λ-calcul et logique informatique

leroux@lsv.fr

Exercice 1 — Combinateurs

On définit $\mathcal{C}$ le calcul de combinateurs **SK** : les termes sont construits suivant la grammaire

$$M := \mathcal{V} \mid (M\ M) \mid \mathbf{S} \mid \mathbf{K}$$

Par convention, MNP représente $((MN)P)$. La réduction $\to$ est plus petite congruence contenant

$$\mathbf{K}\ M\ N \to M \qquad \mathbf{S}\ M\ N\ P \to (M\ P)\ (N\ P)$$

1. Définir l'ensemble $V(M)$ des variables apparaissant dans un terme M de $\mathcal{C}$.
2. Définir $\to$ formellement, i.e. au moyen de règles d'inférence.
3. Montrer que $M \to^* M'$ et $N \to^* N'$ implique $MN \to^* M'N'$.
4. (a) Définir une notion naturelle de substitution dans le $\mathcal{C}$ calcul, i.e. définir $M[x := N]$ pour $x \in \mathcal{V}$ et $M, N \in \mathcal{C}$.
   (b) Que vaut $M[x := N]$ si $x \notin V(M)$?
5. (a) On pose $\mathbf{I} := \mathbf{S}\ \mathbf{K}\ \mathbf{K}$. Réduire $\mathbf{I}\ M$ pour un terme M quelconque.
   (b) Donner un terme $\mathbf{I}'$ différent de $\mathbf{I}$, tel que $\mathbf{I}M$ et $\mathbf{I}'M$ se réduisent en le même terme.
6. Construire une traduction simple de $\mathcal{C}$ dans Λ telle que $M \to N$ implique $[M]_{\mathcal{C}} \to_\beta^* [N]_{\mathcal{C}}$ pour tout $M, N \in \mathcal{C}$.
7. (a) Soit $x \in \mathcal{V}$. Pour tout $M \in \mathcal{C}$ on définit $[x]M$, par récurrence sur M.
   — $[x]x := \mathbf{I}$
   — $[x]M := \mathbf{K}\ M$ si $x \notin V(M)$.
   — $[x](AB) := \mathbf{S}\ ([x]A)\ ([x]B)$ si $x \in V(AB)$.
   Montrer que pour tout x, M et N, on a $([x]M)N \to^* M[x := N]$.
   (b) Définir une construction $\{x\}M$ légèrement différente de $[x]M$ avec la même propriété que ci-dessus. (Toujours avec $\mathbf{I}$, pas un $\mathbf{I}'$.)
8. (a) Montrer que pour tout $M, N \in \mathcal{C}$ et $x, y \in \mathcal{V}$ tels que $y \neq x$ et $y \notin V(N)$, on a $([y]M)[x := N] = [y](M[x := N])$.
   (b) Montrer que chacune des hypothèses $y \neq x$ et $y \notin V(N)$ ci-dessus sont utiles.
   (c) Montrer que la construction $\{x\}M$ ne vérifie pas cette propriété de substitution.
9. On définit une traduction $u \mapsto u^*$ de Λ dans $\mathcal{C}$ comme suit.
   — $x^* := x$
   — $(uv)^* = u^*v^*$
   — $(\lambda x.u)^* = [x]u^*$
   Montrer que pour tout $x \in \mathcal{V}$ et $A, B \in \Lambda$, on a $A^*[x := B^*] = (A[x := B])^*$.

10. Montrer que pour tout $x \in \mathcal{V}$ et $M \in \mathcal{C}$, on a $[[x]M]_{\mathcal{C}} \to_\beta^* \lambda x.[M]_{\mathcal{C}}$.
11. On appelle $\rhd$ la restriction de la β-réduction qui ne réduit pas sous les λ.
    (a) Définir $\rhd$ formellement.
    (b) Montrer que $u \rhd v$ implique $u^* \to^* v^*$.
12. Montrer que tout lambda-terme u est β-équivalent à $[u^*]_{\mathcal{C}}$.
13. (a) Le $\mathcal{C}$ calcul termine-t-il ?
    (b) Définir une réduction parallèle $\Rightarrow$ dans le $\mathcal{C}$ calcul et montrer sa confluence forte.
    (c) Montrer que $\to \subseteq \Rightarrow \subseteq \to^*$.
    (d) Montrer que si $M \leftrightarrow^* N$, alors il existe P tel que $M \to^* P$ et $N \to^* P$.
    (e) A-t-on $\mathbf{K} \leftrightarrow^* [x][y]x$?

