λ-Calcul et Logique Informatique

David Baelde
baelde@lsv.ens-cachan.fr

Exercice 1 — Ackermann

On considère le système $\mathbf{HA}_2$, auquel on ajoute la quantification existentielle au premier ordre ainsi que la conjonction :

$$\frac{\Gamma \vdash u : P[i := t]}{\Gamma \vdash \langle t, u\rangle : \exists i.P} \qquad \frac{\Gamma \vdash u : \exists i.P \quad \Gamma, x : P \vdash v : C}{\Gamma \vdash (\mathsf{let}\ \langle i, x\rangle = u\ \mathsf{in}\ v) : C}$$

$$\frac{\Gamma \vdash u : P \quad \Gamma \vdash v : Q}{\Gamma \vdash \langle u, v\rangle : P \wedge Q} \qquad \frac{\Gamma \vdash u : P \wedge Q \quad \Gamma, x : P, y : Q \vdash v : C}{\Gamma \vdash (\mathsf{let}\ \langle x, y\rangle = u\ \mathsf{in}\ v) : C}$$

1. Prouver la totalité de la fonction d'Ackermann, $\forall i \forall j \exists k.\mathsf{ack}(i, j, k)$, où $\mathsf{ack}(t, t', t'')$ est défini comme :

$$\begin{aligned}\forall A.\ \big(&(\forall j.\ A(0, j, \mathsf{s}(j))) \Rightarrow\\ &(\forall i \forall k.\ A(i, \mathsf{s}(0), k) \Rightarrow A(\mathsf{s}(i), 0, k)) \Rightarrow\\ &(\forall i \forall j \forall k \forall k'.\ A(\mathsf{s}(i), j, k) \Rightarrow A(i, k, k') \Rightarrow A(\mathsf{s}(i), \mathsf{s}(j), k')) \Rightarrow\\ &A(t, t', t'')\big)\end{aligned}$$

   a. Donner v_0 clos de type $\forall j \exists k.\ \mathsf{ack}(0, j, k)$.
   b. On pose $H_i \stackrel{\text{def}}{=} \forall j \exists k.\ \mathsf{ack}(i, j, k)$.
   Donner u_0 tel que $h_i : H_i \vdash u_0 : \exists k.\ \mathsf{ack}(\mathsf{s}(i), 0, k)$.
   c. Donner u_{s} tel que

$$h_i : H_i \vdash u_{\mathsf{s}} : \forall j.\ (\exists k.\ \mathsf{ack}(\mathsf{s}(i), j, k)) \Rightarrow (\exists k.\ \mathsf{ack}(\mathsf{s}(i), \mathsf{s}(j), k)).$$

   d. Donner v_{s} clos de type $\forall i.\ (\forall j \exists k.\ \mathsf{ack}(i, j, k)) \Rightarrow (\forall j \exists k.\ \mathsf{ack}(\mathsf{s}(i), j, k))$.
   e. Donner un terme de preuve pour $\forall i \forall j \exists k.\ \mathsf{ack}(i, j, k)$.

2. Soit nat le type des entiers naturels sans structure du premier ordre, c'est à dire $\forall N.\ N \Rightarrow (N \Rightarrow N) \Rightarrow N$. On considère un effacement de la structure de premier ordre comme dans le cours, avec :

$$\begin{aligned} E(\forall i.\ P) &:= N \Rightarrow E(P)\\ E(\exists i.\ P) &:= N \wedge E(P)\end{aligned}$$

   a. Quand $\Gamma \vdash u : P$, on souhaite avoir $E(\Gamma), \Gamma_u \vdash E(u) : E(P)$ pour $\Gamma_u = \{\ x_i : \mathsf{nat} \mid i \text{ libre dans } u\ \}$, avec de plus $u \to v$ ssi $E(u) \to E(v)$.

i. Définir $E(\lambda i.\ u)$ pour que ce résultat puisse être vrai.
ii. Définir $E(Ruvi)$.
iii. Définir $E(\langle t, u\rangle)$ et $E(Ruvt)$.

b. Appliquer cet effacement au terme prouvant la totalité de ack. On se concentrera sur l'entier calculé et non la preuve qu'il est correct : on pourra ignorer les sous-termes correspondant aux ellipses dans $E(\exists z.\ \ldots) = \mathsf{nat} \wedge \ldots$.

Exercice 2 — $\lambda\sigma$ simule λ

Nous allons démontrer le résultat de simulation pour $\lambda\sigma$: si $u \to v$ alors $u^*(\ell) \to^+ v^*(\ell)$ pour tout ℓ. On pose $\uparrow^0 = \mathsf{id}$, $\uparrow^{n+1} = \uparrow \circ \uparrow^n$. On pose aussi $\Uparrow S = 1 \cdot (S \circ \uparrow)$, et $\Uparrow^n S$ est défini naturellement.

1. Montrer $\uparrow \circ \Uparrow(S) \to_\sigma S \circ \uparrow$.
2. Montrer $(q+i)[\Uparrow^q(S)] =_\sigma i[S \circ \uparrow^q]$ pour $q \geq 0$ et $i \geq 1$.
3. Montrer $i[\Uparrow^q(S) \circ \uparrow] =_\sigma i$ pour $i \leq q$.
4. Pour des variables x_i et y_j suffisamment fraîches, montrer
$$v^*(x_1 :: \ldots :: x_q :: \ell)[\Uparrow^q(\uparrow^p)] =_\sigma v^*(x_1 :: \ldots :: x_q :: y_1 :: \ldots :: y_p :: \ell).$$
5. Pour des variables y_i assez fraîches, montrer
$$u^*(y_1 :: \ldots :: y_p :: x :: \ell)[\Uparrow^p(v^*(\ell) \cdot \mathsf{id})] =_\sigma (u[x := v])^*(y_1 :: \ldots :: y_p :: \ell).$$
6. Conclure.

Exercice 3 — $\lambda\sigma$ ne préserve pas la forte normalisation

On pose les définitions suivantes :

$$\begin{array}{rcl}
\mathsf{rec}(S) & := & \uparrow \circ (1[S] \cdot \mathsf{id}) \\
S_1 & := & (\lambda 1)1 \cdot \mathsf{id} \\
S_{n+1} & := & \mathsf{rec}(S_n) \\
D_S(S') & := & 1[1[S] \cdot S'] \cdot S \\
C_S(S') & := & \uparrow \circ (1[S'] \cdot S)
\end{array}$$

1. Montrer $S_1 \circ S \to^+ D_S(S \circ \mathsf{rec}(S))$. Pour cela, ne pas choisir les règles qui simplifient mais distribuer la pile au maximum, en retardant β.
2. Montrer $\mathsf{rec}(S') \circ S \to^+ C_S(S' \circ S)$.
3. Montrer $S_n \circ S_{n+1} \to^+ C^{n-1}_{S_{n+1}}(D_{S_{n+1}}(S_{n+1} \circ S_{n+2}))$.
4. On considère le terme suivant :
$$u := \lambda z'.\big(\lambda x.(\lambda y.y)((\lambda z.z)x)\big)((\lambda y.y)z')$$
Montrer que $u^*(\epsilon) \to^+ \lambda(1[S_1 \circ S_1])$.
5. Conclure.