NOM : PINAULT Prénom : Laureline Jury :

~~Algèbre~~ ← Entourez l'épreuve → ~~Analyse~~ Info.

Sujet choisi : (924) Théories et modèles en logique du 1er ordre (expo

Autre sujet :

Références : Introduction à la logique, David, Nour & Raffalli (DNR)
Logique mathématique, T1&2, Cori, Lascar
Les démonstrations et les algorithmes, Dowek

Problématique : Un groupe est un ensemble muni d'une loi interne admettant l'associativité, l'existence d'un élément neutre et l'existence d'un inverse. On peut alors démontrer l'unicité de l'inverse mais on ne peut démontrer la commutativité. Comment formaliser et interpréter ces notions ?

I Formalisation syntaxique : ce qu'on peut écrire

1 Grammaire

Déf 1. Un langage est la donnée d'un ensemble de symboles de fonctions $\mathcal{F}$ munies de leur arité et d'un ensemble de symboles de relation $\mathcal{R}$ munies de leur arité. Les fonctions d'arité 0 sont appelées constantes. Il peut être fini ou infini.

Ex 2. $\mathcal{L}_{groupe} = \{e, *, ^{-1}\}, \{=\}$
$\mathcal{F}$ $\mathcal{R}$

Cas particuliers. Quand le langage ne contient que des symboles de relation d'arité 0, on parle de calcul propositionnel.

Déf 4. On x donne un ensemble infini de variables et un langage $\mathcal{L}$. L'ensemble des termes est le plus petit ensemble contenant les constantes, les variables et clos par application de symboles de fonction.

Ex 5. Sur $\mathcal{L}_{groupe}$: $x^{-1} * (y * e^{-1})^{-1} = t_{ex}$

Arité (théorème unique). Si t est un terme alors t est une constante ou t est une variable ou t s'écrit $f(u_1, \dots, u_n)$ où f est un symbole de fonction d'arité k et $u_1, \dots, u_k$ sont des termes.

Notation. On note $t[y_1/x_1, \dots, y_n/x_n]$ la substitution simultanée des x_i dans t où tous les x_i sont remplacés par les y_i.

Ex 6. $t_{ex}[y/x, x*y/y] = y^{-1} * (x * x * e^{-1})^{-1}$

Déf 9. Les formules atomiques sont de la forme $r(u_1, \dots, u_n)$ où r est un symbole de relation d'arité k et $u_1, \dots, u_k$ sont des termes.

L'ensemble des formules est $\Phi, \Psi ::= A(u_1, \dots, u_n) \mid \top \mid \bot \mid \neg\Phi \mid \Phi \wedge \Psi \mid \Phi \vee \Psi \mid \Phi \Rightarrow \Psi \mid \forall x \Phi \mid \exists x \Phi$ où $e \in \{\forall, \exists\}$, $\circ \in \{\wedge, \vee, \Rightarrow\}$, $A \in \mathcal{R}$ et x est une variable.

Ex 10. Sur $\mathcal{L}_{groupe}$: $\forall x \forall y (x * y = e \rightarrow y = x^{-1})$
et $\forall x \forall y \quad xy = yx \quad$ et $x * e = x$

Arité (théorème unique) : Si Φ est une formule, elle s'écrit $r(u_1, \dots, u_n)$ ou $\neg\Psi$ ou $\Psi \circ \Psi'$ ou $Q x \Psi$.

Déf 12. Les variables libres $FV(\Phi)$ sont définies par récurrence :
- Si $\Phi = r(u_1, \dots, u_n)$, $FV(\Phi)$ sont les variables qui sont dans les u_i
- Si $\Phi = \neg\Psi$, $FV(\Phi) = FV(\Psi)$
- Si $\Phi = \Psi \circ \Psi'$, $FV(\Phi) = FV(\Psi) \cup FV(\Psi')$
- Si $\Phi = Qx\Psi$, $FV(\Phi) = FV(\Psi) \setminus \{x\}$

Les variables liées sont les variables de Φ qui ne sont pas dans $FV(\Phi)$.

