918 : Systèmes Formels de Preuve en logique du 1er ordre : Exemples

Référence : David, Nour, Raffali. Intro à la logique. Théorie de la démo.

But : Déf. formellement un raisonnement "correct". Automatiser le processus de démonstration.

I - Système Formel. 1er ordre : définitions

1) Vocabulaire

LF	langage	mot	sous-langage	mot du ss-langage
Logique	Syntaxe	Formule	Théorie	Axiome

- Séquent : $T \vdash A \in \mathcal{P}(L) \times L$ (L = Syntaxe)
- Règle de déduction : $\dfrac{\text{Prémisses}}{\text{Conclusion}}$ Nom : fonction partielle $r(\text{Séquents})^{k\in\mathbb{N}} \longrightarrow \text{Séquents}$.
- <u>Système Formel de Preuve</u> : Ensemble de règles.
- A se déduit de T dans S, noté $T \vdash_S A$ si $T \vdash A = r(T_i \vdash A_i)$, $r \in S$, $T_i \vdash_S A_i$ (induction)

2) Logique du 1er ordre

Un langage du 1er ordre est la donnée de $\mathcal{E}, \mathcal{V}, F, R$

La syntaxe associée a pour grammaire :

$\mathcal{F} \to R(\mathcal{T} .. \mathcal{T}) \mid \neg\mathcal{F} \mid \mathcal{F} * \mathcal{F} \mid \Pi_x \mathcal{F}$

$\mathcal{T} \to \mathcal{E} \mid \mathcal{V} \mid F(\mathcal{T} .. \mathcal{T})$.

Une interprétation du langage dans une structure $\mathcal{M}$ donne une valeur de vérité à chaque formule.

On note $\mathcal{M} \models T$ si tout axiome de T est vrai dans $\mathcal{M}$.

On note $T \models A$ si tout modèle de T est modèle A

T est dite contradictoire si elle n'admet aucun modèle.

II - Les principaux Systèmes du 1er ordre

1) Déduction naturelle

$$\frac{}{\Gamma, A \vdash A}\,ax \qquad \frac{\Gamma \vdash A}{\Gamma, B \vdash A}\,aff$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\,\to_i \qquad \frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\,\to_e$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,\wedge_i \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,\wedge_e^g \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,\wedge_e^d$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,\vee_i^g \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,\vee_i^d \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\,\vee_e$$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\,\neg_i \qquad \frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \bot}\,\neg_e \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\,\bot_c$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x A}\,\forall_i \quad x \notin FV(\Gamma) \qquad \frac{\Gamma \vdash \forall x A}{\Gamma \vdash A[t/x]}\,\forall_e$$

$$\frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x A}\,\exists_i \qquad \frac{\Gamma \vdash \exists x A \quad \Gamma, A \vdash C}{\Gamma \vdash C}\,\exists_e \quad x \notin FV(\Gamma, C)$$

Exemple :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A\wedge B \vdash A \wedge B}\,ax}{A \wedge B \vdash B}\,\wedge_e^d \qquad \dfrac{\dfrac{}{A\wedge B \vdash A \wedge B}\,ax}{A \wedge B \vdash A}\,\wedge_e^g}{A \wedge B \vdash B \wedge A}\,\wedge_i}{\vdash A \wedge B \to B \wedge A}\,\to_i$$

C'est le système le plus "classique", proche des définitions.

[DEV 1] : On prouve en déduction naturelle qu'une involution est bijective.

Théorème 1 (Complétude).

On a : $T \models A$ ssi $T \vdash A$

__Conséquence__ : Compacité sémantique

[Si $T \models A$, alors il existe $T_0 \subset T$ fini tq $T_0 \models A$

2) __Calcul des séquents__ (LK)

On veut un système plus symétrique. Les preuves sont plus automatiques, mais parfois moins intuitives

Un séquent est de la forme $\Gamma \vdash \Delta$ Γ, Δ multi-ensemble

__Quelques règles__ : $\dfrac{}{\bot \vdash}\bot_g$ $\qquad \dfrac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\text{contr}_d$

$$\dfrac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\vee_g \qquad \dfrac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\vee_d$$

$$\dfrac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\to_g \qquad \dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\to_d$$

$$\dfrac{\Gamma, A[t/x] \vdash \Delta}{\Gamma, \forall x A \vdash \Delta}\forall_g \qquad \dfrac{\Gamma \vdash A, \Delta}{\Gamma \vdash \forall x A, \Delta}\forall_d \quad x \notin FV(\Gamma, \Delta)$$

__Théorème 2__ : [LK est équivalent au système de déduction naturelle.]

Conséquence : On a $A_1, \dots A_n \vdash_{LK} B_1, \dots B_m$

ssi $\models A_1 \wedge \dots \wedge A_n \to B_1 \vee \dots \vee B_m$

• La règle $\dfrac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\text{coupure}$

joue un rôle particulier dans LK.

