Oraux Blancs Janvier

NOM : PINAULT Prénom : Lauréline Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : (918) Systèmes formels de preuve en logique du 1er ordre

Autre sujet : (906. Prog Dyn).

(1) Une volonté de formalisation des mathématiques

1] Syntaxe de la logique du 1er ordre

Def1 (langage du premier ordre)
$\mathcal{L} = \mathcal{L}_f \cup \mathcal{L}_R$ où $f^n \in \mathcal{L}_f$ est un symbole de fonction d'arité n et $R^n \in \mathcal{L}_R$ est un symbole de relation d'arité n.

Exple 2 $\mathcal{L}_1 = (e^0, *^2, {}^{-1}{}^1, =^2)$ est le langage de la théorie des groupes.

Def3 (ensemble des termes d'un langage)
C'est le plus petit ensemble contenant V, un ensemble infini de variables, et stable par application des symboles de fonction de $\mathcal{L}$

Exple 4. $x * e^{-1}$ est un terme de $\mathcal{L}_1$

Def5 (ensemble des formule d'un langage)
- $A = \{ R^n(t_1, \dots t_n) \mid R^n \in \mathcal{L}_R, t_i \in \mathcal{L} \}$
- $\mathcal{F}$ est le plus petit ensemble contenant A et stable par application des connecteur $\vee^2, \wedge^2, \to^2, \neg^1, \exists x^1, \forall x^1$ où $x \in V$.

Exple 6 $\forall x \exists y ((x*y=e) \wedge \neg(y*x=e)))$ est une formule de $\mathcal{L}_1$

Def7 (Variables libres) $VL(F)$
- Si $F = R(t_1, \dots t_n)$, $VL(F) = \bigcup \{x \in V \text{ où } t_i\}$
- Si $F = F_1 \oplus F_2$ où $\oplus \in \{\vee, \wedge, \to\}$, $VL(F) = VL(F_1) \cup VL(F_2)$
- Si $F = \neg F_1$, $VL(F) = VL(F_1)$
- Si $F = Qx F_1$ où $Q \in \{\forall, \exists\}$, $VL(F) = VL(F_1) \setminus \{x\}$

2] Démonstration en déduction naturelle.

Def8 (Les règles de la déduction naturelle : NK) Voir annexe 1.

Def9 (prouvabilité).
- Un séquent $\Gamma \vdash F$, où $\Gamma \subset \mathcal{F}$ et $F \in \mathcal{F}$, est prouvable en déduction naturelle (on notera $\Gamma \vdash_{NK} F$) si il peut être obtenu par une application finie de règles de NK.
- Une formule F est prouvable en déduction naturelle si $\vdash F$ est prouvable.

Exple 10
- $\exists x (A \wedge B) \to (\exists x A \wedge \exists x B)$ est prouvable
- $\vdash (A \wedge B \to C) \to (A \to B \to C)$ est prouvable

Def11 (Les règles de la déduction naturelle intuitionniste : NJ)
(Ce sont les règles de NK (annexe 1) moins la règle $\perp_c$ (absurdité classique) remplacée par la règle $\perp_i$: $\frac{\perp}{F} \perp_i$)

Def12 (Règle dérivable) Une règle est dérivable en déduction naturelle si on peut, par application des règles NK, obtenir un arbre dont la racine est la conclusion de la règle et dont les feuilles en sont les prémisses.

Exple 13 Les règles suivantes sont dérivables :
- Coupure : $\dfrac{\Gamma, A \vdash B \quad \Gamma \vdash A}{\Gamma \vdash B}$ coupure

- Loi de Peirce : $\dfrac{\Gamma, \neg A \vdash A}{\Gamma \vdash A}$ lp
- Tiers exclu : $\dfrac{\Gamma, A \vdash B \quad \Gamma, \neg A \vdash B}{\Gamma \vdash B}$ te

II Raisonner sur les démonstrations elles-mêmes

1] Recherche de systèmes équivalents

Def 14 (Système formel de preuve)
C'est la donnée d'un ensemble d'hypothèses et de règles.
Une preuve est l'utilisation d'un nombre fini d'hypothèse et d'application d'un nombre fini de règle.