Déf 13. Une formule Φ est close si $FV(\Phi) = \emptyset$

Ex 14. $\exists x (xe = x)$ est close mais $\forall y \; xy = e$ ne l'est pas

Déf 15. La clôture universelle de Φ est $\forall x_1 \forall x_2 \dots \forall x_n \Phi$ où $FV(\Phi) = \{x_1, \dots, x_n\}$

Notation 16. On note $\Phi(t/x, \dots)$ la substitution simultanée des x_i après renommage éventuel des variables liées.

2 Théories

Déf 17. Une théorie sur un langage $\mathcal{L}$ est un ensemble (fini ou infini) de formules closes sur ce langage. Les formules sont appelées axiomes de la théorie.

Ex 18. (Théorie de Pégalité) Soit $\mathcal{L}$ contenant $=_2$. Axiomes :
- $\forall x (x = x) \wedge \forall x \forall y (x = y \rightarrow y = x) \wedge \forall x \forall y \forall z (x = y \wedge y = z \rightarrow x = z)$
- $\forall x_1 \dots x_n \; y_1 \dots y_n \; (x_1 = y_1 \wedge \dots \wedge x_n = y_n) \Rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n)$, $f \in \mathcal{F}$
- $\forall x_1 \dots x_n \; y_1 \dots y_n \; (x_1 = y_1 \wedge \dots \wedge x_n = y_n) \Rightarrow (r(x_1, \dots, x_n) \rightarrow r(y_1, \dots, y_n))$, $r \in \mathcal{R}$

Dans toute la suite on ne considèrera que des théories contenant l'égalité.

Ex 19. (Théorie des groupes) $\mathcal{L}_{groupe} = (e, *, ^{-1}, =_2)$. Axiomes :
- associativité : $\forall x \forall y \forall z \; (x * y) * z = x * (y * z)$ (Ass)
- élt neutre : $\forall x \; (x * e = x \wedge e * x = x)$ (ENT)
- inverse : $\forall x \; (x * x^{-1} = e \wedge x^{-1} * x = e)$ (INV)

Ex 20. (Théorie des anneaux) $\mathcal{L}_A = (0, 1, +, -, \times, =_2)$. Axiomes :
- associativité de + : $\forall x \forall y \forall z \; (x + y) + z = x + (y + z)$ (Ass+)
- associativité de $\times$: $\forall x \forall y \forall z \; (x \times y) \times z = x \times (y \times z)$ (Ass×)
- commutativité de + : $\forall x \forall y \; x + y = y + x$ (Com+)

- 0 est élément neutre pour +: $\forall x\ (x+0=x)$ ($\in \mathbb{N}_+$)
- - est inverse pour +: $\forall x\ (x+(-x)=0)$ (Inv_+)
- distributivité: $\forall xyz\ ((x+y)\times z = x\times z + y\times z \wedge z\times(x+y) = z\times x + z\times y)$ (D_{ij})
- 1 est élément neutre pour x: $\forall x\ (x\times 1 = x \wedge 1\times x = x)$ (G_{rx})

Exple 21 (théorie des corps). $\mathcal{L}_K = \mathcal{L}_A$. Axiomes:
$A \cup \forall x\ (x\neq 0 \to \exists y\ (x\times y = 1 \wedge y\times x = 1))$ ($Inv_\times$) $= K$

Exple 22 (arithmétique de Peano). $\mathcal{L}_{PA} = \{0_0, S_1, +_2, \times_2, =_2\}$. PA:
- A_1: $\forall x\ (Sx \neq 0)$
- A_2: $\forall x\ (x=0 \vee \exists y\ (x = Sy))$
- A_3: $\forall xy\ (Sx = Sy \to x = y)$
- A_4: $\forall x\ (x+0=x)$
- A_5: $\forall xy\ (x+Sy = S(x+y))$
- A_6: $\forall x\ (x\times 0 = 0)$
- A_7: $\forall xy\ (x\times Sy = x\times y + x)$
- $Rec = \{Rec_{F,x} / F$ formule$\}$ où $Rec_{F,x}$ est la clôture universelle de: $(F[0/x] \wedge \forall y(F[y/x] \to F[Sy/x])) \to \forall x F$

(P_0 = A_1 à A_7; PA = $P_0 \cup Rec$)

