MPRI, cours 2–2
Domaines

Thomas Ehrhard
Preuves, Programmes, Systèmes (UMR 7126)
Université Paris Diderot – Paris 7 et CNRS
http://www.pps.jussieu.fr/~ehrhard/

22 janvier 2009

Table des matières

On conseille de faire les exercices au fur et à mesure de la lecture (parfois, la solution d'un exercice se trouve plus loin dans le texte). Les exercices avec un astérique sont à faire en priorité (ils sont simples, et servent à vérifier que les notions ont été comprises).

Nos principaux ouvrages de référence, dont ce cours s'inspire d'ailleurs largement, sont [Kri90], [GLT89] (épuisé, mais accessible sur la page Web d'Yves Lafont) et [AC98].

Notations et terminologie générales

Si I est un ensemble, $\mathcal{P}(I)$ est l'ensemble de ses parties et $\mathcal{P}_{\text{fin}}(I)$ est l'ensemble de ses parties finies et $\mathcal{P}^*_{\text{fin}}(I)$ est l'ensemble des éléments non vides de $\mathcal{P}_{\text{fin}}(I)$. Si I est un ensemble, on note $\#I$ son cardinal.

Soient $s \subseteq A \times B$ et $t \subseteq B \times C$ des relations binaires. On note $t \cdot s \subseteq A \times C$ leur composée relationnelle, donnée par

$$t \cdot s = \{(a, c) \in A \times C \mid \exists b \in B (a, b) \in s \text{ et } (b, c) \in t\} .$$

Si R est une relation binaire sur un sensemble S, on note R^* sa *clôture transitive et reflexive*, c'est-à-dire la plus petite relation binaire sur S contenant R qui est réflexive et transitive. On voit facilement que $a\ R^*\ b$ ssi on peut trouver une suite $a_1, \ldots, a_n \in S$ telle que $a_1 = a$, $a_n = b$ et $a_i\ R\ a_{i+1}$ pour $i = 1, \ldots, n-1$.

Un *ensemble filtrant* est un ensemble non vide partiellement ordonné Γ tel que

$$\forall \gamma, \gamma' \in \Gamma\ \exists \delta \in \Gamma \quad \gamma, \gamma' \leq \delta\,.$$

Si Γ et Δ sont des ensembles filtrants, alors $\Gamma \times \Delta$ (avec l'ordre produit) est aussi un ensemble filtrant. Une *famille filtrante* est une famille indexée par un ensemble filtrant.

On note $\mathbb{N}^+$ l'ensemble des entiers naturels non nuls.

Chapitre 1

Lambda-calcul pur et typé

1.1 Syntaxe

On suppose donné un ensemble infini dénombrable de variables, notées typiquement par les lettres x, y, z, avec ou sans indices, primes etc. L'ensemble des lambda-termes est défini par la syntaxe suivante :

- si x est une variable, alors x est un terme ;
- si P et Q sont des termes, alors $(P)\,Q$ est un terme (application) ;
- si P est un terme et x est une variable, alors $\lambda x\,P$ est un terme (abstraction).

On note $\mathsf{VL}(P)$ l'ensemble des variables libres de P, qui est défini par récurrence sur les termes : $\mathsf{VL}(x) = \{x\}$, $\mathsf{VL}((P)\,Q) = \mathsf{VL}(P) \cup \mathsf{VL}(Q)$ et $\mathsf{VL}(\lambda x\,P) = \mathsf{VL}(P) \setminus \{x\}$.

On note Λ l'ensemble des lambda-termes.

1.1.1 Alpha-conversion. L'opération d'abstraction est liante, c'est-à-dire que la variable x, dans $\lambda x\,P$, est une variable muette. Autrement dit, on peut remplacer x par n'importe quelle autre variable, *à condition qu'elle ne soit pas libre dans* P. Cette transformation s'appelle alpha-conversion, et nous la passerons sous silence, bien qu'elle soit parfois indispensable, au cours de la beta-réduction. Il y a des syntaxes alternatives qui évitent l'alpha-conversion (notamment, les *indices de De Bruijn*), mais elles sont généralement bien plus lourdes que la syntaxe originale ; elles sont très utiles par contre pour les implémentations du lambda-calcul et des langages fonctionnels.

1.1.2 Beta-réduction. On note $M\,[N/x]$ le terme M dans lequel toutes les occurrences libres de x ont été remplacées par le terme N. Il faut faire très attention : si on n'y prend pas garde, des variables qui étaient libres dans N pourraient devenir liées par des abstractions figurant dans M.

On peut éviter ce problème en supposant qu'*aucune des variables liées dans M n'est libre dans N*. Quitte à remplacer M par un terme qui lui est alpha-équivalent, c'est une hypothèse qu'on peut toujours faire.

Cette précaution étant prise, la *substitution* est définie par récurrence sur M :

- $x\,[N/x] = N$ et $y\,[N/x] = y$ si y est une variable distincte de x ;
- $((P)\,Q)\,[N/x] = (P\,[N/x])\,Q\,[N/x]$;
- $(\lambda y\,P)\,[N/x] = \lambda y\,(P\,[N/x])$, et c'est ici qu'il faut faire attention : il ne faut pas que la variable y soit libre dans N. On peut toujours réaliser cette condition par alpha-conversion de $M = \lambda y\,P$. Il faut aussi supposer que $x \neq y$, ce qui, encore une fois, est possible par alpha-conversion de M.

On définit de façon similaire la *substitution parallèle* $M\,[N_1/x_1, \ldots, N_k/x_k]$ (avec les x_i des variables deux à deux distinctes) :

- $x\,[N_1/x_1,\ldots,N_k/x_k] = N_i$ si $x = x_i$ et $x\,[N_1/x_1,\ldots,N_k/x_k] = x$ si $x \notin \{x_1,\ldots,x_k\}$;
- $((P)\,Q)\,[N_1/x_1,\ldots,N_k/x_k] = (P\,[N_1/x_1,\ldots,N_k/x_k])\,Q\,[N_1/x_1,\ldots,N_k/x_k]$;
- $(\lambda y\,P)\,[N_1/x_1,\ldots,N_k/x_k] = \lambda y\,(P\,[N_1/x_1,\ldots,N_k/x_k])$, et c'est encore ici qu'il faut faire attention : il ne faut pas que la variable y soit libre dans l'un des N_i. On peut toujours réaliser cette condition par alpha-conversion de $M = \lambda y\,P$. Il faut aussi supposer que $y \notin \{x_1,\ldots,x_n\}$, ce qui, encore une fois, est possible par alpha-conversion de M.

Observer que si x n'est libre dans aucun des N_i, on a

$$M\,[N_1/x_1,\ldots,N_k/x_k]\,[N/x] = M\,[N_1/x_1,\ldots,N_k/x_k,N/x]\ .$$

Un beta-redex est un terme de la forme $(\lambda x\,M)\,N$, et la beta réduction consiste à le transformer en $M\,[N/x]$. Mais cette opération peut être effectuée n'importe où dans un lambda-terme.

On va définir la relation de beta-réduction dans toute sa généralité. C'est une relation binaire entre les lambda-termes (une relation de réécriture) que l'on note β. Par récurrence sur M, on définit l'ensembles des termes N tels que $M\;\beta\;N$, par les clauses suivantes :

- $x\;\beta\;N$ n'est jamais vrai.
- $\lambda x\,P\;\beta\;N$ si $N = \lambda x\,Q$ et $P\;\beta\;Q$.
- $(P_1)\,P_2\;\beta\;N$ dans l'un des cas suivants :
  - $N = (Q_1)\,P_2$ et $P_1\;\beta\;Q_1$,
  - $N = (P_1)\,Q_2$ et $P_2\;\beta\;Q_2$,
  - $P_1 = \lambda x\,R$ et $N = R\,[P_2/x]$.

On note donc β^* la clôture réflexive-transitive de cette relation. On rappelle le premier théorème fondamental du lambda-calcul.

Théorème 1.1.1 (Church-Rosser) *La relation β^* est confluente, c'est-à-dire que si $M\;\beta^*\;M_1$ et $M\;\beta^*\;M_2$, alors il existe N tel que $M_1\;\beta^*\;N$ et $M_2\;\beta^*\;N$.*

Un terme M est *normal* s'il ne contient aucun beta-redex. Il est *normalisable* s'il existe N normal tel que $M\;\beta^*\;N$. Il est *fortement normalisable* s'il n'existe aucune suite infinie de lambda-termes $M_1, M_2, \ldots$ avec $M = M_1$ et $M_i\;\beta\;M_{i+1}$ pour tout i.

Un terme fortement normalisable est normalisable, mais la réciproque est fausse. Un terme normalisable a une unique forme normale, à cause du théorème de Church-Rosser.

1.1.3 Le système F de Girard (à la Curry). Il s'agit d'un système de typage pour le lambda-calcul pur. Les types obéissent à la syntaxe suivante, un ensemble infini dénombrable de variables de types étant donné, notées ζ, ξ, avec des indices, des primes etc. :

- si ζ est une variable de type, c'est un type ;
- si A et B sont des types, alors $A \Rightarrow B$ est un type ;
- si ζ est une variable de type et si A est un type, alors $\forall\zeta\,A$ est un type.

La quantification universelle est une opération liante ; l'ensemble $\mathsf{VL}(A)$ des variables de types d'un type A est défini par $\mathsf{VL}(\zeta) = \{\zeta\}$, $\mathsf{VL}(A \Rightarrow B) = \mathsf{VL}(A) \cup \mathsf{VL}(B)$ et $\mathsf{VL}(\forall\zeta\,A) = \forall(\,A) \setminus \{\zeta\}$.

Un contexte de typage est une suite finie $\Gamma = (x_1 : A_1, \ldots, x_n : A_n)$ où les x_i sont des variables deux à deux distinctes, et les A_i sont des types. Quand on écrit $\Gamma, x : A$, cela suppose que x n'est pas dans le domaine $\{x_1,\ldots,x_n\}$ de Γ, et alors cette notation désigne le contexte Γ étendu en ajoutant $x : A$ à Γ.

Un jugement de typage est une expression de la forme $\Gamma \vdash M : A$ où Γ est un contexte de typage, M est un lambda-terme pur et A est un type. L'ensemble $\mathsf{VL}(\Gamma)$ est la réunion des $\mathsf{VL}(A_i)$, si $\Gamma = (x_1 : A_1, \ldots, x_n : A_n)$.

Les règles de typage sont les suivantes.

$$\frac{}{\Gamma, x : A \vdash x : A}$$

$$\frac{\Gamma \vdash M : A \Rightarrow B \qquad \Gamma \vdash N : A}{\Gamma \vdash (M)\, N : B}$$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x\, M : A \Rightarrow B}$$

$$\frac{\Gamma \vdash M : \forall \zeta\, A}{\Gamma \vdash M : A\, [B/\zeta]}$$

$$\frac{\Gamma \vdash M : A}{\Gamma \vdash M : \forall \zeta\, A} \quad \text{à condition que } \zeta \notin \mathsf{VL}(\Gamma)$$

Le résultat classique suivant ne nous servira pas, mais doit être mentionné.

Proposition 1.1.2 (réduction du sujet) *Si $\Gamma \vdash M : A$ et $M\ \beta\ M'$, alors $\Gamma \vdash M' : A$.*

1.1.4 Normalisation forte du système F. Le résultat suivant est dû à Girard. Il n'admet aucune preuve «combinatoire» connue (par là, on entendrait typiquement une preuve montrant qu'une certaine mesure définie sur les termes, à valeur dans un ensemble ordonné bien fondé — typiquement un ordinal —, diminue strictement au cours de la réduction). La seule preuve connue est celle qu'on va donner ici, qui est celle de Girard (voir [GLT89]), dans la présentation très élégante de Krivine [Kri90]. C'est une première illustration de la très puissante méthode de *réductibilité* que nous rencontrerons plusieurs fois dans ce cours.

Théorème 1.1.3 *Si $\Gamma \vdash M : A$, alors M est fortement normalisable.*

On va maintenant prouver ce théorème fondamental, en utilisant la méthode de réductibilité, qu'on peut voir comme une méthode sémantique, car elle consiste à définir une *interprétation* des types par des ensembles de termes.

Soit $\mathcal{N}$ l'ensemble des termes fortement normalisables et $\mathcal{N}_0$ l'ensemble des termes de la forme $(x)\, N_1 \ldots N_n$ où les N_i sont dans $\mathcal{N}$.

Une partie $\mathcal{X}$ de Λ est *saturée* si

$$\forall M, N, N_1, \ldots, N_n \in \mathcal{N} \quad (M\, [N/x])\, N_1 \ldots N_n \in \mathcal{X} \Rightarrow (\lambda x\, M)\, N N_1 \ldots N_n \in \mathcal{X}\ .$$

[**NB:** Bien noter l'hypothèse que tous les termes considérés sont dans $\mathcal{N}$.]

Lemme 1.1.4 *L'ensemble $\mathcal{N}$ est saturé.*

Démonstration. Soient $M, N, N_1, \ldots, N_n \in \mathcal{N}$, tels que $(M\, [N/x])\, N_1 \ldots N_n \in \mathcal{N}$.

Supposons $P = (\lambda x\, M)\, N N_1 \ldots N_n$ non fortement normalisable et soit $P = P_1\ \beta\ P_2\ \beta\ P_3 \ldots$ une suite infinie de beta-réduction à partir de P. Deux cas sont possibles :

- Ou bien le redex le plus à gauche n'est jamais réduit, et dans ce cas chaque P_i est de la forme $P_i = \left(\lambda x\, M^i\right) N^i N_1^i \ldots N_n^i$ et, pour chaque i, on a $M^i\ \beta\ M^{i+1}$, $N^i\ \beta\ N^{i+1}$ ou $N_j^i\ \beta\ N_j^{i+1}$ pour un $j \in \{1, \ldots, n\}$. Mais cela contredit notre hypothèse que $M, N, N_1, \ldots, N_n \in \mathcal{N}$.

– Ou bien le redex le plus à gauche est réduit à l'étape m de notre suite infinie de beta-réduction, qui est donc de la forme

$$\begin{aligned} P = P_1 \quad \beta^* \quad & P_m = (\lambda x\, M')\, N' N'_1 \ldots N'_n \\ \beta \quad & P_{m+1} = (M'\,[N'/x])\, N'_1 \ldots N'_n \;\beta\; P_{m+2} \ldots \end{aligned}$$

où, dans les $m-1$ premières étapes de réduction, seuls les termes M, N, $N_1, \ldots, N_n$ sont réduits. Mais alors, on a

$$(M\,[N/x])\, N_1 \ldots N_n \;\beta^*\; P_{m+1} \;\beta\; P_{m+2} \ldots$$

ce qui contredit notre hypothèse que $(M\,[N/x])\, N_1 \ldots N_n \in \mathcal{N}$.

Exercice 1.1.1 Enoncer et prouver la propriété de β^* qu'on vient d'utiliser implicitement.

□

Soient $\mathcal{X}, \mathcal{Y} \subseteq \Lambda$. On définit

$$(\mathcal{X} \Rightarrow \mathcal{Y}) = \{M \in \Lambda \mid \forall N \in \mathcal{X} \;\; (M)\, N \in \mathcal{Y}\}\,. \tag{1.1}$$

Observer que si $\mathcal{X}' \subseteq \mathcal{X} \subseteq \Lambda$ et $\mathcal{Y} \subseteq \mathcal{Y}' \subseteq \Lambda$, alors $(\mathcal{X} \Rightarrow \mathcal{Y}) \subseteq (\mathcal{X}' \Rightarrow \mathcal{Y}')$ (l'implication est croissante à droite et décroissante à gauche).

Lemme 1.1.5 *Soit $\mathcal{X} \subseteq \mathcal{N}$ et soit $\mathcal{Y}$ saturée. Alors $\mathcal{X} \Rightarrow \mathcal{Y}$ est saturée.*
L'intersection d'une famille non vide *de parties saturées est saturée.*

Exercice* **1.1.2** Démontrer ce lemme.

Lemme 1.1.6 *On a les inclusions suivantes :*

$$\mathcal{N}_0 \subseteq (\mathcal{N} \Rightarrow \mathcal{N}_0) \subseteq (\mathcal{N}_0 \Rightarrow \mathcal{N}) \subseteq \mathcal{N}\ .$$

Démonstration. La première inclusion résulte de la définition de $\mathcal{N}_0$. La seconde résulte du fait que $\mathcal{N}_0 \subseteq \mathcal{N}$ et du fait que l'opération $\_ \Rightarrow \_$ est croissante à droite et décroissante à gauche. Pour la dernière inclusion, soit $M \in (\mathcal{N}_0 \Rightarrow \mathcal{N})$; soit x une variable. Comme $x \in \mathcal{N}_0$, le terme $(M)\, x$ est fortement normalisable, ce qui implique que M est fortement normalisable. □

Une *valuation* est une application $\mathcal{I}$ des variables de types vers les sous-ensembles de Λ qui sont saturés, inclus dans $\mathcal{N}$ et contiennent $\mathcal{N}_0$. Si $\mathcal{I}$ est une valuation, ζ une variable de type et $\mathcal{X}$ une partie saturée de Λ telle que $\mathcal{N}_0 \subseteq \mathcal{X} \subseteq \mathcal{N}$, on note $\mathcal{I}(\zeta \mapsto \mathcal{X})$ la valuation définie par

$$\mathcal{I}(\zeta \mapsto \mathcal{X})(\xi) = \begin{cases} \mathcal{I}(\xi) & \text{si } \xi \neq \zeta \\ \mathcal{X} & \text{si } \xi = \zeta. \end{cases}$$

Par récurrence sur le type A, on définit $[A]_{\mathcal{I}} \subseteq \mathcal{N}$ saturé et contenant $\mathcal{N}_0$, pour toute valuation $\mathcal{I}$, de la façon suivante :

– $[\zeta]_{\mathcal{I}} = \mathcal{I}(\zeta)$ qui est saturé et inclus dans $\mathcal{N}$ car $\mathcal{I}$ est une valuation.
– $[A \Rightarrow B]_{\mathcal{I}} = [A]_{\mathcal{I}} \Rightarrow [B]_{\mathcal{I}}$. Par hypothèse de récurrence, $\mathcal{N}_0 \subseteq [A]_{\mathcal{I}} \subseteq \mathcal{N}$, $\mathcal{N}_0 \subseteq [B]_{\mathcal{I}} \subseteq \mathcal{N}$ et donc $\mathcal{N}_0 \subseteq [A \Rightarrow B]_{\mathcal{I}} \subseteq \mathcal{N}$ par le lemme 1.1.6. Toujours par hypothèse de récurrence, $[A]_{\mathcal{I}} \subseteq \mathcal{N}$ et $[B]_{\mathcal{I}}$ est saturé, sonc $[A \Rightarrow B]_{\mathcal{I}}$ est saturé par le lemme 1.1.5.

– Enfin, $[\forall\zeta\, A]_{\mathcal{I}}$ est l'intersection de tous les ensembles $[A]_{\mathcal{J}(\zeta\mapsto\mathcal{X})}$ où $\mathcal{X}$ est une partie saturée de Λ telle que $\mathcal{N}_0 \subseteq \mathcal{X} \subseteq \mathcal{N}$. Par hypothèse de récurrence, on a que $[A]_{\mathcal{I}(\zeta\mapsto\mathcal{X})}$ est saturé et vérifie $\mathcal{N}_0 \subseteq [A]_{\mathcal{I}(\zeta\mapsto\mathcal{X})} \subseteq \mathcal{N}$. Donc $[\forall\zeta\, A]_{\mathcal{I}}$ est saturé (par le lemme 1.1.5) et contient $\mathcal{N}_0$. L'ensemble $[\forall\zeta\, A]_{\mathcal{I}}$ est contenu dans $\mathcal{N}$ car il existe au moins une partie $\mathcal{X}$ de Λ qui est saturée et vérifie $\mathcal{N}_0 \subseteq \mathcal{X} \subseteq \mathcal{N}$, à savoir $\mathcal{N}$.

Lemme 1.1.7 *Si A est un type et si $\mathcal{I}$ et $\mathcal{J}$ sont des valuations qui coïncident sur toutes les variables libres de A, alors $[A]_{\mathcal{I}} = [A]_{\mathcal{J}}$.*

Exercice 1.1.3 Rédiger la preuve.

Lemme 1.1.8 *Soient A et B deux types, soit ζ une variable de type et $\mathcal{I}$ une valuation. On a*

$$[A\,[B/\zeta]]_{\mathcal{I}} = [A]_{\mathcal{I}(\zeta\mapsto[B]_{\mathcal{I}})}\,.$$

Exercice 1.1.4 Rédiger la preuve.

On peut maintenant prouver le lemme principal, qui énonce fondamentalement qu'un terme d'un type donné appartient à l'interprétation de ce type. Pour des raisons techniques, l'énoncé est légèrement plus compliqué (il faut tenir compte du contexte).

Lemme 1.1.9 (adéquation) *Soient $\Gamma = (x_1 : A_1, \ldots, x_n : A_n)$ un contexte de typage, A un type et M un terme tel que $\Gamma \vdash M : A$. Soit $\mathcal{I}$ une valuation et soient $N_1, \ldots, N_n$ des termes tels que $N_i \in [A_i]_{\mathcal{I}}$ pour $i = 1, \ldots, n$. On a*

$$M\,[N_1/x_1, \ldots, N_n/x_n] \in [A]_{\mathcal{I}}\,.$$

Démonstration. La preuve est par récurrence, non pas exactement sur M, mais sur la dérivation de typage menant à $\Gamma \vdash M : A$. Pour alléger les notations dans cette preuve, si P est un terme, P' désignera le terme $P\,[N_1/x_1, \ldots, N_n/x_n]$.

Si la dernière règle est une règle de variable (et donc la dérivation se réduit à cette seule règle) et $M = x_i$, alors $M' = N_i$ et $A = A_i$. On a par hypothèse $N_i \in [A_i]_{\mathcal{I}}$.

On traite ensuite les règles d'élimination, qui sont les plus directes.

Si la dernière règle est une règle d'élimination de $\Rightarrow$, alors M est une application $M = (P)\,Q$, et les prémisses de la règle sont de la forme $\Gamma \vdash P : B \Rightarrow A$ et $\Gamma \vdash Q : B$. Par hypothèse de récurrence, on a $P' \in [B \Rightarrow A]_{\mathcal{I}} = [B]_{\mathcal{I}} \Rightarrow [A]_{\mathcal{I}}$ et $Q' \in [B]_{\mathcal{I}}$, et donc $M' = (P')\,Q' \in [A]_{\mathcal{I}}$ par définition de $[B]_{\mathcal{I}} \Rightarrow [A]_{\mathcal{I}}$.

Si le dernière règle est une règle d'élimination du $\forall$, alors $A = B\,[C/\zeta]$ et la prémisse est $\Gamma \vdash M : \forall\zeta\, B$. Par hypothèse de récurrence, on a $M' \in [\forall\zeta\, B]_{\mathcal{I}}$ et on conclut car

$$[\forall\zeta\, B]_{\mathcal{I}} \subseteq [A]_{\mathcal{I}(\zeta\mapsto[C]_{\mathcal{I}})}\,,$$

puisque $[C]_{\mathcal{I}}$ est une partie saturée et comprise entre $\mathcal{N}_0$ et $\mathcal{N}$. Or $[B]_{\mathcal{I}(\zeta\mapsto[C]_{\mathcal{I}})} = [B\,[C/\zeta]]_{\mathcal{I}}$ par le lemme 1.1.8 et on conclut.

On finit avec les règles d'introduction, en ménageant le suspens (mais à quoi donc peut bien servir la condition de saturation, qu'on n'a toujours pas utilisée ?).

Si la dernière règle est une règle d'introduction du $\forall$, alors $A = \forall\zeta B$ et la prémisse est $\Gamma \vdash M : B$, et de plus on sait que ζ n'est libre dans aucune des formules A_i. On doit montrer que $M' \in [\forall\zeta\, B]_{\mathcal{I}}$. Soit donc $\mathcal{X}$ un ensemble saturé tel que $\mathcal{N}_0 \subseteq \mathcal{X} \subseteq \mathcal{N}$. Il faut montrer que $M' \in [B]_{\mathcal{J}}$, où $\mathcal{J} = \mathcal{I}(\zeta \mapsto \mathcal{X})$. Or on sait que, pour chaque $i \in \{1, \ldots, n\}$, on a $N_i \in [A_i]_{\mathcal{I}}$, et de plus on a $[A_i]_{\mathcal{I}} = [A_i]_{\mathcal{J}}$ par le lemme 1.1.7. On conclut en appliquant l'hypothèse de récurrence.

Si la dernière règle est une règle d'introduction de $\Rightarrow$, alors $A = B \Rightarrow C$, $M = \lambda x\, P$ et la prémisse est de la forme $\Gamma, x : B \vdash P : C$. Il faut montrer que $\lambda x\, P' \in [A \Rightarrow B]_{\mathcal{I}}$ (on prend x n'apparaissant dans aucun des termes N_i, et on a bien $(\lambda x\, P)' = \lambda x\, P'$). Soit donc $N \in [B]_{\mathcal{I}}$, il s'agit de montrer que $(\lambda x\, P')\, N \in [C]_{\mathcal{I}}$. Or, comme $N \in [B]_{\mathcal{I}}$, et comme $P'\,[N/x] = P\,[M_1/x_1, \ldots, M_n/x_n, N/x]$ (on suppose que x ne figure libre dans aucun des M_i) on a, par hypothèse de récurrence, que $P'\,[N/x] \in [C]_{\mathcal{I}}$. D'autre part, comme $x \in \mathcal{N}_0 \subseteq [B]_{\mathcal{I}}$, on a, également par hypothèse de récurrence, que $P' = P'\,[x/x] \in [B]_{\mathcal{I}} \subseteq \mathcal{N}$. Enfin, on a $N \in [B]_{\mathcal{I}} \subseteq \mathcal{N}$. Donc, comme $P'\,[N/x] \in [C]_{\mathcal{I}}$ et comme $[C]_{\mathcal{I}}$ est saturé, on a $(\lambda x\, P')\, N \in [C]_{\mathcal{I}}$. □

Voici maintenant la preuve du théorème 1.1.3.

