

## λ-Calcul et Logique Informatique

Guillaume Bury  
bury@lsv.ens-cachan.fr

### Exercice 1 — Paradoxe de Russell

On formalise (une partie de) la théorie naïve des ensemble en ajoutant à la logique du premier ordre les constructions suivantes :

- les termes du premier-ordre  $\{ x \mid F \}$  représentant intuitivement un ensemble défini par compréhension ;
- les formules  $t \in s$  représentant intuitivement l'appartenance ;
- les termes de preuve  $I_\in$  et  $E_\in$  pour introduire et éliminer les types  $\in$  ;
- les règles de typage suivantes :

$$\frac{\Gamma \vdash u : F[x := t]}{\Gamma \vdash I_\in(u) : t \in \{ x \mid F \}} \quad \frac{\Gamma \vdash u : t \in \{ x \mid F \}}{\Gamma \vdash E_\in(u) : F[x := t]}$$

- et enfin la nouvelle réduction  $E_\in(I_\in(u)) \rightarrow u$ .

Nous allons formaliser le paradoxe de Russell (aussi appelé paradoxe du menteur) dans ce système, et ainsi montrer son incohérence. Pour cela, on pose  $S := \{ x \mid \neg(x \in x) \}$ .

1. Donner un terme de type  $(S \in S) \Rightarrow \neg(S \in S)$ .
2. En déduire un terme de type  $S \in S$  et un terme de type  $\perp$ .
3. Ce terme vous rappelle-t-il quelque chose ? réduisez-le si besoin.

### Exercice 2 — Axiomatique de Heyting et système $\mathbf{HA}_1$

On considère, d'une part, le système  $\mathbf{HA}_1$  vu en cours, dont les termes sont ceux de  $\lambda\nabla R$  et dont les règles de typage comportent la règle  $\leftrightarrow_{\mathbb{N}}$ . On considère d'autre part les axiomes de Peano (1–9).

1. Montrer que l'axiome (1), c'est à dire  $\forall s. s \approx s$ , est dérivable en  $\mathbf{HA}_1$ . On utilisera la règle (Rec) sur  $s$ .
2. Montrer que (3–8) sont aussi dérivables, de même que toutes les instances de (9).

On s'attache maintenant à montrer que (2) est dérivable. Comme les dérivations se font lourdes, on se permettra de ne pas forcément écrire les termes de preuve, ni même les arbres de dérivation : les principales étapes de la dérivation devraient suffire à se convaincre.

1. Montrer que  $\lambda x.x$  est une preuve de  $s \approx t \Rightarrow \mathbf{S} s \approx \mathbf{S} t$ .
2. Dérivée  $s_1 \approx t_1 \Rightarrow s_2 \approx t_2 \Rightarrow s_1 + s_2 \approx t_1 + t_2$ , par induction (Rec) sur  $s_2$  puis  $t_2$ . De même pour la multiplication.

3. Conclure que pour tout terme  $u$  on peut dériver :

$$s_1 \approx t_1 \Rightarrow u[i := s_1] \approx u[i := t_1]$$

4. Montrer  $\forall i \cdot \forall j \cdot i \approx j \Rightarrow j \approx i$  en  $\mathbf{HA}_1$ , en utilisant (Rec) sur  $i$  puis  $j$ .  
 5. Montrer  $\forall i \cdot \forall j \cdot \forall k \cdot i \approx j \Rightarrow j \approx k \Rightarrow i \approx k$  en  $\mathbf{HA}_1$ , en utilisant (Rec) sur  $i$  puis  $j$  et  $k$ .  
 6. Conclure que pour tout  $F$ , on peut dériver en  $\mathbf{HA}_1$  l'instance de l'axiome (2) pour  $F$  :

$$s_1 \approx t_1 \Rightarrow F[i := s_1] \Rightarrow F[i := t_1]$$

**Exercice 3 — Dédution modulo**

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 précisément, nous prendrons le système vu en cours pour la logique intuitionniste du premier ordre,  $\lambda\nabla$ , auquel on ajoute la règle de conversion suivante permettant de changer un type  $F$  en  $G$  quand  $F \equiv G$  :

$$\frac{\Gamma \vdash u : Q \quad P \equiv Q}{\Gamma \vdash u : P}$$

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' $\alpha$ -renommage (i.e.,  $P =_\alpha P'$  entraîne  $P \equiv P'$ ).

