NOM : BERNARD Prénom : Sophie Jury :

Algèbre ← Entourez l'épreuve → Analyse Informatique

Sujet choisi : 918 : Systèmes formels de preuve en logique du premier ordre : exemples

Autre sujet : Réf : David, Nour, Raffalli
Introduction à la logique : théorie de la démonstration

On suppose connus la syntaxe et la sémantique de la logique du premier ordre

## I - SYSTEMES FORMELS ET DEFINITIONS

On se donne L un langage et T une théorie.

**Def 1** : Un séquent est un couple noté $\Gamma \vdash A$ où $\Gamma$ est un ensemble fini de formules sur L et A est une formule de L ; sous les hypothèses $\Gamma$, on montre A.

**Def 2** : Une règle d'inférence notée $\frac{\text{prémisses}}{\text{conclusion}}$ nom est un couple où les prémisses sont un ensemble fini de séquents et la conclusion est un séquent.

**Def 3** : Un système formel de preuves est un couple composé d'un ensemble d'axiomes (de théorie T) et d'un ensemble de règles d'inférence.

**Rq 4** : Un séquent est prouvable dans un système s'il en existe une dérivation dans ce système. C'est une propriété syntaxique.

**Def 5** : Un système formel de preuves est dit
- consistant si $\vdash \bot$ n'est pas dérivable
- complet s'il permet de prouver toutes les propriétés valides dans tout modèle.
- correct si tout séquent prouvable est valide dans tout modèle.

**Rq 6** : Les propriétés de complétude et correction d'un système de preuves permet de faire le lien entre syntaxe et sémantique.

## II - SYSTEMES FORMELS CLASSIQUES

### 1 - Déduction naturelle

**Règles** : on les trouvera en annexe

**Rq 7** : On peut aussi écrire l'ensemble de ces règles sous la forme de séquents

ex 8 : la règle $\frac{\vdots}{\frac{\bot}{A}\bot_c}$ d'absurdité classique peut aussi s'écrire : $\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\bot_c$

**Def 9** : La logique classique avec les règles de la déduction naturelle est appelée NK

**Def 10** : La logique intuitionniste en déduction naturelle est notée NJ et est obtenue en remplaçant la règle d'absurdité classique $\bot_c$ par la règle d'absurdité intuitionniste : $\frac{\bot}{A}\bot_i$.

ex 11 : $\frac{\dfrac{\dfrac{[A]^1}{B}\to_e}{(A\to B)\to B}\to_i^1}{A \to (A\to B)\to B}\to_i$ Preuve dans NK de $\vdash A \to (A \to B) \to B$

**DEV 1** : Traduction de la preuve que les simulations sont des bijections dans NK.

**App 12** : NK est correct et complet, NJ aussi.

**App 13** : NK et NJ sont consistants.

### 2 - Calculs des séquents

**Rq 14** : On cherche à avoir des règles plus symétriques. On obtient une version généralisée des séquents : les prémisses et la conclusion sont des multi-ensembles finis de formules.

**Règles** : Axiomes : $\frac{}{\Gamma, \bot \vdash \Delta}\bot_g$ $\frac{}{A \vdash A}ax$

Règles structurelles : $\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}affg$ $\frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}affd$ $\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}contrg$ $\frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}contrd$

Règles des connecteurs logiques :

$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\wedge_g$ $\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\wedge_d$ $\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\vee_d$

$\frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\vee_g$ $\frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\to_g$

$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\to_d$ $\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\neg_g$ $\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\neg_d$

Règles pour les quantificateurs :

$\frac{\Gamma, A[x := t] \vdash \Delta}{\Gamma, \forall x A \vdash \Delta}\forall_g$ $\frac{\Gamma \vdash A, \Delta \quad x \notin FV(\Gamma, A)}{\Gamma \vdash \forall x A, \Delta}\forall_d$

$\frac{\Gamma, A \vdash \Delta \quad x \notin FV(\Gamma,\Delta)}{\Gamma, \exists x A \vdash \Delta}\exists_g$ $\quad \frac{\Gamma \vdash A[x:=t], \Delta}{\Gamma \vdash \exists x A, \Delta}\exists_d$ Coupure: $\frac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$ coup

**Def 15:** La logique classique avec les règles du calcul des séquents est **LK**.

**Def 16:** La logique intuitionniste du calcul des séquents, noté **LJ**, est obtenue en obligeant chaque règle de LK à n'avoir que des séquents avec au plus une formule à droite.