__Théorème 3__ (Elimination des coupures)

[Si $\Gamma \vdash_{LK} \Delta$ alors il existe une démonstration qui n'utilise pas la règle de coupure

__Corollaire 4__ (Consistance syntaxique)

[Le séquent $\vdash$, qui signifie "absurde", n'est pas dérivable dans LK]

3) __Système de Hilbert__

plus historique

Plus ancien, plus "mathématique" la plupart de ses règles sont appelées axiomes : c'est une autre terminologie.

On note $\vdash_\Gamma A$ s'il existe une suite $A_1 \dots A_n, A$ de formules telles que • A_i est un axiome • $A_i \in \Gamma$

ou • A_i se déduit de formules précédentes par une règle.

__Axiomes__ : $H_1 : A \to B \to A$ $\quad H_2 : (A \to B \to C) \to (A \to B) \to (A \to C)$

$H_3 : A \wedge B \to A$ $\quad H_4 : A \wedge B \to B$ $\quad H_5 : A \to B \to A \wedge B$

$H_6 : A \to A \vee B$ $\quad H_7 : B \to A \vee B$ $\quad H_8 : (A \to C) \to (B \to C) \to (A \vee B) \to C$

$H_9 : \neg A \leftrightarrow (A \to \bot)$ $\quad H_{10} : \bot \to A$ $\quad H_{11} : A \vee \neg A$

$H_{12} : A[t/x] \to \exists x A$ $\quad H_{13} : \forall x A \to A[t/x]$

__Règles__ : $\dfrac{A \quad A \to B}{B}\text{MP}$ $\qquad \dfrac{C \to A}{C \to \forall x A} \qquad \dfrac{A \to C}{\exists x A \to C} \quad x \notin FV(C)$

__Exemple__ : On note $B = A \to A$ et on prouve $A \to A$.

1	$(A \to (B \to A)) \to (A \to B) \to (A \to A)$	H_2
2	$A \to (B \to A)$	H_1
3	$(A \to B) \to (A \to A)$	MP, 1, 2
4	$A \to B$	H_1
5	$A \to A$	MP, 3, 4.

Il n'y a pas d'équivalent de la règle $\to_i$ car Γ est fixé.

Théorème 5 (de la déduction) [DEV. 2]

[On a $\vdash_{\Gamma} A \to B$ ssi $\vdash_{\Gamma, A} B$

Théorème 6 : Ce système est équivalent aux deux précédents. Il est donc valide et complet]

5) Résolution par coupure

Autre terminologie : on ne cherche que des preuves de $\Gamma \vdash \bot$ où les formules de Γ sont sous forme normale conjonctive ;

Un littéral est une formule atomique sans quantificateur.
Une clause est un ensemble fini de littéraux (disjonction).
Une formule est un ensemble de clauses.

Définition 7 : Soit $\sigma : \mathcal{V} \to \mathcal{T}$ une substitution.
[L et L' des littéraux et $L[\sigma]$, $L'[\sigma]$ leur image par σ. Si $L[\sigma] = L'[\sigma]$, on dit que L et L' sont unifiables par σ.]

L'algorithme d'unification détermine si deux littéraux sont unifiables et fournit un unificateur principal. En le notant $Unif(L, L')$, les règles de la résolution par coupure sont :

$$\frac{C_1, L_1 \quad C_2, L_2}{C_1[\sigma], C_2[\sigma]} \text{res} \quad \sigma = Unif(L_1, \overline{L_2}) \qquad \frac{C_1, L_1, L_2}{C_1[\sigma], L_1[\sigma]} \text{contr} \quad \sigma = Unif(L_1, L_2)$$

Théorème 8 : (Complétude de la résolution) [DEV. 3]

[Γ sous CNF est contradictoire ssi $\Gamma \vdash_{Rés} \bot$]

Puisque toute formule peut être mise sous CNF, ce système est donc équivalent aux précédents.

III - Systèmes Intuitionnistes

Avec les systèmes précédents, si $\Gamma \vdash A \vee B$, on ne sait pas si $\Gamma \vdash A$, ni si $\Gamma \vdash B$. Si $\Gamma \vdash \exists x A$, on aimerait aussi connaître $t \in \mathcal{T}$ tel que $\Gamma \vdash A[t/x]$.
Un système qui permet cela est dit constructiviste.

1) En déduction naturelle

On s'interdit le raisonnement par l'absurde, c'est à dire la règle $\bot_c$, on la remplace par $\dfrac{\Gamma \vdash \bot}{\Gamma \vdash A} \bot_i$

2) En calcul des séquents

Le système LJ se déduit de LK en n'autorisant qu'au plus une formule à droite des séquents, et la règle $\vee_d$ est remplacée par $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee_d^1$ $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee_d^2$

Théorème 9 Ces deux systèmes sont équivalents.