Exple 15 Le système (NK). (voir annexe) n'a pas d'hypothèses et ses règles sont présentées en annexe 1.

Def 16 (Systèmes équivalents)
Deux systèmes formels de preuve sont équivalents s'ils ont le même ensemble de formules prouvables.

Prop 17 Deux systèmes sont équivalents si chaque hypothèse de l'un est prouvable dans l'autre et si chaque règle de l'un est dérivable dans l'autre.

Exemple 18 (NK) et ((NJ) ∪ te) sont équivalents.

2] Le calcul des séquents

Def 19 (Les règles du calcul des séquents : LK) : Voir annexe 2

Def 20 (Les règles du calcul des séquents intuitionniste : LJ)
Elles sont obtenues à partir des règle de LK en se restreignant à des séquents ayant au plus une formule à droite.

Thm 21
- $\vdash_{NK} \Leftrightarrow \vdash_{LK}$
- $\vdash_{NJ} \Leftrightarrow \vdash_{LJ}$

Thm 22 (Elimination des coupures)
Si $\Gamma \vdash \Delta$ est dérivable dans LK, il en existe une dérivation dans LK qui n'utilise pas la règle de la coupure.

Thm 23 (Elimination des coupures intuitionniste) Si $\Gamma \vdash F$ est dérivable dans LJ, il en existe une dérivation dans LJ qui n'utilise pas la règle de la coupure

Csq 24 (consistance de LK et LJ)
- $\vdash_{LK}$ et $\vdash_{LJ}$ ne sont pas dérivables
- $A \in \mathcal{A} \Rightarrow \vdash_{LK} A$ n'est pas dérivable
- $A \neq \bot \Rightarrow \vdash_{LK} A$ et $\vdash_{LK} \neg A$ ne sont pas dérivables

Csq 25 (constructivité de la logique intuitionniste)
- Si $\vdash_{LJ} A_1 \vee A_2$ alors $\vdash_{LJ} A_1$ ou $\vdash_{LJ} A_2$ et on a un algorithme pour nous dire si c'est A_1 ou A_2.
- Si $\vdash_{LJ} \exists x A$ alors $\exists t \in \mathcal{C}$ tel que $\vdash_{LJ} A(x := t)$ et on a un algorithme qui nous donne t.

Csq 26 (prop de la sous formule)
Si $\Gamma \vdash_{LK} \Delta$ alors il existe une dérivation dans LK de ce séquent dont toutes les formules sont de la forme $A(x_1 := t_1, \dots, x_n := t_n)$

où A est une sous formule d'une des formules de Γ ou de Δ.

dvt1

Csq 27 (Théorème d'interpolation)
~~Si Γ est un ensemble de formules, on note~~ Si $\vdash_{LK} A \to B$ alors $\exists F$ tq $\vdash_{LK} A \to F$ et $\vdash_{LK} F \to B$ et F n'est écrit qu'en utilisant des symboles communs à A et B

3] Les systèmes à la Hilbert

Def 28 (système à la Hilbert)
- C'est la donnée d'un ensemble d'axiomes et d'un ensemble de règles.
- Une P-dérivation est une suite finie $A_1 .. A_n$ tq $A_i \in \Gamma$ ou A_i axiome ou A_i conclusion d'une règle dont les prémisses sont dans $A_1, .., A_{i-1}$.
- $\Gamma \vdash A$ si il existe une P-dérivation terminant par A.
- A prouvable si il existe une $\emptyset$-dérivation

III Vers l'automatisation de preuves

1] L'unification

Def 29 u et v $\in \mathcal{C}$ sont unifiable ssi il existe σ tq $u[\sigma] = v[\sigma]$.

