Devoir de λ-calcul 2015

(Version 4 du 30 avril)

$\mathbf{NJ}_1^{\equiv}$

<david.baelde@lsv.ens-cachan.fr>

À rendre le 5 mai

Nous nous intéressons à la logique du premier ordre, sur un ensemble de symboles de fonction $\mathcal{F}$ et un ensemble de symboles de prédicats $\mathcal{P}$. Nous considérons la possibilité d'identifier les termes et formules selon une certaine relation $\equiv$. Plus précisemment, nous prendrons le système vu en cours pour la logique intuitionniste du premier ordre (incluant le faux, la conjonction et la disjonction) et nous ajoutons une règle de *conversion* permettant de changer un type F en G quand $F \equiv G$. Le système résultant est donné en Figure 1.

On notera Λ l'ensemble de ses termes de preuve, et $\mathcal{T}(\mathcal{F})$ l'ensemble des termes du premier ordre (pas forcément clos) construits sur $\mathcal{F}$. Les éléments de Λ seront notés u, v, etc. tandis que les éléments de $\mathcal{T}(\mathcal{F})$ seront notés s, t, etc. On distinguera de même deux sortes de variables : les variables "de preuve" notées x, y, z, etc. sont destinées à être instantiées en des λ-termes de Λ ; les variables "de terme" notées i, j, etc. sont destinées à être instantiées en des termes de $\mathcal{T}(\mathcal{F})$. Dans cet énoncé, la notation $\mathrm{FV}(u)$ est uniquement utilisée pour les variables de terme libres dans u. Pour parler des variables de preuve libres, on utilisera la notation $\mathrm{FV}_\Lambda(u)$.

Dans tout l'énoncé on suppose que la relation $\equiv$ est une congruence (i.e., $P \equiv P'$ entraîne $C[P] \equiv C[P']$ pour tout contexte) compatible avec la substitution (i.e., $P \equiv P'$ entraîne $P\theta \equiv P'\theta$) et qui contienne l'α-renommage (i.e., $P =_\alpha P'$ entraîne $P \equiv P'$).

Question 1

Dans cette question les termes sont construits sur la constante 0 et la fonction successeur notée s. On se permettra d'écrire directement un entier n au lieu du terme $s^n(0)$ qui le représente. On considère de plus qu'on dispose du symbole de fonction binaire $+$ et le prédicat binaire d'égalité $=$, pour lesquels on utilisera la notation infixe usuelle.

On suppose que la congruence satisfait les équations suivantes :

$$0 + x \equiv x \qquad s(x) + y \equiv s(x + y) \qquad x + y \equiv y + x \qquad (x = x) \equiv \top$$
$$(s(x) = s(y)) \equiv (x = y) \qquad (0 = 0) \equiv \top \qquad (0 = s(x)) \equiv \bot \qquad (x = y) \equiv (y = x)$$

Merci RB !

Montrer que les types suivants sont habités en $\mathbf{NJ}_1^{\equiv}$ (on donnera les dérivations de typage et pas seulement les termes, en précisant quelles équations ci-dessus sont utilisées) :

(a) $2 + 3 = 5$

(b) $\forall i.\ 2 + i = 1 + (1 + i)$

(c) $1 + 1 = 0 \Rightarrow 16 + 64 = 42$

(d) $\forall i.\ i = 2 \Rightarrow 1 + i = 3$

$$\frac{(x : A) \in \Gamma}{\Gamma \vdash x : A} \qquad \frac{\Gamma \vdash u : Q \quad P \equiv Q}{\Gamma \vdash u : P}$$

$$\frac{}{\Gamma \vdash \langle\rangle : \top} \qquad \frac{\Gamma \vdash u : \bot}{\Gamma \vdash \nabla u : P}$$

$$\frac{\Gamma, x : P \vdash u : Q}{\Gamma \vdash \lambda x.\, u : P \Rightarrow Q}\ (x \text{ frais}) \qquad \frac{\Gamma \vdash u : P \Rightarrow Q \quad \Gamma \vdash v : P}{\Gamma \vdash u\, v : Q}$$

$$\frac{\Gamma \vdash u_1 : P_1 \quad \Gamma \vdash u_2 : P_2}{\Gamma \vdash \langle u_1, u_2\rangle : P_1 \wedge P_2} \qquad \frac{\Gamma \vdash u : P_1 \wedge P_2}{\Gamma \vdash \pi_i u : P_i}$$

Merci HM&NM !