Propriété 10 (cq de Thm 3) [• LJ est un système constructiviste
• On a $LJ \subsetneq LK$]

3) En Système de Hilbert

On supprime H_{11} : $A \vee \neg A$ pour retrouver un système équivalent aux deux précédents.

Nou1

Pratique de la déduction naturelle

Systèmes égalitaires:

Un système est dit égalitaire lorsqu'il est muni d'un symbole de fonction particulier, noté $=$, représentant une fonction d'arité 2.

On dispose alors des deux règles suivantes:

$$\frac{}{\Gamma \vdash t = t} =_i \quad , \text{ introduction de l'égalité.}$$

→ C'est la réflexivité de l'égalité.

$$\frac{\Gamma \vdash A[t/x] \qquad \Gamma \vdash t = u}{\Gamma \vdash A[u/x]} =_e \quad \text{élimination de l'égalité.}$$

Règles dérivées

Pour simplifier les démonstrations, on utilise des règles dérivées, c-a-d qui peuvent se déduire à partir des seules règles et axiomes du systèmes.

Exemple:

La règle $\dfrac{}{\Gamma, u = v \vdash t[u/z] = t[v/z]} =_c$ est dérivable

On pose $A[y] := t[u/z] = t[y/z]$.

__Preuve:__

$$\dfrac{\dfrac{\overline{\Gamma, u=v \vdash t[u/y]=t[u/y]}\ {=_i}}{\Gamma, u=v \vdash A[u/y]} \qquad \overline{\Gamma, u=v \vdash u=v}\ ax}{\Gamma, u=v \vdash A[v/y]}\ {=_e}$$

même chôse réécrite

Exemple de demonstration :

On va MQ les involutions sont injectives.

On pose:

$Inv(f)$ pour $\forall x\ f(f(x))=x$

$Inj(f)$ pour $\forall x \forall y\ \ f(x)=f(y) \Rightarrow x=y$

$Surj(f)$ pour $\forall y\ \exists x\ \ f(x)=y$.

$Bij(f)$ pour $Inj(f) \wedge Surj(f)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{f(x)=f(y) \vdash f(f(x))=f(f(y))}{Inv(f), f(x)=f(y) \vdash f(f(x))=y}\ {=_e} \qquad \dfrac{Inv(f) \vdash Inv(f)}{Inv(f) \vdash f(f(x))=x}\ \forall_e}{Inv(f), f(x)=f(y) \vdash x=y}\ {=_e}}{Inv(f) \vdash f(x)=f(y) \Rightarrow x=y}\ {\Rightarrow_i}}{Inv(f) \vdash \forall y\, f(x)=f(y) \Rightarrow x=y}\ \forall_i}{Inv(f) \vdash Inj(f)}\ \forall_i \qquad Inv(f) \vdash Surj(f)}{}\ \wedge_i$$

① : $=_c$ est appliquée avec $t := f(z)$
$u := f(x)$
$v := f(y)$

② Il y a des affaiblissements implicites

③ Simple réécriture !

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{f(x)=f(y) \vdash f(f(x))=f(f(y))}\,{=_c}\ ①
\qquad
\dfrac{\dfrac{}{Inv(f) \vdash Inv(f)}\,ax}{②\ Inv(f) \vdash f(f(y))=y}\,\forall_e
}{Inv(f),\, f(x)=f(y) \vdash f(f(x))=y}\,{=_e}
\qquad
\dfrac{\dfrac{}{Inv(f) \vdash Inv(f)}\,ax}{②\ Inv(f) \vdash f(f(x))=x}\,\forall_e
}{Inv(f),\, f(x)=f(y) \vdash x=y}\,{=_e}
}{Inv(f) \vdash f(x)=f(y) \to x=y}\,\to_i
}{Inv(f) \vdash \forall y\ f(x)=f(y) \to x=y}\,\forall_i
}{Inv(f) \vdash Inj(f)}\,\forall_i
\qquad
\dfrac{
\dfrac{
\dfrac{
\dfrac{\dfrac{}{Inv(f) \vdash Inv(f)}\,ax}{Inv(f) \vdash f(f(y))=y}\,\forall_e
}{Inv(f) \vdash (f(x)=y)[f(y)/x]}\,③
}{Inv(f) \vdash \exists x\ f(x)=y}\,\exists_i
}{Inv(f) \vdash Surj(f)}\,\forall_i
}{Inv(f) \vdash Bij(f)}\,\wedge_i
$$

Nom (½)

Théorème de la déduction

Thm : $\vdash_{\Gamma,A} B$ ssi $\vdash_{\Gamma} A \to B$

Admis : $\vdash_{\Gamma} (A \to B \to C) \leftrightarrow (A \wedge B \to C)$ (D1)

$\vdash_{\Gamma} (A \to B \to C) \leftrightarrow (B \to A \to C)$ (D2)

$\vdash_{\Gamma} A \to A$ (D3)

($\Leftarrow$) Si $\vdash_{\Gamma} A \to B$.

