918 - SYSTÈMES FORMELS DE PREUVE EN LOGIQUE DU PREMIER ORDRE : EXEMPLES

I/ Logique du premier ordre

1) Syntaxe

Soit $V = \{v_i\}_i$ un ensemble dénombrable de symboles de variables, $F = \{f_i\}_i$ un ensemble dénombrable de symboles de fonctions, $C = \{c_i\}_i$ un ensemble dénombrable de symboles de constantes et $P = \{p_i\}_i$ un ensemble dénombrable de symboles de prédicats.

def 1 L'ensemble T des termes est le plus petit ensemble tel que $C \subset T$, $V \subset T$ et si $t_i \in T$ et $f \in F$, $f(t_i) \in T$

ex 2 $f_1(v_1)$, c_1, v_1 et $f_2(v_1, v_2, v_3)$ sont des termes.

def 3 L'ensemble A des formules atomiques est le plus petit ensemble tel que si $p \in P$ et $t \in T$, $p(t) \in A$.

ex 4 $p_1(c_1)$ et $p_2(c_1, f(v_1))$ sont des formules atomiques

def 5 L'ensemble des formules du 1er ordre, FO, est le plus petit ensemble tel que $A \subset FO$ et si $F, F' \in FO$ et $x \in V$, $(F \vee F')$, $\neg(F)$, $(F \wedge F')$, $\exists x F$ et $\forall x F$ sont dans FO

ex 6 $\forall v_2\ p_2(c_1, f(v_2))$ est une formule

def 7 Si $F = \forall v F'$ ou $F = \exists v F'$, les occurrences de v dans F' sont dites quantifiées. Les occurrences non quantifiées sont dites libres

ex 8 Dans $(\forall v_1\ p_1(v_1)) \vee p_2(c_1, f(v_1))$, la 1ère occurrence de v_1 est quantifiée, pas la 2e

def 9 La substitution de la variable v par le terme t dans la formule F est la formule $F[v := t]$ dans laquelle toutes les occurrences de v sont remplacées par t

2) Sémantique

def 10 Une structure est la donnée d'un domaine M et, pour chaque symbole c_i (resp f_i, resp p_i) d'un élément $c_i^M \in M$ (d'une fonction f_i^M sur M, resp. d'un prédicat p_i^M sur M)

ex 11 - $\{\mathbb{N}, \{+\}, \{=\}\}$ est une structure, notée M_0

def 12 : La valeur d'un terme dans une structure M munie d'une valuation μ est définie par induction : la valeur des variables libres est donnée par μ et celle des constantes et fonctions par la structure

ex 13 La valeur de $v_1 + v_2$ dans M_0 munie de la valuation $(v_1 = 3, v_2 = 5)$ est 8

def 14 On définit le fait pour une structure M munie d'une valuation μ d'être un modèle pour la formule F (noté $M, \mu \models F$) par induction :

- si $F = p_i(t_j) \in A$, $M, \mu \models F$ si $p_i^M(\mu(t_i)) = 1$
- si $F = F_1 \wedge F_2$; $M, \mu \models F$ si $M, \mu \models F_1$ et $M, \mu \models F_2$
- si $F = F_1 \vee F_2$; $M, \mu \models F$ si $M, \mu \models F_1$ ou $M, \mu \models F_2$
- si $F = \neg F_1$; $M, \mu \models F$ si M, μ n'est pas modèle de F_1
- si $F = \exists v_i F_1$; $M, \mu \models F$ si il existe $e \in M$ et μ' une valuation tels que $\mu'(v_i) = e$, $\forall j \neq i$, $\mu'(v_j) = \mu(v_j)$ et $M, \mu' \models F_1$.
- si $F = \forall v_i F_1$; $M, \mu \models F$ si pour tout $e \in M$ et toute valuation μ' tq $\mu'(v_i) = e$ et $\forall j \neq i$, $\mu'(v_j) = \mu(v_j)$ on a $M, \mu' \models F_1$.

def 15 Une formule F est satisfiable si il existe une structure M et une valuation μ tq $M, \mu \models F$. Elle est valide si pour toutes structure M et valuation μ, $M, \mu \models F$

ex 16 M_0 est un modèle de $\forall v_1 \forall v_2\ (v_1 + v_2) = (v_2 + v_1)$. Cette formule est donc satisfiable. La formule $\forall v_1 (p(v_1) \vee \neg p(v_1))$ est valide.

3) Théories et modèles

def 17 Une théorie est un ensemble de formules closes (sans occurrences libres de variables)

ex 18 La théorie de Presburger est une théorie

def 19 Une structure M est un modèle de la théorie T si M est modèle de toutes les formules de T (pas besoin de valuation car les formules de T sont closes)

ex 20 M_0 est un modèle de la théorie de Presburger.

def 21 Une formule F est conséquence sémantique de la théorie T (noté $T \models F$) si tout modèle de T est modèle de F.