Algorithme 30 (Unification)

$E_0 = \{u_1 \nu v_1, .. u_n \nu v_n\}$, $\sigma_0 = Id$

1. Si $E_n = E' \cup \{f(u_1, .. u_q) \nu g(v_1, .. v_p)\}$
   - Si $f = g$ et $p = q$, $E_{n+1} = E' \cup \{u_1 \nu v_1, .. u_q \nu v_q\}$, $\sigma_{n+1} = \sigma_n$
   - Sinon échec
2. Si $E_n = E' \cup \{x \nu x\}$, $E_{n+1} = E'$ et $\sigma_{n+1} = \sigma_n$
3. Si $E_n = E' \cup \{x \nu v\}$ avec $v \neq x$
   - Si $x \in v$, $\sigma_{n+1} = [x := v] \circ \sigma_n$
   - $E_{n+1} = E'[x := v]$
   - Sinon échec
4. Si $E_n = \emptyset$ l'algorithme s'arrête σ_n est le most general unificator. (mgu)

dvt2

2] La méthode des tableaux

Utilisation du calcul des séquents un peu modifié.

3] La résolution

Idée: On cherche à partir d'un ensemble de clause à dériver la clause vide, ce qui revient à dire que l'ensemble des clauses est contradictoire.

C'est un algorithme de décision pour le calcul propositionnel.

Annexe 1 : Déduction naturelle (NK)

	Introduction	Élimination
Ax	$\dfrac{}{\Gamma, A \vdash A}\ ax$	$\dfrac{\Gamma \vdash A}{\Gamma, B \vdash A}\ aff$
$\to$	$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to i$	$\dfrac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \to e$
$\wedge$	$\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge i$	$\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge e_g$ $\quad$ $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge e_d$
$\vee$	$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee i_g$ $\quad$ $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee i_d$	$\dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee e$
$\neg$	$\dfrac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg i$	$\dfrac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \bot}\ \neg e$
$\forall$	$\dfrac{\Gamma \vdash A \quad x \notin VL(\Gamma)}{\Gamma \vdash \forall x A}\ \forall i$	$\dfrac{\Gamma \vdash \forall x A}{\Gamma \vdash A[x := t]}\ \forall e$
$\exists$	$\dfrac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x A}\ \exists i$	$\dfrac{\Gamma \vdash \exists x A \quad \Gamma, A \vdash C \quad x \notin VL(\Gamma, C)}{\Gamma \vdash C}\ \exists e$
=	$\dfrac{}{\Gamma \vdash t = t}\ =i$	$\dfrac{\Gamma \vdash A[x := t] \quad \Gamma \vdash t = u}{\Gamma \vdash A[x := u]}\ =e$
$\bot_c$	$\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \bot_c$	

Annexe 2 : Calcul des séquents (LK)

	Droite	Gauche
Ax	$\dfrac{}{A \vdash A}\ ax$	$\dfrac{}{\bot \vdash}\ \bot g$
$\to$	$\dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\ \to d$	$\dfrac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\ \to g$
$\wedge$	$\dfrac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ \wedge d$	$\dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge g$
$\vee$	$\dfrac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee d$	$\dfrac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ \vee g$
$\neg$	$\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\ \neg d$	$\dfrac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\ \neg g$
$\forall$	$\dfrac{\Gamma, A[x := t] \vdash \Delta}{\Gamma, \forall x A \vdash \Delta}\ \forall g$	$\dfrac{\Gamma \vdash A, \Delta \quad x \notin VL(\Gamma, \Delta)}{\Gamma \vdash \forall x A, \Delta}\ \forall d$
$\exists$	$\dfrac{\Gamma \vdash A[x := t], \Delta}{\Gamma \vdash \exists x A, \Delta}\ \exists d$	$\dfrac{\Gamma, A \vdash \Delta \quad x \notin VL(\Gamma, \Delta)}{\Gamma, \exists x A \vdash \Delta}\ \exists g$
Aff	$\dfrac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\ aff_d$	$\dfrac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ aff_g$
Contr	$\dfrac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ cont_d$	$\dfrac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ cont_g$
Cap	$\dfrac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ cap$	