Solution Exercice 1

1. — $V(x) := \{x\}$
   — $V(\mathbf{K}) := V(\mathbf{S}) := \emptyset$
   — $V(MN) := V(M) \cup V(N)$.
2. Aux deux règles déjà données, il suffit de rajouter les deux suivantes :

$$\frac{M \to M'}{MN \to M'N} \qquad \frac{N \to N'}{MN \to MN'}$$

3. On montre d'une part que $M \to^* M'$ implique $MN \to^* M'N$, par récurrence sur $M \to^* M'$. D'autre part, on montre que $N \to^* N'$ implique $MN \to^* MN'$, par récurrence sur $N \to^* N'$. Supposons maintenant que $M \to^* M'$ et $N \to^* N'$. Alors $MN \to^* M'N \to^* M'N'$. Par définition de $\to^*$, on trouve $MN \to^* M'N'$.
4. (a) Soit $x \in \mathcal{V}$ et $N \in \mathcal{C}$. Pour tout $M \in C$, on définit $M[x := N]$ par récurrence sur M.
   — Si $M := x$, alors $M[x := N] := N$.
   — Si $M := y$, alors $M[x := N] := y$.
   — Si $M \in \{\mathbf{S}, \mathbf{K}\}$, alors $M[x := N] := M$. (Comme pour y.)
   — Si $M = AB$, alors $M[x := N] := A[x := N]B[x := N]$.
   (b) Alors $M[x := N] = M$.
5. (a) $\mathbf{I}M = \mathbf{S}\ \mathbf{K}\ \mathbf{K}\ M \to (\mathbf{K}\ M)\ (\mathbf{K}\ M) \to M$.
   (b) Pour tout terme P, $I' := \mathbf{S}\ \mathbf{K}\ P$ convient, i.e. $I'\ M \to M$ pour tout M.
6. On définit $[\cdot]_{\mathcal{C}}$ par récurrence.
   — $[x]_{\mathcal{C}} := x$, $[K]_{\mathcal{C}} := \lambda xy.x$ et $[S]_{\mathcal{C}} := \lambda xyz.xz(yz)$.
   — $[MN]_{\mathcal{C}} := [M]_{\mathcal{C}}[N]_{\mathcal{C}}$.
   On montre par récurrence sur $M \to N$ que cela implique $[M]_{\mathcal{C}} \to_\beta [N]_{\mathcal{C}}$.
   — Cas $\mathbf{K}\ M\ N \to M$: on a $[\mathbf{K}\ M\ N]_{\mathcal{C}} = [\mathbf{K}\ M]_{\mathcal{C}}[N]_{\mathcal{C}} = [\mathbf{K}]_{\mathcal{C}}[M]_{\mathcal{C}}[N]_{\mathcal{C}} = (\lambda xy.x)[M]_{\mathcal{C}}[N]_{\mathcal{C}} \to_\beta^* [M]_{\mathcal{C}}$.
   — Cas $\mathbf{S}\ M\ N\ P \to (M\ P)\ (N\ P)$: on a $[\mathbf{S}\ M\ N\ P]_{\mathcal{C}} = [\mathbf{S}]_{\mathcal{C}}[M]_{\mathcal{C}}[N]_{\mathcal{C}}[P]_{\mathcal{C}} = (\lambda xyz.xz(yz))[M]_{\mathcal{C}}[N]_{\mathcal{C}}[P]_{\mathcal{C}} \to_\beta^* [M]_{\mathcal{C}}[P]_{\mathcal{C}}([N]_{\mathcal{C}}[P]_{\mathcal{C}})$.
   — Cas $MN \to M'N$ avec $M \to M'$. Par HR $[M]_{\mathcal{C}} \to_\beta^* [M']_{\mathcal{C}}$. Donc $[MN]_{\mathcal{C}} = [M]_{\mathcal{C}}[N]_{\mathcal{C}} \to_\beta^* [M']_{\mathcal{C}}[N]_{\mathcal{C}} = [M'N]_{\mathcal{C}}$.
   — Cas $MN \to MN'$ avec $N \to N'$. Similaire.