Démonstration. Supposons que $x_1 : A_1, \ldots, x_n : A_n \vdash M : A$ et soit $\mathcal{I}$ une valuation quelconque (il en existe, on peut toujours prendre $\mathcal{I}(\zeta) = \mathcal{N}$ pour tout ζ). Pour chaque $i \in \{1, \ldots, n\}$, on a $x_i \in \mathcal{N}_0 \subseteq [A_i]_{\mathcal{I}}$. Donc, par le lemme d'adéquation, on a $M = M\,[x_1/x_1, \ldots, x_n/x_n] \in [A]_{\mathcal{I}} \subseteq \mathcal{N}$, donc M est fortement normalisable. □

On verra un peu plus loin une autre application de la même technique, dans un cadre de sémantique dénotationnelle, au lieu du typage.

1.2 Sémantique dénotationnelle du lambda-calcul pur

La notion la plus générale de modèle dénotationnel du lambda-calcul pur est celle d'objet réflexif dans une catégorie cartésienne fermée. On va définir cette notion, et en donner un exemple, ce qui sera l'occasion de présenter les domaines de Scott.

1.2.1 Objet réflexif dans une CCC. Soit $\mathcal{C}$ une catégorie cartésienne fermée. On adopte les notations suivantes :

- $\top$ est l'*objet terminal*, et si $X \in \mathcal{C}$, alors $\mathsf{t}_X : X \to \top$ est l'unique élément de $\mathcal{C}(X, \top)$.
- Le *produit cartésien* de deux objets X_1 et X_2 est noté $X_1 \ \&\ X_2$ (notation pas très standard, mais correspondant à la logique linéaire). Les deux projections sont notées π_1 et π_2. Si $f_i \in \mathcal{C}(Y, X_i)$ pour $i = 1, 2$, on note $\langle f_1, f_2 \rangle \in \mathcal{C}(Y, X_1 \ \&\ X_2)$ l'unique morphisme associé («pairing» de f_1 et f_2). On rappelle les 3 équations fondamentales qui expriment que $\mathcal{C}$ est cartésienne :

$$\begin{aligned} \langle f_1, f_2 \rangle \circ g &= \langle f_1 \circ g, f_2 \circ g \rangle \\ \pi_i \circ \langle f_1, f_2 \rangle &= f_i \\ \langle \pi_1, \pi_2 \rangle &= \mathsf{Id}_{X_1 \& X_2} \end{aligned}$$

- L'*objet des morphismes* de X vers Y est noté $X \Rightarrow Y$. On note $\mathsf{Ev} : \mathcal{C}((X \Rightarrow Y) \ \&\ X, Y)$ le morphisme d'évaluation, et si $f \in \mathcal{C}(Z \ \&\ X, Y)$, on note $\Lambda(f) \in \mathcal{C}(Z, X \Rightarrow Y)$ le morphisme «curryfié» associé. On rappelle que la clôture cartésienne est caractérisée par les 3 équations suivantes, dans lesquelles $g \in \mathcal{C}(Z', Z)$ est un autre morphisme :

$$\begin{aligned} \Lambda(f) \circ g &= \Lambda(f \circ \langle g \circ \pi_1, \pi_2 \rangle) \\ \mathsf{Ev} \circ \langle \Lambda(f) \circ \pi_1, \pi_2 \rangle &= f \\ \Lambda(\mathsf{Ev}) &= \mathsf{Id}_{X \Rightarrow Y} \end{aligned}$$

Cette présentation équationnelle du produit cartésien et de l'objet des morphismes est équivalente à la présentation par propriété universelle.

Un *objet réflexif* dans $\mathcal{C}$ est un triplet $(U, \mathsf{abs}, \mathsf{app})$ où U est un objet de $\mathcal{C}$ et $\mathsf{abs} : (U \Rightarrow U) \to U$ et $\mathsf{app} : U \to (U \Rightarrow U)$ qui satisfont $\mathsf{app} \circ \mathsf{abs} = \mathsf{Id}_{U \Rightarrow U}$. Etant donné un tel objet réflexif, on peut définir une sémantique pour tout lambda-terme pur. On dit que $(U, \mathsf{abs}, \mathsf{app})$ est *extensionnel* si de plus $\mathsf{abs} \circ \mathsf{app} = \mathsf{Id}_U$.

Plus précisément, étant donné un lambda-terme pur M et une liste $x_1, \ldots, x_n$ de variables deux à deux distinctes et contenant toutes les variables libres de M, on définit un morphisme

$$[M]^{x_1,\ldots,x_n} : U^n \to U$$

où U^n est le produit cartésien $U \mathbin{\&} \cdots \mathbin{\&} U$ (n termes). Cette interprétation est définie par récurrence sur M :

- si M est la variable x_i, alors $[M]^{x_1,\ldots,x_n} = \pi_i$;
- si $M = \lambda x\, P$, alors par hypothèse de récurrence, $[M]^{x_1,\ldots,x_n,x} : U^n \mathbin{\&} U \to U$, et on pose $[M]^{x_1,\ldots,x_n} = \mathsf{abs} \circ \Lambda([P]^{x_1,\ldots,x_n,x})$ (bien sûr, on suppose x distinct de tous les x_i, ce qui est possible par alpha-conversion) ;
- si $M = (P)\, Q$, alors par hypothèse de récurrence, $[P]^{x_1,\ldots,x_n} : U^n \to U$ et donc $\mathsf{app} \circ [P]^{x_1,\ldots,x_n} : U^n \to (U \Rightarrow U)$, et on pose $[M]^{x_1,\ldots,x_n} = \mathsf{Ev} \circ \langle \mathsf{app} \circ [P]^{x_1,\ldots,x_n}, [Q]^{x_1,\ldots,x_n} \rangle$.

Pour démontrer que cette interprétation est invariante par beta-réduction, il faut d'abord prouver un lemme de substitution.

Lemme 1.2.1 (substitution) *Soit P un lambda-terme et $x, x_1, \ldots, x_n$ une liste de variables deux à deux distinctes, contenant toutes les variables libres de P. Soit Q un lambda-terme, dont toutes les variables libres figurent dans la liste $x_1, \ldots, x_n$. Alors on a*

$$[P\,[Q/x]]^{x_1,\ldots,x_n} = [P]^{x,x_1,\ldots,x_n} \circ \langle [Q]^{x_1,\ldots,x_n}, \mathit{Id}_{U^n} \rangle\,.$$

Exercice 1.2.1 Rédiger la preuve, par récurrence sur P.

Proposition 1.2.2 *Si M et N sont des lambda-termes beta-équivalents et dont les variables libres figurent dans la liste de variables $x_1, \ldots, x_n$ (sans répétitions), alors on a $[M]^{x_1,\ldots,x_n} = [N]^{x_1,\ldots,x_n}$.*

Exercice* 1.2.2 Démontrer cette proposition. Il suffira de montrer que, si $M \ \beta\ N$, alors $[M]^{x_1,\ldots,x_n} = [N]^{x_1,\ldots,x_n}$, pour toute liste de variables $x_1, \ldots, x_n$ sans répétitions et contenant toutes les variables libres de M (et donc de N).

Chapitre 2

Sémantique de Scott

2.1 Domaines de Scott.

Cette section n'est pas essentielle pour la suite ; elle est surtout là pour la culture générale. Elle présente des notions plus générales que celles sur lesquelles nous concentrerons notre attention à partir de la section 2.2. On trouvera plus de détails sur ce sujet dans [AC98].

Si X est un ensemble partiellement ordonné (la relation d'ordre sera toujours notée $\leq$), un sous-ensemble D de X est dit *filtrant* s'il est filtrant pour l'ordre de X restreint à D.

Si une partie C de X a un sup, ce sup sera toujours noté $\bigvee C$. Le sup de deux éléments $x, y \in X$, s'il existe, sera noté $x \vee y$.

Un *cpo* (*ordre partiel complet*) est un ordre partiel dans lequel toutes les parties filtrantes ont un sup. Autrement dit, toute famille filtrante $(x_\gamma)_{\gamma\in\Gamma}$ croissante d'éléments de X doit avoir un sup $\bigvee_{\gamma\in G} x_\gamma \in X$.

Un élément x_0 d'un cpo X est dit *isolé* (on dit souvent *compact* mais ce n'est pas une très bonne terminologie) si, pour toute partie filtrante D de X, on a

$$x_0 \leq \bigvee D \Rightarrow \exists x \in D \; x_0 \leq x$$

(la réciproque étant toujours vraie). L'intuition est qu'un élément isolé est «fini». Par exemple, si $X = \mathcal{P}(\mathbb{N})$, ordonné par l'inclusion, les isolés de D sont les parties finies de $\mathbb{N}$.

Lemme 2.1.1 *Soit X un cpo et $B \subseteq X$ un ensemble fini d'éléments isolés de X. Si B a un sup, alors $\bigvee B$ est isolé.*

Démonstration. Soient $x_1, \ldots, x_n$ les éléments de B. Soit $D \subseteq X$ une partie filtrante telle que $\bigvee B \leq \bigvee D$, c'est-à-dire que pour tout $i \in \{1, \ldots, n\}$, $x_i \leq \bigvee D$. Comme x_i est isolé et D est filtrant, il existe $y_i \in D$ tel que $x_i \leq y_i$. Comme D est filtrant, il existe $y \in D$ tel que $y_i \leq y$ pour tout i. On a $\bigvee B \leq y$. □

Un *domaine de Scott* est un cpo X tel que

1. toute partie bornée de X a un sup (en particulier la partie vide a un sup, donc X a un élément minimal, qu'on note $\perp$) ;
2. l'ensemble des éléments isolés de X est dénombrable ;
3. tout élément de x est le sup de l'ensemble de ses minorants isolés (on dit que X est *algébrique*).

La condition correspondant à la conjonction des deux dernières conditions est souvent appelée *ω-algébricité*. Observer que, par la condition (1), et par le lemme 2.1.1, l'ensemble des minorants isolés d'un élément est filtrant.

Lemme 2.1.2 *Soit X un domaine de Scott et soient $x, y \in X$. On a $x \leq y$ si et seulement si, pour tout élément isolé x_0 de X, si $x_0 \leq x$, alors $x_0 \leq y$.*

Exercice 2.1.1 Prouver ce lemme.

Exercice 2.1.2 Soit X l'ensemble des fonctions partielles de $\mathbb{N}$ vers $\mathbb{N}$, ordonnées par l'inclusion des graphes (autrement dit, $f \leq g$ si le domaine de f est contenu dans celui de g et f et g coïncident sur le domaine de f). Montrer que X est un domaine de Scott.

Soient X et Y deux ensembles partiellement ordonnés. Soit $f : X \to Y$ une fonction croissante. Si $D \subseteq X$ est filtrant dans X, alors $f(X)$ est filtrant dans Y. Supposons que X et Y sont des cpo. Alors $f : X \to Y$ est *continue* si

- f est croissante (et donc l'image par f de toute partie filtrante de X est filtrante dans Y)
- et pour tout $D \subseteq X$ filtrant, on a $f(\bigvee D) = \bigvee f(D)$.

Observer que, dès que f est croissante, on a $\bigvee f(D) \leq f(\bigvee D)$. Donc, pour montrer qu'une fonction croissante f est continue, il suffit de montrer que, pour toute partie filtrante D, on a $f(\bigvee D) \leq \bigvee f(D)$.

L'exercice suivant est essentiel pour comprendre l'intuition derrière cette définition, dans le cas des domaines de Scott : une fonction est continue si, pour obtenir une information finie sur le résultat, il suffit d'une information finie sur l'argument.

Exercice* 2.1.3 Soient X et Y des domaines de Scott et soit $f : X \to Y$ une fonction. Alors f est continue si et seulement si

- f est croissante
- et, pour tout $x \in X$ et tout élément isolé y_0 de Y, si $y_0 \leq f(x)$, il existe un élément isolé x_0 de X tel que $x_0 \leq x$ et $y_0 \leq f(x_0)$.

Exercice 2.1.4 Soient X et Y des domaines de Scott et soit $f : X \to Y$ une fonction croissante. Montrer que f est continue si et seulement si, pour toute suite croissante $(x_n)_{n\in\mathbb{N}}$ d'éléments de X, on a $f(\bigvee_{n=0}^{\infty} x_n) = \bigvee_{n=0}^{\infty} f(x_n)$. [*Indication:* utiliser le fait que X a un nombre au plus dénombrable d'élements isolés.]

Soit $\mathbb{O}$ le domaine de Scott $\mathbb{O} = \{\perp < \top\}$. Soit X un domaine de Scott. On dit que $U \subseteq X$ est un *ouvert de Scott* si la «fonction caractéristique» de U, de X vers $\mathbb{O}$, qui envoie x sur $\top$ si $x \in U$ et sur $\perp$ sinon, est continue. Autrement dit, $U \subseteq X$ est un ouvert de Scott si les deux conditions suivantes sont vérifiées :

- si $x \in U$ et $x \leq y$, alors $y \in U$;
- pour toute partie filtrante D de X, si $\bigvee D \in U$, alors $U \cap D \neq \emptyset$.

Exercice 2.1.5 Soit X un domaine de Scott. Montrer que les ouverts de Scott définissent une topologie sur X, et que cette topologie est *séparée au sens T_0* : si $x, y \in X$ sont distincts, alors il existe un ouvert U tel que $x \in U$ et $y \notin U$, ou un ouvert U tel que $y \in U$ et $x \notin U$. C'est la notion la plus faible de séparation on topologie.

Exercice 2.1.6 Soient X et Y des domaines de Scott. Montrer qu'une fonction $f : X \to Y$ est continue (au sens ci-dessus) si et seulement si f est continue au sens de la *topologie de Scott* qu'on vient de définir sur X et sur Y.

2.1.1 La catégorie des domaines de Scott. Soit **Scott** la catégorie dont les objets sont les domaines de Scott et les morphismes sont les fonctions continues (il est clair que l'identité est continue et que la composée de deux fonctions continues et continue, donc il s'agit bien d'une catégorie).

Proposition 2.1.3 *La catégorie* **Scott** *est cartésienne.*

Démonstration. L'objet terminal est $\{\bot\}$. Le produit cartésien de deux domaines de Scott X_1 et X_2 est l'ensemble $X_1 \times X_2$, avec l'ordre produit ($(x_1, x_2) \leq (y_1, y_2)$ si $x_1 \leq y_1$ et $x_2 \leq y_2$). On notera aussi ce produit $X_1 \mathbin{\&} X_2$. Les projections sont définies de façon standard.

Exercice 2.1.7 Vérifier que $X_1 \mathbin{\&} X_2$ est bien un domaine de Scott. Il faudra vérifier en particulier que (x, y) est isolé si et seulement si x et y le sont.

□

La remarque suivante nous sera utile dans la suite.

Lemme 2.1.4 *Soient X, Y et Z des domaines de Scott et soit $f : X \mathbin{\&} Y \to Z$ une fonction croissante. Alors f est continue si et seulement si, pour toutes $D \subseteq X$ et $E \subseteq Y$ filtrantes, on a*

$$f(\bigvee D, \bigvee E) = \bigvee f(D \times E)\,.$$

Démonstration. On suppose d'abord f continue est on prend D et E comme dans l'énoncé du lemme. Alors $D \times E$ est une partie filtrante de $X \mathbin{\&} Y$, dont le sup est clairement $(\bigvee D, \bigvee E)$. Donc on a bien l'égalité voulue.

Pour la réciproque, soit $F \subseteq X \mathbin{\&} Y$ une partie filtrante. Soit $D = \pi_1(F)$ et $E = \pi_2(F)$, ce sont des parties filtrantes de X et Y respectivement. On a $\bigvee F = (\bigvee D, \bigvee E)$, car les projections sont continues. On doit montrer que $f(\bigvee F) \leq \bigvee f(F)$. Or, par hypothèse,

$$f(\bigvee F) = f(\bigvee D, \bigvee E) = \bigvee f(D \times E)$$

et il s'agit donc de vérifier que $\bigvee f(D \times E) \leq f(F)$. Pour cela, il suffit de montrer que tout élément de $D \times E$ est majoré par un élément de F dans $X \mathbin{\&} Y$. Si $(x, y) \in D \times E$, on peut trouver $x' \in X$ et $y' \in Y$ tels que $(x, y'), (x', y) \in F$, et comme F est filtrant, on peut trouver $(x'', y'') \in F$ tel que $(x'', y'') \geq (x, y'), (x', y)$, et donc $(x'', y'') \geq (x, y)$. □

Exercice 2.1.8 Déduire de ce lemme qu'une fonction $f : X \mathbin{\&} Y \to Z$ est continue si et seulement si elle est séparément continue (*i.e.* pour chaque $x \in X$, la fonction $y \mapsto f(x, y)$ et continue, et pour tout $y \in Y$, la fonction $x \mapsto f(x, y)$ est continue). Cette propriété est-elle vraie des fonctions $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$?

Théorème 2.1.5 *La catégorie* **Scott** *est cartésienne fermée.*

Démonstration. Soient X et Y des domaines de Scott. Soit $X \Rightarrow Y$ l'ensemble des fonctions continues de X vers Y, muni de la relation d'ordre dite *ordre extensionnel* :

$$f \leq g \quad \text{si} \quad \forall x \in X\ f(x) \leq g(x)\,.$$

On va vérifier que $X \Rightarrow Y$, avec cette relation d'ordre, est un domaine de Scott.

Soit $\mathcal{D} \subseteq X \Rightarrow Y$ un ensemble filtrant. Pour tout $x \in X$, l'ensemble $\{f(x) \mid f \in \mathcal{D}\} \subseteq Y$ est filtrant. Soit $h : X \to Y$ définie par $h(x) = \bigvee_{f \in \mathcal{D}} f(x)$. Alors h

est croissante (le vérifier). Soit D une partie filtrante de X. On doit montrer que $h(\bigvee D) \leq \bigvee_{x\in D} h(x)$.

Comme chaque $f \in \mathcal{D}$ est continue, on a

$$h(\bigvee D) = \bigvee_{f\in\mathcal{D}} \bigvee_{x\in D} f(x)\,.$$

Il suffit donc de voir que, pour tout $f \in \mathcal{D}$, on a $\bigvee_{x\in D} f(x) \leq \bigvee_{x\in D} h(x)$, ce qui est clair car $\forall x \in X\ f(x) \leq h(x)$. Par suite, h est continue. D'autre part, soit $g \in X \Rightarrow Y$ tel que $g \geq f$ pour tout $f \in D$. Soit $x \in X$. On a $g(x) \geq f(x)$ pour tout $f \in D$, et donc $g(x) \geq h(x)$. Donc $g \geq h$. Par suite h est le sup de D dans $X \Rightarrow Y$.

Donc $X \Rightarrow Y$ est un cpo.

Exercice 2.1.9 Montrer que $X \Rightarrow Y$ est *borné-complet* (toute partie bornée a un sup) et que le sup d'une partie bornée $\mathcal{B}$ de $X \Rightarrow Y$ est donné par

$$(\bigvee \mathcal{B})(x) = \bigvee_{f\in\mathcal{B}} f(x)\,.$$

Le raisonnement est similaire à celui qu'on vient de faire.

Soient $x_0 \in X$ et $y_0 \in Y$ isolés. Soit $[x_0, y_0]$ la *fonction de seuil* $[x_0, y_0] : X \to Y$ définie par

$$[x_0, y_0](x) = \begin{cases} y_0 & \text{si } x \geq x_0 \\ \perp & \text{sinon.} \end{cases}$$

Comme x_0 est isolé, cette fonction est continue. Soit $f \in X \Rightarrow Y$. On a

$$[x_0, y_0] \leq f \Leftrightarrow y_0 \leq f(x_0)\,.$$

Soit $\mathcal{D} \subseteq X \Rightarrow Y$ un ensemble filtrant, et supposons que $[x_0, y_0] \leq \bigvee \mathcal{D}$. Cela signifie que

$$y_0 \leq \bigvee_{f\in\mathcal{D}} f(x_0)$$

et donc, comme y_0 est isolé, il existe $f \in \mathcal{D}$ tel que $y_0 \leq f(x_0)$, c'est-à-dire $[x_0, y_0] \leq f$. Donc les fonctions de seuil sont isolées dans $X \Rightarrow Y$.

Si $f \in X \Rightarrow Y$, soit $s(f)$ l'ensemble des fonctions de seuil majorées par f, autrement dit

$$s(f) = \{[x_0, y_0] \mid x_0 \in \mathsf{i}(X),\ y_0 \in \mathsf{i}(Y) \text{ et } y_0 \leq f(x_0)\}\,,$$

où $\mathsf{i}(X)$ est l'ensemble des éléments isolés de X.

On montre que $f = \bigvee s(f)$ (ce sup existe, puisque $X \Rightarrow Y$ est borné-complet). Il suffit de montrer que $f \leq \bigvee s(f)$, l'autre inégalité étant évidente. Soit $x \in X$, on montre que $f(x) \leq \bigvee_{f_0\in s(f)} f_0(x)$. Soit y_1 un élément isolé de Y ; par le lemme 2.1.2, il suffit de montrer que, si $y_1 \leq f(x)$, alors $y_1 \leq \bigvee_{f_0\in s(f)} f_0(x)$. On suppose donc que $y_1 \leq f(x)$. Comme f est continue, il existe x_1, isolé dans X, tel que $x_1 \leq x$ et $y_1 \leq f(x_1)$. Donc $f_1 = [x_1, y_1] \in s(f)$ et comme $f_1(x) = y_1$, on en déduit que $y_1 \leq \bigvee_{f_0\in s(f)} f_0(x)$.

Soit alors $f \in X \Rightarrow Y$ et soit $\mathcal{B}$ l'ensemble des minorants de f qui sont isolés dans $X \Rightarrow Y$. On a bien sûr $\bigvee \mathcal{B} \leq f$. Mais $s(f) \subseteq \mathcal{B}$ (toute fonction de seuil est isolée) et on vient de voir que $\bigvee s(f) = f$, donc $\bigvee \mathcal{B} = f$. On a ainsi montré que $X \Rightarrow Y$ est algébrique. Pour conclure que c'est un domaine de Scott, il suffit de montrer qu'il n'a qu'un nombre dénombrable d'éléments isolés.

Soit donc $f_0 \in X \Rightarrow Y$ isolé. Pour toute partie finie $\mathcal{B}$ de $s(f)$, $\bigvee \mathcal{B}$ est un élément isolé de $X \Rightarrow Y$ qui est majoré par f_0. De plus, si $\mathcal{B}, \mathcal{B}' \in \mathcal{P}_{\mathrm{fin}}(s(f))$, on a $\mathcal{B} \subseteq \mathcal{B}' \Rightarrow \bigvee \mathcal{B} \leq \bigvee \mathcal{B}'$. Donc l'ensemble

$$\mathcal{D} = \{\bigvee \mathcal{B} \mid \mathcal{B} \in \mathcal{P}_{\mathrm{fin}}(s(f_0))\}$$

est une partie filtrante de $X \Rightarrow Y$, bornée par f_0 et contenant $s(f)$, ces deux dernières propriétés impliquant que $f_0 = \bigvee \mathcal{D}$. Donc comme f_0 est isolé, il existe une partie finie $\mathcal{B}$ de $s(f_0)$ telle que $f_0 = \bigvee \mathcal{B}$.

On a ainsi montré que tout élément isolé de $X \Rightarrow Y$ est le sup d'une famille finie de fonctions de seuil. Or, comme X et Y sont ω-algébriques, l'ensemble des fonctions de seuil est au plus dénombrable, et par conséquent, l'ensemble des fonctions isolées est au plus dénombrable (l'ensemble des parties finies d'un ensemble dénombrable est dénombrable).

Soit $\mathsf{Ev} : (X \Rightarrow Y) \,\&\, X \to Y$ définie par $\mathsf{Ev}(f, x) = f(x)$. Cette fonction est clairement croissante. Pour montrer qu'elle est continue, on applique le lemme 2.1.4. Soient $\mathcal{D} \subseteq X \Rightarrow Y$ et $D \subseteq X$ filtrantes. On a

$$\begin{aligned} (\bigvee \mathcal{D})(\bigvee D) &= \bigvee_{f \in \mathcal{D}} f(\bigvee D) \\ &= \bigvee_{f \in \mathcal{D}} \bigvee_{x \in D} f(x) \\ &= \bigvee \mathsf{Ev}(\mathcal{D} \times D) \end{aligned}$$

et on conclut.

Soient X, Y et Z des domaines de Scott et soit $f : Z \,\&\, X \to Y$ une fonction continue. Pour chaque $z \in Z$, la fonction $f_z : X \to Y$ définie par $f_z(x) = f(z, x)$ est continue, et on définit $\Lambda(f) : Z \to (X \Rightarrow Y)$ par $\Lambda(f)(z) = f_z$.

Exercice 2.1.10 Vérifier que $\Lambda(f)$ est continue. Vérifier que les trois équations de clôture cartésienne sont satisfaites.

On a ainsi prouvé que **Scott** est une catégorie cartésienne fermée. $\square$

2.2 Treillis complets premier-algébriques

On va travailler avec des domaines de Scott très particuliers, qui sont les treillis complets premier-algébriques. Ils ont d'excellentes propriétés de symétrie (un peu comme les espaces de cohérence), que les domaines de Scott généraux ne possèdent pas.

Un *treillis complet* est un ensemble partiellement ordonné dont tout sous-ensemble a un sup. Soit E un treillis complet. Si $A \subseteq E$, on note $\bigvee A$ le sup de A dans E. On note $\perp_E$ le plus petit élément de E (qui existe, c'est $\bigvee \emptyset$) et $\top_E$ le plus grand, qui est $\bigvee E$.

Un élément p de E est *premier* si, pour tout $A \subseteq E$, si $p \leq \bigvee A$, alors il existe $x \in A$ tel que $p \leq x$. On dit que E est *premier-algébrique* si tout élément de E est le sup de ses minorants premiers. On dénote par $\mathsf{Pr}\, E$ l'ensemble des éléments premiers de E, considéré comme ordre partiel (avec la restriction de l'ordre de E).

2.2.1 Représentation des treillis complets premier-algébriques. Soit S un ensemble préordonné (on note $\leq$ la relation de préordre). On rappelle qu'une relation de préordre est une relation réflexive et transitive. La relation sur S définie par $a \sim b$ si $a \leq b$ et $b \leq a$ est alors une relation d'équivalence, sur les classes d'équivalence de laquelle $\leq$ induit une relation d'ordre.

