NOM : Rouhling **Prénom :** Damien **Jury :**

Algèbre ← Entourez l'épreuve → **Analyse**

Sujet choisi : 917 - Logique du premier ordre : syntaxe et sémantique

Autre sujet : Réf : DNR, Introduction à la logique
Dowek, les démonstrations et les algorithmes

I Langages du premier ordre, formules et théories

Idée : les termes représentent les objets que l'on étudie, les formules leurs propriétés et les théories les hypothèses que l'on fait sur eux

Déf 1 : Un langage est un triplet $L(C, F, P)$ où
- C est un ensemble de "constantes"
- F est un ensemble de "symboles de fonction" chacun muni d'une "arité" (un entier)
- P est un ensemble de "symboles de prédicat" chacun muni d'une arité

Ex 1 : le langage de la théorie des groupes est $(\{e\}, \{*, ^{-1}\}, \{=\})$ où $*$ et $=$ sont d'arité 2 et $^{-1}$ d'arité 1

Déf 2 : On fixe un ensemble infini V de "variables".
L'ensemble des termes $T(L, V)$ est donné par la grammaire $t ::= x \mid c \mid f(t_1, \dots, t_n)$ où $x \in V$, $c \in C$ et $f \in F$ est d'arité n.
Un terme est dit clos s'il ne possède pas de variable

Ex 2 : $x * y^{-1}$ est un terme qui n'est pas clos, $e * e^{-1}$ l'est en revanche.

Déf 3 : L'ensemble des formules du premier ordre est donné par la grammaire :
$A ::= p(t_1, \dots, t_n) \mid \bot \mid \top \mid A_1 \vee A_2 \mid A_1 \wedge A_2 \mid A_1 \to A_2 \mid \neg A \mid \exists x A \mid \forall x A$
où $x \in V$, $(t_1, \dots, t_n) \in T(L, V)^n$ et $p \in P$ d'arité n

Ex 3 : $\forall x (x * e = x) \wedge \forall x (e * x = x)$

Déf 4 : On définit par induction l'ensemble des variables libres d'une formule :
$VL(p(t_1 \dots t_n)) \equiv \bigcup_{i=1}^{n} \{x \in V, x \text{ variable de } t_i\}$
$VL(\bot) \equiv VL(\top) \equiv \emptyset$
$VL(A_1 \vee A_2) \equiv VL(A_1 \wedge A_2) \equiv VL(A_1 \to A_2) \equiv VL(A_1) \cup VL(A_2)$
$VL(\neg A) \equiv VL(A)$ $VL(\exists x A) \equiv VL(\forall x A) \equiv VL(A) \setminus \{x\}$

Ex 4 : $VL(\forall x (x * y = y * x)) \equiv \{y\}$

Déf 5 : A est dite close si $VL(A) \equiv \emptyset$
Une variable apparaissant dans A qui n'est pas libre est dite liée.
A et B sont α-équivalentes si elles sont syntaxiquement identiques modulo renommage des variables liées
On identifiera les formules α-équivalentes

Ex 5 : $\forall y (x * y = y * x)$ et $\forall z (x * z = z * x)$ sont α-équivalentes mais ne sont pas α-équivalentes à $\forall z (y * x = x * z)$

Déf 6 : Si $x \in VL(A)$, on définit par induction la substitution de x par t dans A :
$p(t_1 \dots t_n)[x := t] \equiv p(u_1 \dots u_n)$ où pour tout $i \in [\![1, n]\!]$ u_i est t_i où chaque occurrence de x est remplacée par t
$\bot[x := t] \equiv \bot$ $\top[x := t] \equiv \top$
$(A_1 \vee A_2)[x := t] \equiv A_1[x := t] \vee A_2[x := t]$
$(A_1 \wedge A_2)[x := t] \equiv A_1[x := t] \wedge A_2[x := t]$
$(A_1 \to A_2)[x := t] \equiv A_1[x := t] \to A_2[x := t]$
$(\neg A)[x := t] \equiv \neg (A[x := t])$
$(\exists y A)[x := t] \equiv \exists y (A[x := t])$ où $y \not\equiv x$ et y n'apparaît
$(\forall y A)[x := t] \equiv \forall y (A[x := t])$ pas dans t
$(\exists x A)[x := t] \equiv \exists x A$ $(\forall x A)[x := t] \equiv \forall x A$

Rq 1 : si y apparaît dans t, on travaillera avec une version α-équivalente de la formule afin d'éviter de capturer les variables de t.

Ex 6 : $(\forall y (x * y = y * x))[x := e * y]$
$\equiv \forall z ((e * y) * z = z * (e * y))$

Déf 7 : Une théorie est un ensemble de formules closes

Ex 7 : théorie des groupes : $\{\forall x \forall y \forall z\, (x * (y * z) = (x * y) * z),\ \forall x\, (x * e = x \wedge e * x = x),\ \forall x\, (x * x^{-1} = e \wedge x^{-1} * x = e)\}$

II Interprétations : les modèles

Idée : les modèles sont des contextes liant les termes aux objets, les formules aux propriétés qu'elles expriment. Ils permettent d'étudier la "véracité" d'une formule vis-à-vis de ce contexte.