7. (a) Soit $x \in \mathcal{V}$ et $N \in \mathcal{C}$. On montre par récurrence sur M que pour tout M on a $[x]MN = ([x]M)N \to^* M[x := N]$.
   - Cas $M = x$. Alors, on a $[x]M\ N = \mathbf{I}\ N \to^* N = M[x := N]$.
   - Cas $x \notin V(M)$. Alors, on a $[x]M\ N = \mathbf{K}\ M\ N \to M = M[x := N]$.
   - Cas $M = AB$, avec $x \in V(M)$. Alors, on a $[x](AB)\ N = \mathbf{S}\ [x]A\ [x]B\ N \to [x]A\ N\ ([x]B\ N)$. Par HR on a $[x]A\ N \to^* A[x := N]$ et $[x]B\ N \to^* B[x := N]$. Donc $[x]A\ N([x]B\ N) \to^* A[x := N]B[x := N]$ par une question précédente. Or $A[x := N]B[x := N] = (AB)[x := N]$ par définition de la substitution, donc en combinant les remarques ci-dessus, on obtient $[x](AB)\ N \to^* (AB)[x := N]$.

   (b) Soit $x \in \mathcal{V}$. On définit $\{x\}M$ par récurrence sur M.
   - $\{x\}x := \mathbf{I}$
   - $\{x\}M := \mathbf{K}\ M$ si M est $\mathbf{K}$, $\mathbf{S}$, ou une variable différente de x.
   - $\{x\}(AB) := \mathbf{S}\ (\{x\}A)\ (\{x\}B)$.

   La preuve que $\{x\}MN \to^* M[x := N]$ est presque la même que pour $[x]MN$.
   - Cas $M = x$. Idem.
   - Cas M est $\mathbf{K}$, $\mathbf{S}$, ou une variable différente de x. Alors, on a $\{x\}M\ N = \mathbf{K}\ M\ N \to M = M[x := N]$.
   - Cas $M = AB$. Idem, sans supposer que $x \in V(AB)$.

8. (a) Soient $N \in \mathcal{C}$ et $x, y \in \mathcal{V}$ tels que $y \neq x$ et $y \notin V(N)$. On montre par récurrence sur M que pour tout M on a $([y]M)[x := N] = [y](M[x := N])$.
   - Si $M = y$, alors $([y]M)[x := N] = ([y]y)[x := N] = \mathbf{I} = [y]y = [y](y[x := N]) = [y](M[x := N])$.
   - Si $y \notin V(M)$. Alors $([y]M)[x := N] = \mathbf{K}M[x := N] = \mathbf{K}M = [y]M = [y](M[x := N])$.
   - Cas où $M = AB$ et $y \in V(AB)$. Alors

$$\begin{aligned} ([y]M)[x := N] =& ([y]AB)[x := N] = (\mathbf{S}\ [y]A\ [y]B)[x := N] \\ &= \mathbf{S}\ ([y]A)[x := N]\ ([y]B)[x := N] \\ &= \mathbf{S}\ [y](A[x := N])\ [y](B[x := N]) \text{ par HR} \\ &= [y](A[x := N]B[x := N]) = [y]((AB)[x := N]) \\ &= [y](M[x := N]) \end{aligned}$$

   (b)
   - Exemple montrant que $y \neq x$ est utile : si $M := x = y$ et $N := \mathbf{K}$, alors $([y]M)[x := N]) = \mathbf{I} \neq \mathbf{KK} = [y](M[x := N])$.
   - Exemple montrant que $y \notin V(N)$ est utile : si $M := x$ et $N := y$, alors $([y]M)[x := N]) = \mathbf{K}y \neq \mathbf{I} = [y](M[x := N])$.

   (c) Avec $M := x$ et $N := \mathbf{KK}$, on obtient $(\{y\}M)[x := N] = \mathbf{K}(\mathbf{KK}) \neq \mathbf{S}(\mathbf{KK}))(\mathbf{KK})) = \{y\}(M[x := N])$.

