Master 1 Année 2010/2011

Logique pour l'Informatique Avancée

Feuille de TD n° 1

Nous allons dans ce premier TD apprendre à utiliser le langage et le formalisme de la logique du premier ordre (calcul des prédicats) afin d'être à l'aise en manipulant les notions vues en cours.

Exercice 1 — Soient a et b des symboles de constante, f (resp. R) un symbole de fonction (resp. de relation) unaire et g (resp. S) un symbole de fonction (resp. de relation) binaire. Les expressions suivantes sont-elles des termes ? Des formules ? Si oui, quelle en est la taille ?

1. $g(a, f(b))$
2. $f(g(f(x), g(a, f(y))))$
3. $g(R(a), b)$
4. $S(f(a), g(x, R(y)))$
5. $(\forall x, g(x, x) = b) \wedge (\exists x, f(x) = b)$
6. $\forall x \exists y, (S(x, a) \wedge R(b) \Rightarrow S(f(b), y))$
7. $\forall x, (S(a, f(x)) \vee \exists y, f(y))$
8. $R(a, f(x)) \Rightarrow S(a, \exists y, g(y, b) = a)$

Exercice 2 — Déterminer les variables libres et les variables liées dans chacune des formules suivantes (on considère a comme un symbole de constante) :

- $A : p(f(x, y)) \vee \forall z, r(a, z)$
- $B : \forall x, p(x, y, z) \vee \forall z, (p(z) \Rightarrow r(z))$
- $C : \forall x, \exists y, (p(x, y) \Rightarrow \forall z, r(x, y, z))$
- $D : \forall z, \exists y, (P(x, y) \wedge (\forall z, Q(z, x)) \Rightarrow R(z))$
- $E : \forall \alpha \in \mathbb{R}^+, \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} \alpha^n \int_0^{\infty} e^{-t} x^{2n} t^{2n} \mathrm{d}\, t = \frac{1}{1 + \alpha x^2}$

Quelles sont les formules closes parmi les précédentes ?

Exercice 3 — Renommer les formules suivantes de sorte à lever les ambiguïtés éventuelles (utiliser un nom unique pour chaque variable liée ; séparer l'espace des noms de variables libres et des variables liées) :

- $A : \forall x, (P(x) \wedge (\exists x, Q(x, z)) \Rightarrow \exists y, R(x, y)) \vee Q(z, x)$
- $B : \forall y, (P(y) \wedge (\exists x, Q(x, z)) \Rightarrow \exists z, R(y, z)) \vee Q(z, x)$
- $C : \forall x, (P(x) \wedge (\exists x, Q(x, z)) \Rightarrow \exists x, R(x, x)) \vee Q(z, y)$
- $D : \forall z, (P(z) \wedge (\exists x, Q(x, z)) \Rightarrow \exists y, R(z, y)) \vee Q(z, x)$
- $E : \forall x, (P(x) \wedge (\exists x, Q(x, z) \Rightarrow \exists y, R(x, y))) \vee Q(z, y)$
- $F : \forall x, \exists y, (R(x, y) \wedge S(z, y)) \Rightarrow \exists x, (\forall y, R(x, y) \vee S(x, z))$
- $G : \forall x, (R(x, y) \Rightarrow \exists x, \forall y, S(y, x)) \vee \exists z, (S(z, x) \Rightarrow \exists y, \forall x, R(x, y))$
- $H : \forall x, \forall y, (R(f(x), a)$
  $\Rightarrow R(g(a, f(y)), x) \vee ((\exists z, \forall x, \exists y, R(z, f(x)) \wedge R(z, y)) \wedge \exists x, \forall z, R(g(y, z), f(x))))$

Certaines de ces formules sont-elles équivalentes ? Si oui, lesquelles ?

Exercice 4 — Soient les deux formules $F = (\exists y, R(x,y)) \Rightarrow \forall x, \forall z, (R(x,z) \vee R(y,z))$ et $G = (\exists x, R(x,y)) \wedge \forall y, \forall z, (R(x,z) \vee R(y,z))$.

1. Peut-on substituer, sans effectuer de renommage, $f(x,y)$ à x dans F ? Si oui, quelle formule obtient-on ?
2. Peut-on substituer, sans effectuer de renommage, $g(x,z)$ à y dans F ? Si oui, quelle formule obtient-on ?
3. Peut-on substituer, sans effectuer de renommage, $f(x,z)$ à x dans F ? Si oui, quelle formule obtient-on ?
4. Peut-on substituer, sans effectuer de renommage, $f(x)$ à x dans G ? Si oui, quelle formule obtient-on ?
5. Peut-on substituer, sans effectuer de renommage, $g(x,z)$ à y dans G ? Si oui, quelle formule obtient-on ?
6. Peut-on substituer, sans effectuer de renommage, $f(x,z)$ à x dans G ? Si oui, quelle formule obtient-on ?

Exercice 5 —

1. Effectuer la substitution (après renommage éventuel) $\sigma = [f(y,u)/x]$ dans la formule $A = p(x) \vee \forall y, \exists x, r(x,y)$.
2. Soient les substitutions $\sigma_1 = [f(y)/x]$, $\sigma_2 = [g(z)/y]$ et $\sigma_3 = [f(x)/z]$, et la formule $B = p(x,y,z)$.
   Appliquer les substitutions (après renommage éventuel) $\sigma_3 \circ \sigma_2 \circ \sigma_1$, $\sigma_2 \circ \sigma_1 \circ \sigma_3$ et $\sigma_1 \circ \sigma_3 \circ \sigma_2$ à B. Que peut-on en déduire ?

Exercice 6 — Soit f (resp. R) un symbole de fonction (resp. de relation) binaire. Soient $A : \forall z, (R(x,z) \wedge R(z,y)) \Rightarrow \exists z, (R(z,y) \vee R(x,z))$, $u = f(z,x)$ et $v = g(x,z)$.

1. Écrire les formules $A[u/x]$ et $A[v/y]$.
2. Comparer les formules $A[v/y][u/x]$ et $A[u/x][v[u/x]/y]$.
3. Comparer les formules $A[u/x][v/y]$ et $A[v/y][u[v/y]/x]$.

Exercice 7 — Traduire dans le langage du calcul des prédicats du premier ordre (sans égalité) les énoncés suivants :

1. La définition de l'union de deux ensembles : $A = B \cup C \iff \forall e \in A, e \in B \vee e \in C$
2. Tous les hommes sont mortels, et Socrate est un homme ; donc Socrate est mortel.
3. Le dernier théorème de Fermat : il n'existe pas de nombres entiers non nuls x, y et z tels que $x^m + y^m = z^m$ dès que m est un entier strictement supérieur à 2.
   Indication : On pourra partir de la formule suivante :

$$\forall m \in \mathbb{N}, (m > 2 \Rightarrow (\neg \exists (x,y,z) \in \mathbb{N}^{*3}, x^m + y^m = z^m))$$