$$\frac{\Gamma \vdash u : P_i}{\Gamma \vdash \iota_i u : P_1 \vee P_2} \qquad \frac{\Gamma \vdash u : P_1 \vee P_2 \quad \Gamma, x : P_1 \vdash v_1 : Q \quad \Gamma, y : P_2 \vdash v_2 : Q}{\Gamma \vdash \text{case } u\, \{\iota_1 x \mapsto v_1, \iota_2 y \mapsto v_2\} : Q}\ (x, y \text{ frais})$$

$$\frac{\Gamma \vdash u : P}{\Gamma \vdash \lambda i.\, u : \forall i.\, P}\ (i \text{ frais}) \qquad \frac{\Gamma \vdash u : \forall i.\, P}{\Gamma \vdash u\, t : P[i := t]}$$

$$\frac{\Gamma \vdash u : P[i := t]}{\Gamma \vdash \iota t u : \exists i.\, P} \qquad \frac{\Gamma \vdash u : \exists i.\, P \quad \Gamma, x : P \vdash v : Q}{\Gamma \vdash \text{case } u\, \{\iota i x \mapsto v\} : Q}\ (i, x \text{ frais})$$

FIGURE 1 – Règles de typage de $\mathbf{NJ}_1^{\equiv}$

Question 2
On reprend le langage et la congruence de la question précédente, et on ajoute le prédicats unaire N ainsi que l'équation $N(i) \equiv (i = 0 \vee \exists j.\, i = s(j) \wedge N(j))$. Démontrer $\forall i.\, N(i) \Rightarrow N(s(i))$ en $\mathbf{NJ}_1^{\equiv}$. (Donner un terme de preuve.) Merci HM&RB !

Question 3
On suppose qu'on dispose d'un prédicat p d'arité 0 tel que $p \equiv (p \Rightarrow \bot)$. Montrer $\bot$ en $\mathbf{NJ}_1^{\equiv}$.

1 Méta-théorie

On étudie maintenant $\mathbf{NJ}_1^{\equiv}$ de façon générale : on considère une relation $\equiv$ quelconque, et on se demande sous quelles conditions on peut assurer l'auto-réduction, la forte normalisation, et la cohérence. Pour cette partie, on restreint le langage des types à l'implication et la quantification universelle. Les termes de preuve sont restreints de façon correspondante aux variables, abstractions et applications. On ne garde comme règles de typage que la conversion, l'axiome, et les règles d'introduction et d'élimination pour $\Rightarrow$ et $\forall$.

On définit $\to_\beta$ comme la plus petite congruence telle que :

$$(\lambda x.\, u)\, v \to_\beta u[x := v] \qquad\qquad (\lambda i.\, u)\, t \to_\beta u[i := t]$$

1.1 Formes normales

Question 4
On suppose que $\equiv$ est *sans confusion*, c'est à dire que si $P \equiv Q$ où P et Q sont des formules non

atomiques, alors le connecteur logique le plus externe dans P est le même que dans Q. (Par exemple, cela interdit d'avoir $P \vee P' \equiv Q \wedge Q'$ ou $P \wedge Q \equiv \top$.) Montrer, dans ce cas, qu'il n'existe pas de terme u en forme normale tel que $\vdash u : \bot$.

1.2 Auto-réduction

On admettra le lemme de substitution usuel, qui se démontre aisément : si $\Gamma, x : P \vdash u : Q$ et $\Gamma \vdash v : P$ sont dérivables, alors $\Gamma \vdash u[x := v] : Q$ l'est aussi. On admettra aussi le lemme d'affaiblissement : $\Gamma \vdash u : P$ entraîne $\Gamma, x : Q \vdash u : P$.

Question 5
Démontrer que si $\Gamma \vdash u : P$ est dérivable, alors $\Gamma[i := t] \vdash u[i := t] : P[i := t]$ l'est aussi.

Question 6
On s'intéresse à la propriété d'auto-réduction, i.e., si $\Gamma \vdash u : P$ et $u \to_\beta v$, alors $\Gamma \vdash v : P$. Cette propriété n'est pas vraie en général :

- donner un contre-exemple,
- proposer une condition simple sur $\equiv$ qui permette de garantir l'auto-réduction,
- donner une preuve d'auto-réduction sous cette hypothèse supplémentaire.

1.3 Normalisation forte

Nous allons démontrer la forte normalisation de façon générique par rapport à $\equiv$. On note $\mathbf{CR}$ l'ensemble des candidats de réductibilité, définis comme dans le cours, sur les termes de $\mathbf{NJ}_1^{\equiv}$ et par rapport à la relation de réduction $\to_\beta$. Un terme est neutre s'il n'est pas de la forme $\lambda x.\ u$ ou $\lambda i.\ u$. On note $\mathbf{SN}$ l'ensemble des termes fortement normalisants.

Une *structure* sur $\mathcal{F}$ et $\mathcal{P}$ est donnée par :

- un ensemble non vide D appelé domaine ;
- pour chaque $f \in \mathcal{F}$ d'arité n, une fonction $\hat{f} : D^n \to D$;
- pour chaque $p \in \mathcal{P}$ d'arité n, une fonction $\hat{p} : D^n \to \mathbf{CR}$.

Dans la suite de cette section, on suppose fixée une certaine structure.