On note $\mathcal{I}(S)$ l'ensemble des *segments initiaux* de S, c'est-à-dire, des sous-ensembles u de S tels que $\forall a \in u, \forall b \in S\ b \leq a \Rightarrow b \in u$. Noter que si $a \in u \in \mathcal{I}(S)$ et si $b \sim a$ ($\sim$ étant la relation d'équivalence définie ci-dessus), alors $b \in u$: les éléments de $\mathcal{I}(S)$ sont clos pour la relation d'équivalence associée au préordre de S.

Muni de l'inclusion comme relation d'ordre, $\mathcal{I}(S)$ est un treillis complet : une réunion quelconque d'éléments de $\mathcal{I}(S)$ est un élément de $\mathcal{I}(S)$. Si $u \subseteq S$, on note $\downarrow u$ le plus petit élément de $\mathcal{I}(S)$ contenant u, on a donc

$$\downarrow u = \{b \in S \mid \exists a \in u\ b \leq a\}\,.$$

Si $a \in E$, on note $\downarrow a = \downarrow \{a\}$.

Lemme 2.2.1 $(\mathcal{I}(S), \subseteq)$ *est un treillis complet premier-algébrique dont les éléments premiers sont les* $\downarrow a$*, pour* $a \in S$*.*

Exercice* 2.2.1 Prouver ce lemme.

Proposition 2.2.2 *Soit* E *un treillis complet premier-algébrique. La fonction* φ *qui envoie* $x \in E$ *sur* $\{p \in \mathsf{Pr}\,E \mid p \leq x\}$ *est un isomorphisme entre* E *et* $\mathcal{I}(\mathsf{Pr}\,E)$*.*

Démonstration. Il suffit de montrer que φ est une bijection croissante dont la récipoque est aussi croissante. La fonction φ est croissante car si $p \leq x \leq y$, alors $p \leq y$ et donc $\varphi(x) \subseteq \varphi(y)$.

Soit $\psi : \mathcal{I}(\mathsf{Pr}\,E) \to E$ définie par $\psi(u) = \bigvee u$. Si $x \in E$, alors $\psi(\varphi(x)) = \bigvee\{p \in \mathsf{Pr}\,E \mid p \leq x\} = x$ car E est premier-algébrique. Soit $u \in \mathcal{I}(\mathsf{Pr}\,E)$. Si $p \in u$, on a $p \leq \bigvee u = \psi(u)$, donc $p \in \varphi(\psi(u))$, et donc $u \subseteq \varphi(\psi(u))$. Réciproquement, soit $p \in \mathsf{Pr}\,E$ tel que $p \in \varphi(\psi(u))$, c'est-à-dire $p \leq \bigvee u$. Comme p est premier, il existe $q \in u$ tel que $p \leq q$, et comme $u \in \mathcal{I}(\mathsf{Pr}\,E)$ (u est un segment initial), on a $p \in u$.

Donc ψ est l'inverse de φ, ce qui montre que φ est une bijection, et comme ψ est clairement croissante, φ est un isomorphisme d'ordres partiels entre E et $\mathcal{I}(\mathsf{Pr}\,E)$. $\square$

Donc tout treillis complet premier-algébrique E est de la forme $\mathcal{I}(S)$, pour un préordre S. La proposition ci-dessus montre qu'on peut prendre pour S un ordre partiel (l'ordre induit sur les premiers de E). Mais la construction des exponentielles qu'on va voir en section 2.6 montre qu'il est plus commode de considérer des préordres quelconques.

2.2.2 Morphismes linéaires. Soient E et F deux treillis complets. Une fonction $f : E \to F$ est linéaire si, pour toute partie A de E, on a $f(\bigvee A) = \bigvee f(A)$ (où, comme d'habitude, $f(A)$ est l'image directe de A par f, c'est-à-dire l'ensemble $\{f(x) \mid x \in A\}$). Il est clair que la composée de deux fonctions linéaires est linéaire et que l'identité est une fonction linéaire, donc les treillis complets et les fonctions linéaires forment une catégorie.

Remarquer que si $f : E \to F$ est linéaire, alors $f(\bot_E) = \bot_F$, mais par contre on n'a pas forcément $f(\top_E) = \top_F$. Remarquer aussi que f est croissante, car si $x \leq y$ dans E, on a $y = x \vee y$ et donc $f(y) = f(x \vee y) = f(x) \vee f(y)$.

2.3 La catégorie PoL

C'est la catégorie dont les objets sont les ensembles préordonnés, et les morphismes sont les fonctions linéaires entre treillis complets associés. Plus précisément, un objet de **PoL** est un ensemble préordonné S au plus dénombrable et un morphisme $f \in \mathbf{PoL}(S, T)$ est une fonction linéaire $\mathcal{I}(S) \to \mathcal{I}(T)$.

Si S et T sont des préordres, S^{op} désigne le préordre opposé (autrement dit, $a \leq_{S^{\mathrm{op}}} a'$ si $a' \leq_S a$) et $S \times T$ désigne le préordre produit, dont le support est le produit cartésien des supports de S et de T, avec $(a,b) \leq_{S\times T} (a',b')$ si $a \leq_S a'$ et $b \leq_T b'$.

2.3.1 Trace linéaire associée à une fonction linéaire. Soient S et T des péordres et soit $f \in \mathbf{PoL}(S,T)$. On définit la trace linéaire de f

$$\mathsf{tr}(f) = \{(a,b) \in S \times T \mid a \in f(\downarrow a)\}\,.$$

On vérifie que $\mathsf{tr}(f) \in \mathcal{I}(S^{\mathrm{op}} \times T)$. Soit $(a,b) \in \mathsf{tr}(f)$ et soit $(a',b') \in S \times T$ tel que $(a',b') \leq_{S^{\mathrm{op}}\times T} (a,b)$, c'est-à-dire $a \leq a'$ et $b' \leq b$. On a $\downarrow a \subseteq \downarrow a'$ donc $f(\downarrow a) \subseteq f(\downarrow a')$ et par suite $b \in f(\downarrow a')$, donc $(a',b') \in \mathsf{tr}(f)$ puisque $f(\downarrow a')$ est un segment initial.

On a en particulier $\mathsf{tr}(\mathsf{Id}_S) = \{(a,a') \in S \mid a' \leq a\}$.

Lemme 2.3.1 *Soient $f \in \mathbf{PoL}(S,T)$ et $g \in \mathbf{PoL}(T,U)$. On a $\mathsf{tr}(g \circ f) = \mathsf{tr}(g) \cdot \mathsf{tr}(f)$.*

Démonstration. Soit $(a,c) \in \mathsf{tr}(g \circ f)$, c'est-à-dire $c \in g(y)$ où $y = f(\downarrow a)$. Comme g est linéaire et comme $g(y) = \bigcup_{b\in y} g(\downarrow b)$, il existe $b \in y$ tel que $c \in g(\downarrow b)$, c'est-à-dire $(b,c) \in \mathsf{tr}(g)$. Comme $b \in f(\downarrow a)$, on a $(a,b) \in \mathsf{tr}(f)$. Donc $(a,c) \in \mathsf{tr}(g) \cdot \mathsf{tr}(f)$. Réciproquement, soit $(a,c) \in \mathsf{tr}(g) \cdot \mathsf{tr}(f)$. Soit $b \in T$ tel que $(a,b) \in \mathsf{tr}(f)$ et $(b,c) \in \mathsf{tr}(g)$. On a $b \in f(\downarrow a)$, donc $\downarrow b \subseteq f(\downarrow a)$ et donc $g(\downarrow b) \subseteq g(f(\downarrow a))$ par croissance de g. Or $c \in g(\downarrow b)$, ce qui montre que $c \in g(f(\downarrow a))$, c'est-à-dire $c \in \mathsf{tr}(g \circ f)$. $\square$

2.3.2 Fonction linéaire associée à une relation. Soit $t \in \mathcal{I}(S^{\mathrm{op}} \times T)$. On définit la fonction

$$\begin{aligned} \mathsf{fun}(t) : \mathcal{I}(S) &\rightarrow \mathcal{P}(T) \\ x &\mapsto \{b \mid \exists a \in x\ (a,b) \in t\}\,. \end{aligned}$$

Soit $b \in \mathsf{fun}(t)(x)$ et soit $b' \in T$ tel que $b' \leq b$. Soit $x \in S$ tel que $(a,b) \in t$. On a $(a,b') \leq_{S^{\mathrm{op}}\times T} (a,b)$, donc $(a,b') \in t$. Par suite $b' \in \mathsf{fun}(t)(x)$, et donc $\mathsf{fun}(t)$ prend ses valeurs dans $\mathcal{I}(T)$. De plus, cette fonction est linéaire, car si $A \subseteq \mathcal{I}(S)$ et si $b \in T$, on a $b \in \mathsf{fun}(t)(\bigcup A)$ ss'il existe $a \in \bigcup A$ tel que $(a,b) \in t$, ce qui est équivalent à dire qu'il existe $u \in A$ tel que $a \in u$ et $(a,b) \in t$, et cette dernière propriété est équivalente à dire que $b \in \bigcup\{\mathsf{fun}(t)(u) \mid u \in A\}$.

2.3.3 Un isomorphisme d'ordre. Donc $\mathsf{fun}(t) \in \mathbf{PoL}(S,T)$. On considère $\mathbf{PoL}(S,T)$ comme un ensemble partiellement ordonné, par l'ordre ponctuel (dit parfois aussi ordre extensionnel) : $f \leq g$ si $\forall x \in \mathcal{I}(S)\ f(x) \subseteq g(x)$.

Proposition 2.3.2 *Les fonctions* tr *et* fun *sont inverses l'une de l'autre et définissent un isomorphisme d'ordre entre $\mathbf{PoL}(S,T)$ et $\mathcal{I}(S^{\mathrm{op}} \times T)$.*

Démonstration. Soit $f \in \mathbf{PoL}(S,T)$. On montre que $\mathsf{fun}(\mathsf{tr}(f)) = f$. Soit donc $x \in \mathcal{I}(S)$. Soit $b \in f(x)$. Comme $x = \bigcup_{a\in x} \downarrow a$ et comme f est linéaire, on a $f(x) = \bigcup_{a\in x} f(\downarrow a)$. Donc, il existe $a \in x$ tel que $b \in f(\downarrow a)$, c'est-à-dire $(a,b) \in \mathsf{tr}(f)$. Par suite $b \in \mathsf{fun}(\mathsf{tr}(f))(x)$. Réciproquement, soit $b \in \mathsf{fun}(\mathsf{tr}(f))(x)$. Soit donc $a \in x$ tel que $(a,b) \in \mathsf{tr}(f)$. Cela signifie que $b \in f(\downarrow a)$, et comme $\downarrow a \subseteq x$ et comme f est croissante, on a $b \in f(x)$.

Soit maintenant $t \in \mathcal{I}(S^{\mathrm{op}} \times T)$, montrons que $\mathsf{tr}(\mathsf{fun}(t)) = t$. Soit donc $(a,b) \in S \times T$. Supposons que $(a,b) \in t$ et montrons que $(a,b) \in \mathsf{tr}(\mathsf{fun}(t))$. Comme $a \in$

$\downarrow a$, on a $b \in \mathsf{fun}(t)(\downarrow a)$ et donc $(a,b) \in \mathsf{tr}(\mathsf{fun}(t))(x)$. Réciproquement, supposons $(a,b) \in \mathsf{tr}(\mathsf{fun}(t))$. Cela signifie que $b \in \mathsf{fun}(t)(\downarrow a)$, c'est-à-dire qu'il existe $a' \in \downarrow a$ tel que $(a',b) \in t$. On a $a' \leq a$ et donc $(a,b) \leq_{S^{\mathrm{op}} \times T} (a',b)$ et comme $t \in \mathcal{I}(S^{\mathrm{op}} \times T)$, on a $(a,b) \in t$.

Les fonctions fun et tr sont donc inverses l'une de l'autre. Montrons que fun est croissante. Soient donc $s,t \in \mathcal{I}(S^{\mathrm{op}} \times T)$ tels que $s \subseteq t$, on montre que $\mathsf{fun}(s) \leq \mathsf{fun}(t)$. Soit donc $x \in \mathcal{I}(S)$ et soit $b \in \mathsf{fun}(s)(x)$. Cela signifie qu'il existe $a \in x$ tel que $(a,b) \in s$ tel que $a \in x$. Comme $s \subseteq t$, on a $(a,b) \in t$ et par suite $b \in \mathsf{fun}(t)(x)$, ce qui montre que $\mathsf{fun}(s) \leq \mathsf{fun}(t)$. Réciproquement, soient $f, g \in \mathbf{PoL}(S,T)$ tels que $f \leq g$ et montrons que $\mathsf{tr}(f) \subseteq \mathsf{tr}(g)$. Soit $(a,b) \in \mathsf{tr}(f)$. Cela signifie que $b \in f(\downarrow a)$. Comme $f \leq g$, on a $f(\downarrow a) \subseteq g(\downarrow a)$ et donc $b \in g(\downarrow a)$, c'est-à-dire que $(a,b) \in \mathsf{tr}(g)$. Donc $\mathsf{tr}(f) \subseteq \mathsf{tr}(g)$.

On a montré que fun et tr définissent un isomorphisme entre ensembles partiellement ordonnés. □

Il découle de ce qui précède que $\mathbf{PoL}(S,T)$ est un treillis complet.

Exercice* 2.3.1 Montrer que, si $\mathcal{F} \subseteq \mathbf{PoL}(S,T)$, alors $f = \bigvee \mathcal{F}$ est donné par $f(x) = \bigcup_{f \in \mathcal{F}} f(x)$.

Remarque 2.3.3 On peut donc, au choix, considérer un morphisme de S vers T dans $\mathbf{PoL}$ soit comme une fonction linéaire de $\mathcal{I}(S)$ vers $\mathcal{I}(T)$, soit comme un élément de $\mathcal{I}(S^{\mathrm{op}} \times T)$. On passera d'un point de vue à l'autre selon le contexte. On pose $S \multimap T = S^{\mathrm{op}} \times T$.

2.3.4 Isomorphismes forts. Par définition, un isomorphisme de S vers T est une fonction linéaire $f : \mathcal{I}(S) \to \mathcal{I}(T)$ qui est bijective, croissante, et dont la réciproque est aussi croissante. Deux ensembles préordonnés peuvent être isomorphes tout en étant très différents. Par exemple, si S a un seul élément, et si $T = \mathbb{N}$ (l'ensemble des entiers naturels), avec le préordre tel que $n \leq m$ pour tous $n, m \in \mathbb{N}$, alors $\mathcal{I}(S)$ et $\mathcal{I}(T)$ sont isomorphes (et isomorphes à l'ordre partiel $\{\bot, \top\}$ avec $\bot < \top$). Toutefois, dans la suite, on aura affaire à des isomorphismes beaucoup plus restrictifs.

On appelle *isomorphisme fort* de S vers T une application $\theta : S \to T$ qui est une bijection telle que, pour tous $a, a' \in S$, on ait $a \leq a'$ si et seulement si $\theta(a) \leq \theta(a')$. Autrement dit, un isomorphisme fort est un isomorphisme de préordres. On écrit $S \simeq T$ s'il existe un isomorphisme fort de S vers T.

Un tel isomorphisme fort $\theta : S \to T$ induit un isomorphisme de S vers T dans la catégorie $\mathbf{PoL}$, à savoir la fonction $\widehat{\theta} : \mathcal{I}(S) \to \mathcal{I}(T)$ défine par $\widehat{\theta}(x) = \{\theta(a) \mid a \in S\}$.

Exercice* 2.3.2 Vérifier que, si $\theta : S \to T$ est un isomorphisme fort, alors $\widehat{\theta}$ est bien à valeur dans $\mathcal{I}(T)$, que c'est un isomorphisme d'ordres partiels et que $\widehat{\theta^{-1}} = \widehat{\theta}^{-1}$. Vérifier également que $\mathsf{tr}(\widehat{\theta}) = \downarrow_{S^{\mathrm{op}} \times T} \mathsf{Gr}(\theta)$ (où $\mathsf{Gr}(\theta) \subseteq S \times T$ est le graphe de la fonction θ), c'est-à-dire, $\mathsf{tr}(\widehat{\theta}) = \{(a,b) \in S \times T \mid b \leq \theta(a)\}$.

2.4 Structure monoïdale

A partir de maintenant, nous verrons les morphismes de S vers T comme les éléments de $\mathcal{I}(S \multimap T)$. Pour éviter les confusions, nous noterons $\mathbf{PoLR}$ la catégorie dont les objets sont les préordres partiels et telle que $\mathbf{PoLR}(S,T) = \mathcal{I}(S \multimap T)$, l'identité Id_S sur S étant donné par $\mathsf{Id}_S = \{(a,a') \in S \multimap S \mid a' \leq a\}$ et la composition étant définie de façon relationnelle : si $s \in \mathcal{I}(S \multimap T)$ et $t \in \mathcal{I}(T \multimap U)$, la composition de s et t est

$$t \cdot s = \{(a,c) \in S \multimap U \mid \exists b \in T\ (a,b) \in s \text{ et } (b,c) \in t\}\,.$$

Si $s \in \mathbf{PoLR}(S,T)$ et $x \in \mathcal{I}(S)$, l'application de s (vue comme fonction linéaire) à x est notée $s \cdot x$. On a donc

$$s \cdot x = \mathsf{fun}(s)(x) = \{b \in T \mid \exists a \in S\ (a,b) \in S\}\,.$$

Exercice 2.4.1 Vérifier directement que Id ainsi défini est bien l'élément neutre de la composition, à gauche et à droite. Vérifier aussi que $(t \cdot s) \cdot x = t \cdot (s \cdot x)$.

On a montré à la section 2.3 que les catégories **PoL** et **PoLR** sont isomorphes.

2.4.1 Le foncteur produit tensoriel. On note 1 le préordre qui n'a qu'un élément (que l'on notera $*$). Si S_1 et S_2 sont des préordres, on définit $S_1 \otimes S_2 = S_1 \times S_2$, muni du préordre produit. Si $x_i \in \mathcal{I}(S_i)$, on pose $x_1 \otimes x_2 = x_1 \times x_2$, et il est clair que $x_1 \otimes x_2 \in S_1 \otimes S_2$.

Soient $s_i \in \mathbf{PoL}(S_i, T_i)$ pour $i = 1,2$. On définit

$$s_1 \otimes s_2 = \{((a_1,a_2),(b_1,b_2)) \mid (a_i,b_i) \in s_i \text{ pour } i = 1,2\} \subseteq (S_1 \otimes S_2) \multimap (T_1 \otimes T_2)\,.$$

Exercice* 2.4.2 Montrer que $s_1 \otimes s_2 \in \mathbf{PoLR}(S_1 \otimes S_2, T_1 \otimes T_2)$.

Proposition 2.4.1 *Soient $s_i \in \mathbf{PoLR}(S_i, T_i)$ et $t_i \in \mathbf{PoLR}(T_i, U_i)$ pour $i = 1,2$. On a*

$$(t_1 \otimes t_2) \cdot (s_1 \otimes s_2) = (t_1 \cdot s_1) \otimes (t_2 \cdot s_2)\,.$$

On a aussi $\mathsf{Id}_{S_1} \otimes \mathsf{Id}_{S_2} = \mathsf{Id}_{S_1 \otimes S_2}$. Si $x_i \in \mathcal{I}(S_i)$ (pour $i = 1,2$), on a $(s_1 \otimes s_2) \cdot (x_1 \otimes x_2) = (s_1 \cdot x_1) \otimes (s_2 \cdot x_2)$.

Démonstration. On montre la dernière équation, les deux autres sont laissées au lecteur. Soit $(b_1,b_2) \in (s_1 \otimes s_2) \cdot (x_1 \otimes x_2)$. Il existe $(a_1,a_2) \in x_1 \otimes x_2$ tel que $((a_1,a_2),(b_1,b_2)) \in s_1 \otimes s_2$. Cela signifie que $a_i \in x_i$ et $(a_i,b_i) \in s_i$ pour $i = 1,2$. On a donc $b_i \in s_i \cdot x_i$ pour $i = 1,2$, et donc $(b_1,b_2) \in (s_1 \cdot x_1) \otimes (s_2 \cdot x_2)$.

Réciproquement, si $(b_1,b_2) \in (s_1 \cdot x_1) \otimes (s_2 \cdot x_2)$, il existe $a_i \in x_i$ tel que $(a_i,b_i) \in s_i$ pour $i = 1,2$. On a $(a_1,a_2) \in x_1 \otimes x_2$ et $((a_1,a_2),(b_1,b_2)) \in s_1 \otimes s_2$. Donc $(b_1,b_2) \in (s_1 \otimes s_2) \cdot (x_1 \otimes x_2)$. □

Donc $\otimes$ est un foncteur $\mathbf{PoLR}^2 \to \mathbf{PoLR}$. On définit facilement des isomorphismes forts $\nu^G : 1 \otimes S \to S$, $\nu^D : S \otimes 1 \to S$, $\alpha : (S_1 \otimes S_2) \otimes S_3 \to S_1 \otimes (S_2 \otimes S_3)$ et $\sigma : S_1 \otimes S_2 \to S_2 \otimes S_1$, et on vérifie facilement que ces isomorphismes forts satisfont les commutations de diagrammes voulues pour faire de $(\mathbf{PoLR}, \otimes, 1, \nu^G, \nu^D, \alpha, \sigma)$ une catégorie monoïdale symétrique.

Comme tout foncteur, $\otimes$ envoie les isomorphismes sur des isomorphismes. On a mieux.

Lemme 2.4.2 *Si $S \simeq S'$ et $T \simeq T'$, alors $S \otimes T \simeq S' \otimes T'$.*

La vérification est immédiate. En toute rigueur, si $\eta : S \to S'$ et $\theta : T \to T'$ sont des isomorphismes fort, il faut vérifier que l'isomorphisme fort $S \otimes T \to S' \otimes T'$ associés (notons-le $\eta \otimes \theta$) vérifie $\widehat{\eta \otimes \theta} = \widehat{\eta} \otimes \widehat{\theta}$. Là aussi, la vérification est immédiate.

2.4.2 Propriété universelle du produit tensoriel. Soit S, T et U des préordres. Une fonction $f : \mathcal{I}(S) \times \mathcal{I}(T) \to \mathcal{I}(U)$ est dite *bilinéaire* si elle est croissante et vérifie

$$\forall A \subseteq \mathcal{I}(X)\, \forall y \in \mathcal{I}(Y) \quad f(\bigcup A, y) = \bigcup_{x \in A} f(x, y)$$

et

$$\forall x \in \mathcal{I}(X)\, \forall B \subseteq \mathcal{I}(Y) \quad f(x, \bigcup B) = \bigcup_{y \in B} f(x, y)\,.$$

Comme d'habitude, à cause de la croissance de f, ces égalités sont équivalentes à des inclusions, à savoir $f(\bigcup A, y) \subseteq \bigcup_{x \in A} f(x, y)$ et $f(x, \bigcup B) \subseteq \bigcup_{y \in B} f(x, y)$.

Soit $\tau : \mathcal{I}(S) \times \mathcal{I}(T) \to \mathcal{I}(S \otimes T)$ la fonction définie par $\tau(x, y) = x \times y = x \otimes y$.

Lemme 2.4.3 *La fonction τ est bilinéaire.*

Démonstration. On a $(a, b) \in (\bigcup A) \times y$ si et seulement s'il existe $x \in A$ tel que $(a, b) \in x \times y$. □

On peut maintenant exprimer la propriété universelle du produit tensoriel.

Proposition 2.4.4 *Soit $f : \mathcal{I}(S) \times \mathcal{I}(T) \to \mathcal{I}(U)$ une fonction bilinéaire. Il existe une et une seule fonction linéaire $g : \mathcal{I}(S \otimes T) \to \mathcal{I}(U)$ telle que $f = g \circ \tau$.*

Démonstration. On définit une notion de *trace* pour une fonction bilinéaire :

$$\mathsf{tr_b}(f) = \{((a, b), c) \in (S \times T) \times U \mid c \in f(\underset{S}{\downarrow} a, \underset{T}{\downarrow} b)\}\,.$$

Par croissance de f, on a $\mathsf{tr_b}(f) \in (S^{\mathrm{op}} \times T^{\mathrm{op}}) \times U = (S \otimes T) \multimap U$. Soit $g = \mathsf{fun}(\mathsf{tr_b}(f)) : \mathcal{I}(S \otimes T) \to \mathcal{I}(U)$, c'est une fonction linéaire.

Pour toute fonction bilinéaire $h : \mathcal{I}(S) \times \mathcal{I}(T) \to \mathcal{I}(U)$, on a

$$h(x, y) = \bigcup_{(a,b) \in x \times y} h(\underset{S}{\downarrow} a, \underset{T}{\downarrow} b)$$

car $x = \bigcup_{a \in x} \downarrow_S a$ et $y = \bigcup_{b \in y} \downarrow_T b$ pour tous $x \in \mathcal{I}(S)$ et $y \in \mathcal{I}(T)$. Donc le fonction h est connue dès qu'on connaît ses valeurs sur les éléments $(\downarrow_S a, \downarrow_T b)$ de $\mathcal{I}(S) \times \mathcal{I}(T)$.

Or $g \circ \tau$ est bilinéaire car g est linéaire. On a

$$\begin{array}{rcl}
(g \circ \tau)(\underset{S}{\downarrow} a, \underset{T}{\downarrow} b) & = & g(\underset{S}{\downarrow} a \times \underset{T}{\downarrow} b) \\
& = & g(\underset{S \otimes T}{\downarrow} (a, b)) \\
& = & \{c \mid \exists (a', b') \leq_{S \times T} (a, b) \ \ ((a', b'), c) \in \mathsf{tr_b}(f)\} \\
& = & \{c \mid \exists (a', b') \leq (a, b) \ \ c \in f(\underset{S}{\downarrow} a', \underset{T}{\downarrow} b')\} \\
& = & f(\underset{S}{\downarrow} a, \underset{T}{\downarrow} b)
\end{array}$$

donc $g \circ \tau = f$. Il reste à voir que g est caractérisée de façon unique par cette propriété. Or g est linéaire sur $S \otimes T$ et est donc caractérisée par sa valeur sur les $\downarrow_{S \otimes T} (a, b)$, et on a $g(\downarrow_{S \otimes T} (a, b)) = f(\downarrow_S a, \downarrow_T b)$ comme on vient de le voir. □

2.4.3 Clôture monoïdale. Soient S, T et U des préordres.

Soit $\mathsf{ev} \subseteq ((S \multimap T) \otimes S) \multimap T$ défini par

$$\mathsf{ev} = \{(((a', b), a), b') \mid a' \leq_S a \text{ et } b' \leq_T b\} .$$

On vérifie que $\mathsf{ev} \in \mathbf{PoLR}((S \multimap T) \otimes S, T)$. Soit donc $(((a', b), a), b') \in \mathsf{ev}$ et soit $(((a'_1, b_1), a_1), b'_1) \in ((S \multimap T) \otimes S) \multimap T$ tel que $(((a'_1, b_1), a_1), b'_1) \leq_{((S \multimap T) \otimes S) \multimap T} (((a', b), a), b')$. Cela signifie que $b'_1 \leq b'$, $a \leq a_1$, $b \leq b_1$ et $a'_1 \leq a'$. Comme $a' \leq a$ et $b' \leq b$, on a $a'_1 \leq a_1$ et $b'_1 \leq b_1$. Par suite, $(((a'_1, b_1), a_1), b'_1) \in \mathsf{ev}$, et donc $\mathsf{ev} \in \mathcal{I}(((S \multimap T) \otimes S) \multimap T) = \mathbf{PoLR}((S \multimap T) \otimes S, T)$.