Exple 23 (théorie des ensemble de Zermelo-Fraenkel). $\mathcal{L}_{ZF} = \{=_2, \in_2\}$. ZF:
- extensionnalité: $\forall xy\ (\forall z(z\in x \to z\in y) \to x = y)$
- paire: $\forall xy\ \exists z\ \forall t\ (t\in z \leftrightarrow t = x \vee t = y)$
- réunion: $\forall x\ \exists y\ \forall z\ (z\in y \leftrightarrow \exists t\ (t\in x \wedge z\in t))$
- parties: $\forall x\ \exists y\ \forall z\ (z\in y \leftrightarrow z\subset x)$ où $a\subset b := \forall x\ (x\in a \to x\in b)$
- schéma de remplacement = $\{Rempl_F / F$ formule$\}$ où $Rempl_F$ est la clôture univ de: $\forall xyy'\ (F[x,y] \wedge F[x,y'] \to y = y') \to \exists b\ \forall y\ (y\in b \leftrightarrow \exists x\ (x\in a \wedge F[x,y]))$
- infini: $\exists x\ (\emptyset \in x \wedge \forall y\ (y\in x \to \exists y\ (y\cup y \in x)))$

Rq 24. On pourrait se passer de = en définissant $x=y$ par $\forall z(z\in x \leftrightarrow z\in y)$.

Rq 25. En ajoutant l'axiome de fondation, l'axiome du choix et l'hypothèse du continu à ZF alors on peut modéliser l'ensemble des mathématiques.

3 Notion de prouvabilité et de démonstration

Def 26. Soit F une formule et Γ un ensemble fini de formules. On dit que F est prouvable sous les hypothèses Γ et on note $\Gamma \vdash F$ s'il peut être déduit par une application finie des règles de la déduction naturelle (cf annexe).

Exercice 27. Montrer que $\vdash \neg(A\wedge B) \to (\neg A \vee \neg B)$ avec la déduction naturelle.

Rq 28. Il existe d'autres système de preuve tels que le calcul des séquents et les systèmes à la Hilbert.

Def 29. F une formule, $\mathcal{T}$ une théorie. $\mathcal{T} \vdash F$ ssi $\exists \mathcal{T}'$ fini $\subset \mathcal{T}$, $\mathcal{T}' \vdash F$.

Def 30. $\mathcal{T}$ est consistante ssi $\mathcal{T} \nvdash \bot$. On dit parfois que $\mathcal{T}$ est cohérente.

Def 31. $\mathcal{T}$ est complète si $\mathcal{T}$ est consistante et $\forall F$ $\mathcal{T} \vdash F$ ou $\mathcal{T} \vdash \neg F$.

Rq 32. La plupart des théories utilisées en mathématiques ne sont pas complètes. Par exemple dans G on ne peut ni prouver $\forall xy\ (x*y = y*x)$ ni prouver $\neg\forall xy\ (x*y = y*x)$.

II Interprétation sémantique: à quoi ça correspond

1 Interprétations du langage et valeur d'une formule

Def 33. $\mathcal{L}$ un langage. Une interprétation de $\mathcal{L}$ ou $\mathcal{L}$-structure est un structure $\mathcal{M}$ tq:
- $\mathcal{M}$ a un ensemble non vide noté $|\mathcal{M}|$ et appelé domaine de $\mathcal{M}$
- Pour chaque constante c de $\mathcal{L}$, il existe $c_{\mathcal{M}} \in |\mathcal{M}|$
- Pour chaque fonction f_n de $\mathcal{L}$, il existe $f_{\mathcal{M}} : |\mathcal{M}|^k \to |\mathcal{M}|$
- Pour chaque relation r_n de $\mathcal{L}$, il existe $r_{\mathcal{M}} \subset |\mathcal{M}|^n$

Exple 34.
- $(\mathbb{N}, 1, \times, S, =)$ est une $\mathcal{L}_{groupe}$-structure
- $(\mathbb{R}, 0, 1, +, -, \times, =)$ est une $\mathcal{L}_{\mathbb{R}}$-structure
- $(\mathbb{N}, 0, x\mapsto x+2, +, \times, =)$ est une $\mathcal{L}_{PA}$-structure

Def 35. $\mathcal{M}$ une $\mathcal{L}$-structure. Un environnement est une fonction $e: V \to |\mathcal{M}|$.