Déf 8 : On appelle modèle du langage L la donnée $\mathcal{M}$ de :
- un ensemble $|\mathcal{M}|$ appelé domaine de $\mathcal{M}$
- pour tout $c \in C$, $c_{\mathcal{M}} \in |\mathcal{M}|$
- pour tout $f \in F$ d'arité n, $f_{\mathcal{M}} : |\mathcal{M}|^n \longrightarrow |\mathcal{M}|$
- pour tout $p \in P$ d'arité n, $p_{\mathcal{M}} \in \mathcal{P}(|\mathcal{M}|^n)$

Ex 8 : théorie des groupes : $|\mathcal{M}| = \mathbb{Z}/p\mathbb{Z}$, $e_{\mathcal{M}} \equiv \bar{0}$, $*_{\mathcal{M}} \equiv$ addition mod p, ${}^{-1}{}_{\mathcal{M}} \equiv$ multiplication par -1 mod p, $=_{\mathcal{M}} \equiv \{(\bar{x}, \bar{y}) \mid x \equiv y\, [p]\}$

Déf 9 : On appelle environnement toute fonction $e : V \to |\mathcal{M}|$

Déf 10 : On définit par induction l'interprétation d'un terme ou d'une formule dans l'environnement e par rapport au modèle $\mathcal{M}$:

$[\![c]\!]_e^{\mathcal{M}} \equiv c_{\mathcal{M}}$ $\quad [\![x]\!]_e^{\mathcal{M}} \equiv e(x)$ $\quad [\![f(t_1 \dots t_n)]\!]_e^{\mathcal{M}} \equiv f_{\mathcal{M}}([\![t_1]\!]_e^{\mathcal{M}} \dots [\![t_n]\!]_e^{\mathcal{M}})$

$[\![A]\!]_e^{\mathcal{M}} \in \{0, 1\}$ avec :

$[\![p(t_1 \dots t_n)]\!]_e^{\mathcal{M}} \equiv 1$ ssi $([\![t_1]\!]_e^{\mathcal{M}}, \dots, [\![t_n]\!]_e^{\mathcal{M}}) \in p_{\mathcal{M}}$

$[\![\bot]\!]_e^{\mathcal{M}} \equiv 0$ $\quad [\![\top]\!]_e^{\mathcal{M}} \equiv 1$

$[\![A_1 \vee A_2]\!]_e^{\mathcal{M}} \equiv 1$ ssi $[\![A_1]\!]_e^{\mathcal{M}} \equiv 1$ ou $[\![A_2]\!]_e^{\mathcal{M}} \equiv 1$

$[\![A_1 \wedge A_2]\!]_e^{\mathcal{M}} \equiv 1$ ssi $[\![A_1]\!]_e^{\mathcal{M}} \equiv 1$ et $[\![A_2]\!]_e^{\mathcal{M}} \equiv 1$

$[\![A_1 \to A_2]\!]_e^{\mathcal{M}} \equiv 1$ ssi $[\![A_1]\!]_e^{\mathcal{M}} \equiv 0$ ou $[\![A_2]\!]_e^{\mathcal{M}} \equiv 1$

$[\![\neg A]\!]_e^{\mathcal{M}} \equiv 1$ ssi $[\![A]\!]_e^{\mathcal{M}} \equiv 0$

$[\![\exists x A]\!]_e^{\mathcal{M}} \equiv 1$ ssi il existe $a \in |\mathcal{M}|$ tel que $[\![A]\!]_{e[x:=a]}^{\mathcal{M}} \equiv 1$

$[\![\forall x A]\!]_e^{\mathcal{M}} \equiv 1$ ssi pour tout $a \in |\mathcal{M}|$, $[\![A]\!]_{e[x:=a]}^{\mathcal{M}} \equiv 1$

Ex 9 : pour tout $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$ $\quad [\![e * x = x]\!]_{x \mapsto \bar{x}}^{\mathcal{M}} \equiv 1$

Déf 11 : Si $[\![A]\!]_e^{\mathcal{M}} \equiv 1$ on dit que A est vraie par rapport au modèle $\mathcal{M}$ dans l'environnement e et on note $\mathcal{M}, e \models A$

A est satisfiable ssi il existe $\mathcal{M}$ et e tels que $\mathcal{M}, e \models A$

A est un théorème ssi pour tous $\mathcal{M}$ et e, $\mathcal{M}, e \models A$

Prop 1 : $[\![A]\!]_e^{\mathcal{M}}$ ne dépend que de la valeur de e sur les variables libres de A.

Cor 1 : Si A est close, $[\![A]\!]_e^{\mathcal{M}}$ ne dépend pas de e

Rq 2 : $[\![A]\!]_e^{\mathcal{M}}$ dépend tout de même de $\mathcal{M}$: ni l'axiome du choix, ni sa négation ne sont des théorèmes

Déf 12 : Un modèle $\mathcal{M}$ de L est un modèle de la théorie T ssi pour tout $A \in T$, $\mathcal{M} \models A$

T est contradictoire ssi il n'existe pas de modèle de T

A close est valide dans T ($T \models A$) ssi pour tout modèle $\mathcal{M}$ de T, $\mathcal{M} \models A$

Développement 1

Thm 1 (Lowenheim-Skolem) : si L est au plus dénombrable, Si T admet un modèle infini, alors T admet un modèle dénombrable.