On a une preuve de $A \to B$ dans Γ :

$\vdots$

$\vdash_{\Gamma} A \to B$

On recopie cette preuve dans Γ, A car $\Gamma, A \subset \Gamma$

$\vdots$

(1) $\vdash_{\Gamma,A} A \to B$

(2) $\vdash_{\Gamma,A} A$

$\vdash_{\Gamma,A} B$ $\quad R_{\to}$ (1)(2)

($\Rightarrow$) $\vdash_{\Gamma,A} B$ $\quad \Gamma' = \Gamma, A$

On a une Γ'-dérivation de B :

$\vdash_{\Gamma'} A_0$

$\vdash_{\Gamma'} A_n$ (avec $A_n = B$)

On va montrer par récurrence forte sur $i \leq n$ que pour tout $i \in [\![0, n]\!]$

on a $\vdash_{\Gamma} A \to A_i$

l'hérédité et l'initialisation sont en fait traités simultanément.

Soit $i \in [\![0, n]\!]$.

Si $i \neq 0$, on suppose que $\vdash_\Gamma A \to A_j$ pour tout $j < i$

Distinction de cas sur A_i:

- (*) Soit $A_i \in \Gamma \cup \{A\}$ ou A_i est un axiome

  - si $A_i = A$, on utilise $\vdash_\Gamma A \to A$

  - si $A_i \in \Gamma$ ou A_i axiome

  On a $\vdash_\Gamma A_i$

  $\vdash_\Gamma A_i \to A \to A_i$

  $\vdash_\Gamma A \to A_i \qquad (R_\to)$

- (*) Soit A_i se déduit d'une règle.

  - Si A_i se déduit par $R_\to$ de A_j et $A_j \to A_i = A_k$ $\quad j<i$, $k<i$

  Par hypothèse de récurrence, on a:

(1) $\vdash_\Gamma A \to A_j$

(2) $\vdash_\Gamma A \to A_j \to A_i$

(3) $\vdash_\Gamma (A \to A_j \to A_i) \to (A \to A_j) \to (A \to A_i) \qquad H_2$

(4) $\vdash_\Gamma (A \to A_j) \to (A \to A_i) \qquad R_\to (3), (2)$

(5) $\vdash_\Gamma A \to A_i \qquad R_\to (4)(1)$

- Si A_i se déduit par $R_\forall$ de $A_j = C \to D[x]$, $j<i$

Alors $A_i = C \to \forall x D[x]$

Hyp. de rec.: on a

(1) $\vdash_\Gamma A \to C \to D[x]$

(2) $\vdash_\Gamma (A \to C \to D[x]) \to (A \wedge C) \to D[x]$ (D1)

(3) $\vdash_\Gamma A \wedge C \to D[x]$ $R_\to$ (1)(2).

(4) $\vdash_\Gamma A \wedge C \to \forall x D[x]$ $R_\forall$(3).

(5) $\vdash_\Gamma (A \wedge C \to \forall x D[x]) \to (A \to C \to \forall x D[x])$ (D1)

(6) $\vdash_\Gamma A \to C \to \forall x D[x]$ $R_\to$ (4)(5).

- Si A_i se déduit par $R_\exists$ de $A_j = D[x] \to C$ $j<i$.

Alors $A_i = \exists x D[x] \to C$.

Hyp. de rec.:

(1) $\vdash_\Gamma A \to D[x] \to C$

(2) $\vdash_\Gamma (A \to D[x] \to C) \to (D[x] \to A \to C)$ (D2)

(3) $\vdash_\Gamma D[x] \to A \to C$. $R_\to$ (2)(1).

(4) $\vdash_\Gamma \exists x D[x] \to A \to C$ $R_\exists$(3)

(5) $\vdash_\Gamma (\exists x D[x] \to A \to C) \to (A \to \exists x D[x] \to C)$ (D2).

(6) $\vdash_\Gamma A \to \exists x D[x] \to C$ $R_\to$ (5)(4).

Par récurrence, pour tout $i \leq n$, on a $\vdash_\Gamma A \to A_i$

en $i = n$ $\vdash_\Gamma A \to B$

Preuve de D3 :

On pose $B = A \to A$

(1) $\vdash_F (A \to (B \to A)) \to ((A \to B) \to B)$ $\quad H_2$

(2) $\vdash_F (A \to B \to A)$ $\quad H_1$

(3) $\vdash_F (A \to B) \to B$ $\quad R_{\to}(2)(1)$

(4) $\vdash_F A \to B$ $\quad H_1$

(5) $\vdash B$ $\quad R_{\to}(3)(4)$