Def 36. La valeur d'un terme t $Val_{\mathcal{M}}(t,e)$ est définie par récurrence:
$Val(c,e) = c_{\mathcal{M}}$; $Val(x,e) = e(x)$; $Val(f(u_1,\dots,u_n),e) = f_{\mathcal{M}}(Val(u_1,e),\dots,Val(u_n,e))$

Def 37. La valeur d'une formule F $Val_{\mathcal{M}}(F,e)$ est définie par récurrence:
- $Val(\bot,e) = 0$;
- $Val(r(u_1,\dots,u_n),e) = 1$ ssi $(Val(u_1,e),\dots,Val(u_n,e)) \in r_{\mathcal{M}}$;
- $Val(\neg F) = 1$ ssi $Val(F,e) = 0$;
- $Val(F_1 \wedge F_2) = 1$ ssi $Val(F_1,e) = 1$ et $Val(F_2,e) = 1$;
- $Val(F_1 \vee F_2) = 1$ ssi $Val(F_1,e) = 1$ ou $Val(F_2,e) = 1$;
- $Val(F_1 \to F_2,e) = 1$ ssi $Val(F_1,e) = 0$ ou $Val(F_2,e) = 1$;
- $Val(\forall x\, F_1,e) = 1$ ssi $\forall a \in |\mathcal{M}|$, $Val(F_1, e[a/x]) = 1$;
- $Val(\exists x\, F_1,e) = 1$ ssi $\exists a \in |\mathcal{M}|$, $Val(F_1, e[a/x]) = 1$

Notation 38. On note $\mathcal{M}, e \models F$ pour $Val_{\mathcal{M}}(F,e) = 1$.

Prop 39. Si F est close alors $Val_{\mathcal{M}}(F,e)$ est indépendante de e. On note alors $\mathcal{M} \models F$.

2 Modèle d'une théorie

Def 40 $\mathcal{T}$ une théorie sur $\mathcal{L}$ et $\mathcal{M}$ une $\mathcal{L}$-structure. On dit que $\mathcal{M}$ est un modèle de $\mathcal{T}$ et on note $\mathcal{M} \models \mathcal{T}$ ssi $\forall F \in \mathcal{T}$, $\mathcal{M} \models F$.

Exple 41
- $(\mathbb{Z}, 0, +, -, =)$ est un modèle de $\mathcal{G}$
- $(\mathbb{R}, 0, 1, +, -, \times, =)$ est un modèle de $\mathcal{A}$ et de $\mathcal{K}$
- $(\mathbb{N}, 0, x \mapsto x+1, +, \times, =)$ est un modèle de PA.

Def 42 On dit qu'un modèle est égalitaire si $=$ est interprété par $\{(a,a) \in M^2\}$. On ne considérera que des modèles égalitaires.

Def 43 F formule close. F est valide dans $\mathcal{T}$, noté $\mathcal{T} \models F$ ssi $\forall \mathcal{M}$ modèle de $\mathcal{T}$, $\mathcal{M} \models F$

Def 44 $\mathcal{T}$ est contradictoire ssi il n'existe pas de modèle de $\mathcal{T}$.

3 Lien entre la syntaxe et la sémantique

Thm 45 (Correction) (i) Si $\mathcal{T}$ est non contradictoire alors $\mathcal{T}$ est consistante
(ii) F close. $\mathcal{T} \vdash F \Rightarrow \mathcal{T} \models F$

Cor 46 S'il existe $\mathcal{M}$ modèle de $\mathcal{T}$ tq $\mathcal{M} \not\models F$ alors F n'est pas démontrable dans $\mathcal{T}$.

Exple 47 $\forall x y\ (x*y = y*x)$ n'est pas démontrable dans $\mathcal{G}$, de même que sa négation.

Thm 48 (Complétude) (i) Si $\mathcal{T}$ est consistante alors $\mathcal{T}$ est non contradictoire
(ii) F close. $\mathcal{T} \models F \Rightarrow \mathcal{T} \vdash F$

DNT (1)

Cas particulier 49 Théorème de complétude du calcul prépositionnel.

Thm 50 (Compacité) $\mathcal{T}$ admet un modèle ssi $\forall$ ensemble fini de $\mathcal{T}$ admet un modèle.