III La notion de preuve

Idée : déterminer si une formule est "vraie" à l'aide de critères syntaxiques. Définir rigoureusement la notion de démonstration.

1 - Prouvabilité

Déf 13 : Un séquent est un couple $\Gamma \vdash A$ où Γ est un ensemble de formules (fini) appelées hypothèses et A est une formule : la conclusion.

Déf 14 (déduction naturelle) : Un séquent $\Gamma \vdash A$ est prouvable ou dérivable si, à l'aide des règles Figure 1, on peut construire un arbre (de dérivation) de racine $\Gamma \vdash A$ et dont toutes les feuilles sont vides.

Ex 10 : le séquent $\vdash \neg A \Leftrightarrow (A \to \bot)$ est prouvé Figure 2

Déf 15 : Une théorie T prouve la formule A s'il existe $\Gamma \subseteq T$ fini tel que $\Gamma \vdash A$ est dérivable. On note $T \vdash A$.

T est consistante ssi $T \nvdash \bot$

T est complète si pour toute formule close A, $T \vdash A$ ou $T \vdash \neg A$

Rq 3 : les théories que l'on manipule sont souvent incomplètes.

Déf 16 : T est décidable si le problème suivant l'est : étant donné une formule A, est-ce que $T \vdash A$?

Ex 11 : l'arithmétique de Presburger est décidable. L'arithmétique de Peano est indécidable.

Thm 2 : Si T est complète et récursive sur L au plus dénombrable, alors T est décidable.

Thm 3 : Si T est non contradictoire et contient l'arithmétique élémentaire (Figure 3), alors T est indécidable.

Cor 2 : La logique du premier ordre est indécidable sur le langage de l'arithmétique.

2 - Lien avec les modèles

Développement 2
Thm 4 (correction) : Si T est non contradictoire, alors T est consistante

Thm 5 (complétude) : Si T est consistante alors T est non contradictoire

D Lemme 1 : Il existe $Th \supseteq T$ sur un langage $L' \supseteq L$, complète et telle que pour toute formule A sur L' vérifiant $VL(A) = \{x\}$, il existe $c_A \in C'$ tel que $Th \vdash \exists x A \to A[x := c_A]$

Lemme 2 : Th est non contradictoire $\square$

Cor 3 : Si A est close, $T \vdash A$ ssi $T \models A$

Thm 6 (compacité) :

- Version sémantique : T est contradictoire ssi il existe un sous-ensemble fini de T qui est contradictoire
- Version syntaxique : T est consistante ssi tout sous-ensemble fini de T est consistant.

Application 1 : Si T a des modèles finis de cardinal arbitrairement grand, alors T a un modèle infini.

Application 2 : Si T a un modèle infini, alors T a un modèle infini non dénombrable.

Figure 1 :

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

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

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

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

$$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}\,\bot_e \qquad \dfrac{}{\Gamma \vdash \top}\,\top_i \qquad \dfrac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\,\neg_i \qquad \dfrac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\,\neg_e$$

$$\dfrac{\Gamma \vdash A}{\Gamma \vdash \forall x A}\,x \notin VL(\Gamma)\ \forall_i \qquad \dfrac{\Gamma \vdash \forall x A}{\Gamma \vdash A[x := t]}\,\forall_e$$

$$\dfrac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x A}\,\exists_i \qquad \dfrac{\Gamma \vdash \exists x A \qquad \Gamma, A \vdash C}{\Gamma \vdash C}\,x \notin VL(\Gamma, C)\ \exists_e$$

$$\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\,\bot_c$$

Figure 2 :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg A, A \vdash \neg A}\,ax \qquad \dfrac{}{\neg A, A \vdash A}\,ax}{\neg A, A \vdash \bot}\,\neg_e}{\neg A \vdash A \to \bot}\,\to_i}{\vdash \neg A \to (A \to \bot)}\,\to_i \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A \to \bot, A \vdash A \to \bot}\,ax \qquad \dfrac{}{A \to \bot, A \vdash A}\,ax}{A \to \bot, A \vdash \bot}\,\to_e}{A \to \bot \vdash \neg A}\,\neg_i}{\vdash (A \to \bot) \to \neg A}\,\to_i}{\vdash \neg A \leftrightarrow (A \to \bot)}\,\wedge_i$$

Figure 3 :

$\forall x\ (Sx \neq 0)$

$\forall x\ (x = 0 \vee \exists y\ (x = Sy))$

$\forall x \forall y\ (Sx = Sy \to x = y)$

$\forall x\ (x + 0 = x)$

$\forall x \forall y\ (x + Sy = S(x + y))$

$\forall x\ (x * 0 = 0)$

$\forall x \forall y\ (x * Sy = x * y + x)$