**ex 17:** la règle contrd disparaît et les règles $\to_g$ et $\vee_d$ de LK deviennent:

$\frac{\Gamma \vdash A \quad \Gamma, B \vdash [C]}{\Gamma, A \to B \vdash [C]}\to_g$ ; $\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\vee_d^1$ ; $\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\vee_d^2$ où $[C]$ signifie que la formule C n'est pas forcément présente.

**Prop 18:** Pour $\Gamma$ un ensemble de formules, A une formule:
$(\Gamma \vdash_{NJ} A$ ssi $\Gamma \vdash_{LJ} A)$ et $(\Gamma \vdash_{NJ} \bot$ ssi $\Gamma \vdash_{LJ})$.

**Dev 2:** Pour $\Gamma$ un ensemble de formules et A une formule:
Si $\Gamma \vdash_{NK} A$ alors $\Gamma \vdash_{LK} A$.
Pour $\Gamma$ et $\Delta$ deux ensembles de formules:
Si $\Gamma \vdash_{LK} \Delta$ alors $\Gamma, \neg\Delta \vdash_{NK} \bot$ où si $\Delta = A_1, \dots, A_m$ alors $\neg\Delta = \neg A_1, \dots, \neg A_m$.

**Th 19** (Elimination des coupures): Dans LK ou LJ, si $\Gamma \vdash \Delta$, séquent généralisé quelconque, il existe une dérivation sans utiliser la règle de coupure.

**Th 20:** LK et LJ sont consistants.

**Th 21:** LK et LJ sont complets et corrects.

## 3_Systèmes à la Hilbert

**Rq 22:** Les systèmes à la Hilbert comptent beaucoup plus d'axiomes et très peu de règles.

Axiomes:

$H_1: A \to B \to A$
$H_2: (A \to B \to C) \to (A \to B) \to (A \to C)$
$H_3: A \wedge B \to A$
$H_4: A \wedge B \to B$
$H_5: A \to B \to A \wedge B$
$H_6: A \to A \vee B$
$H_7: B \to A \vee B$
$H_8: (A \to C) \to (B \to C) \to (A \vee B) \to C$
$H_9: \neg A \leftrightarrow (A \to \bot)$
$H_{10}: \bot \to A$
$H_{11}: A \vee \neg A$
$H_{12}: A[x:=t] \to \exists x A[x]$ *
$H_{13}: \forall x A[x] \to A[x:=t]$ *

*: t est un terme

Règles:

$\frac{A \quad A \to B}{B} R_\to$ $\quad \frac{C \to A[x]}{C \to \forall x A[x]} R_\forall$ * $\quad \frac{A[x] \to C}{\exists x A[x] \to C} R_\exists$ *

*: x n'a pas d'occurences libres dans C ni dans les formules précédentes

**Def 23:** Pour $\Gamma$ un ensemble de formules, une **$\Gamma$-dérivation** est une suite finie $A_1, \dots, A_m$ de formules telle que pour tout $i \leq m$:
- $A_i \in$ axiomes ou $A_i \in \Gamma$ ou $A_i$ est la conclusion d'une des règles ($R_\to$, $R_\vee$ ou $R_\exists$) dont les prémisses sont dans $\{A_1, \dots, A_{i-1}\}$.

**Def 24:** Pour $\Gamma$ un ensemble de formules, une formule A est **$\Gamma$-dérivable**, noté $\vdash_\Gamma A$, s'il existe une $\Gamma$-dérivation qui se termine par A.

**ex 25:** On va montrer $\vdash A \to A$.

1: $(A \to (A \to A) \to A) \to ((A \to (A \to A)) \to (A \to A))$ — $H_2(A, A\to A, A)$
2: $A \to (A \to A) \to A$ — $H_1(A, A \to A)$
3: $(A \to A \to A) \to A \to A$ — $R_\to(1,2)$
4: $A \to A \to A$ — $H_1(A, A)$
5: $A \to A$ — $R_\to(3,4)$

**Rq 26:** On peut démontrer d'autres théorèmes pour faciliter les preuves comme le théorème de déduction ou la transitivité de l'implication.

