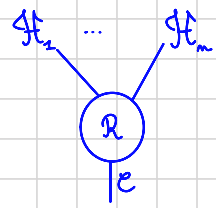
15.03.2021 (présentiel)

OL4 : CNTD 6

Systèmes de preuve : le calcul des séquents

Déf : Un système de preuve consiste en des règles d'inférence $\mathcal{R}$

$$\dfrac{\mathcal{H}_1 \quad \dots \quad \mathcal{H}_m}{\mathcal{C}}\,(\mathcal{R})$$



où $\mathcal{H}_1 \dots \mathcal{H}_m$ est un nb fini (éventuellement 0) d'hypothèses de $\mathcal{R}$

et $\mathcal{C}$ est la conclusion de $\mathcal{R}$

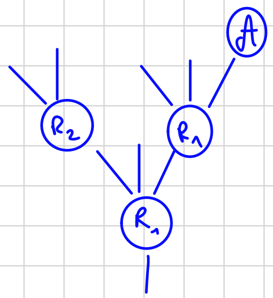
Rmq : Une règle peut avoir un nombre quelconque fini d'hypothèses mais a UNE et une seule conclusion.

Déf : Un axiome d'un système de preuve est une règle sans hypothèse

$$\dfrac{}{\mathcal{C}}\,\mathcal{A}$$

Déf : Un arbre de démonstration est un arbre dont les noeuds sont des règles et les arrêtes sont des hypothèses et/ou conclusions des noeuds

ex :



$$\dfrac{\dfrac{\mathcal{H}_4 \quad \mathcal{H}_5}{\mathcal{C}_2}\,R_1 \qquad \mathcal{H}_1 \qquad \dfrac{\mathcal{H}_3 \quad \mathcal{H}_2 \quad \dfrac{}{\mathcal{C}_4}\,\mathcal{A}}{\mathcal{C}_3}\,R_1}{\mathcal{C}_1}\,R_1$$

Rmq : Pour nous, les hypothèses et conclusions seront tjs des formules ou des séquents.

Déf : Une preuve d'un système de preuve est un arbre de démonstration sans hypothèses (sans feuilles).

Autrement dit, tout chemin vers le haut termine en un axiome.

Exemple : Système de Hilbert

Règles : où A, B, C sont des formules quelconques.

$$\dfrac{}{A \Rightarrow (B \Rightarrow A)}\,\mathcal{A}_1 \qquad \dfrac{}{(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (B \Rightarrow C))}\,\mathcal{A}_2 \qquad \dfrac{}{(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)}\,\mathcal{A}_3 \qquad \dfrac{A \qquad A \Rightarrow B}{B}\,\mathcal{R}$$

appelé modus ponens

Déf : Une formule A est prouvable dans un système de preuve s'il existe une preuve (dans le même système) avec conclusion (racine) A.

Exemple : dans le système de Hilbert

$A \Rightarrow (B \Rightarrow A)$ $\qquad$ $[A \Rightarrow (B \Rightarrow C)] \Rightarrow [(A \Rightarrow B) \Rightarrow (A \Rightarrow C)]$

$$\dfrac{\dfrac{}{A \Rightarrow (A \Rightarrow A)}\,\mathcal{A}_1 \qquad \dfrac{\dfrac{}{A \Rightarrow ((A \Rightarrow A) \Rightarrow A)}\,\mathcal{A}_1 \qquad \dfrac{}{[A \Rightarrow ((A \Rightarrow A) \Rightarrow A)] \Rightarrow [(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)]}\,\mathcal{A}_2}{A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)}\,\mathcal{R}}{A \Rightarrow A}\,\mathcal{R}$$

On construit à partir de la conclusion (en bas). Si c'est déjà de la forme d'un axiome, c'est bon. Sinon on trouve les hypothèses nécessaires pour écrire la règle et on recommence.

Déf : Un système est
* **correct** si la conclusion de toute preuve du système est une formule valide.
* **complet** si toute formule valide est la conclusion d'au moins une preuve du système.

Donc un système est correct et complet <u>ssi</u> VAL = ensemble des formules prouvables dans le système.

<u>Théorème :</u> Le système de Hilbert est correct et complet.

<u>Indice :</u> Pour montrer (1) ssi (2)
- soit on montre si (1) alors (2) ET si (2) alors (1)
- soit on montre si (1) alors (2) ET si ¬(1) alors ¬(2)

<u>Exercice :</u> Si $m \geq 2$ et $A = \ell_1 \vee \dots \vee \ell_m$ est une clause
Mq il existe ℓ_i et ℓ_j tels que $\ell_i = \neg \ell_j$ ssi $\models A$

<u>Mq (1) ⇒ (2)</u>
Supposons $\ell_i = \neg \ell_j$, alors $A \equiv \ell_1 \vee \dots \vee \ell_{i-1} \vee \neg \ell_j \vee \dots \vee \ell_j \vee \dots \vee \ell_m$

$\equiv \mathbb{1}$ par commutativité de la disjonction et car $\neg \ell_j \vee \ell_j = \mathbb{1}$

Autre méthode : on peut faire avec une affectatO
$[\![A]\!]_v = \mathrm{OR}([\![\ell_1]\!]_v, \dots [\![\ell_m]\!]_v)$

<u>Mq ¬(1) ⇒ ¬(2)</u>
Supposons qu'il n'existe pas de $1 \leq i < j \leq m$ tq $\ell_i = \neg \ell_j$