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

Naturellement, on se demande sous quelles conditions sur  $\equiv$  on peut assurer l'auto-réduction, la forte normalisation, et la cohérence.

**Question 1.** 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  $\vdash u : \perp$ .

**Question 2.** On s'intéresse à la propriété d'auto-réduction, i.e., si  $\Gamma \vdash u : P$  et  $u \rightarrow_\beta v$ , 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.

Nous allons démontrer la forte normalisation de façon générique par rapport à  $\equiv$ . On note **SN** l'ensemble des termes fortement normalisants. On note **CR** l'ensemble des *candidats de réductibilité* : un candidat est un ensemble  $X$  de termes de preuve de  $\mathbf{NJ}_1^{\equiv}$  satisfaisant (CR1)  $X \subseteq \mathbf{SN}$ , (CR2) si  $u \in X$  et  $u \rightarrow_{\beta} v$  alors  $v \in X$ , et (CR3) si  $u$  est neutre (i.e., pas de la forme  $\lambda x. u'$  ni  $\lambda i. u'$ ) et que tous ses réduits immédiats par  $\rightarrow_{\beta}$  sont dans  $X$  alors  $u \in X$ .

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  $\hat{f} : D^n \rightarrow D$  ;
- pour chaque  $p \in \mathcal{P}$  d'arité  $n$ , une fonction  $\hat{p} : D^n \rightarrow \mathbf{CR}$ .

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  $\sigma$  qui à toute variable libre de  $t$  associe un élément de  $D$  (i.e.,  $\text{FV}(t) \subseteq \text{Dom}(\sigma)$  et  $\text{Img}(\sigma) \subseteq D$ ) on définit  $|t|_{\sigma}$  par induction sur  $t$  :

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

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

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

**Question 3.** Montrer que pour tout  $P$  et  $\sigma$  tel que  $\text{FV}(P) \subseteq \text{Dom}(\sigma)$ ,  $|P|_{\sigma}$  est un candidat de réductibilité.

**Question 4.** Montrer que  $u \in |P \Rightarrow Q|_{\sigma}$  et  $v \in |P|_{\sigma}$  entraînent  $(u v) \in |Q|_{\sigma}$ .

**Question 5.** Montrer que  $u \in |\forall i. P|_{\sigma}$  entraîne  $(u (t\rho)) \in |P[i := t]|_{\sigma}$  pour tout terme  $t$  tel que  $\text{FV}(t) \subseteq \text{Dom}(\sigma)$  et toute substitution  $\rho : \text{FV}(t) \rightarrow \mathcal{T}(\mathcal{F})$ .

**Question 6.** On suppose que la structure considérée est *adéquate* pour  $\equiv$ , c'est à dire que pour toutes formules  $P$  et  $Q$ ,  $P \equiv Q$  entraîne, pour tout  $\sigma$ ,  $|P|_{\sigma} = |Q|_{\sigma}$ . Soit une dérivation de  $\Gamma \vdash u : P$  et des valuations

- $\sigma : \text{FV}(\Gamma, P) \rightarrow D$ ,
- $\theta$  telle que pour tout  $(x : Q) \in \Gamma$ ,  $\theta(x) \in |Q|_{\sigma}$ ,
- et  $\rho : \text{FV}(u) \rightarrow \mathcal{T}(\mathcal{F})$ .

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

Nous n'aurons certainement pas le temps de le faire, mais il est aisé de construire une structure adéquate pour un  $\equiv$  qui nous donne l'arithmétique de Heyting, par exemple.