**Th 27:** Soit $\Gamma$ un ensemble de formules, A et B des formules.
$\vdash_{\Gamma, A} B$ ssi $\vdash_\Gamma A \to B$

**Th 28:** Soit $\Gamma$ un ensemble de formules et A une formule.
$\vdash_\Gamma A$ ssi $\Gamma \vdash_{NK} A$.

parler de complexité d'indécidabilité

# III_ AUTOMATISATION DES PREUVES

0. Indécidable ⇒ → partie décidable ; → partie indécidable

## 1_Unification

**Def 29:** Une substitution $\sigma$ est une fonction qui associe à chaque variable un terme: pour u un terme, on note $u[\sigma]$ le terme obtenu en remplaçant, dans u, chaque variable x par $\sigma(x)$.

**Def 30:** Un unificateur de deux termes u et v est une substitution $\sigma$ telle que $u[\sigma] = v[\sigma]$. On dit que $\sigma$ unifie u et v.

**ex 31:** $[x:=f(a,a,z), y:=a]$ unifie $u = f(x,x,y)$ et $v = f(f(y,y,z), f(y,y,z), a)$
$f(x,x,y)$ et $f(f(y,y,z), f(y,x,z), a)$ ne sont pas unifiables.

**Th 32:** Pour u et v deux termes du premier ordre unifiable, il existe un unificateur $\sigma$ de u et v tel que pour tout unificateur $\sigma'$ de u et v, il existe une substitution $\sigma''$ vérifiant $\sigma' = \sigma'' \circ \sigma$. On l'appelle unificateur le plus général, noté $\sigma = mgu(u,v)$ (pour most general unifier).

9.18_Systèmes formels de preuve en logique du premier ordre: exemples.

**Dev 3:** L'algorithme d'unification permet d'obtenir le mgu d'un ensemble d'équations ssi cet ensemble est unifiable

ex 33: Unification de $f(x,x,y)$ et $f(g(y,y,z),f(y,y,z),a)$:

0: $\{f(x,x,y) \sim f(g(y,y,z);f(y,y,z),a)\}$ et $\sigma_0 = Id$

1: $\{x \sim g(y,y,z); x \sim f(y,y,z); y \sim a\}$ et $\sigma_1 = Id$

2: $\{g(y,y,z) \sim f(y,y,z); y \sim a\}$ et $\sigma_2 = [x := g(y,y,z)]$

3: Echec par clash.

← peut bouclier à l'∞

## 2. Méthode des tableaux

Rq 34: Le calcul des séquents dont on enlève la règle de coupure a la propriété de la sous-formule: Si $\Gamma$ et $\Delta$ sont des ensembles de formules et si $\Gamma \vdash \Delta$, alors il existe une dérivation dont toutes les formules sont de la forme $A[x_1 := t_1; \dots; x_m := t_m]$, où $A$ est une sous-formule d'une des formules de $\Gamma$ et $\Delta$ et les $t_i$ sont des termes n'apparaissant pas forcément dans $\Gamma$ ou $\Delta$.

Principe: Dans le calcul des séquents sans la coupure (dont on peut se passer), on va chercher à limiter les règles qui nécessitent de deviner quelque chose: $\forall_g$ et $\exists_d$ pour les termes, la contraction car on ne sait pas à l'avance combien seront nécessaires et l'affaiblissement car on doit deviner à quel moment une hypothèse n'est plus nécessaire

Règles: On enlève la coupure et les contractions. On remplace les règles d'axiome et d'affaiblissement par: $\Gamma, A \vdash A, \Delta \overset{ax_0}{}$ où $A$ est atomique

On contrôle le nombre de fois où l'on utilise les règles $\forall_g$ et $\exists_d$:

$$\frac{\Gamma, A[x := y], \forall^{m-1} x\, A \vdash \Delta}{\Gamma, \forall^m x\, A \vdash \Delta}\ \forall_g^m \qquad \frac{\Gamma \vdash A[x := y], \exists^{m-1} x\, A, \Delta}{\Gamma \vdash \exists^m x\, A, \Delta}\ \exists_d^m$$

où $y$ est une nouvelle variable qui n'apparaît ni dans le séquent conclusion, ni dans les autres branches de la preuve. Si $m = 1$, on efface les formules $\forall^0 x\, A$ et $\exists^0 x\, A$.

$$\frac{\Gamma \vdash A[x := f(x_1, \dots, x_k)], \Delta}{\Gamma \vdash \forall^m x\, A, \Delta}\ \forall_d^s \qquad \frac{\Gamma, A[x := f(x_1, \dots, x_k)] \vdash \Delta}{\Gamma, \exists^m x\, A \vdash \Delta}\ \exists_g^s$$

où $\{x_1, \dots, x_k\} = FV(A)$ et $f$ est un nouveau symbole de fonction qui n'apparaît ni dans le séquent conclusion, ni dans les autres branches de la preuve.