Lemme 2.4.5 *Soient $s \in \mathcal{I}(S \multimap T)$ et $x \in \mathcal{I}(S)$. On a $\mathsf{ev} \cdot (s \otimes x) = s \cdot x$.*

Démonstration. Soit $b' \in \mathsf{ev} \cdot (s \otimes x)$. On peut trouver $(a', b) \in s$ et $a \in x$ tels que $a' \leq a$ et $b' \leq b$. Comme $x \in \mathcal{I}(S)$, on a $a' \in x$ et comme $s \in \mathcal{I}(S \multimap T)$, on a $(a, b') \in s$, donc $b' \in s \cdot x$. Réciproquement, si $b \in s \cdot x$, on peut trouver $a \in x$ tel que $(a, b) \in s$. On a $(((a, b), a), b) \in \mathsf{ev}$ et $((a, b), a) \in s \otimes x$. Donc $b \in \mathsf{ev} \cdot (s \otimes x)$. □

Soit $s \in \mathbf{PoLR}(U \otimes S, T)$. Soit

$$\lambda s = \{((c, (a, b)) \in U \multimap (S \multimap T) \mid ((c, a), b) \in s\} .$$

Exercice* 2.4.3 Montrer que $\lambda s \in \mathbf{PoLR}(U, S \multimap T)$, que $\mathsf{ev} \cdot (\lambda s \otimes \mathsf{Id}_S) = s$ et que λs est le seul élément de $\mathbf{PoLR}(U, S \multimap T)$ qui vérifie cette équation.

On a montré que **PoLR**, avec la structure monoïdale symétrique définie cidessus, est monoïdale fermée.

Soit $\perp = 1$ (on utilise deux noms différents pour le même objet car, en logique linéaire, il représente deux formules distinctes).

Soit S un préordre. La bijection $S \to (S \multimap \perp)$ qui envoie a sur $(a, *)$ définit un isomorphisme fort de S^{op} vers $S \multimap \perp$.

On a $\mathsf{ev} \in \mathbf{PoLR}((S \multimap \perp) \otimes S, \perp)$ et donc $\mathsf{ev} \cdot \sigma \in \mathbf{PoLR}(S \otimes (S \multimap \perp), \perp)$, et donc $\lambda\mathsf{ev} \cdot \widehat{\sigma} \in \mathbf{PoLR}(S, (S \multimap \perp) \multimap \perp)$. On a $\mathsf{ev} = \{(((a', *), a), *) \mid a' \leq_S a\}$, et donc $\lambda\mathsf{ev} \cdot \widehat{\sigma} = \{(a, ((a', *), *)) \mid a' \leq a\}$. Donc $\lambda\mathsf{ev} \cdot \widehat{\sigma} = \widehat{\eta}$ où $\eta : S \to ((S \multimap \perp) \multimap \perp)$ est l'isomorphisme fort évident.

On dit que la catégorie monoïdale **PoLR** est $\star$-*autonome*, avec $\perp$ comme objet dualisant. Le dual $S^\perp = S \multimap \perp$ sera assimilé à S^{op}. En particulier, on peut définir un cotenseur (appelé *par*), défini par $S \parr T = (S^\perp \otimes T^\perp)^\perp$; il se trouve qu'ici, on a $S \parr T = S \otimes T$ (mais on rappelle que ce n'est pas le cas dans la catégorie des espaces cohérents, par exemple).

Lemme 2.4.6 *Si $S \simeq S'$, alors $S^\perp \simeq (S')^\perp$.*

Vérification immédiate.

2.5 Structure additive

Soit $(S_i)_{i \in I}$ une famille de préordres. On définit $S = \&_{i \in I} S_i$, le *avec* des S_i, de la façon suivante : $S = \bigcup_{i \in I} \{i\} \times S_i$, avec la relation de préordre selon laquelle $(i, a) \leq (j, b)$ si $i = j$ et $a \leq_{S_i} b$. On définit également, pour chaque $i \in I$:

$$\pi_i = \{((i, a), a') \mid a' \leq_{S_i} a\} .$$

On voit facilement que $\pi_i \in \mathbf{PoLR}(S, S_i)$. Soit T un préordre et soient $s_i \in \mathbf{PoLR}(T, S_i)$. Soit

$$s = \{(b, (i, a)) \mid i \in I \text{ et } (b, a) \in s_i\} .$$

On vérifie que $s \in \mathbf{PoLR}(T, \&_{i\in I} S_i)$. Soit $i \in I$ et $(b, a) \in s_i$. Soit $(b', (j, a')) \in T \multimap \&_{k\in I} S_k$ tel que $(b', (j, a')) \leq_{T\multimap\&_{k\in I} S_k} (b, (i, a))$. Cela signifie que $b \leq_T b'$, $i = j$ et $a' \leq_{S_i} a$, et donc $(b', a') \in s_i$. Par suite, on a bien $(b', (j, a')) \in s$ et donc $s \in \mathbf{PoLR}(T, \&_{i\in I} S_i)$. De plus, on vérifie facilement que $\pi_i \cdot s = s_i$ pour tout $i \in I$. On note $s = \langle s_i\rangle_{i\in I}$.

Soit maintenant $s \in \mathbf{PoLR}(T, \&_{i\in I} S_i)$ tel qu'on ait $\pi_i \cdot s = s_i$ pour tout $i \in I$. Soit $(b, (i, a)) \in T \multimap \&_{k\in I} S_k$ tel que $(b, (i, a)) \in s$. Comme $((i, a), a) \in \pi_i$, on a $(a, b) \in \pi_i \cdot s = s_i$. Cela montre que $s \subseteq \langle s_i\rangle_{i\in I}$. Réciproquement, soit $i \in I$ et soit $(b, a) \in s_i$. Comme $s_i = \pi_i\cdot s$, il existe $a' \in S_i$ tel que $((i, a'), a) \in \pi_i$ et $(b, (i, a')) \in s$. On a donc $a \leq a'$, et par suite $(b, (i, a)) \in s$, ce qui montre que $\langle s_i\rangle_{i\in I} \subseteq s$.

On a donc montré que $\&_{i\in I} S_i$, avec les projections π_i, est le produit cartésien de la famille $(S_i)_{i\in I}$. Dans le cas particulier où $I = \emptyset$, le produit cartésien est l'objet terminal de **PoLR**, qui est le préordre $\emptyset$, que l'on note $\top$.

Lemme 2.5.1 *Si $S_i \simeq S'_i$ pour tout $i \in I$, alors $\&_{i\in I} S_i \simeq \&_{i\in I} S'_i$*

Vérification immédiate.

2.5.1 Foncteur produit cartésien. Si S est un préordre, on note S^I le produit cartésien $\&_{i\in I} S_i$ dans lequel $S_i = S$ pour chaque $i \in I$. Autrement dit, $S^I = I \times S$, en mettant sur I le préordre *discret* ($i \leq j$ iff $i = j$). Cette opération est fonctorielle : si $s \in \mathbf{PoLR}(S, T)$, alors $s^I = \langle s\cdot\pi_i\rangle_{i\in I} \in \mathbf{PoLR}(S^I, T^I)$ est donné par

$$s^I = \{((i, a), (i, b)) \mid i \in I \text{ et } (a, b) \in S\} .$$

2.5.2 Coproduit On a aussi un coproduit, défini par $\bigoplus_{i\in I} S_i = \left(\&_{i\in I} {S_i}^{\perp}\right)^{\perp}$. On voit facilement que $\bigoplus_{i\in I} S_i = \&_{i\in I} S_i$.

2.6 Exponentielles

On définit $!S = \mathcal{P}_{\mathrm{fin}}(S)$, l'ensemble des parties finies de S. On munit cet ensemble du préordre suivant : si $u, u' \in !S$, on dira que $u \leq u'$ si, pour tout $a \in u$, il existe $a' \in u'$ tel que $a \leq a'$. Observer que cette relation est transitive et réflexive (c'est un préordre), et qu'elle n'est pas antisymétrique en général, même quand $\leq_S$ l'est. Observer aussi que $u \leq_{!S} u'$ si et seulement si $\downarrow u \subseteq \downarrow u'$.

Exercice* 2.6.1 Trouver un ensemble partiellement ordonné S tel que $!S$ ne soit pas un ordre partiel.

Le treillis complet $\mathcal{I}(S)$ est en particulier un cpo.

Lemme 2.6.1 *Un élément x_0 de $\mathcal{I}(S)$ est isolé si et seulement si $x_0 = \downarrow u$ où $u \in !S$.*

Démonstration. Soit $x_0 \in \mathcal{I}(S)$ isolé. Soit $D = \{\downarrow u \mid u \in \mathcal{P}_{\mathrm{fin}}(x_0)\}$. L'ensemble D est filtrant et on a $x_0 = \bigcup D$. Comme x_0 est isolé, il existe $u \in \mathcal{P}_{\mathrm{fin}}(x_0)$ tel que $x_0 \subseteq \downarrow u$, et donc $x_0 = \downarrow u$ (puisque $u \subseteq x_0$).

Réciproquement, soit $x_0 = \downarrow u$ avec $u \in !S$. Soit D une partie filtrante de $\mathcal{I}(S)$ et supposons que $x_0 \subseteq \bigcup D$. Comme $u \subseteq \bigcup D$ et comme D est filtrant, il existe $x \in D$ tel que $u \subseteq x$. Mais comme $x \in \mathcal{I}(S)$, on a aussi $x_0 \subseteq x$, ce qui prove que x_0 est isolé. $\square$

2.6.1 Trace d'une fonction continue. Soit $f : \mathcal{I}(S) \to \mathcal{I}(T)$ une fonction Scott-continue. Cela signifie que f est croissante et commute aux unions des familles filtrantes. Autrement dit, pour toute partie filtrante D de $\mathcal{I}(S)$, on a $f(\bigcup D) \subseteq \bigcup f(D)$ (l'autre inclusion résulte simplement du fait que f est croissante).

On définit
$$\mathsf{Tr}(f) = \{(u, b) \in {!S} \times T \mid b \in f(\downarrow u)\} .$$

On voit facilement que $\mathsf{Tr}(f) \in \mathcal{I}({!S} \multimap T)$. Réciproquement, soit $t \in \mathcal{I}({!S} \multimap T)$. On définit une fonction

$$\begin{array}{rcl} \mathsf{Fun}(t) : \mathcal{I}(S) & \to & \mathcal{P}(T) \\ x & \mapsto & \{b \mid \exists u \subseteq x \ (u, b) \in t\} \end{array}$$

On vérifie facilement que $\mathsf{Fun}(t)$ prend ses valeurs dans $\mathcal{I}(T)$ et est croissante. On montre que $f = \mathsf{Fun}(t)$ est continue. Soit donc $D \subseteq \mathcal{I}(S)$ un ensemble filtrant, il faut montrer que $f(\bigcup D) \subseteq \bigcup f(D)$. Soit $b \in f(\bigcup D)$, il existe $u \in {!S}$ tel que $u \subseteq \bigcup D$ et $(u, b) \in t$. Comme u est fini et D filtrant, il existe $x \in D$ tel que $u \subseteq x$. Donc $b \in f(x) \subseteq \bigcup f(D)$ (vu que $x \in D$).

Soit **PoC** la catégorie dont les objets sont les préordres, et telle que $\mathbf{PoC}(S, T)$ soit l'ensemble des fonctions continues de $\mathcal{I}(S)$ vers $\mathcal{I}(T)$. On munit cet ensemble de morphismes de l'ordre ponctuel déjà vu : $f \leq g$ si et seulement si $f(x) \subseteq g(x)$ pour tout $x \in \mathcal{I}(S)$.

Exercice* 2.6.2 Montrer que $\mathbf{PoL}(S, T) \subseteq \mathbf{PoC}(S, T)$, et que cette inclusion est stricte en général (donner un contre-exemple).

Proposition 2.6.2 *Les fonctions* Tr *et* Fun *définissent un isomorphisme d'ordre entre* $\mathbf{PoC}(S, T)$ *et* $\mathcal{I}({!S} \multimap T)$.

Démonstration. Soit $f \in \mathbf{PoC}(S, T)$ et montrons que $\mathsf{Fun}(\mathsf{Tr}(f)) = f$. Soit donc $x \in \mathcal{I}(S)$, on montre que $\mathsf{Fun}(\mathsf{Tr}(f))(x) = f(x)$. Soit $b \in T$. Supposons d'abord que $b \in f(x)$. Soit $D = \{\downarrow u \mid u \in \mathcal{P}_{\mathrm{fin}}(x)\}$. On a $\bigcup D = x$, et D est filtrant. Donc $f(x) = f(\bigcup D) \subseteq \bigcup f(D)$, et par suite il existe $u \in \mathcal{P}_{\mathrm{fin}}(x)$ tel que $b \in f(\downarrow u)$, c'est-à-dire $(u, b) \in \mathsf{Tr}(f)$. Comme $u \subseteq x$, on a $b \in \mathsf{Fun}(\mathsf{Tr}(x))$. Supposons maintenant que $b \in \mathsf{Fun}(\mathsf{Tr}(f))(x)$. Soit donc $u \in {!S}$ tel que $(u, b) \in \mathsf{Tr}(f)$ et $u \subseteq x$. On a $b \in f(\downarrow u)$, et comme $\downarrow u \subseteq x$ et comme f est croissante, on a $b \in f(x)$.

Soit $t \in \mathcal{I}({!S} \multimap T)$. On montre que $t = \mathsf{Tr}(\mathsf{Fun}(t))$. Soient $u \in {!S}$ et $b \in T$. On suppose d'abord $(u, b) \in t$. On a $b \in \mathsf{Fun}(t)(\downarrow u)$, puisque $u \subseteq \downarrow u$, et donc $(u, b) \in \mathsf{Tr}(\mathsf{Fun}(t))$. Réciproquement, supposons $(u, b) \in \mathsf{Tr}(\mathsf{Fun}(t))$. Cela signifie que $b \in \mathsf{Fun}(t)(\downarrow u)$, et donc il existe $u' \in {!S}$ tel que $u' \subseteq \downarrow u$ et $(u', b) \in t$. On a $u' \leq_{!S} u$ et donc $(u, b) \in t$ puisque $t \in \mathcal{I}({!S} \multimap T)$.

On montre ensuite que Tr est croissante. Soient donc $f, f' \in \mathbf{PoC}(S, T)$ telles que $f \leq f'$ et soit $(u, b) \in \mathsf{Tr}(f)$. C'est que $b \in f(\downarrow u)$, or $f(\downarrow u) \subseteq f'(\downarrow u)$ et donc $(u, b) \in \mathsf{Tr}(f')$, ce qui montre que $\mathsf{Tr}(f) \subseteq \mathsf{Tr}(f')$.

Soient $t, t' \in \mathbf{PoC}(S, T)$ tels que $t \subseteq t'$ et soit $x \in \mathcal{I}(S)$. Soit $b \in \mathsf{Fun}(t)(x)$. Soit u tel que $(u, b) \in t$ et $u \subseteq x$. Comme $t \subseteq t'$, on a $(u, b) \in t'$ et donc $b \in \mathsf{Fun}(t')(x)$, ce qui montre que $\mathsf{Fun}(t) \leq \mathsf{Fun}(t')$. $\square$

2.6.2 L'exponentielle comme foncteur. Si $x \in \mathcal{I}(S)$, on définit $x^! \in \mathcal{I}({!S})$ en posant $x^! = \mathcal{P}_{\mathrm{fin}}(x)$. Il faut remarquer qu'on a bien $x^! \in \mathcal{I}({!S})$. Soit en effet $u \in x^!$ et $u' \in {!S}$ tel que $u' \subseteq_{!S} u$. Soit $a' \in u'$, il existe $a \in u$ tel que $a' \leq_S a$, or $a \in x$ et donc $a' \in x$ puisque $x \in \mathcal{I}(S)$. Il en résulte que $u' \subseteq x$ et donc que $u' \in x^!$.

Lemme 2.6.3 *Soit* $t \in \mathbf{PoL}({!S}, T)$. *On a* $\mathsf{Fun}(t)(x) = t \cdot x^!$.

Démonstration. Soit $b \in \mathsf{Fun}(t)(x)$. Soit $u \in {!S}$ tel que $u \subseteq x$ et $(u,b) \in t$. On a $u \in x^!$ et donc $b \in t \cdot x^!$. Réciproquement, soit $b \in t \cdot x^!$. Soit $u \in x^!$ tel que $(u,b) \in t$. On a $u \subseteq x$ et donc $b \in \mathsf{Fun}(t)(x)$. □

Ce lemme très simple est important car il a la conséquence suivante.

Lemme 2.6.4 *Soient $t, t' \in \mathbf{PoL}(!S, T)$. Si on a $t \cdot x^! = t' \cdot x^!$ pour tout $x \in \mathcal{I}(S)$, alors $t = t'$.*

Démonstration. En effet, on a alors $\mathsf{Fun}(t) = \mathsf{Fun}(t')$, et donc $t = t'$ par la proposition 2.6.2. □

Soit $t \in \mathbf{PoL}(S, T)$. Soit

$$!t = \{(u, v) \in {!S} \times {!T} \mid \forall b \in v\, \exists a \in u\ (a, b) \in t\}\,.$$

Lemme 2.6.5 *Si $t \in \mathbf{PoL}(S, T)$, alors $!t \in \mathbf{PoL}(!S, !T)$.*

Démonstration. Soit $(u, v) \in {!t}$ est soit $(u', v') \in {!S} \times {!T}$ tel que $(u', v') \leq_{!S \multimap !T} (u, v)$, il faut voir que $(u', v') \in {!t}$. Soit $b' \in v'$. Comme $v' \leq_{!T} v$, il existe $b \in v$ tel que $b' \leq_T b$. Comme $(u, v) \in {!t}$, il existe $a \in u$ tel que $(a, b) \in t$. Comme $u \leq_{!S} u'$, il existe $a' \in u'$ tel que $a \leq_S a'$. On a $(a', b') \leq_{S \multimap T} (a, b)$, et donc $(a', b') \in t$ puisque $t \in \mathcal{I}(S \multimap T)$. Puisque $a' \in u'$, on a montré que $(u', v') \in {!t}$, et donc $!t \in \mathbf{PoL}(!S, !T)$. □

Lemme 2.6.6 *Si $t \in \mathbf{PoL}(S, T)$ et $x \in \mathcal{I}(S)$, alors $!t \cdot x^! = (t \cdot x)^!$.*

Démonstration. Soit $v \in {!t} \cdot x^!$, montrons que $v \in (t \cdot x)^!$. Il existe $u \in x^!$ tel que $(u, v) \in {!t}$. Soit $b \in v$, il existe $a \in u$ tel que $(a, b) \in t$. Comme $u \subseteq x$, on a $a \in x$ et donc $b \in t \cdot x$, et donc $v \in (t \cdot x)^!$. Réciproquement, soit $v \in (t \cdot x)^!$, c'est-à-dire que $v \in {!S}$ et $v \subseteq t \cdot x$. Pour chaque $b \in v$, on choisit $a_b \in x$ tel que $(a_b, b) \in t$. Soit $u \in {!S}$ qui contient tous les a_b (pour $b \in v$). On a $(u, v) \in {!t}$ et $u \in x^!$ et donc $v \in {!t} \cdot x^!$. □

Proposition 2.6.7 *L'opération $t \mapsto {!t}$ est fonctorielle. Autrement dit, $!\mathsf{Id}_S = \mathsf{Id}_{!S}$ et, si $s \in \mathbf{PoL}(S, T)$ et $t \in \mathbf{PoL}(T, U)$, on a $!(t \cdot s) = {!t} \cdot {!s}$.*

Démonstration. Soit $x \in \mathcal{I}(S)$. On a $!\mathsf{Id}_S \cdot x^! = x^!$ par le lemme 2.6.6, donc $!\mathsf{Id}_S = \mathsf{Id}_{!S}$ par le lemme 2.6.4. Et on a $!(t \cdot s) \cdot x^! = ((t \cdot s) \cdot x)^!$ par le lemme 2.6.6, donc $!(t \cdot s) \cdot x^! = (t \cdot (s \cdot x))^! = {!t} \cdot (s \cdot x)^! = ({!t} \cdot {!s}) \cdot x^!$ en appliquant deux fois le lemme 2.6.6, et on conclut grâce au lemme 2.6.4. □

Lemme 2.6.8 *Si $S \simeq S'$, alors $!S \simeq {!S'}$.*

La vérification est immédiate.

2.6.3 Structure de comonade de l'exponentielle. Soit $\mathsf{d}_S \subseteq {!S} \multimap S$ donné par

$$\mathsf{d}_S = \{(u, a) \mid \exists a' \in u\ a \leq a'\}\,.$$

Lemme 2.6.9 *On a $\mathsf{d}_S \in \mathbf{PoL}(!S, S)$ et, pour tout $x \in \mathcal{I}(S)$, on a $\mathsf{d}_S \cdot x^! = x$. De plus d_S est naturel en S ; autrement dit, si $s \in \mathbf{PoL}(S, T)$, on a $\mathsf{d}_T \cdot {!s} = s \cdot \mathsf{d}_S$.*

Démonstration. Soit $(u, a) \in \mathsf{d}_S$ et soit $(u', a') \in !S \multimap S$ tel que $(u', a') \leq_{!S \multimap S} (u, a)$. Soit $a'' \in u$ tel que $a \leq a''$. Comme $u \leq_{!S} u'$, il existe $a''' \in u'$ tel que $a'' \leq a'''$. Comme $a' \leq a$, on a $a' \leq a''' \in u'$, ce qui montre que $(u', a') \in \mathsf{d}_S$, et donc $\mathsf{d}_S \in \mathbf{PoL}(!S, S)$.

Soit $x \in \mathcal{I}(S)$. Soit $a \in x$. On a $(\{a\}, a) \in \mathsf{d}_S$, donc $a \in \mathsf{d}_S \cdot x^!$ puisque $\{a\} \in x^!$. Si $a \in \mathsf{d}_S \cdot x^!$, soit $u \in x^!$ tel que $(u, a) \in \mathsf{d}_S$. Soit $a' \in u$ tel que $a \leq a'$. Comme $a' \in u \subseteq x$ et comme $x \in \mathcal{I}(S)$, on a $a \in x$. Donc $\mathsf{d}_S \cdot x^! = x$.

La naturalité en résulte : on a $(\mathsf{d}_T \cdot !s) \cdot x^! = \mathsf{d}_T \cdot (s \cdot x)^! = s \cdot x = (s \cdot \mathsf{d}_S) \cdot x^!$. On conclut par le lemme 2.6.4. □

On définit ensuite $\mathsf{p}_S \subseteq !S \multimap !!S$ par

$$\mathsf{p}_S = \{(u, A) \mid \bigcup A \leq_{!S} u\}\,.$$

Lemme 2.6.10 *On a $\mathsf{p}_S \in \mathbf{PoL}(!S, !!S)$ et, pour tout $x \in \mathcal{I}(S)$, on a $\mathsf{p}_S \cdot x^! = x^{!!}$. De plus, p_S est naturel en S ; autrement dit, si $s \in \mathbf{PoL}(S, T)$, on a $\mathsf{p}_T \cdot !s = !!s \cdot \mathsf{p}_S$.*

Démonstration. Soit $(u, A) \in \mathsf{p}_S$ et soit $(u', A') \in !S \multimap !!S$ tel que $(u', A') \leq_{!S \multimap !!S} (u, A)$, on doit montrer que $\bigcup A' \leq_{!S} u'$. Soit $a' \in \bigcup A'$. Soit $u' \in A'$ tel que $a' \in u'$. Comme $A' \leq_{!!S} A$, on peut trouver $u'' \in A$ tel que $u' \leq_{!S} u''$. Comme $a' \in u'$, il existe $a \in u''$ tel que $a' \leq a$. Or $u'' \subseteq \bigcup A \leq_{!S} u$, donc $u'' \leq_{!S} u$. Or $u \leq_{!S} u'$, donc on peut trouver $a''' \in u'$ tel que $a' \leq a'''$. On a montré que $\bigcup A' \leq_{!S} u'$, ce qui montre que $(u', A') \in \mathsf{p}_S$, et donc que $\mathsf{p}_S \in \mathbf{PoL}(!S, !!S)$.

Soit $x \in \mathcal{I}(S)$. On montre que $\mathsf{p}_S \cdot x^! = x^{!!}$. Soit donc $A \in !!S$. On suppose d'abord que $A \in \mathsf{p}_S \cdot x^!$. Comme $x^! \in \mathcal{I}(!S)$, on a $\bigcup A \in x^!$, et donc $A \subseteq x^!$, c'est-à-dire que $A \in x^{!!}$. Réciproquement, supposons que $A \in x^{!!}$. Cela signifie que $A \subseteq x^!$. Soit $u = \bigcup A$, on a $u \in x^!$ et $(u, A) \in \mathsf{p}_S$, donc $A \in \mathsf{p}_S \cdot x^!$.