Définissons $b_1, \dots, b_m \in \mathbb{B}$ avec $b_k := \begin{cases} 0 & \text{si } \ell_k = x_k \\ 1 & \text{si } \ell_k = \neg x_k \end{cases}$ donc $[\![\ell_k]\!](^{b_k}/_{x_k}) = 0$

Alors pour v l'affectation $(^{b_1}/_{x_1}, \dots, ^{b_m}/_{x_m})$ on a $[\![A]\!]_v = \mathrm{OR}([\![\ell_1]\!]_v, \dots, [\![\ell_m]\!]_v)$

$= \mathrm{OR}([\![\ell_1]\!](^{b_1}/_{x_1}), \dots, [\![\ell_m]\!](^{b_m}/_{x_m}))$

$= \mathrm{OR}(0, \dots, 0)$

<u>Exercice :</u> Mq
① $(v \models A$ et $v \models B)$ ssi $v \models (A \wedge B)$

② $(v \models B$ ou $v \models A)$ ssi $v \models (A \vee B)$

③ $v \models (B \Rightarrow (\neg A \vee C))$ ssi $v \models (B \wedge A) \Rightarrow C$

④ $v \models (B \wedge \neg A) \Rightarrow C$ ssi $v \models B \Rightarrow (A \vee C)$

1) $(v \models A$ et $v \models B)$ ssi $[\![A]\!]_v = 1$ et $[\![B]\!]_v = 1$

ssi $\mathrm{AND}([\![A]\!]_v, [\![B]\!]_v) = 1$

ssi $[\![A \wedge B]\!]_v = 1$

ssi $v \models (A \wedge B)$

2) $(v \models A$ ou $v \models B)$ ssi $[\![A]\!]_v = 1$ ou $[\![B]\!]_v = 1$
ssi $\mathrm{OR}([\![A]\!]_v, [\![B]\!]_v) = 1$
ssi $[\![A \vee B]\!]_v = 1$
ssi $v \models (A \vee B)$

3) Montrons que $B \Rightarrow (\neg A \vee C) \equiv (B \wedge A) \Rightarrow C$

$$\begin{aligned} B \Rightarrow (\neg A \vee C) &\equiv \neg B \vee (\neg A \vee C) \\ &\equiv (\neg B \vee \neg A) \vee C \\ &\equiv \neg (B \wedge A) \vee C \\ &\equiv (B \wedge A) \Rightarrow C \end{aligned}$$

4) Mq les 2 formules sont équivalentes

$$\begin{aligned} (B \wedge \neg A) \Rightarrow C &\equiv \neg (B \wedge \neg A) \vee C \\ &\equiv \neg B \vee \neg\neg A \vee C \\ &\equiv \neg B \vee (A \vee C) \\ &\equiv B \Rightarrow (A \vee C) \end{aligned}$$

Rappels

Si I est un ensemble fini de formules.
On écrit $\bigwedge I := \bigwedge\limits_{A \in I} A$ et $\bigvee I := \bigvee\limits_{A \in I} A$

Par convention, $\bigwedge \emptyset := \mathbb{1}$ et $\bigvee \emptyset := \mathbf{0}$ donc $\bigwedge (I \cup I') = (\bigwedge I) \wedge (\bigwedge I')$ (et de même pour $\bigvee$)

↑ zéro en gras

Système de Gentzen ou Calcul des séquents propositionnels

Déf: Un séquent est une paire (Γ, Δ) d'ensembles finis de formules. On l'écrit $\Gamma \vdash \Delta$
↑ "thèse"

Déf: $\Gamma \vdash \Delta$ est valide si $(\bigwedge \Gamma) \Rightarrow (\bigvee \Delta)$ est valide.

Système de Gentzen:

$$\dfrac{}{\underbrace{A, \Gamma}_{\{A\} \cup \Gamma} \vdash A, \Delta} \; Ax \quad \text{(règle Axiome)}$$

$$\dfrac{A, B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} \wedge_L \qquad \dfrac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} \wedge_R$$

$$\dfrac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta} \vee_L \qquad \dfrac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee_R$$

$$\dfrac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} \neg_L \qquad \dfrac{A, \Gamma \vdash \Delta}{\Gamma \vdash \neg A, \Delta} \neg_R$$

Exemple: l'implicat°

$$\dfrac{\dfrac{\Gamma \vdash A, \Delta}{\neg A, \Gamma \vdash \Delta} \neg_L \quad B, \Gamma \vdash \Delta}{\underbrace{\neg A \vee B}_{= A \Rightarrow B}, \Gamma \vdash \Delta} \vee_L$$

donc $\dfrac{\Gamma \vdash A, B \quad B, \Gamma \vdash \Delta}{A \Rightarrow B, \Gamma \vdash \Delta}$ $\Rightarrow_L$ est une règle dérivable

De m̂ à droite:

$$\dfrac{\dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash \neg A, B, \Delta} \neg_R}{\Gamma \vdash \neg A \vee B, \Delta} \vee_R$$

donc $\dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}$ $\Rightarrow_R$ et dérivable.

Exemple :

$$\dfrac{\dfrac{}{A \vdash A}\,Ax}{\vdash A \Rightarrow A} \Rightarrow_R$$

donc $A \Rightarrow A$ est bien prouvable.