Méthode: 1: On décore chaque quantificateur avec un entier

2: On applique les règles jusqu'à ce que l'ensemble des séquents $S$ n'ait que des formules atomiques.

3: On utilise un algorithme d'unification pour trouver une substitution $\sigma$ telle que pour tout séquent $\Gamma \vdash \Delta$ de $S$, $\Gamma[\sigma] \vdash \Delta[\sigma]$ soit une instance de la règle $ax_0$.

Th 35: Si un séquent est prouvable, la méthode des tableaux appliquée à ce séquent réussit.

Th 36: Si la méthode des tableaux appliquée à un séquent qui ne contient que des formules closes, réussit, alors il est prouvable.

## 3. Méthode de résolution

Def 37: Un littéral est une formule atomique ou sa négation.

Def 38: Une clause est un ensemble fini de littéraux.

Principe: On va chercher à montrer qu'un ensemble de clauses est contradictoire, c'est-à-dire qu'il n'est vrai dans aucune interprétation. Pour cela, on va chercher à dériver la clause vide.

Règles: Pour $C_1, C_2$ des clauses et $L_1, L_2$ des littéraux.

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

Th 39: Un ensemble de clauses $E$ est contradictoire ssi on peut en dériver la clause vide

Ex 40: On veut étudier: $\{C_1: \neg R(x,A), R(x,x);\ C_2: \neg R(v, f(y)), \neg R(v,y);$ $C_3: \neg R(z,z), R(z,a);\ C_4: R(u, f(y)), R(u,y)\}$.

$R(z,z)$ et $R(u, f(y))$

$$\dfrac{\dfrac{C_3 \quad C_4}{R(f(y),a), R(f(y),y)}\ res \quad \dfrac{\dfrac{C_1 \quad C_2}{\neg R(f(y),a), \neg R(f,y,y)}\ res}{\neg R(f(a), f(a))}\ contr \quad R(x,x) \text{ et } R(v, f(y))}{\emptyset}\ res$$

Méthode: Pour prouver $\Gamma \vdash F$, on met $\{\Gamma, \neg F\}$ en forme normale de Skolem (plus de $\exists$, remplacés par des fonctions, tous les $\forall$ en début de formule), on enlève tous les quantificateurs puis on réécrit sous forme normale conjonctive.

On fait alors la résolution de l'ensemble de clauses obtenu.

Th 41: Pour $\Gamma \vdash F$ un séquent, $\Gamma \vdash F$ est prouvable ssi la méthode de résolution sur $\Gamma \vdash F$ renvoie la clause vide.

Appl: Le langage Prolog est basé sur la méthode de résolution.

Règles de la déduction naturelle :

$$\frac{}{A}\,ax \qquad \frac{A \quad B}{A}\,aff \qquad \frac{\begin{array}{c}[A]\\ B\end{array}}{A \to B}\,{\to}i \qquad \frac{A \to B \quad A}{B}\,{\to}e$$

$$\frac{A \quad B}{A \wedge B}\,{\wedge}i \qquad \frac{A \wedge B}{A}\,{\wedge}e^g \qquad \frac{A \wedge B}{B}\,{\wedge}e^d \qquad \frac{A}{A \vee B}\,{\vee}i^g \qquad \frac{B}{A \vee B}\,{\vee}i^d$$

$$\frac{A \vee B \quad \begin{array}{c}[A]\\ C\end{array} \quad \begin{array}{c}[B]\\ C\end{array}}{C}\,{\vee}e \qquad \frac{\begin{array}{c}[A]\\ \bot\end{array}}{\neg A}\,{\neg}i \qquad \frac{\neg A \quad A}{\bot}\,{\neg}e \qquad \frac{\begin{array}{c}[\neg A]\\ \bot\end{array}}{A}\,\bot c$$

$$\frac{A}{\forall x A}\,{\forall}i\ {}^{*}1 \qquad \frac{\forall x A}{A[x:=t]}\,{\forall}e \qquad \frac{A[x:=t]}{\exists x A}\,{\exists}i \qquad \frac{\exists x A \quad \begin{array}{c}[A]\\ C\end{array}}{C}\,{\exists}e\ {}^{*}2$$

*1 $x$ non libre dans les hypothèses de la dérivation de $A$

*2 $x$ non libre dans les hypothèses des dérivations de $\exists x A$ et de $C$ (sous l'hypothèse $A$).