4) Systèmes de déduction

def 22 Un séquent est un couple (Γ, F), noté $\Gamma \vdash F$, où Γ est un ensemble fini de formules (nommées prémisses) et F une formule (nommée conséquence)

ex 23 $\forall v_1\ p_1(v_1), \neg p_2(v_2) \vdash \neg p_2(v_2)$ est un séquent

def 24 Une règle de déduction est un couple formé d'une liste de séquents $S_1, \dots S_n$ et d'un séquent S_f. On la note $\dfrac{S_1 \ \dots\ S_n}{S_f}$

ex 25 : Modus ponens $\dfrac{\Gamma \vdash \forall v_1 (F_1 \to F_2) \quad \Gamma \vdash \forall v_1 F_1}{\Gamma \vdash \forall v_1 F_2}$

def 26 Un système de déduction est un ensemble de règles de déduction.

ex 27 La déduction naturelle, présentée au II, est un système de déduction.

déf 28 Un séquent est prouvable dans un système de déduction s'il peut être obtenu en utilisant un nombre fini de règles de déduction.

déf 29 Une formule F est prouvable dans la théorie T (noté $T \vdash F$) si $\exists T_0 \subset T$ fini tq $T_0 \vdash F$ est prouvable

déf 30 Une théorie est cohérente si il n'y a aucune formule F telle que F et $\neg F$ sont prouvables. Une théorie est complète si pour toute formule F, soit F, soit $\neg F$ est prouvable.

II / Déduction naturelle

1) Formules

La déduction naturelle est le système de déduction composé des règles suivantes :

$$\frac{}{\Gamma, F \vdash F}\text{ axiome} \;;\quad \frac{\Gamma, F_1 \vdash F_2}{\Gamma \vdash F_1 \to F_2}\text{ intro} \to \;;\quad \frac{\Gamma \vdash F_1 \quad \Gamma \vdash F_1 \to F_2}{\Gamma \vdash F_2}\text{ elim} \to$$

$$\frac{\Gamma \vdash F_1 \quad \Gamma \vdash F_2}{\Gamma \vdash F_1 \wedge F_2}\text{ intro} \wedge \;;\quad \frac{\Gamma \vdash F_1 \wedge F_2}{\Gamma \vdash F_1}\text{ elim} \wedge 1 \;;\quad \frac{\Gamma \vdash F_1 \wedge F_2}{\Gamma \vdash F_2}\text{ elim} \wedge 2$$

$$\frac{\Gamma \vdash F_1}{\Gamma \vdash F_1 \vee F_2}\text{ intro} \vee 1 \quad \frac{\Gamma \vdash F_2}{\Gamma \vdash F_1 \vee F_2}\text{ intro} \vee 2 \;;\quad \frac{\Gamma \vdash F_1 \vee F_2 \quad \Gamma, F_1 \vdash F_3 \quad \Gamma, F_2 \vdash F_3}{\Gamma \vdash F_3}\text{ elim} \vee$$

$$\frac{\Gamma \vdash F \text{ où v est libre dans } F}{\Gamma \vdash \forall v F}\text{ intro} \forall \;;\quad \frac{\Gamma \vdash \forall v F}{\Gamma \vdash F[v := t]}\text{ elim} \forall$$

$$\frac{\Gamma \vdash F[v := t]}{\Gamma \vdash \exists v F}\text{ intro} \exists \;;\quad \frac{\Gamma \vdash \exists v F_1 \quad \Gamma, F_1 \vdash F_2}{\Gamma \vdash F_2}\text{ elim} \exists \text{ où v est quantifié dans } \Gamma \text{ et } F_2$$

2) Propriétés

th 31 La déduction naturelle est correcte : si F est une formule et T une théorie telles que $T \vdash F$ alors $T \models F$

déf 32 Une théorie T_H est dite de Henkin si pour toute formule F telle que $T_H \vdash \exists v F$ et v est libre dans F il existe un symbole $c \in C$ tq que $T_H \vdash F[v := c]$

th 33 Une théorie de Henkin cohérente et complète admet un modèle.

th 34 Pour toute théorie cohérente il existe une extension de la syntaxe (ajout de symboles de constantes) et une extension T' de T ($T' = T \cup \{$formules utilisant les anciens et les nouveaux symboles$\}$) telle que T' est une théorie de Henkin cohérente et complète.

appli 35 Les théories cohérentes admettent un modèle.

th 36 Complétude de la déduction naturelle en logique du premier ordre : Si F est une formule et T une théorie telles que $T \models F$ alors $T \vdash F$

appli 37 Les conséquences sémantiques d'une théorie sont récursivement énumérables alors que la classe des modèles ne l'est pas (ce qui empêche de tester de façon récursivement énumérable si chaque structure possible est un modèle pour la théorie T et pour la formule F)

rq 38 Il existe un système de déduction similaire à la déduction naturelle, nommé calcul des séquents, qui symétrise les règles de la déduction naturelle.