Cor 51 Si $\mathcal{T}$ a des modèles finis de cardinal arbitrairement grands alors $\mathcal{T}$ a un modèle infini.

Cor 52 Si $\mathcal{T}$ a un modèle infini alors $\mathcal{T}$ a un modèle infini non dénombrable.

Exercice 52 bis Il n'existe pas de théorie finie des corps de caractéristique 0.

III Décidabilité d'une théorie

Def 53
- Une théorie est récursive si le problème "$F \in \mathcal{T}$?" est décidable
- Une théorie est décidable si le problème "$\mathcal{T} \vdash F$?" est décidable

1 Décidabilité

Prop 54 Une théorie complète et récursive sur un langage au plus dénombrable est décidable.

Def 55 $\mathcal{T}$ admet l'élimination des quantificateurs ssi $\forall F$ close $\exists G$ close et sans quantificateurs telle que $\mathcal{T} \vdash F \leftrightarrow G$

Thm 56 Si $\mathcal{T}$ admet l'élimination des quantificateurs et $\forall A$ atomique close on a $\mathcal{T} \vdash A$ ou $\mathcal{T} \vdash \neg A$ alors $\mathcal{T}$ est complète.

Application 57 L'arithmétique de Presburger est décidable. ← DNT (2)

2 Indécidabilité

Prop 58 Si on peut construire dans un langage de propositions N, Null, Succ, Pred, Mult et Eq et une théorie permettant d'encoder les programmes alors cette théorie est indécidable. ← DNT (3)

Application 59 PA est indécidable

Application 60 (Church) Si $\mathcal{L}$ contient un symbole de relation binaire alors la théorie vide sur $\mathcal{L}$ est indécidable.

IV Limites de la logique du premier ordre

Exple 61 On ne peut pas, en logique du premier ordre définir la théorie des anneaux principaux car il faudrait pour cela quantifier sur des ensembles et non plus des variables → voir la logiques d'ordre supérieur

Exple 62 Il est difficile de théoriser les espaces vectoriels en logique du 1er ordre car on manipule deux types d'objets : les vecteurs et les scalaires.
Une solution est d'étendre le langage avec des $(\forall)^{\text{vect}}$ mais alors on ne peut pas, par exemple, exprimer l'indépendance linéaire.
Une autre solution est de rajouter des prédicats V et S correspondant à "x est un vecteur" ou "x est un scalaire" mais alors on peut écrire, par exple, $\forall x\ V(x)$
→ voir les logique multisorte

Exple 63 Il est impossible, par exemple, de théoriser $\mathbb{N}$. En effet, par le corollaire 52, toute théorie qui a $\mathbb{N}$ pour modèle a également un modèle non dénombrable.
On peut parler de modèles standard de PA qui sont tous isomorphes à $\mathbb{N}$ et de modèles non standard dans lesquels il existe des entiers non standards.

Annexe 1 : Règles de la déduction naturelle

(i) $\dfrac{}{\Gamma, A \vdash A}\ ax$ (ii) $\dfrac{\Gamma \vdash A}{\Gamma, B \vdash A}\ aff$

(iii) $\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_i$ (iv) $\dfrac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \to_e$

(v) $\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge_i$ (vi)$_a$ $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge_e^g$ (vi)$_b$ $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge_e^d$

(vii)$_a$ $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_i^g$ (vii)$_b$ $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee_i^d$ (viii) $\dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee_e$

(ix) $\dfrac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_i$ (x) $\dfrac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \bot}\ \neg_e$ (xi) $\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \bot_c$

(xii) $\dfrac{\Gamma \vdash A \quad x \notin VL(\Gamma)}{\Gamma \vdash \forall x\, A}\ \forall_i$ (xiii) $\dfrac{\Gamma \vdash \forall x\, A}{\Gamma \vdash A[t/x]}\ \forall_e$

(xiv) $\dfrac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x\, A}\ \exists_i$ (xv) $\dfrac{\Gamma \vdash \exists x\, A \quad \Gamma, A \vdash C \quad x \notin VL(\Gamma) \; x \notin VL(C)}{\Gamma \vdash C}\ \exists_e$