On définit ensuite l'interprétation des termes et formules dans une structure. Étant donné un terme t et une valuation σ qui à toute variable libre de t associe un élément de D (i.e., $\mathrm{FV}(t) \subseteq \mathrm{Dom}(\sigma)$ et $\mathrm{Img}(\sigma) \subseteq D$) on définit $|t|_\sigma$ par induction sur t :

$$|x|_\sigma = \sigma(x) \quad \text{et} \quad |f(t_1, \ldots, t_n)|_\sigma = \hat{f}(|t_1|_\sigma, \ldots, |t_n|_\sigma).$$

Enfin, on définit $|P|_\sigma$ pour une formule P et une valuation σ telle que $\mathrm{FV}(P) \subseteq \mathrm{Dom}(\sigma)$:

$$\begin{aligned}
|p(t_1, \ldots, t_n)|_\sigma &= \hat{p}(|t_1|_\sigma, \ldots, |t_n|_\sigma) \\
|P \Rightarrow Q|_\sigma &= \{\ u \in \mathbf{SN}\ :\ u \to_\beta^* \lambda x.\ u' \text{ entraîne} \\
&\qquad\qquad u'[x := v] \in |Q|_\sigma \text{ pour tout } v \in |P|_\sigma\ \} \\
|\forall i.\ P|_\sigma &= \{\ u \in \mathbf{SN}\ :\ u \to_\beta^* \lambda i.\ u' \text{ entraîne} \\
&\qquad\qquad u'[i := t] \in |P|_{\sigma + (i \mapsto v)} \text{ pour tout } t \in \mathcal{T}(\mathcal{F}) \text{ et } v \in D\ \}
\end{aligned}$$

Question 7
Montrer que pour tout P et σ tel que $\mathrm{FV}(P) \subseteq \mathrm{Dom}(\sigma)$, $|P|_\sigma$ est un candidat de réductibilité.

Question 8
Montrer que $u \in |P \Rightarrow Q|_\sigma$ et $v \in |P|_\sigma$ entraînent $(u\ v) \in |Q|_\sigma$.

Question 9
Montrer que $u \in |\forall i.\ P|_\sigma$ entraîne $(u\ (t\rho)) \in |P[i := t]|_\sigma$ pour tout terme t tel que $\mathrm{FV}(t) \subseteq \mathrm{Dom}(\sigma)$ et toute substitution $\rho : \mathrm{FV}(t) \to \mathcal{T}(\mathcal{F})$.

Énoncé renforcé.

On dit qu'une structure est *adéquate* vis-à-vis de $\equiv$ si, pour toutes formules P et Q, $P \equiv Q$ entraîne, pour tout σ, $|P|_\sigma = |Q|_\sigma$.

Question 10
On suppose que la structure est adéquate pour $\equiv$. Soit une dérivation de $\Gamma \vdash u : P$ et des valuations
- $\sigma : \mathrm{FV}(\Gamma, P) \to D$,
- θ telle que pour tout $(x : Q) \in \Gamma$, $\theta(x) \in |Q|_\sigma$,
- et $\rho : \mathrm{FV}(u) \to \mathcal{T}(\mathcal{F})$.

Montrer $u\rho\theta \in |P|_\sigma$.

2 Application

On souhaite maintenant appliquer le résultat précédent sur divers exemples de relation $\equiv$. Pour cela il suffit, pour une relation $\equiv$ donnée, de définir une structure adéquate. On obtient ainsi **SN** par les résultats précédents, et ainsi la cohérence de la logique obtenue, sous l'hypothèse (facile à vérifier) que la relation $\equiv$ considérée est sans confusion.

Question 11
Définir une structure adéquate pour $\equiv$ dans le cas de la première question.

On ignorera ci-dessous la restriction de la section précédente aux seuls connecteurs logiques $\Rightarrow$ et $\forall$: on supposera que l'interprétation a été définie pour toute formule [1], et on admettra que les propriétés vues précédemment restent vraies.

Question 12
Définir une structure adéquate pour $\equiv$ dans le cas de la deuxième question.

Question 13
Sur le langage $\mathcal{F} = \{0(0),\ s(1)\}$ et $\mathcal{P} = \{E(1)\}$, on considère la congruence engendrée par les équations $E(0) \equiv \top$ et $E(s(x)) \equiv \neg E(x)$. Donner une structure adéquate pour $\equiv$.

Les choses sont-elles différentes si l'on considère, au lieu de ces deux équations, l'unique équation $E(i) \equiv i = 0 \vee \exists j.\ i = s(j) \wedge \neg E(j)$?

1. On précise, si besoin, qu'on aura notamment $|P_1 \vee P_2|_\sigma = \{\ u \in \mathbf{SN}\ :\ u \to_\beta^* \iota_i u'$ entraîne $u' \in |P_i|_\sigma\ \}$ et $|\exists i.\ P|_\sigma = \{\ u \in \mathbf{SN}\ :$ si $u \to_\beta^* \iota t u'$ alors il existe $v \in D$ tel que $u' \in |P|_{\sigma+(x\mapsto v)}\ \}$.