III / Résolution

1) Clauses

déf 39 Une clause est une disjonction de formules atomiques ou de négation de formules atomiques. La clause vide est notée $\perp$

ex 40 $\neg P_1(v_1) \wedge P_2(f(v_1, v_2), v_3)$ est une clause.

th 41 Pour toute formule F, il existe une formule F' telle que
- F et F' sont équisatisfiables (F admet 1 modèle ssi F' en admet 1)
- F' ne contient aucun quantificateur existentiel.
- F' est une conjonction de clôtures universelles de clauses.

ex 42. On part de $F = \forall v_1 \exists v_2\ P_1(f_1(v_1, v_2)) \wedge \exists v_3\ P_2(f_2(v_3), f_3(v_2))$

On applique alors la transformation de Skolem à F pour éliminer les $\exists$:

$\forall v_1\ P_1(f_1(v_1, f_{v_2}(v_1))) \wedge P_2(f_2(f_{v_3}(v_1)), f_3(f_{v_2}(v_1)))$

Puis on distribue le $\forall$ et on obtient

$F' = \forall v_1\ P_1(f_1(v_1, f_{v_2}(v_1))) \wedge P_2(f_2(f_{v_3}(v_1)), f_3(f_{v_2}(v_1)))$ de la forme voulue.

2) Unification

def 43 : Une substitution σ telle que $\sigma(F_1) = \sigma(F_2)$ est un unificateur de F_1 et F_2

Exemple 44 : $\{v_1 := c_1, v := c_2\}$ est un unificateur de $P(c_1, c_1)$ et $P(v_1, v_2)$.

def 45 : Un unificateur σ_1 est plus général que σ_2 si $\exists \sigma_3$, $\sigma_2 = \sigma_3 \circ \sigma_1$

ex 46 : $\{v_1 := f(v_2, v_3)\}$ est plus général que $\{v_1 := c_1, f(c_2)\}$

Thm 47: Si il existe un unificateur pour F_1 et F_2 alors il existe un unificateur principal σ_p tel que pour tout unificateur σ, σ_p est plus général que σ.

Remarque 48: Les résultats sur les unificateurs s'étendent à un nombre fini de formules.

XVI **Thm 49**: L'algorithme suivant calcule l'unificateur principal de deux formules atomiques si elles sont unifiables.

Algorithme d'unification:

Si les prédicats des deux formules sont différents ou que l'une est niée et l'autre pas, les formules ne sont pas unifiables.

Sinon il faut et il suffit d'unifier les termes arguments des prédicats.

Pour ceci on pose $E = \{t_i \sim t_i'\}$ où t_i et t_i' sont les termes arguments des prédicats et $\sigma = \text{Identité}$

Tant que $E \neq \emptyset$
- prendre $t_1 \sim t_2 \in E$.
- Si $t_1 = f_1(t_{1i})$ et $t_2 = f_2(t_{2i})$ et $f_1 \neq f_2$
  - t_1 et t_2 ne sont pas unifiables.
- Sinon si $f_1 = f_2$
  - retirer $t_1 \sim t_2$ de E
  - ajouter $t_{1i} \sim t_{2i}$ pour tout i.

  } cas 1
- Si $t_1 = v$ et $t_2 = v$
  - retirer $t_1 \sim t_2$ de E

  } cas 2.
- si $t_1 = v$ ou $t_2 = v$ et $t_1 \neq t_2$
  - On suppose $t_1 = v$.
  - Si v a une occurence dans t_2
    - E n'est pas unifiable.
  - Sinon

    cas 3 { $\sigma := \sigma \circ \{v := t_2\}$ ~~et~~ t_2 est substitué à v dans toutes les égalités de E et $t_1 \sim t_2$ est retiré de E.

Remarque 50: La complexité de cet algorithme peut être exponentielle. Par exemple pour l'unification de $f(u_n, v_n)$ et $f(v_n, w_n)$ où $u_{n+1} = f(u_n, v_n)$ et $w_{n+1} = f(v_n, w_n)$.

3) Résolution

def 51: La résolution est un système de déduction composé des règles suivantes:

résolution $\dfrac{C_1 \vee A \quad C_2 \vee \neg A'}{\sigma(C_1 \vee C_2)}$ où σ est unificateur principal de A et A'.

contraction $\dfrac{C_1 \vee A \quad C_2 \vee A'}{\sigma(A \vee C_1 \vee C_2)}$ où σ est unificateur principal de A et A'.

def 52: Une preuve par résolution d'une clause C à partir d'un ensemble S est une suite $C_1 \dots C_n$ telle que $C_n = C$ et $\forall i \in [\![1, n]\!]$ $C_i \in S$ ou $\exists j, k < i$ $\dfrac{C_j \quad C_k}{C_i}$

def 53: Une preuve de C par réfutation est une preuve de la clause vide $\perp$ à partir de $S \cup \neg C$.

thm 54: Correction de la résolution: Si il existe une réfutation de C à partir de S, il n'existe pas de modèle de S qui soit un modèle de C.

def 55: Un modèle de Herbrand est un modèle dont le domaine est l'ensemble des termes clos et l'interprétation des fonctions $f(t_i)$ est $f^M(t_i) = f(t_i)$ le terme correspondant à la fonction. Il n'y a pas de contrainte sur l'interprétation des prédicats.

thm 56: Complétude de la résolution: Si aucun modèle de S n'est modèle de C alors il existe une réfutation de C dans S. XVI

Refs: Logique et fondements de l'informatique Lassaigne Rougemont
David Nour Raffalli. (Introduction à la logique)