TD4 Logique: Premier Ordre, Curry-Howard Classique

Romain Demangeon et Pierre Lescanne

23 et 24 Février 2008

1 Calcul des prédicats

On rappelle les règles de déduction naturelle pour les quantificateurs :

$$(\forall - \mathbf{I})\ \frac{\Gamma \vdash A(x) \qquad x \text{ non-libre dans } \Gamma}{\Gamma \vdash \forall x.A(x)} \qquad\qquad (\forall - \mathbf{E})\ \frac{\Gamma \vdash \forall x.A(x)}{\Gamma \vdash A[a/x]}$$

$$(\exists - \mathbf{I})\ \frac{\Gamma \vdash A[a/x]}{\Gamma \vdash \exists x.A(x)} \qquad\qquad (\exists - \mathbf{E})\ \frac{\Gamma \vdash \exists x.A(x) \qquad \Gamma, A \vdash B \qquad x \text{ non libre dans } \Gamma, B}{\Gamma \vdash B}$$

Q 1.1 Montrer dans NJ ou NK :

$$\vdash \forall x.(p \wedge q) \Leftrightarrow (\forall x.p) \wedge (\forall x.q) \qquad\qquad \vdash \forall x.p \vee \exists x.\neg p \text{ avec } x \text{ libre dans } p$$

$$\forall x.(p \Rightarrow q) \Leftrightarrow (p \Rightarrow \forall x.q) \text{ avec } x \text{ pas libre dans } q \qquad\qquad \vdash \neg\forall x.p \Leftrightarrow \exists x.\neg p$$

Q 1.2 On rappelle les règles associée à l'égalité :

$$(= -\mathbf{I})\ \Delta \vdash t = t \qquad\qquad (= -\mathbf{E})\ \frac{\Delta \vdash A[u/x] \qquad \Delta \vdash t = u}{\Delta \vdash A[t/x]}$$

Prouver la symétrie et la transitivité de =.

Q 1.3 Montrer (dans NK surtout) :

$$\vdash \forall x.P(x) \rightarrow \exists y.P(y) \qquad\qquad \vdash \exists x.\forall y.(R(x) \Rightarrow R(y))$$

$$\vdash \exists x.\forall y.[S(y) \Rightarrow R(x)] \Rightarrow [S(x) \Rightarrow R(y)]$$

$$\vdash \exists x.\forall y.[[R(f(x)) \Rightarrow R(f(y))] \Rightarrow R(x)] \Rightarrow R(y)$$

2 Théories Mathématiques

2.1 Groupes

Q 2.1 Axiomatiser la théorie des groupes avec deux symboles de fonction seulement.

Q 2.2 Axiomatiser la théorie des groupes abéliens de deux manières. Monter qu'une formule prouvée dans une des deux théories peut être prouvée dans l'autre théorie.

Q 2.3 Axiomatiser la théorie des groupes où tous les éléments sont d'ordre 2. Montrer $\forall x, x = i(x)$. Qu'en déduire ?

2.2 Peano

Q 2.4 Rappeler le langage et la théorie de l'arithmétique de Peano et son extension $\leq$.

Q 2.5 Prouver que :

1. 0 est neutre pour $+$.
2. $S(0)$ est neutre pour $\times$.
3. $+$ est associative.
4. $+$ est commutative.
5. $\times$ est associative.
6. $\times$ est commutative.
7. $\leq$ est une relation d'ordre.

2.3 Infini

Q 2.6 Donner une théorie dont les modèles sont exactement les structures à au moins 3 éléments.

Q 2.7 Donner une théorie dont les modèles sont exactement les structures à au plus 3 éléments.

Q 2.8 Donner une théorie dont les modèles sont exactement les structures à exactement 3 éléments.

Q 2.9 Généraliser les résultats à n éléments.

Q 2.10 Peut-on définir une théorie dont les modèles sont exactement les structures dont le cardinal est transfini ?

Q 2.11 Peut-on définir une théorie dont les modèles sont exactement les structures dont le cardinal est fini ?

3 Curry-Howard classique

Fig. 1 – Encore.

Q 3.1 On veut représenter une stratégie d'évaluation du λ-calcul par la recherche du redex à l'aide d'un *contexte d'évaluation*. Pour l'appel par nom, on définit ainsi les contextes d'évaluation par la syntaxe :

$$E \ ::= \ [] \ | \ E\,N$$

et on remarque que tout terme qui n'est pas une valeur s'écrit de manière unique $M = E[(\lambda x.M')\,N]$. L'appel par nom est alors défini par la règle $E[(\lambda x.M')\,N] \to E[M'[N/x]]$. Exprimer de la même façon l'appel par valeur.

Q 3.2 On se place désormais en appel par valeur.

On étend la syntaxe du λ-calcul avec deux opérations $\mathcal{C}(M)$ et $\mathcal{A}(M)$, auxquelles on associe les règles de réduction suivantes :

$$\begin{array}{rcll} E[\mathcal{A}(M)] & \rightarrow & M & \text{(abort)} \\ E[\mathcal{C}(M)] & \rightarrow & M\,\lambda z.\mathcal{A}(E[z]) \quad z \notin \mathrm{fn}(E) & \text{(control)} \end{array}$$

1. Expliquer comment $\mathcal{C}$ permet de programmer avec des exceptions en λ-calcul, en s'intéressant à $\mathcal{K}(M) = \mathcal{C}(\lambda k.\, k\,(M\ k))$.
2. Montrer que l'on peut encoder $\mathcal{A}(M)$ uniquement avec la constante $\mathcal{C}$.
3. En répondant à la question 1, vous vous êtes en principe rendu compte du fait qu'il y avait plusieurs réponses possibles. Que dire de ces différents cas en présence d'un opérateur tel que $\mathcal{C}$?

Q 3.3 On cherche un système de types préservé par réduction. On prend un E, et on suppose que $E[M]$ est de type β dès que M est de type α. Donner le type de $\lambda z.\mathcal{A}(E[z])$. En déduire la règle suivante :

$$\frac{\Gamma \vdash M : (\alpha \rightarrow \beta) \rightarrow \beta}{\mathcal{C}(M) : \alpha}$$

Q 3.4 Quelle est la règle pour $\mathcal{A}(M)$? Reformuler la règle de typage de $\mathcal{C}$ et interpréter ces règles dans le cadre de la correspondance de Curry-Howard. Est-ce qu'on peut interpréter tous les termes en tant que preuve ?

Q 3.5 En logique classique, on peut définir les connecteurs $\wedge$ et $\vee$ comme suit :

$$\alpha \wedge \beta \triangleq \neg(\alpha \rightarrow \neg\beta) \qquad\qquad \alpha \vee \beta \triangleq \neg\alpha \rightarrow \beta$$

Rappelez les règles standard d'introduction et d'élimination de ces connecteurs (en déduction naturelle) ; montrez qu'elles sont admissibles lorsque l'on utilise les encodages précédents.

Q 3.6 Donnez les termes correspondant à ces introductions et éliminations (constructeurs / projections / pattern matching).

Q 3.7 Dérivez le tiers exclu à partir de la double négation ; dérivez-en un terme qui réalise le tiers-exclu.