La naturalité découle de ce qui précède et du lemme 2.6.4. □

Proposition 2.6.11 *Le foncteur $!\_$, équippé des transformations naturelles d et p, est une comonade.*

Démonstration. Il s'agit de prouver les trois équations suivantes :

$$\begin{aligned} \mathsf{d}_{!S} \cdot \mathsf{p}_S &= \mathsf{Id}_{!S} \\ !\mathsf{d}_S \cdot \mathsf{p}_S &= \mathsf{Id}_{!S} \\ \mathsf{p}_{!S} \cdot \mathsf{p}_S &= !\mathsf{p}_S \cdot \mathsf{p}_S \end{aligned}$$

La vérification de ces équations est immédiate, en utilisant les lemmes 2.6.9, 2.6.10 et 2.6.4. □

2.6.4 Isomorphisme fondamental. Soient S et T des préordres. On observe qu'un élément w de $!(S \mathbin{\&} T)$ s'écrit de façon unique sous la forme $w = (\{1\} \times u) \cup (\{2\} \times v)$, avec $u \in !S$ et $v \in !T$ (identifie le produit cartésien $S \mathbin{\&} T$ avec le produit de la famille $(S_i)_{i \in \{1,2\}}$, dans laquelle $S_1 = S$ et $S_2 = T$). Cela définit une bijection $\theta : !(S \mathbin{\&} T) \to !S \otimes !T$.

Exercice* 2.6.3 Montrer que θ est un isomorphisme fort de $!(S \mathbin{\&} T)$ vers $!S \otimes !T$.

2.6.5 Catégorie de Kleisli. C'est la "catégorie des coalgèbres libres" de la comonade $(!\_, \mathsf{d}, \mathsf{p})$. On la notera $\mathbf{PoLR}_{\mathsf{K}}$ et elle est définie comme suit.

Ses objets sont ceux de $\mathbf{PoLR}$, et $\mathbf{PoLR}_{\mathsf{K}}(S, T) = \mathbf{PoLR}(!S, T)$. L'identité est $\mathrm{Id}^{\mathsf{K}} = \mathsf{d}_S \in \mathbf{PoLR}(!S, S)$. Etant donnés $s \in \mathbf{PoLR}(!S, T)$ et $t \in \mathbf{PoLR}(!T, U)$, la composition $t \circ^{\mathsf{K}} s$ est définie par

$$t \circ^{\mathsf{K}} s = t \cdot !s \cdot \mathsf{p}_s\,.$$

Exercice 2.6.4 En utilsant les équations de comonade, montrer qu'on a bien défini ainsi une catégorie.

Lemme 2.6.12 *On a* $\mathsf{Fun}\,(\mathrm{Id}^{\mathsf{K}}) = \mathit{Id}$ *et* $\mathsf{Fun}\,(t \circ^{\mathsf{K}} s) = \mathsf{Fun}(t) \circ \mathsf{Fun}(s)$*, autrement dit, la correspondance qui envoie l'objet* S *de* $\mathbf{PoLR}_{\mathsf{K}}$ *sur le même objet* S *de* $\mathbf{PoC}$ *et le morphisme* $s \in \mathbf{PoLR}_{\mathsf{K}}(S,T)$ *sur le morphisme* $\mathsf{Fun}(s) \in \mathbf{PoC}(S,T)$ *est un foncteur de* $\mathbf{PoLR}_{\mathsf{K}}$ *vers* $\mathbf{PoC}$*, que l'on note encore* Fun*. Réciproquement, si* $f \in \mathbf{PoC}(S,T)$ *et* $g \in \mathbf{PoC}(T,U)$*, on a* $\mathsf{Tr}(g \circ f) = \mathsf{Tr}(g) \circ^{\mathsf{K}} \mathsf{Tr}(f)$ *et* $\mathsf{Tr}(\mathit{Id}) = \mathrm{Id}^{\mathsf{K}}$*, c'est-à-dire que* Tr *définit un foncteur de la catégorie* $\mathbf{PoC}$ *vers la catégorie* $\mathbf{PoLR}_{\mathsf{K}}$ *(qui est l'identité sur les objets). Ces foncteurs sont inverses l'un de l'autre et définissent donc un isomorphisme entre les catégories* $\mathbf{PoLR}_{\mathsf{K}}$ *et* $\mathbf{PoC}$*.*

Exercice* 2.6.5 Vérifier la fonctorialité des opérations Fun et Tr.

Lemme 2.6.13 *La catégorie* $\mathbf{PoLR}_{\mathsf{K}}$ *est cartésienne. Le produit cartésien de la famille* $(S_i)_{i\in I}$ *est* $S = \&_{i\in I} S_i$*. La i-ème projection est* $\pi_i^{\mathsf{K}} = \pi_i \cdot \mathsf{d}_S \in \mathbf{PoLR}_{\mathsf{K}}(S, S_i)$*.*

Démonstration. Si $t_i \in \mathbf{PoLR}_{\mathsf{K}}(T, S_i)$ pour $i \in I$, alors $t = \langle t_i \rangle_{i\in I} \in \mathbf{PoLR}_{\mathsf{K}}(T,S)$ et vérifie $\pi_i^{\mathsf{K}} \circ^{\mathsf{K}} t = t_i$, et est caractérisé par cette propriété, comme on le voit facilement. □

Remarque 2.6.14 Observer que $\mathcal{I}(\&_{i\in I} S_i) \simeq \prod_{i\in I} \mathcal{I}(S_i)$. Modulo cet isomorphisme d'ordre, on a $\pi_i^{\mathsf{K}} \cdot (x_j)_{j\in I} = x_i$, et si les $f_i : \mathcal{I}(T) \to \mathcal{I}(S_i)$ sont des fonctions continues, la fonction continue associée $f : \mathcal{I}(T) \to \prod_{i\in I} \mathcal{I}(S_i)$ est donnée par $f(x) = (f_i(x))_{i\in I}$.

Proposition 2.6.15 *La catégorie* $\mathbf{PoLR}_{\mathsf{K}}$ *est cartésienne fermée. L'objet des morphismes de* S *vers* T *dans* $\mathbf{PoLR}_{\mathsf{K}}$ *est* $S \Rightarrow T = {!S} \multimap T$*. Le morphisme d'évaluation* $\mathit{Ev} \in \mathbf{PoLR}_{\mathsf{K}}((S \Rightarrow T) \,\&\, S, T)$ *est*

$$\mathit{Ev} = \mathit{ev} \cdot (\mathit{d}_{S\Rightarrow T} \otimes \mathit{Id}_{!S}) \cdot \widehat{\theta} \tag{2.1}$$

où $\theta : {!((S \Rightarrow T) \,\&\, S)} \to {!(S \Rightarrow T)} \otimes {!S}$ *est l'isomorphisme fondamental (on rappelle que* $\widehat{\theta} \in \mathbf{PoL}({!((S \Rightarrow T) \,\&\, S)}, {!(S \Rightarrow T)} \otimes {!S})$ *est l'isomorphisme, dans* $\mathbf{PoL}$*, associé à l'isomorphisme fort* θ*, voir le paragraphe 2.3.4). De plus, modulo cet isomorphisme, on a*

$$\mathit{Ev} = \{((w,u),b) \in ({!(S \Rightarrow T)} \otimes {!S}) \multimap T \mid \exists (u',b') \in w \quad (u,b) \leq_{S\Rightarrow T} (u',b')\} \tag{2.2}$$

Démonstration. Soit Ev le morphisme de $\mathbf{PoLR}_{\mathsf{K}}$ défini par (2.1). Soit $z = (s,x) \in \mathcal{I}((S \Rightarrow T) \,\&\, S)$ (on identifie $\mathcal{I}((S \Rightarrow T) \,\&\, S)$ et $\mathcal{I}(S \Rightarrow T) \times \mathcal{I}(S)$, voir remarque 2.6.14). Alors $\widehat{\theta} \cdot z^! = s^! \otimes x^!$, et donc $(\mathsf{d}_{S\Rightarrow T} \otimes \mathsf{Id}_{!S}) \cdot \widehat{\theta} \cdot z^! = s \otimes x^!$ par la proposition 2.4.1 et le lemme 2.6.9, par suite $\mathsf{Ev} \cdot z^! = s \cdot x^!$ par le lemme 2.4.5, et finalement

$$\mathsf{Fun}(\mathsf{Ev})(z) = \mathsf{Fun}(s)(x)$$

par le lemme 2.6.3, et cette propriété catactérise Ev, puisque Fun est une bijection. L'équation (2.2) résulte de cette propriété, car $\mathsf{Ev} = \mathsf{Tr}(\mathsf{Fun}(\mathsf{Ev}))$, donc (toujours modulo l'isomorphisme θ), on a $((w,u),b) \in \mathsf{Ev}$ ssi $b \in \mathsf{Fun}(\downarrow_{S\Rightarrow T} w)(\downarrow_S u)$, ce qui est vrai ss'il existe u'' tel que $u'' \leq_{!S} u$ et $(u'',b) \in \downarrow_{S\Rightarrow T} w$, ce qui est équivalent à dire qu'il existe u' tel que $u' \leq_{!S} u''$ et b' tel que $b \leq_S b'$, et $(u',b') \in w$.

On en déduit la clôture cartésienne. Soit U un préordre, et soit $t \in \mathbf{PoLR}_{\mathsf{K}}(U \,\&\, S, T)$. Soit $\Lambda t \subseteq {!U} \multimap (S \Rightarrow T)$ donné par

$$\Lambda t = \{(w,(u,b)) \mid ((w,u),b) \in t\}$$

où on utilise implicitement l'isomorphisme fort θ.

On vérifie d'abord que $\Lambda t \in \mathbf{PoLR}_{\mathsf{K}}(U, S \Rightarrow T) = \mathcal{I}(U \Rightarrow (S \Rightarrow T))$; c'est une conséquene immédiate du fait que $t \in \mathcal{I}((U \,\&\, S) \Rightarrow T)$. On a donc $\mathsf{Fun}(\Lambda t) \in \mathbf{PoC}(U, S \Rightarrow T)$. Cette fonction continue associe à $z \in \mathcal{I}(U)$ l'élément $s \in \mathcal{I}(S \Rightarrow T)$ qui est caractérisé par $\mathsf{Fun}(s)(x) = \mathsf{Fun}(t)(z, x)$ (en identifiant $\mathcal{I}(U \,\&\, S)$ et $\mathcal{I}(U) \times \mathcal{I}(S)$, conformément à la remarque 2.6.14). En effet, on a

$$
\begin{aligned}
\mathsf{Fun}(\mathsf{Fun}(\Lambda t)(z))(x) &= \mathsf{Fun}(\{(u, b) \mid \exists w \subseteq z \quad (w, (u, b)) \in \Lambda t\})(x) \\
&= \{b \mid \exists w \subseteq z, \exists u \subseteq x \quad (z, (u, b)) \in \Lambda t\} \\
&= \{b \mid \exists w \subseteq z, \exists u \subseteq x \quad ((z, u), b) \in t\} \,.
\end{aligned}
$$

Il résulte de cela que

$$\mathsf{Ev} \circ^{\mathsf{K}} (\Lambda t \,\&\, \mathrm{Id}_S^{\mathsf{K}}) = t \,. \tag{2.3}$$

Pour conclure que $\mathbf{PoLR}_{\mathsf{K}}$ est cartésienne fermée, il faut montrer que Λt est caractérisé par cette propriété. Un autre façon de prouver la clôture cartésienne est de prouver les équations suivantes, en plus de (2.3) :

$$\Lambda(\mathsf{Ev}) = \mathrm{Id}_{S \Rightarrow T}^{\mathsf{K}} \tag{2.4}$$

$$\Lambda t \circ^{\mathsf{K}} s = \Lambda(t \circ^{\mathsf{K}} (s \,\&\, \mathrm{Id}_S^{\mathsf{K}})) \tag{2.5}$$

où $s \in \mathbf{PoLR}_{\mathsf{K}}(V, U)$. La preuve de (2.4) est immédiate à partir de (2.2). □

Exercice* **2.6.6** Prouver l'équation (2.5).

2.7 Deux modèles du lambda-calcul pur

2.7.1 Ordre sur les préordres. Etant donnés deux préordres S et T, on écrira que $S \sqsubseteq T$ si $S \subseteq T$, et, pour $a, a' \in S$, on a $a \leq_S a'$ ssi $a \leq_T a'$. Autrement dit, $S \subseteq T$ comme ensembles, et la restriction du préordre T à S coïncide avec le préordre S.

On définit alors $\mathsf{inj}^+ \in \mathbf{PoL}(S, T)$ et $\mathsf{inj}^- \in \mathbf{PoL}(S, T)$ (on mettra parfois des indices pour préciser les objets concernés, quand ce sera utile, par exemple $\mathsf{inj}^+_{S,T}$ et $\mathsf{inj}^-_{S,T}$ pour les deux morphismes que nous sommes en train de définir) comme

$$
\begin{aligned}
\mathsf{inj}^+ &= \{(a, b) \in S \times T \mid b \leq_T a\} \\
\mathsf{inj}^- &= \{(b, a) \in T \times S \mid a \leq_T b\}
\end{aligned}
$$

Exercice* **2.7.1** Montrer que $\mathsf{inj}^- \cdot \mathsf{inj}^+ = \mathsf{Id}_S$ et que $\mathsf{inj}^+ \cdot \mathsf{inj}^- \leq \mathsf{Id}_T$.

Soit Γ un ensemble filtrant (c'est-à-dire un ensemble partiellement ordonné tel que, pour tous $\gamma, \gamma' \in \Gamma$, il existe $\delta \in \Gamma$ tel que $\gamma, \gamma' \leq \delta$). Soit $(S_\gamma)_{\gamma \in \Gamma}$ une famille croissante de préordres, autrement dit : $\gamma \leq \delta \Rightarrow S_\gamma \sqsubseteq T_\delta$. On dit que $(S_\gamma)_{\gamma \in \Gamma}$ est une *famille filtrante de préordres*.

On construit le préordre $\bigsqcup_{\gamma \in \Gamma} S_\gamma$ comme $\bigcup_{\gamma \in \Gamma} S_\gamma$ muni de la relation de préordre suivante : si $a, a' \in S = \bigsqcup_{\gamma \in \Gamma} S_\gamma$, on dira que $a \leq_S a'$ s'il existe $\gamma \in \Gamma$ tel que $a, a' \in S_\gamma$ et $a \leq_{S_\gamma} a'$. Il faut remarquer les points suivants :

- Si $a, a' \in S$, il existe $\delta \in \Gamma$ tel que $a, a' \in S_\delta$. En effet, il existe $\gamma, \gamma' \in \Gamma$ tels que $a \in S_\gamma$ et $a' \in S_{\gamma'}$. Il suffit de prendre $\delta \in \Gamma$ tel que $\gamma, \gamma' \leq \delta$.
- Si $a, a' \in S$ sont tels que $a \leq_S a'$, alors on a $a \leq_{S_{\gamma'}} a'$ pour tout $\gamma' \in \Gamma$ tel que $a, a' \in S_{\gamma'}$. Soit en effet $\gamma \in \Gamma$ tel que $a \leq_{S_\gamma} a'$. Soit $\delta \in \Gamma$ tel que $\gamma, \gamma' \leq \delta$. Comme $S_\gamma \sqsubseteq S_\delta$, on a $a \leq_{S_\delta} a'$, et comme $S'_\gamma \sqsubseteq S_\delta$, on a $a \leq_{S_{\gamma'}} a'$.

Soit **PoLI** la catégorie dont les objets sont les préordres, et dans laquelle on a un morphisme de S vers T si et seulement si $S \sqsubseteq T$. Il s'agit d'une classe (ce n'est pas un ensemble au sens de la théorie des ensembles, mais peu importe pour nous) partiellement ordonnée. Dans cette classe partiellement ordonnée, $\bigsqcup_{\gamma\in\Gamma} S_\gamma$ est le sup des S_γ.

Soit $n \in \mathbb{N}$, on décrit explicitement la classe partiellement ordonnée $\mathbf{PoLI}^n$ (produit n-aire de **PoLI** avec lui-même). Si $\vec{S} = (S_1, \dots, S_n)$ et $\vec{T} = (T_1, \dots, T_n)$, on a $\vec{S} \sqsubseteq \vec{T}$ si $S_i \sqsubseteq T_i$ pour chaque $i = 1, \dots, n$. Si $(\vec{S_\gamma})_{\gamma\in\Gamma}$ est une famille filtrante de tels n-uples, on définit $\vec{S} = \bigsqcup_{\gamma\in\Gamma} \vec{S_\gamma}$ de même, composante par composante : $S_i = \bigsqcup_{\gamma\in\Gamma} S_{\gamma,i}$. C'est le sup des $\vec{S_\gamma}$ dans la classe partiellement ordonnée produit $\mathbf{PoLI}^n$.

2.7.2 Objets variables. Un *objet variable* est une correspondance fonctionnelle $\Phi : \mathbf{PoLI}^n \to \mathbf{PoLI}$ qui vérifie

- $\vec{S} \sqsubseteq \vec{T} \Rightarrow \Phi(\vec{S}) \sqsubseteq \Phi(\vec{T})$ (on dit que Φ est croissant)
- et, si $(\vec{S_\gamma})_{\gamma\in\Gamma}$ est une famille filtrante dans **PoLI**, on a

$$\Phi(\bigsqcup_{\gamma\in\Gamma} S_\gamma) = \bigsqcup_{\gamma\in\Gamma} \Phi(S_\gamma)\,. \tag{2.6}$$

A cause de la croissance de Φ, la condition (2.6) se réduit comme d'habitude à $\Phi(\bigsqcup_{\gamma\in\Gamma} S_\gamma) \sqsubseteq \bigsqcup_{\gamma\in\Gamma} \Phi(S_\gamma)$

Lemme 2.7.1 *L'opération $(S, T) \mapsto S \otimes T$ est un objet variable* $\mathbf{PoLI}^2 \to \mathbf{PoLI}$.

Lemme 2.7.2 *Pour tout ensemble d'indices I, l'opération $S \mapsto S^I$ est un objet variable* $\mathbf{PoLI} \to \mathbf{PoLI}$.

Lemme 2.7.3 *L'opération $S \mapsto\ !S$ est un objet variable* $\mathbf{PoLI} \to \mathbf{PoLI}$.

Démonstration. Soient S et T deux préordres tels que $S \sqsubseteq T$. On vérifie que $!S \sqsubseteq\ !T$. Soient $u, u' \in\ !S$. On suppose $u \leq_{!S} u'$. Soit $a \in u$. Il existe $a' \in u'$ tel que $a \leq_S a'$. Comme $S \sqsubseteq T$, on a $a \leq_T a'$, ce qui montre que $u \leq_{!T} u'$. On montre de même que $u \leq_{!T} u' \Rightarrow u \leq_{!S} u'$.

Soit $(S_\gamma)_{\gamma\in\Gamma}$ une famille filtrante dans **PoLI** et soit $S = \bigsqcup_{\gamma\in\Gamma} S_\gamma$. On montre que $!S \sqsubseteq \bigsqcup_{\gamma\in\Gamma} !S_\gamma$. Soit $u \in\ !S$. Comme u est fini et comme la famille $(S_\gamma)_{\gamma\in\Gamma}$ est filtrante, il existe $\gamma \in \Gamma$ tel que $u \in\ !S_\gamma$. Cela montre que $!S \subseteq \bigsqcup_{\gamma\in\Gamma} !S_\gamma$. Soient maintenant $u, u' \in\ !S$ tels que $u \leq_{!S} u'$. Comme u et u' sont finis, on peut trouver $\gamma \in \Gamma$ tel que $u, u' \in\ !S_\gamma$. Soit $a \in u$. Il existe $a' \in u'$ tel que $a \leq_S a'$, c'est-à-dire $a \leq_{S_\gamma} a'$. On a donc $u \leq_{!S_\gamma} u'$. □

Lemme 2.7.4 *L'opération $S \mapsto S^\perp$ est un objet variable* $\mathbf{PoLI} \to \mathbf{PoLI}$.

Exercice* 2.7.2 Prouver les lemmes 2.7.1, 2.7.2 et 2.7.4, (on peut voir le second comme une conséquence du premier, voir la description du foncteur S^I au paragraphe 2.5.1).

Proposition 2.7.5 *Tout foncteur continu Φ :* **PoLI** $\to$ **PoLI** *admet un plus petit point fixe dans la classe préordonnée* **PoLI**.

Démonstration. La suite $\Phi^n(\emptyset)$ est croissante. En effet, on a $\emptyset \sqsubseteq \Phi(\emptyset)$ car $\emptyset$ est le plus petit élément de **PoLI**. Comme Φ est croissante, $\Phi^n(\emptyset) \sqsubseteq \Phi^{n+1}(\emptyset) \Rightarrow \Phi^{n+1}(\emptyset) \sqsubseteq \Phi^{n+2}(\emptyset)$ et on conclut, par récurrence.

Soit $S = \bigsqcup_{n\in\mathbb{N}} \Phi^n(\emptyset) = \bigsqcup_{n=1}^{\infty} \Phi^n(\emptyset)$ (puisque $\Phi^0(\emptyset) = \emptyset$). Par continuité de S, on a $\Phi(S) = \bigsqcup_{n\in\mathbb{N}} \Phi^{n+1}(\emptyset) = S$. Donc S est un point fixe de Φ. Soit T un autre point fixe. On a $\emptyset \sqsubseteq T$ et donc $\Phi^n(\emptyset) \sqsubseteq \Phi^n(T) = T$ pour tout $n \in \mathbb{N}$, et donc $S \sqsubseteq T$. □

2.7.3 Construction du modèle. Soit Φ : **PoLI** $\rightarrow$ **PoLI** l'objet variable défini par

$$\Phi(S) = (!(S^{\mathbb{N}}))^{\perp}$$

et soit D_∞ le plus petit point fixe de cet objet variable. On va construire un isomorphisme fort entre D_∞ et $\mathsf{D}_\infty \Rightarrow \mathsf{D}_\infty$, ce qui montrera que D_∞ est un modèle du lambda-calcul pur dans la CCC $\mathbf{PoLR}_{\mathsf{K}}$. Par définition, on a $\mathsf{D}_\infty = (!(\mathsf{D}_\infty^{\mathbb{N}}))^{\perp}$. Donc

$$\begin{aligned}
\mathsf{D}_\infty \Rightarrow \mathsf{D}_\infty &= (!\mathsf{D}_\infty)^{\perp} \parr \mathsf{D}_\infty \\
&= (!\mathsf{D}_\infty)^{\perp} \parr (!(\mathsf{D}_\infty^{\mathbb{N}}))^{\perp} \\
&= (!\mathsf{D}_\infty \otimes !(\mathsf{D}_\infty^{\mathbb{N}}))^{\perp} \\
&\simeq (!(\mathsf{D}_\infty \mathbin{\&} \mathsf{D}_\infty^{\mathbb{N}}))^{\perp}
\end{aligned}$$

par l'isomorphisme fondamental. Et on conclut car $\mathsf{D}_\infty \mathbin{\&} \mathsf{D}_\infty^{\mathbb{N}} \simeq \mathsf{D}_\infty^{\mathbb{N}}$ par la bijection qui envoie $(1, a) \in \mathsf{D}_\infty \mathbin{\&} \mathsf{D}_\infty^{\mathbb{N}}$ sur $(0, a) \in \mathsf{D}_\infty^{\mathbb{N}}$, et $(2, (i, a)) \in \mathsf{D}_\infty \mathbin{\&} \mathsf{D}_\infty^{\mathbb{N}}$ sur $(i+1, a) \in \mathsf{D}_\infty^{\mathbb{N}}$ (on renvoie encore à la description de S^I donnée au paragraphe 2.5.1).

Comme $\mathsf{D}_\infty = (!(\mathsf{D}_\infty^{\mathbb{N}}))^{\perp}$, un élément a de D_∞ est une partie finie de $\mathbb{N} \times \mathsf{D}_\infty$ et peut donc être vu comme une suite $\vec{a} = (a_0, a_1, \dots)$ indexée par $\mathbb{N}$, dans laquelle chaque a_i est une partie finie de D_∞ (l'ensemble des $c \in \mathsf{D}_\infty$ tels que $(i, c) \in a$), et on a $a_i = \emptyset$ pour tout indice i, sauf peut-être pour un nombre fini d'entre eux. Donc D_∞ contient en particulier la suite dont tous les éléments sont l'ensemble vide, $* = (\emptyset, \emptyset, \dots)$.

Si $\vec{a}, \vec{b} \in \mathsf{D}_\infty$, on a $\vec{a} \leq_{\mathsf{D}_\infty} \vec{b}$ si, pour tout $i \in \mathbb{N}$, on a $b_i \leq_{!\mathsf{D}_\infty} a_i$ (noter l'inversion du sens de l'ordre, due à la négation linéaire dans la définition récursive de D_∞), c'est-à-dire, chaque $c \in b_i$ a un majorant dans a_i (au sens de D_∞).

Un élément $\vec{a}$ de D_∞ s'écrit donc de façon unique $\vec{a} = (a_0, \vec{b})$ avec $a_0 \in \mathcal{P}_{\mathrm{fin}}(\mathsf{D}_\infty)$ et $\vec{b} \in \mathsf{D}_\infty$, et réciproquement, si $u \in \mathcal{P}_{\mathrm{fin}}(\mathsf{D}_\infty)$ et $\vec{b} \in \mathsf{D}_\infty$, on a $(u, \vec{b}) \in \mathsf{D}_\infty$. Cette bijection entre D_∞ et $!\mathsf{D}_\infty \multimap \mathsf{D}_\infty$ est une autre façon de présenter l'isomorphisme fort entre D_∞ et $\mathsf{D}_\infty \Rightarrow \mathsf{D}_\infty$.

2.7.4 Un modèle plus simple. La construction ci-dessus mène à un modèle de la $\beta\eta$-conversion. Si on ne souhaite interpréter que la β-conversion, une construction plus simple est possible : le modèle de Engeler.

Soit A un ensemble dont aucun élément n'est un couple. On construit une suite d'ensembles E_n comme suit :

$$\begin{aligned}
\mathsf{E}_0 &= \emptyset \\
\mathsf{E}_{n+1} &= A \cup (\mathcal{P}_{\mathrm{fin}}(\mathsf{E}_n) \times \mathsf{E}_n)\,.
\end{aligned}$$

Noter que, grâce à l'hypothèse que A ne contient aucun couple, l'union de la deuxième ligne est disjointe. Cette suite d'ensembles est croissante, soit $\mathsf{E}_\infty = \bigcup_{n=0}^{\infty} \mathsf{E}_n$.

Noter aussi que si $A = \emptyset$, alors $\mathsf{E}_n = \emptyset$ pour tout n et la construction ne produit rien d'intéressant. On suppose donc $A \neq \emptyset$.

Attention : on munit E_∞ du préordre discret ($a \leq a'$ ssi $a = a'$), et, comme tel, on le considère comme un objet de **PoLR**.