9. Soit $x \in \mathcal{V}$ et $B \in \Lambda$. On montre par récurrence sur A que $A^*[x := B^*] = (A[x := B])^*$ pour tout A.
   - Cas où A est une variable
     - Si $A = x$, alors $A^*[x := B^*] = x^*[x := B^*] = x[x := B^*] = B^* = (x[x := B])^* = (A[x := B])^*$.
     - Si $A = y \neq x$, alors $A^*[x := B^*] = y^*[x := B^*] = y[x := B^*] = y = (y[x := B])^* = (A[x := B])^*$.

— Cas où $A = uv$. Alors

$$\begin{aligned}A^*[x := B^*] &= (uv)^*[x := B^*] = (u^*v^*)[x := B^*] = u^*[x := B^*]v^*[x := B^*]\\ &= u[x := B]^*v[x := B]^* \text{ par HR}\\ &= (u[x := B]v[x := B])^* = (uv[x := B])^* = (A[x := B])^*\end{aligned}$$

— Cas où $A = \lambda y.u$ où y est fraîche, en particulier $y \neq x$ et $y \notin V(B^*)(= FV(B) \cup BV(B))$. Alors

$$\begin{aligned}A^*[x := B^*] &= (\lambda y.u)^*[x := B^*] = ([y]u^*)[x := B^*]\\ &= [y](u^*[x := B^*]) \text{ par une question précédente}\\ &= [y](u[x := B]^*) \text{ par HR}\\ &= (\lambda y.u[x := B])^* = (A[x := B])^*\end{aligned}$$

10. Rappelons d'abord que $[\mathbf{S}]_{\mathcal{C}}uv \to_\beta^* \lambda z.uz(vz)$ (z fraîche), que $[\mathbf{S}]_{\mathcal{C}}uvw \to_\beta^* uw(vw)$, que $[\mathbf{K}]_{\mathcal{C}}u \to_\beta \lambda y.u$ (y fraîche) et que $[\mathbf{K}]_{\mathcal{C}}uv \to_\beta^* u$.
Soit $x \in \mathcal{V}$. Montrons maintenant par récurrence sur M que $[[x]M]_{\mathcal{C}}$ se β-réduit en $\lambda x.[M]_{\mathcal{C}}$ pour tout $M \in \mathcal{C}$.
— Cas où $M = x$. Alors

$$\begin{aligned}[[x]M]_{\mathcal{C}} &= [[x]x]_{\mathcal{C}} = [I]_{\mathcal{C}} = [\mathbf{S}]_{\mathcal{C}}[\mathbf{K}]_{\mathcal{C}}[\mathbf{K}]_{\mathcal{C}}\\ &\to_\beta^* \lambda z.[\mathbf{K}]_{\mathcal{C}}z([\mathbf{K}]_{\mathcal{C}}z)\\ &\to_\beta^* \lambda z.z = \lambda x.x = \lambda x.[x]_{\mathcal{C}} = \lambda x.[M]_{\mathcal{C}}\end{aligned}$$

— Cas où $x \notin V(M)$. Alors,

$$\begin{aligned}[[x]M]_{\mathcal{C}} &= [\mathbf{K}M]_{\mathcal{C}} = [\mathbf{K}]_{\mathcal{C}}[M]_{\mathcal{C}}\\ &\to_\beta \lambda x.[M]_{\mathcal{C}}\end{aligned}$$

— Cas où $M = AB$ et $x \in V(AB)$. Alors,

$$\begin{aligned}[[x](AB)]_{\mathcal{C}} &= [\mathbf{S}\ [x]A\ [x]B]_{\mathcal{C}} = [\mathbf{S}]_{\mathcal{C}}\ [[x]A]_{\mathcal{C}}\ [[x]B]_{\mathcal{C}}\\ &\to_\beta^* \lambda z.([[x]A]_{\mathcal{C}})z([[x]B]_{\mathcal{C}}z) \quad z \text{ fraîche}\\ &\to_\beta^* \lambda z.(\lambda x.[A]_{\mathcal{C}})z((\lambda x.[B]_{\mathcal{C}})z) \text{ par HR}\\ &\to_\beta^* \lambda z.[A]_{\mathcal{C}}[x := z][B]_{\mathcal{C}}[x := z] = \lambda x.[A]_{\mathcal{C}}[B]_{\mathcal{C}}\end{aligned}$$

