \;\Rightarrow\; q \wedge p$
- $\vdash \quad p \wedge (q \wedge r) \;\Rightarrow\; (p \wedge q) \wedge r$
- $\vdash \quad p \wedge p \;\Rightarrow\; p$
- $\vdash \quad (p \Rightarrow q) \;\Rightarrow\; p \wedge r \;\Rightarrow\; q \wedge r$

Quelques conséquences (fin)

- $\vdash \quad (p \wedge q) \vee (p \wedge r) \;\Rightarrow\; p \wedge (q \vee r)$
- $\vdash \quad p \wedge (q \vee r) \;\Rightarrow\; (p \wedge q) \vee (p \wedge r))$
- $\vdash \quad (p \vee q) \wedge (p \vee r) \;\Rightarrow\; p \vee (q \wedge r)$
- $\vdash \quad p \vee (q \wedge r) \;\Rightarrow\; (p \vee q) \wedge (p \vee r)$

Quelques conséquences (fin)

- $\vdash \quad (p \wedge q) \vee (p \wedge r) \;\Rightarrow\; p \wedge (q \vee r)$
- $\vdash \quad p \wedge (q \vee r) \;\Rightarrow\; (p \wedge q) \vee (p \wedge r))$
- $\vdash \quad (p \vee q) \wedge (p \vee r) \;\Rightarrow\; p \vee (q \wedge r)$
- $\vdash \quad p \vee (q \wedge r) \;\Rightarrow\; (p \vee q) \wedge (p \vee r)$

Et des règles :

$$\frac{\vdash p \qquad \vdash q}{\vdash p \wedge q} \qquad \frac{\vdash p \Rightarrow q \qquad \vdash p \Rightarrow r}{\vdash p \Rightarrow q \wedge r}$$

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

Le connecteur False

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

Axiome (F)

$\vdash False \Rightarrow p$

Le connecteur False

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

Axiome (F)

$\vdash False \Rightarrow p$

Notation :

False se dit ausssi absurde et se note $\bot$.

La négation est $\quad \neg p \quad \triangleq \quad p \Rightarrow False$.

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.

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.

Exercice

Prouver l'assertion précédente. Voir exercice 29 p. 188 (chapitre 5) dans le livre de van Dalen Logic and structure.

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 x_vaut_zero :
à savoir
«La variable x vaut zéro»[2].

Sa négation est «La variable x ne vaut pas zéro»[3].

---

[2]On devrait préciser «La variable x vaut toujours zéro»
[3]«La variable x ne vaut jamais zéro»

Le tiers exclus

Le tiers exclus est la proposition $p \vee \neg p$.
En informatique, considérons la proposition x_vaut_zero :
à savoir
«La variable x vaut zéro»[2].

Sa négation est «La variable x ne vaut pas zéro»[3].

A-t-on $x\_vaut\_zero \vee \neg\ x\_vaut\_zero$?

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

[2]On devrait préciser «La variable x vaut toujours zéro»
[3]«La variable x ne vaut jamais zéro»

La double négation

En langue naturelle, la double négation ne correspond pas à une affirmation.
Plutôt à une atténuation.

Je ne suis pas contre.	Ça n'est pas impossible.
Cette personne n'est pas idiote.	Cette statue n'est pas laide.
Vous n'êtes pas sans savoir.	Ça n'est pas mal.

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 exhiber une preuve de p.
- on ne peut pas construire une preuve de $p \vee \neg p$, car cet objet est devrait pouvoir être construit à partir d'une preuve de p ou d'une preuve de $\neg p$[4].

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

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 exhiber une preuve de p.
- on ne peut pas construire une preuve de $p \vee \neg p$, car cet objet est devrait pouvoir être construit à partir d'une preuve de p ou d'une preuve de $\neg p$[4].

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

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

La logique intuitionniste et les preuves

Retournons à *MP*.
En fait, dans

$$\vdash \ p \Rightarrow q \longrightarrow \ \vdash \ p \longrightarrow \ \vdash \ q$$

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 $\vdash \ p \Rightarrow q$ représente le type des preuves de $p \Rightarrow q$.

.

La logique intuitionniste et les preuves

Retournons à MP.
En fait, dans

$$\vdash \ p \Rightarrow q \longrightarrow \ \vdash \ p \longrightarrow \ \vdash \ q$$

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 $\vdash \ p \Rightarrow q$ représente le type des preuves de $p \Rightarrow q$.
Plutôt que l'ensemble des preuves de $p \Rightarrow q$.