Noter que

– $(\mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty) \subseteq \mathsf{E}_\infty$ (et cette inclusion est stricte ; en fait E_∞ est l'union disjointe de A et de $\mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty$).
– Comme E_∞ est muni du préordre discret, on a $(u, a) \leq_{\mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty} (u', a')$ ssi $u' \subseteq u$ et $a = a'$.

On va construire $\mathsf{app} \subseteq \mathsf{E}_\infty \multimap (\mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty)$ et $\mathsf{abs} \subseteq (\mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty) \multimap \mathsf{E}_\infty$. On pose

$$\begin{aligned}\mathsf{app} &= \{((u, a), (u', a)) \mid a \in \mathsf{E}_\infty,\ u, u' \in !\mathsf{E}_\infty \text{ avec } u \subseteq u'\} \\ \mathsf{abs} &= \{((u', a), (u, a)) \mid a \in \mathsf{E}_\infty,\ u, u' \in !\mathsf{E}_\infty \text{ avec } u' \subseteq u\}\end{aligned}$$

et on vérifie facilement que $\mathsf{app} \in \mathbf{PoLR}(\mathsf{E}_\infty, \mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty)$ et $\mathsf{abs} \in \mathbf{PoLR}(\mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty, \mathsf{E}_\infty)$ comme annoncé. On a $((u', a), (v', b))) \in \mathsf{app} \cdot \mathsf{abs}$ ssi $a = b$, et il existe $u \in !\mathsf{E}_\infty$ tel que $u \subseteq v'$ (ce qui correspond au fait que $((u, a), (v', a)) \in \mathsf{app}$) et $u' \subseteq u$ (correspondant au fait que $((u', a), (u, a)) \in \mathsf{abs}$). Cela est équivalent à dire que $a = b$ et $u' \subseteq v'$, c'est-à-dire $(v', b) \leq_{\mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty} (u', a)$. Donc $\mathsf{app} \cdot \mathsf{abs} = \mathsf{Id}_{\mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty}$, ce qui montre que E_∞ est un objet réflexif dans $\mathbf{PoLR}_\mathsf{K}$.

Remarque 2.7.6 En toute rigueur, il aurait fallu exhiber $\mathsf{app}' \in \mathbf{PoLR}_\mathsf{K}(\mathsf{E}_\infty, \mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty)$ et $\mathsf{abs}' \in \mathbf{PoLR}_\mathsf{K}(\mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty, \mathsf{E}_\infty)$ tels que $\mathsf{app}' \circ^\mathsf{K} \mathsf{abs}' = \mathrm{Id}^\mathsf{K}_{\mathsf{E}_\infty \Rightarrow \mathsf{E}_\infty}$. Ces deux morphismes sont obtenus en composant app et abs avec des dérelictions. Donner les détails et faire les vérifications en exercice.

2.7.5 Application : le théorème de forme normale de tête. Etant donné un lambda-terme M et une liste $x_1, \ldots, x_n$ sans répétitions de variables contenant toutes les variables libres de M, son interprétation dans ce modèle est donc $[M]^{x_1,\ldots,x_n} \in \mathbf{PoLR}_\mathsf{K}(\mathsf{E}^n_\infty, \mathsf{E}_\infty)$. On va d'abord donner une description directe de cette sémantique.

Proposition 2.7.7 *Soient $u_1, \ldots, u_n \in \mathcal{P}_{\mathrm{fin}}(\mathsf{E}_\infty)$ et soit $b \in \mathsf{E}_\infty$.*
Soit $a = (u_1, \ldots, u_n, b) \in \mathsf{E}_\infty$. Soit M un lambda-terme dont toutes les variables libres sont dans la liste sans répétitions $x_1, \ldots, x_n$.
– *Si $M = x_i$, on a $a \in [M]^{x_1,\ldots,x_n}$ si et seulement si $b \in u_i$.*
– *Si $M = \lambda x\, P$, on a $a \in [M]^{x_1,\ldots,x_n}$ si et seulement si $b = (u, c)$ avec $(u_1, \ldots, u_n, u, c) \in [M]^{x_1,\ldots,x_n,x}$.*
– *Si $M = (P)\, Q$, on a $a \in [M]^{x_1,\ldots,x_n}$ si et seulement si existe $a_1, \ldots, a_p \in \mathsf{E}_\infty$ tels que $(u_1, \ldots, u_n, a_j) \in [Q]^{x_1,\ldots,x_n}$ pour $j = 1, \ldots, p$ et $(u_1, \ldots, u_n, \{a_1, \ldots, a_p\}, b) \in [P]^{x_1,\ldots,x_n}$.*

Démonstration. On ne va traiter que le cas de l'application $M = (P)\, Q$, les autres cas sont laissés en exercice. On a vu en 1.2.1 que

$$[M]^{x_1,\ldots,x_n} = \mathsf{Ev} \circ^\mathsf{K} \langle \mathsf{app} \circ^\mathsf{K} [P]^{x_1,\ldots,x_n}, [Q]^{x_1,\ldots,x_n} \rangle$$

Donc (considérant $[M]^{x_1,\ldots,x_n}$ comme une fonction continue $\mathcal{P}(\mathsf{E}_\infty)^n \to \mathcal{P}(\mathsf{E}_\infty)$),

$$[M]^{x_1,\ldots,x_n}(u_1, \ldots, u_n) = \mathsf{app}([P]^{x_1,\ldots,x_n}(u_1, \ldots, u_n))([Q]^{x_1,\ldots,x_n}(u_1, \ldots, u_n))$$

Or soient $u, v \in \mathcal{P}(\mathsf{E}_\infty)$, on rappelle que, par définition de app,

$$\mathsf{app}(u)(v) = \{b \mid \exists v_0 \in \mathcal{P}_{\mathrm{fin}}(\mathsf{E}_\infty)\ v_0 \subseteq v \text{ et } (v_0, b) \in u)\}$$

donc $b \in [M]^{x_1,\ldots,x_n}(u_1, \ldots, u_n)$ si et seulement si on peut trouver $v_0 = \{a_1, \ldots, a_p\}$ tels que $(\{a_1, \ldots, a_p\}, b) \in [P]^{x_1,\ldots,x_n}(u_1, \ldots, u_n)$ et $a_j \in [Q]^{x_1,\ldots,x_n}(u_1, \ldots, u_n)$ pour tout $j \in \{1, \ldots, p\}$, ce qui est équivalent à la condition annoncée dans la proposition. □

Exercice* 2.7.3 Calculer $[M] \in \mathcal{P}(\mathsf{E}_\infty)$ pour les termes clos M suivants : $\lambda x\, x$, $\lambda x\, \lambda y\, x$, $\lambda f\, \lambda x\, (f)\, (f)\, x$ (l'entier de Church 2), $\delta = \lambda x\, (x)\, x$ et $(\delta)\, \delta$.

Tout lambda-terme M est de la forme

$$M = \lambda x_1 \dots x_p\, (P)\, Q_1 \dots Q_q$$

où le terme P est soit une variable (qui peut figurer dans la liste $x_1, \dots, x_p$ ou être libre dans M), soit un redex. Dans le premier cas, on dit que M est en *forme normale de tête*, et dans le second cas, on dit que P est le *redex de tête* de M.

Une forme normale de tête est une «forme normale partielle» : dans le cas où le terme P est une variable y, tous les réduits de M seront encore de la forme $\lambda x_1 \dots x_p\, (y)\, Q'_1 \dots Q'_q$, où Q'_i est un réduit de Q_i pour chaque i. L'information fournie par la liste des variables liées en tête et par la variable de tête est donc acquise une bonne fois pour toutes.

On dira qu'un terme M admet une forme normale de tête s'il est beta-equivalent à un terme en forme normale de tête. Si M admet deux formes normales de tête N et N', alors ces deux formes normales de tête sont de la forme $\lambda x_1 \dots x_p\, (y)\, Q_1 \dots Q_q$ et $\lambda x_1 \dots x_p\, (y)\, Q'_1 \dots Q'_q$ respectivement avec Q_i beta-équivalent à Q'_i pour chaque i.

On définit une relation de réduction β_h, qui est incluse dans la beta-réduction ordinaire : la *réduction de tête*. On dira que $M\ \beta_h\ M'$ si M a un rédex de tête (*i.e.* M n'est pas en forme normale de tête) et M' est obtenu en réduisant le redex de tête de M. Les formes normales pour cette réduction sont donc les formes normales de tête. On dira qu'un terme est *normalisable de tête* si sa réduction de tête termine.

Lemme 2.7.8 *Soit M un terme en forme normale de tête, et soit $x_1, \dots, x_n$ une liste de variables sans répétitions et contenant toutes les variables libres de M. Alors $[M]^{x_1,\dots,x_n} \neq \emptyset$.*

Démonstration. Par la proposition 2.7.7, il suffit de le montrer quand M est de la forme $M = (x)\, P_1 \dots P_p$. Soit $x_0, \dots, x_n$ une liste sans répétitions de variables contenant toutes les variables libres de M ; sans perte de généralité, on peut supposer que $x_0 = x$. Par la même proposition, on a $(u, \emptyset, \dots, \emptyset, b) \in [M]^{x,x_1,\dots,x_n}$ pour tout $b \in \mathsf{E}_\infty$ et tout $u \in \mathcal{P}_{\mathrm{fin}}(\mathsf{E}_\infty)$ tels que $(\emptyset, \dots, \emptyset, b) \in u$ (n occurrences de $\emptyset$). □

On va montrer que la réciproque est également vraie (on dit que le modèle E_∞ du lamda-calcul pur est *sensible* — au sens anglais du terme, il faudrait dire «raisonnable» ou «sensé» —). Pour cela, on va appliquer la technique de réductibilité qui nous a permis de prouver la normalisation forte du système F.

Soit $\mathcal{N}$ l'ensemble des termes normalisables de tête. Soit $\mathcal{N}_0$ l'ensemble des termes de la forme $(x)\, M_1, \dots, M_n$ (sans restriction sur les M_i).

Une partie $\mathcal{X}$ de Λ est dite *saturée* si, pour tous $M, N, N_1, \dots, N_n \in \Lambda$, si $(M\, [N/x])\, N_1 \dots N_n \in \mathcal{X}$, alors $(\lambda x\, M)\, N N_1 \dots N_n \in \mathcal{X}$. [**NB:** Bien noter qu'ici, on ne fait pas d'hypothèse sur les termes $M, N, N_1, \dots, N_n \in \Lambda$, contrairement à ce qu'on a fait pour la normalisation forte de F.]

Lemme 2.7.9 *L'ensemble $\mathcal{N}$ est saturé.*

Démonstration. C'est évident, puisque $(\lambda x\, M)\, N N_1 \dots N_n\ \beta_h\ (M\, [N/x])\, N_1 \dots N_n$, donc si la réduction de tête de $(M\, [N/x])\, N_1 \dots N_n$ termine (en r étapes), celle de $(\lambda x\, M)\, N N_1 \dots N_n\ \beta_h\ (M\, [N/x])\, N_1 \dots N_n$ termine aussi (en $r + 1$ étapes). □

Soient $\mathcal{X}, \mathcal{Y} \subseteq \Lambda$. On définit

$$(\mathcal{X} \Rightarrow \mathcal{Y}) = \{M \in \Lambda \mid \forall N \in \mathcal{X}\ \ (M)\, N \in \mathcal{Y}\}\,. \tag{2.7}$$

Observer que si $\mathcal{X}' \subseteq \mathcal{X} \subseteq \Lambda$ et $\mathcal{Y} \subseteq \mathcal{Y}' \subseteq \Lambda$, alors $(\mathcal{X} \Rightarrow \mathcal{Y}) \subseteq (\mathcal{X}' \Rightarrow \mathcal{Y}')$ (l'implication est croissante à droite et décroissante à gauche).

Lemme 2.7.10 *Soit $\mathcal{X} \subseteq \Lambda$ et soit $\mathcal{Y}$ saturée. Alors $\mathcal{X} \Rightarrow \mathcal{Y}$ est saturée.*

L'intersection d'une famille quelconque *de parties saturées est saturée.*

Exercice 2.7.4 Démontrer ce lemme.

Lemme 2.7.11 *On a les inclusions suivantes :*

$$\mathcal{N}_0 \subseteq (\Lambda \Rightarrow \mathcal{N}_0) \subseteq (\mathcal{N}_0 \Rightarrow \mathcal{N}) \subseteq \mathcal{N} .$$

Démonstration. La première inclusion résulte de la définition de $\mathcal{N}_0$. La seconde résulte du fait que $\mathcal{N}_0 \subseteq \mathcal{N}$ et du fait que l'opération $\_ \Rightarrow \_$ est croissante à droite et décroissante à gauche. Pour la dernière inclusion, soit $M \in (\mathcal{N}_0 \Rightarrow \mathcal{N})$ et supposons que $M \notin \mathcal{N}$, c'est-à-dire qu'on a une suite infinie de termes $M_1, M_2, \dots$ tels que $M_1 = M$ et $M_r \; \beta_h \; M_{r+1}$ pour tout r. Soit x une variable quelconque. On a $x \in \mathcal{N}_0$ et donc $(M)\,x \in \mathcal{N}$.

Si aucun des termes M_r ne commence par un lambda, alors, pour tout r, on a $(M_r)\,x \; \beta_h \; (M_{r+1})\,x$, ce qui contredit le fait que $M = M_1$ est normalisable de tête. Donc on peut trouver un entier $l \geq 1$ tel que, pour tout $r < l$, le terme M_r ne commence pas par une abstraction, et $M_r = \lambda y\, P_r$ avec $P_r \; \beta_h \; P_{r+1}$, pour tout $r \geq l$. Mais alors, on a la suite infinie de réductions de tête suivante

$$(M_1)\,y \; \beta_h \cdots \beta_h \; (M_l)\,y = (\lambda y\, P_l)\,y \; \beta_h \; P_l\,[y/y] = P_l \; \beta_h \; P_{l+1} \; \beta_h \cdots .$$

ce qui contredit le fait que $(M)\,y \in \mathcal{N}$. □

Une *valuation* est une application $\mathcal{I}$ des éléments de A (à partir duquel sont construits les ensembles E_n au paragraphe 2.7.4) vers les sous-ensembles de Λ qui sont saturés, inclus dans $\mathcal{N}$ et contiennent $\mathcal{N}_0$. Par induction sur $a \in \mathsf{E}_\infty$ (c'est-à-dire, par induction sur le plus petit n tel que $a \in \mathsf{E}_n$), on définit $[a]_\mathcal{I}$, qui est une partie saturée de Λ telle que $\mathcal{N}_0 \subseteq [a]_\mathcal{I} \subseteq \mathcal{N}$:

- $[a]_\mathcal{I} = \mathcal{I}(a)$ si $a \in A$;
- $[a]_\mathcal{I} = (\bigcap_{i=1}^{p} [b_i]_\mathcal{I}) \Rightarrow [b]_\mathcal{I}$ si $a = (\{b_1, \dots, b_p\}, b)$. Alors $[a]_\mathcal{I}$ est saturé par hypothèse de récurrence et par le lemme 2.7.10, et on a $\mathcal{N}_0 \subseteq [a]_\mathcal{I} \subseteq \mathcal{N}$ par hypothèse de récurrence et par le lemme 2.7.11. Observer que, quand $p = 0$, on a $[a]_\mathcal{I} = \Lambda \Rightarrow [b]_\mathcal{I}$, d'où la formulation des lemmes 2.7.10 et 2.7.11, différente de celle du lemme correspondant dans le preuve de normalisation du système F.

Si $u \in \mathcal{P}(\mathsf{E}_\infty)$, on pose $[u]_\mathcal{I} = \bigcap_{a \in u} [a]_\mathcal{I}$, si bien, par exemple, que $[\emptyset]_\mathcal{I} = \Lambda$. Si u est non vide, on a $[u]_\mathcal{I} \subseteq \mathcal{N}$.

On peut maintenant prouver le lemme principal.

Lemme 2.7.12 (adéquation) *Soit M un lambda-terme et $x_1, \dots, x_n$ une liste de variables deux à deux distinctes en contenant toutes les variables libres de M. Soient $u_1, \dots, u_n \in \mathcal{P}_{\mathrm{fin}}(\mathsf{E}_\infty)$ et $a \in \mathsf{E}_\infty$. Soient $M_1, \dots, M_n \in \Lambda$ et soit $\mathcal{I}$ une valuation quelconque.*

Si $(u_1, \dots, u_n, a) \in [M]^{x_1, \dots, x_n}$ et si $M_i \in [u_i]_\mathcal{I}$ pour tout $i \in \{1, \dots, n\}$, alors $M\,[M_1/x_1, \dots, M_n/x_n] \in [a]_\mathcal{I}$.

Démonstration. La preuve se fait par récurrence sur M. Pour tout lambda-terme P, on note P' le lambda-terme $P\,[M_1/x_1, \dots, M_n/x_n]$ (dans cette preuve uniquement).

Si $M = x_i$, comme $(u_1, \dots, u_n, a) \in [M]^{x_1, \dots, x_n}$, on a $a \in u_i$ par la proposition 2.7.7, donc $[u_i]_\mathcal{I} \subseteq [a]_\mathcal{I}$. Or $M_i \in [u_i]_\mathcal{I}$ et $M' = M_i$, donc $M' \in [a]_\mathcal{I}$.

Supposons $M = (P)\,Q$. Comme $(u_1, \ldots, u_n, a) \in [M]^{x_1,\ldots,x_n}$, par la proposition 2.7.7, on peut trouver $a_1, \ldots, a_p \in \mathsf{E}_\infty$ tels que $(u_1, \ldots, u_n, \{a_1, \ldots, a_p\}, a) \in [P]^{x_1,\ldots,x_n}$ et $(u_1, \ldots, u_n, a_j) \in [Q]^{x_1,\ldots,x_n}$ pour $j \in \{1, \ldots, p\}$. Comme $(u_1, \ldots, u_n, a_j) \in [Q]^{x_1,\ldots,x_n}$, on a conséquemment $Q' \in [a_j]_\mathcal{I}$ pour tout j, par hypothèse de récurrence, et donc

$$Q' \in [\{a_1, \ldots, a_p\}]_\mathcal{I}\,.$$

De même, on a par hypothèse de récurrence,

$$P' \in [(\{a_1, \ldots, a_n\}, a)]_\mathcal{I} = [\{a_1, \ldots, a_p\}]_\mathcal{I} \Rightarrow [a]_\mathcal{I}$$

puisqu'on a $(u_1, \ldots, u_n, \{a_1, \ldots, a_p\}, b) \in [P]^{x_1,\ldots,x_n}$. Donc $M' = (P')\,Q' \in [a]_\mathcal{I}$.

Finalement, supposons $M = \lambda x\, P$. Comme $(u_1, \ldots, u_n, a) \in [M]^{x_1,\ldots,x_n}$, on a $a = (u, b)$ avec $(u_1, \ldots, u_n, u, b) \in [P]^{x_1,\ldots,x_n,u}$ par la proposition 2.7.7. On veut montrer que $M' = \lambda x\, P' \in [(u, b)]_\mathcal{I} = [u]_\mathcal{I} \Rightarrow [b]_\mathcal{I}$. Soit donc $N \in [u]_\mathcal{I}$, il faut montrer que $(\lambda x\, P')\, N \in [b]_\mathcal{I}$. Or $[b]_\mathcal{I}$ est saturé. Il suffit donc de montrer que $P'\,[N/x] = P\,[M_1/x_1, \ldots, M_n/x_n, N/x] \in [b]_\mathcal{I}$ (l'égalité est vraie car on peut supposer que x n'apparaît libre dans aucun des M_i), mais cela résulte de l'hypothèse de récurrence. □

Soit alors M tel que $[M]^{x_1,\ldots,x_n} \neq \emptyset$. Soit $(u_1, \ldots, u_n, a) \in [M]^{x_1,\ldots,x_n}$. Comme $x_i \in \mathcal{N}_0 \subseteq [u_i]_\mathcal{I}$ pour tout i, on a, en appliquant le lemme ci-dessus : $M \in [a]_\mathcal{I} \subseteq \mathcal{N}$, et donc M est normalisable de tête. On a donc prouvé le théorème suivant.

Théorème 2.7.13 *Soit M un terme et $x_1, \ldots, x_n$ une liste de variables sans répétitions contenant toutes les variables libres de M. Le terme M est normalisable de tête si et seulement si $[M]^{x_1,\ldots,x_n} \neq \emptyset$, c'est-à-dire, si et seulement si la fonction $[M]^{x_1,\ldots,x_n}$ ne prend pas que la valeur $\emptyset$.*

De là on déduit facilement un théorème purement syntaxique.

Théorème 2.7.14 *Si un terme M est beta-équivalent à un terme en forme normale de tête, alors sa réduction de tête termine.*

Démonstration. Supposons M beta-équivalent à M' qui est en forme normale de tête. Soit $x_1, \ldots, x_n$ une liste de variables sans répétitions contenant toutes les variables de M et de M'. Par le lemme 2.7.8, $[M']^{x_1,\ldots,x_n} \neq \emptyset$. Or $[M]^{x_1,\ldots,x_n} = [M']^{x_1,\ldots,x_n}$ et donc $[M]^{x_1,\ldots,x_n} = [M']^{x_1,\ldots,x_n}$. On conclut que M est normalisable de tête par le théorème 2.7.13. □

Chapitre 3

PCF : syntaxe et sémantique de Scott

On définit un lambda-calcul étendu, qui ressemble plus à un langage de programmation que le lambda-calcul pur : c'est le langage PCF (Programming with Computable Functions). Voir aussi [AC98], et [GLT89] qui parle du *système T* de Gödel, qui est similaire à PCF, avec un opérateur de récursion à la place de l'opérateur de point fixe.

3.1 Syntaxe

On définit d'abord les types : ι est un type (le type des entiers), et si A et B sont des types, alors $A \Rightarrow B$ est un type.

Les termes du langage PCF sont définis par la syntaxe suivante.

- Toute variable est un terme ;
- si P et Q sont des termes, x une variable et A un type, alors $\lambda x^A\, P$ et $(P)\, Q$ sont des termes ;
- si P est un terme, alors $\mathsf{fix}(P)$ est un terme ;
- si P, Q et R sont des termes, alors $\mathsf{if}(P, Q, R)$ est un terme ;
- si n est un entier naturel, alors $\underline{n}$ est un terme ;
- si P est un terme, alors $\mathsf{succ}(P)$ et $\mathsf{pred}(P)$ sont des termes ;

3.1.1 Typage. Voici ensuite les règles de typage. Comme d'habitude, un contexte Γ est une suite $(x_1 : A_1, \ldots, x_n : A_n)$ où les x_i sont des variables deux à deux distinctes et où les A_i sont des types.

$$\frac{}{\Gamma, x : A \vdash x : A} \qquad \frac{\Gamma \vdash M : A \Rightarrow B \qquad \Gamma \vdash N : A}{\Gamma \vdash (M)\, N : B}$$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x^A\, M : A \Rightarrow B} \qquad \frac{\Gamma \vdash M : A \Rightarrow A}{\Gamma \vdash \mathsf{fix}(M) : A}$$

$$\frac{\Gamma \vdash M : \iota \qquad \Gamma \vdash P : \iota \qquad \Gamma \vdash Q : \iota}{\Gamma \vdash \mathsf{if}(M, P, Q) : \iota}$$

$$\frac{}{\Gamma \vdash \underline{n} : \iota} \qquad \frac{\Gamma \vdash M : \iota}{\Gamma \vdash \mathsf{succ}(M) : \iota} \qquad \frac{\Gamma \vdash M : \iota}{\Gamma \vdash \mathsf{pred}(M) : \iota}$$

Remarque 3.1.1 La restriction de typage du $\mathsf{if}(\_, \_, \_)$, selon laquelle les deux branches de la conditionnelle doivent avoir le type ι, n'est pas gênante du point de vue de l'expressivité. Par exemple, si $\Gamma \vdash P, Q : \iota \Rightarrow \iota$, et si $\Gamma \vdash M : \iota$, on peut définir $\mathsf{if}(M, P, Q)$ avec $\Gamma \vdash \mathsf{if}(M, P, Q) : \iota \Rightarrow \iota$ par

$$\mathsf{if}(M, P, Q) = \lambda x^\iota \, \mathsf{if}(M, (P)\, x, (Q)\, x)$$

qui utilise un "$\mathsf{if}(\_, \_, \_)$" dont les deux branches sont de type ι.

3.1.2 Réduction. On définit une relation de *réduction* β_{PCF} sur les termes de PCF, suivant le même schéma que pour la beta-réduction du lambda-calcul. On définit donc, par récurrence sur M, l'ensemble des termes M' tels que $M \; \beta_{\mathsf{PCF}} \; M'$.

- On n'a jamais $x \; \beta_{\mathsf{PCF}} \; M'$.
- On n'a jamais $\underline{n} \; \beta_{\mathsf{PCF}} \; M'$.
- On a $\lambda x^A \, P \; \beta_{\mathsf{PCF}} \; M'$ si $M' = \lambda x^A \, P'$ avec $P \; \beta_{\mathsf{PCF}} \; P'$
- On a $(P)\, Q \; \beta_{\mathsf{PCF}} \; M'$ si
  - $M' = (P')\, Q$ avec $P \; \beta_{\mathsf{PCF}} \; P'$
  - ou $M' = (P)\, Q'$ avec $Q \; \beta_{\mathsf{PCF}} \; Q'$
  - ou $P = \lambda x^A \, R$ et $M' = R\,[Q/x]$
- On a $\mathsf{fix}(P) \; \beta_{\mathsf{PCF}} \; M'$ si
  - $M' = \mathsf{fix}(P')$ avec $P \; \beta_{\mathsf{PCF}} \; P'$
  - ou $M' = (P)\, \mathsf{fix}(P)$
- On a $\mathsf{if}(R, P, Q) \; \beta_{\mathsf{PCF}} \; M'$ si
  - $M' = \mathsf{if}(R', P, Q)$ avec $R \; \beta_{\mathsf{PCF}} \; R'$
  - ou $M' = \mathsf{if}(R, P', Q)$ avec $P \; \beta_{\mathsf{PCF}} \; P'$
  - ou $M' = \mathsf{if}(R, P, Q')$ avec $Q \; \beta_{\mathsf{PCF}} \; Q'$
  - ou $R = \underline{0}$ et $M' = P$
  - ou $R = \underline{n+1}$ et $M' = Q$
- On a $\mathsf{succ}(P) \; \beta_{\mathsf{PCF}} \; M'$ si
  - $M' = \mathsf{succ}(P')$ avec $P \; \beta_{\mathsf{PCF}} \; P'$
  - ou $P = \underline{n}$ et $M' = \underline{n+1}$
- On a $\mathsf{pred}(P) \; \beta_{\mathsf{PCF}} \; M'$ si
  - $M' = \mathsf{pred}(P')$ avec $P \; \beta_{\mathsf{PCF}} \; P'$
  - ou $P = \underline{0}$ et $M' = \underline{0}$
  - ou $P = \underline{n+1}$ et $M' = \underline{n}$

Remarque 3.1.2 Autrement dit, dans PCF, un redex est un terme de l'une des formes suivantes :

- $(\lambda x^A \, R)\, Q$ qui se réduit en $R\,[Q/x]$,
- $\mathsf{fix}(P)$ qui se réduit en $(P)\, \mathsf{fix}(P)$,
- $\mathsf{if}(\underline{n}, P, Q)$ avec $n \in \mathbb{N}$, qui se réduit en P si $n = 0$ et en Q si $n > 0$,
- $\mathsf{succ}(\underline{n})$ qui se réduit en $\underline{n+1}$,
- $\mathsf{pred}(\underline{n})$ qui se réduit en $\underline{0}$ si $n = 0$ et en $\underline{n-1}$ si $n > 0$.