11. (a)

$$\frac{}{(\lambda x.u)v \rhd u[x := v]}$$

$$\frac{M \rhd M'}{MN \rhd M'N} \qquad \frac{N \rhd N'}{MN \rhd MN'}$$

(b) On montre par récurrence sur $u \rhd v$ que $u \rhd v$ implique $u^* \to^* v^*$.
— Cas de base, $u = (\lambda x.A)B$ et $v = A[x := B]$. Alors

$$\begin{aligned}u^* &= ((\lambda x.A)B)^* = (\lambda x.A)^*B^* = ([x]A^*)B^*\\ &\to^* A^*[x := B^*] \text{ d'après une question précédente}\\ &= (A[x := B])^* \text{ d'après une question précédente}\\ &= v^*\end{aligned}$$

— Cas $u = AB$ et $v = A'B$ avec $A \to_\beta A'$. Alors $A^* \to^* A'^*$ par HR, donc $A^*B \to^* A'^*B$ par une question précédente.
— Cas $u = AB$ et $v = AB'$ avec $B \to_\beta B'$. Similaire.

12. Montrons que pour tout lambda-terme u, u est β-équivalent à $[u^*]_\mathcal{C}$, par récurrence sur u.
— Cas de base, $u = x \in \mathcal{V}$. Alors $u = x = [x^*]_\mathcal{C} = [u^*]_\mathcal{C}$.
— Cas où $u = AB$. Par HR $A \leftrightarrow^*_\beta [A^*]_\mathcal{C}$ et $B \leftrightarrow^*_\beta [B^*]_\mathcal{C}$. Donc $AB \leftrightarrow^*_\beta [A^*]_\mathcal{C}B$ et $[A^*]_\mathcal{C}B \leftrightarrow^*_\beta [A^*]_\mathcal{C}[B^*]_\mathcal{C}$ (propriétés du lambda calcul facile à prouver), donc $AB \leftrightarrow^*_\beta [A^*]_\mathcal{C}[B^*]_\mathcal{C}$.
— Cas où $u = \lambda x.A$. Par HR $A \leftrightarrow^*_\beta [A^*]_\mathcal{C}$. Alors $[(\lambda x.A)^*]_\mathcal{C} = [[x]A^*]_\mathcal{C} \to^*_\beta \lambda x.[A^*]_\mathcal{C}$ par une question précédente, donc $[(\lambda x.A)^*]_\mathcal{C} \leftrightarrow^*_\beta \lambda x.A$.

13. (a) Soit $\Omega = (\lambda x.xx)(\lambda x.xx)$. D'après une question précédente, $\Omega^* \to^* \Omega^*$. Plus précisément, $\Omega^* = \mathbf{S}\ \mathbf{I}\ \mathbf{I}\ (\mathbf{S}\ \mathbf{I}\ \mathbf{I}) \to \mathbf{I}\ (\mathbf{S}\ \mathbf{I}\ \mathbf{I})\ (\mathbf{I}\ (\mathbf{S}\ \mathbf{I}\ \mathbf{I})) \to^2 \Omega^*$.

(b) On définit la réduction parallèle par les règles suivantes.

$$\frac{}{M \Rightarrow M} \qquad \frac{M \Rightarrow M' \quad N \Rightarrow N'}{MN \Rightarrow M'N'}$$

$$\frac{M \Rightarrow M'}{\mathbf{K}\ M\ N \Rightarrow M'} \qquad \frac{M \Rightarrow M' \quad N \Rightarrow N' \quad P \Rightarrow P'}{\mathbf{S}\ M\ N\ P \Rightarrow M'P'(N'P')}$$

Montrons par récurrence sur M que $M \Rightarrow M_1$ et $M \Rightarrow M_2$ implique l'existence d'un M' tel que $M_1 \Rightarrow M'$ et $M_2 \Rightarrow M'$. On se débarrasse par cette phrase des cas où $M \in \{M_1, M_2\}$.
— Si M est une variable ou $\mathbf{K}$ ou $\mathbf{S}$, alors $M \in \{M_1, M_2\}$, cas traité ci-dessus.
— Si $M = AB$ alors on fait une disjonction de cas (pas une récurrence) sur les règles de réduction utilisées.
  — Si $M_1 = A_1B_1$ et $M_2 = A_2B_2$, avec $A \Rightarrow A_i$ et $B \Rightarrow B_i$ pour $i \in \{1,2\}$. Par HR, soit A' et B' tels que $A_i \Rightarrow A'$ et $B_i \Rightarrow B'$. Ainsi $M' := A'B'$ est un témoin recherché.
  — Si $M = \mathbf{K}\ A\ B$ et $A \Rightarrow M_1$ et $A \Rightarrow M_2$. Par HR soit M' tel que $M_i \Rightarrow M'$. Ainsi M' est un témoin recherché.
  — Si $M = \mathbf{K}\ A\ B$ et $A \Rightarrow M_1$ et $M_2 = \mathbf{K}\ A'\ B'$ avec $A \Rightarrow A'$ et $B \Rightarrow B'$. Par HR sur A, soit M' tel que $M_1 \Rightarrow M'$ et $A' \Rightarrow M'$. Ainsi M' est un témoin recherché.
  — Si $M = \mathbf{S}\ A\ B\ C$ et $M_i = A_iC_i(B_iC_i)$, avec $A \Rightarrow A_i$, $B \Rightarrow B_i$ et $C \Rightarrow C_i$. Par HR soient A', B', C' tels que $A_i \Rightarrow A'$, $B_i \Rightarrow B'$ et $B_i \Rightarrow B'$. Ainsi $M' := A'C'(B'C')$ est un témoin recherché.
  — Si $M = \mathbf{S}\ A\ B\ C$ et $M_1 = A_1C_1(B_1C_1)$ et $M_2 = \mathbf{S}\ A_2\ B_2\ C_2$, avec $A \Rightarrow A_i$, $B \Rightarrow B_i$ et $C \Rightarrow C_i$. Comme ci-dessus, par HR soient A', B', C' tels que $A_i \Rightarrow A'$, $B_i \Rightarrow B'$ et $B_i \Rightarrow B'$. Ainsi $M' := A'C'(B'C')$ est un témoin recherché.

(c) Il est facile de vérifier que $\to \subseteq \Rightarrow$. Montrons par récurrence sur $M \Rightarrow M'$ que $M \Rightarrow M'$ implique $M \to^* M'$.
— Si $M \Rightarrow M'$ vient de $A \Rightarrow A$ alors $M \to^* M'$.
— Cas où $M \Rightarrow M'$ vient de $AB \Rightarrow A'B'$. Alors $A \Rightarrow A'$ et $B \Rightarrow B'$, donc par HR $A \to^* A'$ et $B \to^* B'$, donc $AB \to^* A'B'$ par une question précédente.

— Cas où $M \Rightarrow M'$ vient de $\mathbf{K}\ A\ B \Rightarrow A'$. Alors $A \Rightarrow A'$, donc par HR $A \to^* A'$. Or $\mathbf{K}\ A\ B \to A$, donc $\mathbf{K}\ A\ B \to^* A'$.

— Cas où $M \Rightarrow M'$ vient de $\mathbf{S}\ A\ B\ C \Rightarrow A'C'(B'C')$. Alors $A \Rightarrow A'$, $B \Rightarrow B'$ et $C \Rightarrow C'$, donc par HR $A \to^* A'$, $B \to^* B'$ et $C \to^* C'$. Par suite, $AC(BC) \to^* A'C'(B'C')$. Or $\mathbf{S}\ A\ B\ C \to AC(BC)$, donc $\mathbf{S}\ A\ B\ C \to^* A'C'(B'C')$.

(d) Par les questions précédentes, $\to$ est confluente. La propriété désirée se démontre par récurrence structurelle sur la clôture reflexive, symmétrique et transitive.

(e) $[x]([y]x) = [x](\mathbf{K}x) = \mathbf{S}\ [x]\mathbf{K}\ [x]x = \mathbf{S}(\mathbf{K}\ \mathbf{K})\ \mathbf{I}$. D'une part, ni $\mathbf{K}$ ni $\mathbf{S}(\mathbf{K}\ \mathbf{K})\ \mathbf{I}$ ne se réduisent. D'autre part, ces deux termes sont différents, donc on n'a pas $\mathbf{K} \leftrightarrow^* [x]([y]x)$, d'après la question précédente.