Et on a $M \; \beta_{\mathsf{PCF}} \; M'$ si on obtient M' en choisissant dans M un redex (en une position quelconque) et en le réduisant.

Exercice 3.1.1 Essayer de démontrer un théorème de confluence pour (la clôture réflexive-transitive de) cette réduction.

3.1.3 Réduction de tête. On définit de même la *réduction de tête* $\beta_{\mathsf{PCF,h}}$.

- On n'a jamais $x \; \beta_{\mathsf{PCF,h}} \; M'$.
- On n'a jamais $\underline{n} \; \beta_{\mathsf{PCF,h}} \; M'$.
- On a $\lambda x^A \, P \; \beta_{\mathsf{PCF,h}} \; M'$ si $M' = \lambda x^A \, P'$ avec $P \; \beta_{\mathsf{PCF,h}} \; P'$.
- On a $(P)\, Q \; \beta_{\mathsf{PCF,h}} \; M'$
  - si P n'est pas de le forme $P = \lambda x^A \, R$ et si $M' = (P')\, Q$ avec $P \; \beta_{\mathsf{PCF,h}} \; P'$
  - ou si $P = \lambda x^A \, R$ et $M' = P\,[Q/x]$.

- On a $\mathsf{fix}(P)\ \beta_{\mathsf{PCF,h}}\ M'$ si $M' = (P)\,\mathsf{fix}(P)$
- On a $\mathsf{if}(R, P, Q)\ \beta_{\mathsf{PCF,h}}\ M'$
  - si $M' = \mathsf{if}(R', P, Q)$ avec $R\ \beta_{\mathsf{PCF,h}}\ R'$
  - ou si $R = \underline{0}$ et $M' = P$
  - ou si $R = \underline{n+1}$ et $M' = Q$.
- On a $\mathsf{succ}(P)\ \beta_{\mathsf{PCF,h}}\ M'$
  - si $M' = \mathsf{succ}(P')$ avec $P\ \beta_{\mathsf{PCF,h}}\ P'$
  - ou si $P = \underline{n}$ et $M' = \underline{n+1}$.
- On a $\mathsf{pred}(P)\ \beta_{\mathsf{PCF,h}}\ M'$
  - si $M' = \mathsf{pred}(P')$ avec $P\ \beta_{\mathsf{PCF,h}}\ P'$
  - ou si $P = \underline{0}$ et $M' = \underline{0}$
  - ou si $P = \underline{n+1}$ et $M' = \underline{n}$.

Remarque 3.1.3 On a $\beta_{\mathsf{PCF,h}} \subseteq \beta_{\mathsf{PCF}}$. Observer que $\beta_{\mathsf{PCF,h}}$ est une *stratégie de réduction*, c'est-à-dire que, étant donné un terme de PCF M, ou bien M est en “forme normale de tête” (non réductible au sens de $\beta_{\mathsf{PCF,h}}$), ou bien M contient exactement un redex tel que $M\ \beta_{\mathsf{PCF,h}}\ M'$.

Exercice* 3.1.2 Donner une description explicite des termes de PCF qui sont en forme normale de tête, c'est-à-dire, en forme normale pour $\beta_{\mathsf{PCF,h}}$. En déduire que, si un terme clos M de PCF est tel que $\vdash M : \iota$ et est normal pour $\beta_{\mathsf{PCF,h}}$ (est en forme normale de tête), alors M est de la forme $\underline{n}$ pour un $n \in \mathbb{N}$.

3.1.4 Invariance de la sémantique.

Lemme 3.1.4 (substitution) *Soient $P, Q \in \mathsf{PCF}$. Si $\Gamma, x : A \vdash P : B$ et si $\Gamma \vdash Q : A$, alors $\Gamma \vdash P\,[Q/x] : B$.*

Proposition 3.1.5 (réduction du sujet) *Soit $M \in \mathsf{PCF}$. Si $\Gamma \vdash M : A$ et $M\ \beta_{\mathsf{PCF}}\ M'$, alors $\Gamma \vdash M' : A$.*

Exercice 3.1.3 Démontrer le lemme de substitution puis la réduction du sujet.

3.2 Sémantique de PCF dans la catégorie $\mathbf{PoLR}_{\mathsf{K}}$

On se place dans la catégorie $\mathbf{PoLR}_{\mathsf{K}}$ qui est cartésienne fermée comme on l'a vu. On en verra les morphismes tantôt comme des fonctions Scott-continues, tantôt comme des relations.

3.2.1 Opérateurs de point fixe. Soit S un préordre et soit $f : \mathcal{I}(S) \to \mathcal{I}(S)$ une fonction continue. Alors $f^n(\emptyset)$ est une suite croissante d'éléments de $\mathcal{I}(S)$ (par récurrence), et, comme f est continue, on a

$$f\left(\bigcup_{n=0}^{\infty} f^n(\emptyset)\right) = \bigcup_{n=0}^{\infty} f^n(\emptyset)\,.$$

On note $\mathsf{Y}^{\mathsf{s}}(f)$ cet élément de $\mathcal{I}(S)$. On vérifie facilement que $\mathsf{Y}^{\mathsf{s}}(f)$ est le plus petit point fixe de f.

Exercice 3.2.1 Soit $s \in \mathbf{PoLR}_{\mathsf{K}}(S, S)$. Exprimer $\mathsf{Y}^{\mathsf{s}}(\mathsf{Fun}\,s)$ en fonction de s.

On a donc une opération $\mathsf{Y}^{\mathsf{s}} : \mathcal{I}(S \Rightarrow S) \to \mathcal{I}(S)$ qui envoie un morphisme sur son plus petit point fixe. Il serait assez facile, ici, de vérifier directement que cette opération elle-même est Scott-continue. Mais dans des modèles plus compliqués (les modèles de jeux, par exemple), la vérification directe que cette opération est un morphisme de la catégorie ambiante peut devenir assez complexe. Elle est en fait tout-à-fait inutile : grâce à la clôture cartésienne, il suffit de remarquer que notre opérateur de point fixe est lui-même le plus petit point fixe d'une fonction d'un type plus compliqué.

Soit donc

$$\begin{array}{rcl}\Phi : \mathcal{I}((S \Rightarrow S) \Rightarrow S) & \to & \mathcal{I}((S \Rightarrow S) \Rightarrow S) \\ Z & \mapsto & \lambda f\,(f)\,(Z)\,f\end{array}$$

Cette fonction est bien définie, et Scott-continue, car la catégorie $\mathbf{PoC}$ (c'est-à-dire, la catégorie $\mathbf{PoLR}_{\mathsf{K}}$: encore une fois, on identifie $\mathcal{I}(U \Rightarrow V)$ et l'ensemble des fonctions continues $\mathcal{I}(U) \to \mathcal{I}(V)$ muni de l'ordre ponctuel ; autrement dit, on laisse implicite l'isomorphisme Fun/Tr) est cartésienne fermée. Soit $Y \in \mathcal{I}((S \Rightarrow S) \Rightarrow S)$ le plus petit point fixe de Φ, on a $Y = \bigcup_{n=0}^{\infty} \Phi^n(\emptyset)$. Soit $s \in \mathcal{I}(S \Rightarrow S)$. On montre par récurrence sur n que $\Phi^n(\emptyset)(s) = s^n(\emptyset)$. *Cas de base* : $\Phi^0(\emptyset)(s) = \emptyset = s^0(\emptyset)$. *Etape de récurrence* : $\Phi^{n+1}(\emptyset)(s) = s(\Phi^n(\emptyset)(s))$ par définition de Φ, donc $\Phi^{n+1}(\emptyset)(s) = s(s^n(\emptyset))$ par hypothèse de récurrence et on conclut. Par suite, $Y(s) = \bigcup_{n=0}^{\infty} s^n(\emptyset)$, ce qui montre que Y envoie toute fonction continue s sur son plus petit point fixe $\mathsf{Y}^{\mathsf{s}}(s)$. Donc $\mathsf{Y}^{\mathsf{s}} = Y \in \mathbf{PoC}(S \Rightarrow S, S)$.

3.2.2 Interprétation des entiers. Soit $\mathbf{N}$ l'ensemble des entiers naturels, muni du préordre discret : $n \leq m$ ssi $n = m$. On a donc $\mathcal{I}(\mathbf{N}) = \mathcal{P}(\mathbb{N})$. C'est une version "non déterministe" du domaine plat des entiers. $\mathcal{I}(\mathbf{N})$ contient le domaine plat des entiers (c'est l'ensemble $\{\emptyset, \{0\}, \{1\}, \ldots\}$), mais aussi toutes les *superpositions non déterministes* de ces entiers de base. On appellera cet objet *préordre des entiers plats*.

On définit $\mathsf{s}^{\mathsf{s}}, \mathsf{p}^{\mathsf{s}} \in \mathbf{PoLR}_{\mathsf{K}}(\mathbf{N}, \mathbf{N})$ par

$$\begin{array}{rcl}\mathsf{s}^{\mathsf{s}} & = & \{(u, n+1) \in \mathcal{P}_{\mathrm{fin}}(\mathbb{N}) \times \mathbb{N} \mid n \in u\}\,, \\ \mathsf{p}^{\mathsf{s}} & = & \{(u, n) \in \mathcal{P}_{\mathrm{fin}}(\mathbb{N}) \times \mathbb{N} \mid n+1 \in u\}\,.\end{array}$$

Vu que l'ordre de $\mathbf{N}$ est discret, on a bien $\mathsf{s}^{\mathsf{s}}, \mathsf{p}^{\mathsf{s}} \in \mathcal{I}(\mathbf{N} \Rightarrow \mathbf{N})$. De plus, on a $\mathsf{p}^{\mathsf{s}} \circ \mathsf{s}^{\mathsf{s}} = \mathsf{Id} = \{(u, n) \in \mathcal{P}_{\mathrm{fin}}(\mathbb{N}) \times \mathbb{N} \mid n \in u\}$.

Exercice 3.2.2 Exprimer p^{s} et s^{s} comme fonctions continues (linéaires en fait) de $\mathcal{I}(\mathbf{N})$ vers $\mathcal{I}(\mathbf{N})$.

Enfin, on définit $\mathsf{if}^{\mathsf{s}} \in \mathbf{PoLR}_{\mathsf{K}}(\mathbf{N}^3, \mathbf{N})$ par

$$\begin{array}{rcl}\mathsf{if}^{\mathsf{s}} & = & \{((u, v, w), n) \in \mathcal{P}_{\mathrm{fin}}(\mathbb{N})^3 \times \mathbb{N} \mid n \in v \text{ et } 0 \in u\} \\ & & \cup\{((u, v, w), n) \in \mathcal{P}_{\mathrm{fin}}(\mathbb{N})^3 \times \mathbb{N} \mid n \in w \text{ et } \exists i \in \mathbb{N}\ i+1 \in u\}\end{array}$$

Exercice* **3.2.3** Exprimer if^{s} comme une fonction continue $\mathcal{I}(\mathbf{N})^3 \to \mathcal{I}(\mathbf{N})$.

Donner une version de if^{s} de type $\mathbf{PoLR}_{\mathsf{K}}(\mathbf{N} \,\&\, S \,\&\, S, S)$ pour S un préordre quelconque.

3.2.3 Interprétation de PCF. Si A est un type, son interprétation $[A]_{\mathsf{s}}$ est le préordre défini par récurrence par

- $[\iota]_{\mathsf{s}} = \mathbf{N}$
- $[A \Rightarrow B]_{\mathsf{s}} = [A]_{\mathsf{s}} \Rightarrow [B]_{\mathsf{s}}$.

Si $\Gamma = (x_1 : A_1, \dots, x_n : A_n)$ est un contexte de typage, on pose $[\Gamma]_{\mathsf{s}} = [A_1]_{\mathsf{s}} \,\&\, \cdots \,\&\, [A_n]_{\mathsf{s}}$.

Étant donné un contexte de typage Γ et un terme M tel que $\Gamma \vdash M : A$, on définit une fonction continue $[M]_{\mathsf{s}}^{\Gamma} : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}([A]_{\mathsf{s}})$, par récurrence sur la dérivation du typage $\Gamma \vdash M : A$ (c'est-à-dire, par récurrence sur M, puisque chaque règle de typage correspond exactement à une construction syntaxique du langage).

Si M est une variable, alors $M = x_i$ pour un $i \in \{1, \dots, n\}$ et $A = A_i$. Alors $[M]_{\mathsf{s}}^{\Gamma} = \pi_i$.

Si $M = (P)\,Q$, alors $\Gamma \vdash P : B \Rightarrow A$ et $\Gamma \vdash Q : B$ pour un certain type B. Par hypothèse de récurrence, on a déjà défini deux fonctions continues $[P]_{\mathsf{s}}^{\Gamma} : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}([B]_{\mathsf{s}} \Rightarrow [A]_{\mathsf{s}})$ et $[Q]_{\mathsf{s}}^{\Gamma} : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}([B]_{\mathsf{s}})$. On pose

$$[M]_{\mathsf{s}}^{\Gamma} = \mathsf{Ev} \circ \langle [P]_{\mathsf{s}}^{\Gamma}, [Q]_{\mathsf{s}}^{\Gamma} \rangle : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}([A]_{\mathsf{s}})$$

qui est une fonction continue. Autrement dit, si $\vec{u} \in [\Gamma]_{\mathsf{s}}$, on a

$$[M]_{\mathsf{s}}^{\Gamma}(\vec{u}) = [P]_{\mathsf{s}}^{\Gamma}(\vec{u})([Q]_{\mathsf{s}}^{\Gamma}(\vec{u}))\,.$$

Si $M = \lambda x^B\, P$, alors $\Gamma, x : B \vdash P : C$ avec $A = B \Rightarrow C$. Par hypothèse de récurrence on a défini une fonction continue $[P]_{\mathsf{s}}^{\Gamma, x:B} : \mathcal{I}([\Gamma]_{\mathsf{s}} \,\&\, [B]_{\mathsf{s}}) \to \mathcal{I}([C]_{\mathsf{s}})$. On pose

$$[M]_{\mathsf{s}}^{\Gamma} = \Lambda([P]_{\mathsf{s}}^{\Gamma, x:B}) : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}([A]_{\mathsf{s}})$$

qui est une fonction continue. Autrement dit, si $\vec{u} \in [\Gamma]_{\mathsf{s}}$ et $v \in [B]_{\mathsf{s}}$, on a $[M]_{\mathsf{s}}^{\Gamma}(\vec{u})(v) = [P]_{\mathsf{s}}^{\Gamma, x:B}(\vec{u}, v)$.

Si $M = \mathsf{if}(R, P, Q)$, alors on a $\Gamma \vdash R : \iota$, $\Gamma \vdash P : \iota$ et $\Gamma \vdash Q : \iota$. Par hypothèse de récurrence, on a déjà défini les fonctions continues $[R]_{\mathsf{s}}^{\Gamma}, [P]_{\mathsf{s}}^{\Gamma}, [Q]_{\mathsf{s}}^{\Gamma} : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}(\mathbf{N})$. On pose

$$[M]_{\mathsf{s}}^{\Gamma} = \mathsf{if}^{\mathsf{s}}_{[A]_{\mathsf{s}}} \circ \langle [R]_{\mathsf{s}}^{\Gamma}, [P]_{\mathsf{s}}^{\Gamma}, [Q]_{\mathsf{s}}^{\Gamma} \rangle\,.$$

Si $M = \underline{k}$, alors $[M]_{\mathsf{s}}^{\Gamma} : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}(\mathbf{N})$ est la fonction constante égale a $\{k\} \in \mathcal{I}(\mathbf{N})$.

Si $M = \mathsf{pred}(P)$, alors on a $\Gamma \vdash P : \iota$. Par hypothèse de récurrence, on a déjà défini la fonction continue $[P]_{\mathsf{s}}^{\Gamma} : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}(\mathbf{N})$. On pose

$$[M]_{\mathsf{s}}^{\Gamma} = \mathsf{p}^{\mathsf{s}} \circ [P]_{\mathsf{s}}^{\Gamma} : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}(\mathbf{N})$$

qui est une fonction continue.

Si $M = \mathsf{succ}(P)$, alors on a $\Gamma \vdash P : \iota$. Par hypothèse de récurrence, on a déjà défini la fonction continue $[P]_{\mathsf{s}}^{\Gamma} : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}(\mathbf{N})$. On pose

$$[M]_{\mathsf{s}}^{\Gamma} = \mathsf{s}^{\mathsf{s}} \circ [P]_{\mathsf{s}}^{\Gamma} : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}(\mathbf{N})$$

qui est une fonction continue.

Si $M = \mathsf{fix}(P)$, alors on a $\Gamma \vdash P : A \Rightarrow A$. Par hypothèse de récurrence on a défini une fonction continue $[P]_{\mathsf{s}}^{\Gamma} : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to ([A]_{\mathsf{s}} \Rightarrow [A]_{\mathsf{s}})$. On pose

$$[M]_{\mathsf{s}}^{\Gamma} = \mathsf{Y}^{\mathsf{s}} \circ [P]_{\mathsf{s}}^{\Gamma} : \mathcal{I}([\Gamma]_{\mathsf{s}}) \to \mathcal{I}([A]_{\mathsf{s}})$$

qui est une fonction continue.

Lemme 3.2.1 (substitution) *Soient $P, Q \in \mathsf{PCF}$. Si $\Gamma, x : A \vdash P : B$ et si $\Gamma \vdash Q : A$, alors $[P\,[Q/x]]_{\mathsf{s}}^{\Gamma} = [P]_{\mathsf{s}}^{\Gamma, x:A} \circ \langle \mathsf{Id}_{\mathcal{I}([\Gamma]_{\mathsf{s}})}, [Q]_{\mathsf{s}}^{\Gamma} \rangle$.*

Preuve directe, par récurrence sur P.

Lemme 3.2.2 *Soient $M, M' \in \mathsf{PCF}$. Si $\Gamma \vdash M : A$ et $M\ \beta_{\mathsf{PCF}}\ M'$, alors $[M]_{\mathsf{s}}^{\Gamma} = [M']_{\mathsf{s}}^{\Gamma}$.*

Démonstration. Par récurrence sur M. Pour illustrer la structure de la preuve, on va traiter un seul cas.

Supposons que $M = \mathsf{if}(R, P, Q)$, on a donc $\Gamma \vdash R : \iota$, $\Gamma \vdash P : \iota$, $\Gamma \vdash Q : \iota$ et

$$[M]^\Gamma_\mathsf{s} = \mathsf{if}^\mathsf{s} \circ \langle [R]^\Gamma_\mathsf{s}, [P]^\Gamma_\mathsf{s}, [Q]^\Gamma_\mathsf{s} \rangle .$$

En se reportant à la définition de β_{PCF} en 3.1.2, on voit qu'il y a cinq cas à traiter :

– si $M' = \mathsf{if}(R', P, Q)$ avec $R \; \beta_{\mathsf{PCF}} \; R'$, alors on a, par hypothèse de récurrence, $[R']^\Gamma_\mathsf{s} = [R]^\Gamma_\mathsf{s}$ et donc

$$[M']^\Gamma_\mathsf{s} = \mathsf{if}^\mathsf{s} \circ \langle [R']^\Gamma_\mathsf{s}, [P]^\Gamma_\mathsf{s}, [Q]^\Gamma_\mathsf{s} \rangle = \mathsf{if}^\mathsf{s} \circ \langle [R]^\Gamma_\mathsf{s}, [P]^\Gamma_\mathsf{s}, [Q]^\Gamma_\mathsf{s} \rangle = [M]^\Gamma_\mathsf{s} \, ;$$

– si $M' = \mathsf{if}(R, P', Q)$ avec $P \; \beta_{\mathsf{PCF}} \; P'$, on raisonne de même ;

– si $M' = \mathsf{if}(R, P, Q')$ avec $Q \; \beta_{\mathsf{PCF}} \; Q'$, on raisonne de même ;

– si $R = \underline{0}$ et $M' = P$, on a, $[R]^\Gamma_\mathsf{s}(w) = \{0\}$ pour tout $w \in [\Gamma]_\mathsf{s}$ et donc

$$[M]^\Gamma_\mathsf{s}(w) = \mathsf{if}^\mathsf{s}_{[A]_\mathsf{s}}(\{0\}, [P]^\Gamma_\mathsf{s}(w), [Q]^\Gamma_\mathsf{s}(w) = [P]^\Gamma_\mathsf{s}(w)$$

et donc $[M]^\Gamma_\mathsf{s} = [P]^\Gamma_\mathsf{s} = [M']^\Gamma_\mathsf{s}$.

– si $R = \underline{n+1}$ et $M' = Q$, on raisonne de même.

Tout cela est plutôt long, ennuyeux et sans surprise, on peut se dispenser de vérifier les détails. . . □

Cela permet d'obtenir un résultat de «cohérence» du langage, qu'on pourrait aussi obtenir en utilisant la confluence de la réduction. Mais la méthode sémantique a l'avantage d'être très conceptuelle et modulaire (si on étend le langage, il suffit de trouver une interprétation pour la nouvelle primitive).

Corollaire 3.2.3 *Soit $M \in \mathsf{PCF}$ tel que $\Gamma \vdash M : \iota$ et soient $p, q \in \mathbb{N}$. Si $M \; \beta^*_{\mathsf{PCF}} \; \underline{p}$ et $M \; \beta^*_{\mathsf{PCF}} \; \underline{q}$, alors $p = q$.*

Démonstration. En effet, $[M]^\Gamma_\mathsf{s} : \mathcal{I}([\Gamma]_\mathsf{s}) \to \mathcal{I}(\mathbf{N}_\perp)$ est la fonction constante qui prend la valeur p, et aussi celle qui prend la valeur q. Donc $p = q$. □

Exercice* 3.2.4 Soit $M \in \mathsf{PCF}$ un terme clos tel que $\vdash M : (\iota \Rightarrow \iota) \Rightarrow \iota$ et soit $P \in \mathsf{PCF}$ un terme clos tel que $\vdash P : \iota \Rightarrow \iota$. On suppose que $(M)\,P$ (qui est clos et de type ι) se réduit en $\underline{n}$ (*i.e.* $(M)\,P \; \beta^*_{\mathsf{PCF}} \; \underline{n}$). Montrer qu'il existe une partie finie I de $\mathbb{N}$ telle que, pour tout terme de PCF clos P' tel que $\vdash P' : \iota$, si on a

$$\forall p \in I \, \forall k \in \mathbb{N} \quad (P)\,\underline{p} \; \beta^*_{\mathsf{PCF}} \; \underline{k} \Rightarrow (P')\,\underline{p} \; \beta^*_{\mathsf{PCF}} \; \underline{k}$$

alors, on a $(M)\,P' \; \beta^*_{\mathsf{PCF}} \; \underline{n}$. [*Indication:* Utiliser la sémantique de Scott !] Expliquer la signification intuitive de ce résultat.

3.2.4 Unicité des valeurs. Avant de pouvoir prouver le théorème d'adéquation de la prochaine section, il nous faut montrer que l'interprétation d'un terme clos de type ι ne peut prendre pour valeurs que des parties de $\mathbf{N}$ ayant au plus un élément. La valeur $\emptyset$ peut être prise, par un terme qui «boucle». C'est une façon de dire que le langage est «déterministe» (un terme ne peut prendre qu'une valeur). Cette vérification n'est pas nécessaire dans les modèles plus standard de PCF, où ι est interprété par le domaine plat des entiers naturels $\{\perp, 0, 1, 2, \ldots\}$ avec $\perp < n$ pour tout $n \in \mathbb{N}$ et $n \leq m$ si $n = m$ (voir [AC98]).

Par récurrence sur le type A, on définit $\mathcal{U}^A \subseteq \mathcal{I}([A]_\mathsf{s})$, l'ensemble des éléments *univalués* de type A.

$$\begin{array}{rcll} \mathcal{U}^\iota & = & \{\emptyset\} \cup \{\{n\} \mid n \in \mathbb{N}\} & \text{le domaine plat des entiers, justement} \\ \mathcal{U}^{A \Rightarrow B} & = & \{f \in \mathbf{PoC}(\mathcal{I}([A]_\mathsf{s}), \mathcal{I}([B]_\mathsf{s})) \mid f(\mathcal{U}^A) \subseteq \mathcal{U}^B\}. & \end{array}$$

Il s'agit donc encore d'une notion de réductibilité, purement sémantique celle-ci.

Lemme 3.2.4 *Pour tout type A, l'ensemble $\mathcal{U}^A$ contient $\emptyset$, et, muni de l'inclusion, est un cpo. De plus, si $u \in \mathcal{U}^A$ et $u' \in \mathcal{I}([A]_{\mathsf{s}})$ vérifient $u' \subseteq u$, alors $u' \in \mathcal{U}^A$.*

Démonstration. Pour $A = \iota$, la vérification est immédiate.

Supposons $A = B \Rightarrow C$, et que les propriétés à prouver sont vraies pour B et C. L'élément $\emptyset \in \mathcal{I}([A]_{\mathsf{s}})$ est la fonction qui envoie tout $u \in \mathcal{I}([B]_{\mathsf{s}})$ sur $\emptyset \in \mathcal{I}([C]_{\mathsf{s}})$. Comme $\emptyset \in \mathcal{U}^C$, on a $\emptyset \in \mathcal{U}^A$. Soit $\mathcal{D} \subseteq \mathcal{U}^A$ une partie filtrante pour l'inclusion. Soit $u \in \mathcal{U}^B \subseteq \mathcal{I}([B]_{\mathsf{s}})$. Alors $\mathcal{D}(u) = \{f(u) \mid f \in \mathcal{D}\}$ est une partie de $\mathcal{U}^C$ (par définition de $\mathcal{U}^A$) qui est filtrante pour l'inclusion (car $f \subseteq g \Rightarrow f(u) \subseteq g(u)$ pour $f, g \in \mathcal{I}([A]_{\mathsf{s}})$), et on a $\bigcup \mathcal{D}(u) \in \mathcal{U}^C$ par hypothèse de récurrence (appliquée à C). Or $\bigcup \mathcal{D}(u) = (\bigcup \mathcal{D})(u)$, et on a donc $\bigcup \mathcal{D} \in \mathcal{U}^A$. Enfin, soit $f \in \mathcal{U}^A$ et $f' \in \mathcal{I}([A]_{\mathsf{s}})$ telle que $f' \subseteq f$. Si $u \in \mathcal{U}^B$, on a $f'(u) \subseteq f(u) \in \mathcal{U}^C$, et donc $f'(u) \in \mathcal{U}^C$ par hypothèse de récurrence appliquée à C. □

Lemme 3.2.5 *Si $u, v, w \in \mathcal{U}^\iota$, alors $\mathsf{p}^{\mathsf{s}}(u), \mathsf{s}^{\mathsf{s}}(u), \mathsf{if}^{\mathsf{s}}(u, v, w) \in \mathcal{U}^\iota$.*

La preuve est immédiate.

Proposition 3.2.6 *Soit $\Gamma = (x_1 : A_1, \ldots, x_n : A_n)$ un contexte de typage. Si $\Gamma \vdash M : B$ et si $u_i \in \mathcal{U}^{A_i}$ pour $i = 1, \ldots, n$, alors $[M]_{\mathsf{s}}^{\Gamma} \in \mathcal{U}^B$. En particulier, si M est clos et de type ι, on a $[M]_{\mathsf{s}} \in \mathcal{U}^\iota$.*

Preuve facile, par récurrence sur M, en utilisant les lemmes 3.2.5 et 3.2.4.

Exercice* 3.2.5 Donner les détails de cette preuve.

3.3 Convergence dans PCF, préordre observationnel

On a vu que si M est un terme clos tel que $\vdash M : \iota$ et $M \ \beta^*_{\mathsf{PCF}} \ \underline{n}$, alors $[M]_{\mathsf{s}} = \{n\}$. On va d'abord prouver la réciproque, et en fait un résultat plus fort que la réciproque, puisqu'il conclut à la convergence pour la réduction de tête.

Théorème 3.3.1 *Soit M clos tel que $\vdash M : \iota$ et soit $n \in \mathbb{N}$. Si $[M]_{\mathsf{s}} = \{n\}$, alors $M \ \beta^*_{\mathsf{PCF,h}} \ \underline{n}$.*

La preuve, due à Plotkin (voir aussi [AC98]), est encore un bel exemple de réductibilité. On définit par induction sur le type A une relation $\mathcal{R}^A$ entre les éléments u de $\mathcal{U}^A$ et les termes *clos* M tels que $\vdash M : A$.

On a $u \ \mathcal{R}^\iota \ M$ si $u \in \mathcal{U}^\iota$, $\vdash M : \iota$ et

$$u = \emptyset \quad \text{ou} \quad (\exists n \in \mathbb{N} \ u = \{n\} \text{ et } M \ \beta^*_{\mathsf{PCF,h}} \ \underline{n})$$

On a $f \ \mathcal{R}^{B \Rightarrow C} \ M$ si $f \in \mathcal{U}^{B \Rightarrow C}$, $\vdash M : B \Rightarrow C$ et

$$\forall u, P \quad (u \in \mathcal{U}^B \ \text{ et } \vdash P : B \text{ et } u \ \mathcal{R}^B \ P) \Rightarrow f(u) \ \mathcal{R}^C \ (M) \, P\,.$$

Il faut d'abord prouver trois propriétés de cette relation, qui se démontrent toutes les trois par récurrence sur les types.

Lemme 3.3.2 *Pour tout type A, tout $u \in \mathcal{U}^A$, tous termes clos M, M' de type A, si $M \ \beta^*_{\mathsf{PCF,h}} \ M'$ et $u \ \mathcal{R}^A \ M'$, alors $u \ \mathcal{R}^A \ M$.*

Démonstration. Par récurrence sur le type A. Pour $A = \iota$, c'est évident (transitivité de le relation $\beta^*_{\mathsf{PCF,h}}$). Soient donc $f \in \mathcal{U}^{B\Rightarrow C}$ et M, M' clos de type $B \Rightarrow C$ et tels que $M\ \beta^*_{\mathsf{PCF,h}}\ M'$ et $f\ \mathcal{R}^{B\Rightarrow C}\ M'$. On doit montrer que $f\ \mathcal{R}^{B\Rightarrow C}\ M$; soient donc $u \in \mathcal{U}^B$ et P clos tels que $u\,\mathcal{R}^B\ P$, il faut voir que $f(u)\ \mathcal{R}^C\ (M)\,P$. Or on a $f(u)\ \mathcal{R}^C\ (M)\,P$, et on conclut par hypothèse de récurrence, puisque $(M)\,P\ \beta^*_{\mathsf{PCF,h}}$ $(M')\,P$ (voir paragraphe 3.1.3). □

Lemme 3.3.3 *Pour tout type A et tout terme clos de type A, on a $\emptyset\ \mathcal{R}^A\ M$.*

La preuve est immédiate, par récurrence sur A (car $\emptyset \in \mathcal{U}^{B\Rightarrow C}$ est la fonction qui envoie tout $u \in \mathcal{I}([B]_{\mathsf{s}})$ sur $\emptyset$).

Lemme 3.3.4 *Pour tout type A, tout terme clos M de type A, et toute suite $(u_n)_{n\in\mathbb{N}}$ croissante d'éléments de $\mathcal{U}^A$,*

$$(\forall n \in \mathbb{N} \quad u_n\ \mathcal{R}^A\ M) \Rightarrow \left(\bigcup_{n=0}^{\infty} u_n\right) \mathcal{R}^A\ M\,.$$

Démonstration. Par récurrence sur A. On suppose qu'on a $u_n\ \mathcal{R}^A\ M$ pour tout $n \in \mathbb{N}$.

Quand $A = \iota$, c'est évident, car la suite $(u_n)_{n\in\mathbb{N}}$ est stationnaire, vu qu'elle est croissante et ne peut prendre pour valeurs que $\emptyset$ ou des singletons (par définition de $\mathcal{U}^\iota$).

Supposons $A = B \Rightarrow C$. Soit $(f_n)_{n\in\mathbb{N}}$ une suite croissante d'éléments de $\mathcal{U}^{B\Rightarrow C}$ et M un terme clos de type $B \Rightarrow C$ tel que $f_n\ \mathcal{R}^{B\Rightarrow C}\ M$ pour tout $n \in \mathbb{N}$. On doit montrer que $(\bigcup_{n=0}^{\infty} f_n)\ \mathcal{R}^{B\Rightarrow C}\ M$. Soient donc $u \in \mathcal{U}^B$ et P un terme clos de type B tels que $u\ \mathcal{R}^B\ P$. Pour chaque n, on a $f_n(u)\ \mathcal{R}^C\ (M)\,P$. Par hypothèse de récurrence, on a $\bigcup_{n=0}^{\infty} f_n(u)\ \mathcal{R}^C\ (M)\,P$, c'est-à-dire $(\bigcup_{n=0}^{\infty} f_n)(u)\ \mathcal{R}^C\ (M)\,P$. □

On peut maintenant prouver le lemme d'adéquation.

Lemme 3.3.5 (adéquation) *Soit $\Gamma = (x_1 : A_1, \ldots, x_p : A_p)$ un contexte de typage, soit M un terme de* PCF *et B un type tels que $\Gamma \vdash M : B$. Soient $N_1,\ldots,N_p$ des termes clos de types respectifs $A_1,\ldots,A_p$. Soient $u_1 \in \mathcal{U}^{A_1},\ldots,u_p \in \mathcal{U}^{A_p}$. Si $u_j\ \mathcal{R}^{A_j}\ N_j$ pour $j = 1, \ldots, p$. On a*

$$[M]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p)\ \mathcal{R}^B\ M\,[N_1/x_1, \ldots, N_p/x_p]\ .$$

Démonstration. Par récurrence sur la dérivation de typage menant à $\Gamma \vdash M : B$ (c'est-à-dire, par récurrence sur M). Comme d'habitude, si R est un terme, on note R' le terme $R\,[N_1/x_1, \ldots, N_p/x_p]$.

On laisse la plupart des cas au lecteur ; on va seulement traiter les trois plus intéressants.

Supposons d'abord $M = \mathsf{if}(R, P, Q)$ avec $\Gamma \vdash R : \iota, \Gamma \vdash P : \iota$ et $\Gamma \vdash Q : \iota$. On doit montrer que $[M]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p)\ \mathcal{R}^\iota\ M'$. On sait que $[M]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p) \in \mathcal{U}^\iota$ (proposition 3.2.6). Si $[M]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p) = \emptyset$, il n'y a rien à prouver. Si $[M]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p) = \{n\}$, on a $[R]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p) \neq \emptyset$, et donc $[R]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p) = \{r\}$ pour un $r \in \mathbb{N}$ (puisque $[R]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p) \in \mathcal{U}^\iota$). Si $r = 0$, c'est que $[P]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p) = \{n\}$. Par hypothèse de récurrence, on a $\{0\}\ \mathcal{R}^\iota\ R'$ et $\{n\}\ \mathcal{R}^\iota\ P'$, et donc $R'\ \beta^*_{\mathsf{PCF,h}}\ \underline{0}$ et $P'\ \beta^*_{\mathsf{PCF,h}}\ \underline{n}$, par définition de la relation $\mathcal{R}^\iota$. Par suite $M'\ \beta^*_{\mathsf{PCF,h}}\ \underline{n}$, ce qu'il fallait prouver, puisque $[M]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p) = \{n\}$. Si $r \neq 0$, on raisonne de même.

Supposons ensuite $M = \lambda x^B\,P$ avec $\Gamma, x : B \vdash P : C$. Il faut montrer que

$$[\lambda x^B\,P]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p)\ \mathcal{R}^{B\Rightarrow C}\ \lambda x^B\,P'\,.$$

Soient donc $v \in \mathcal{U}^B$ et N clos de type B tels que $v\ \mathcal{R}^B\ N$. Il faut montrer que $[\lambda x^B\, P]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p)(v)\ \mathcal{R}^{B\Rightarrow C}\ \left(\lambda x^B\, P'\right) N$. Or, par hypothèse de récurrence, on a $[P]^{\Gamma,x:B}_{\mathsf{s}}(u_1, \ldots, u_p, v)\ \mathcal{R}^C\ P'\,[N/x]$. On conclut, car on a $[\lambda x^B\, P]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p)(v) = [P]^{\Gamma,x:B}_{\mathsf{s}}(u_1, \ldots, u_p, v)$, et en utilisant le lemme 3.3.2, puisque $\left(\lambda x^B\, P'\right) N\ \beta^*_{\mathsf{PCF,h}}\ P'\,[N/x]$.

Supposons pour finir que $M = \mathsf{fix}(P)$, avec $\Gamma \vdash P : A \Rightarrow A$. On doit montrer que

$$[\mathsf{fix}(P)]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p)\ \mathcal{R}^A\ \mathsf{fix}(P')\,.$$

Soit $f = [P]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p) \in \mathcal{U}^{A\Rightarrow A}$ (proposition 3.2.6), et par suite $f^n(\emptyset) \in \mathcal{U}^A$ pour tout n. Et on a

$$[\mathsf{fix}(P)]^\Gamma_{\mathsf{s}}(u_1, \ldots, u_p) = \bigcup_{n=0}^{\infty} f^n(\emptyset) \in \mathcal{U}^A\ .$$

Par le lemme 3.3.4, il suffit de montrer que $f^n(\emptyset)\ \mathcal{R}^A\ \mathsf{fix}(P')$ pour tout $n \in \mathbb{N}$. On le montre par récurrence[1] sur n.

Pour $n = 0$, cela résulte du lemme 3.3.3. On suppose donc $n > 0$. Par le lemme 3.3.2, il suffit de montrer que

$$f^n(\emptyset)\ \mathcal{R}^A\ (P')\,\mathsf{fix}(P')$$

puisque $\mathsf{fix}(P')\ \beta^*_{\mathsf{PCF,h}}\ (P')\,\mathsf{fix}(P')$. Or, par hypothèse de récurrence (dans la récurrence interne, sur les entiers), on a $f^{n-1}(\emptyset)\ \mathcal{R}^A\ \mathsf{fix}(P')$, et par hypothèse de récurrence (dans la récurrence externe, sur les termes), on a $f\ \mathcal{R}^{A\Rightarrow A}\ P'$, et donc $f(f^{n-1}(\emptyset))\ \mathcal{R}^A\ (P')\,\mathsf{fix}(P')$. □

On peut en déduire le résultat suivant, exprimant que la réduction de tête mène toujours au résultat, quand il y en a un.

Théorème 3.3.6 *Soient M un terme clos de* PCF *tel que $\vdash M : \iota$ et $n \in \mathbb{N}$ tel que $M\ \beta^*_{\mathsf{PCF}}\ \underline{n}$. Alors $M\ \beta^*_{\mathsf{PCF,h}}\ \underline{n}$.*

3.3.1 Equivalence observationnelle et pleine adéquation. Soient M et N deux termes de PCF clos de type $A = B_1 \Rightarrow (B_2 \Rightarrow \cdots (B_p \Rightarrow \iota))$. On écrira $M \sqsubseteq_{\mathrm{obs}} N$ si, pour tout terme clos C de type $A \Rightarrow \iota$, on a

$$\forall n \in \mathbb{N} \quad (C)\,M\ \beta^*_{\mathsf{PCF,h}}\ \underline{n} \Rightarrow (C)\,N\ \beta^*_{\mathsf{PCF,h}}\ \underline{n}\,.$$

Clairement, $\sqsubseteq_{\mathrm{obs}}$ est une relation de préordre sur les termes clos de type A.

Le résultat suivant est purement syntaxique, nous l'admettrons. Il exprime que, dans la définition ci-dessus de la relation $\sqsubseteq_{\mathrm{obs}}$, on peut se contenter de considérer des C (contextes) d'une forme particulière.

Théorème 3.3.7 (lemme du contexte) *Si, pour tous termes clos $N_1, \ldots, N_p$ de types $B_1, \ldots, B_p$, on a*

$$\forall n \in \mathbb{N} \quad (M)\,N_1 \ldots N_p\ \beta^*_{\mathsf{PCF,h}}\ \underline{n} \Rightarrow (N)\,N_1 \ldots N_p\ \beta^*_{\mathsf{PCF,h}}\ \underline{n}\,,$$

alors $M \sqsubseteq_{\mathrm{obs}} N$.

On a alors le résultat suivant, qui relie cette relation de préordre observationnel $\sqsubseteq_{\mathrm{obs}}$ avec la relation d'ordre du modèle.

[1] C'est donc une preuve par récurrence à l'intérieur de l'étape de récurrence dans la preuve par récurrence sur les termes que nous sommes en train de développer. Dans la suite, on appellera la première *interne* et la seconde *externe*.

Théorème 3.3.8 *Soient M et N des termes clos de type A. Si $[M]_{\mathsf{s}} \subseteq [N]_{\mathsf{s}}$, alors $M \sqsubseteq_{\mathrm{obs}} N$.*

Démonstration. On suppose que $[M]_{\mathsf{s}} \subseteq [N]_{\mathsf{s}}$. Soient $N_1, \ldots, N_p$ des termes clos de type $B_1, \ldots, B_p$. On suppose que $(M)\, N_1 \ldots N_p\ \beta^*_{\mathsf{PCF,h}}\ \underline{n}$. Alors $[(M)\, N_1 \ldots N_p]_{\mathsf{s}} = \{n\}$ (invariance de la sémantique, paragraphe 3.1.4), c'est-à-dire qu'on a l'égalité $[M]_{\mathsf{s}}([N_1]_{\mathsf{s}}) \ldots ([N_p]_{\mathsf{s}}) = \{n\}$, et donc $[N]_{\mathsf{s}}([N_1]_{\mathsf{s}}) \ldots ([N_p]_{\mathsf{s}}) = \{n\}$ (puisque $[M]_{\mathsf{s}} \subseteq [N]_{\mathsf{s}}$), c'est-à-dire $[(N)\, N_1 \ldots N_p]_{\mathsf{s}} = \{n\}$. Par le théorème 3.3.1, on a $(N)\, N_1 \ldots N_p\ \beta^*_{\mathsf{PCF,h}}\ \underline{n}$. On conclut par le théorème 3.3.7. □

Soit $\simeq_{\mathrm{obs}}$ la relation d'équivalence induite par la relation de préordre $\sqsubseteq_{\mathrm{obs}}$. On a donc $[M]_{\mathsf{s}} = [N]_{\mathsf{s}} \Rightarrow M \simeq_{\mathrm{obs}} N$, pour tous M et N clos de même type. Si la réciproque était vraie, on dirait que le modèle de Scott de PCF est *pleinement adéquat* (*fully abstract*). La recherche de modèles pleinement adéquats de PCF a été l'une des grandes occupations des spécialistes de sémantique dénotationnelle. Les catégories de *jeux* ont permis d'en construire.

3.3.2 Le modèle de Scott de PCF n'est pas pleinement adéquat. On définit une fonction $\mathsf{por} \in \mathbf{PoC}(\mathbf{N}^2, \mathbf{N})$, c'est la fonction $\mathsf{Fun}(t)$, où

$$t = \{((x, y), 0) \mid 0 \in x \cup y\} \cup \{((x, y), 1) \mid 1 \in x \cap y\}$$

C'est clairement une fonction Scott-continue, et c'est donc bien un élément de $\mathbf{PoC}(\mathbf{N}^2, \mathbf{N})$. De plus, on vérifie facilement que $\mathsf{por} \in \mathcal{U}^{\iota \Rightarrow \iota \Rightarrow \iota}$.

On appelle la fonction por le *ou parallèle* car elle est capable de détecter si un de ses deux arguments est égal à 0, même si l'autre ne converge pas. Pour faire cela, il faut pouvoir évaluer «en parallèle» les deux arguments, ce que, intuitivement, un terme de PCF ne peut pas faire.

Cet élément non définissable est cause de non plein adéquation. Soit en effet

$$\mathsf{porg} = \lambda f^{\iota \Rightarrow \iota \Rightarrow \iota}\, \mathsf{if}((f)\, \underline{0}\, \Omega, \mathsf{if}((f)\, \Omega\, \underline{0}, \mathsf{if}((f)\, \underline{1}\, \underline{1}, \Omega, \underline{0}), \Omega), \Omega)$$

où, par exemple, $\Omega = \mathsf{fix}(\lambda u^{\iota}\, u)$, et donc $[\Omega]_{\mathsf{s}} = \emptyset$. C'est un terme clos de type $(\iota \Rightarrow \iota \Rightarrow \iota) \Rightarrow \iota$ et il est facile de voir que $[\mathsf{porg}]_{\mathsf{s}}(\mathsf{por}) = \{0\}$.

Cependant, il est facile de montrer que, dans le modèle des *espace cohérents*, où le langage PCF peut aussi être interprété, la sémantique de porg est $\emptyset$, car il n'y a pas de fonction stable qui envoie $(\{0\}, \emptyset)$ et $(\emptyset, \{0\})$ sur $\{0\}$ et $(\{1\}, \{1\})$ sur $\{1\}$ (on interprète le type des entiers par l'espace cohérent dont la trame est $\mathbb{N}$, avec la cohérence discrète).

Or le modèle des espaces cohérents satisfait aussi le théorème d'adéquation de Plotkin (preuve identique), et par suite $\mathsf{porg} \simeq_{\mathrm{obs}} \lambda f\, \Omega$ alors que ces deux termes ont des sémantiques de Scott différentes.

Mais le modèle des espaces cohérents n'est pas non plus pleinement adéquat (il a ses propres «passagers clandestins», comme le ou parallèle de la sémantique de Scott)...

Exercice* **3.3.1** Montrer, de la façon la plus simple possible, que $[\Omega]_{\mathsf{s}} = \emptyset$.

Chapitre 4

Quelques aspects quantitatifs

La sémantique de Scott développée jusqu'ici est «qualitative», suivant la terminologie de Girard. Dans ce modèle, l'interprétation d'un programme décrit les informations nécessaires au calcul, mais pas le nombre de fois qu'elles sont utilisées pour obtenir un résultat donné.

Considérons par exemple les deux programmes de PCF

$$\begin{aligned} P_1 &= \lambda x^\iota\, \mathsf{if}(x, \underline{0}, \Omega) : \iota \Rightarrow \iota \\ P_2 &= \lambda x^\iota\, \mathsf{if}(x, \mathsf{if}(x, \underline{0}, \Omega), \Omega) : \iota \Rightarrow \iota \end{aligned}$$

dans lequel Ω est un terme clos de type ι et de sémantique $\emptyset$ (par exemple $\Omega = \mathsf{fix}(\lambda y^\iota\, y)$). On vérifie facilement que P_1 et P_2 ont la même sémantique de Scott $[P_1]_{\mathsf{s}} = [P_2]_{\mathsf{s}} = \{(u, 0) \mid u \in \mathbf{!N},\ 0 \in u\}$ alors qu'ils diffèrent par le nombre de fois qu'ils utilisent leur argument x entier.

On commence par introduire la sémantique relationnelle "pure", dans laquelle les types sont interprétés par des ensembles, et les preuves, par des relations entre ces ensembles. Dans ce modèle, l'exponentielle est interprétée au moyen de multi-ensembles finis (et non d'ensembles finis), et rend compte de la différence entre P_1 et P_2. En ce sens, c'est une sémantique «quantitative».

4.1 Sémantique relationnelle de LL

Soit **Rel** la catégorie dont les objets sont les ensembles, et telle que $\mathbf{Rel}(X, Y) = \mathcal{P}(X \times Y)$, la composition étant définie de façon relationnelle. Plus précisément,

$$\mathsf{Id}_X = \{(a, a) \mid a \in X\}$$

et, si $s \in \mathbf{Rel}(X, Y)$ et $t \in \mathbf{Rel}(Y, Z)$, alors

$$t \cdot s = \{(a, c) \in X \times Z \mid \exists b \in Y\, (a, b) \in s \text{ et } (b, c) \in t\}\,.$$

Si on voit s et t comme des matrices (d'incidence) à coefficients dans $\{0, 1\}$, cette composition peut être vue comme un simple produit de matrices.

4.1.1 Structure monoïdale. Le produit tensoriel de deux ensembles X et Y dans **Rel** est leur produit cartésien au sens ensembliste habituel : $X \otimes Y = X \times Y$. Le produit tensoriel des morphismes est défini comme dans la catégorie **PoLR**. Si $s_i \in \mathbf{Rel}(X_i, Y_i)$ pour $i = 1, 2$, alors $s_1 \otimes s_2 \in \mathbf{Rel}(X_1 \otimes X_2, Y_1 \otimes Y_2)$ est donné par

$$s_1 \otimes s_2 = \{((a_1, a_2), (b_1, b_2)) \mid (a_i, b_i) \in s_i \text{ pour } i = 1, 2\}\,.$$

On voit facilement que c'est une opération fonctorielle, et que les isomorphismes d'associativité et de symétrie (et d'élémément neutre) du produit cartésien sont des isomorphismes dans la catégorie **Rel** qui satisfont les axiomes de catégorie monoïdale symétrique. L'objet neutre du produit tensoriel est bien sûr le singleton $1 = \{*\}$.

Exercice* 4.1.1 Montrer que les isomorphismes dans **Rel** sont les bijections.

On définit également $X \multimap Y = X \times Y$, et alors il est facile de voir que $X \multimap Y$ est l'objet des morphismes de X vers Y, l'évaluation linéaire $\mathsf{ev} \in \mathbf{Rel}((X \multimap Y) \otimes X, Y)$ étant donnée par

$$\mathsf{ev} = \{(((a,b),a),b) \mid (a,b) \in X \times Y\}\,.$$

On vérifie facilement que **Rel**, muni de ce produit tensoriel est symétrique monoïdale fermée. C'est une catégorie étoile-autonome : on prend $\perp = 1$ comme objet dualisant, et la négation linéaire $X^\perp$ est X.

Si $s \in \mathbf{Rel}(X,Y)$, le morphisme *transposé* ${}^{\mathsf{t}}s \in \mathbf{Rel}(Y^\perp, X^\perp) = \mathcal{P}(Y \times X)$ est

$${}^{\mathsf{t}}s = \{(b,a) \in Y \times X \mid (a,b) \in s\}\,.$$

4.1.2 Produits et coproduits. Soit $(X_i)_{i \in I}$ une famille d'ensembles. Soit $\&_{i \in I} X_i = \bigcup_{i \in I}(\{i\} \times X_i)$. Cet ensemble est le produit des X_i dans la catégorie **Rel**, avec les projections

$$\pi_i = \{((i,a),a) \mid a \in X_i\} \in \mathbf{Rel}\left(\mathop{\&}_{j \in I} X_j, X_i\right)$$

Si $s_i \in \mathbf{Rel}(Y, X_i)$ est une famille de morphismes dans **Rel**, le morphisme $\langle s_i \rangle_{i \in I} \in \mathbf{Rel}\left(Y, \&_{i \in I} X_i\right)$ est donné par

$$\langle s_i \rangle_{i \in I} = \{(b,(i,a)) \mid i \in I \text{ et } (b,a) \in s_i\}\,.$$

Exercice* 4.1.2 Vérifier que la propriété universelle du produit cartésien est bien satisfaite. Autrment dit, $\langle s_i \rangle_{i \in I}$ est l'unique élément t de $\mathbf{Rel}\left(Y, \&_{i \in I} X_i\right)$ tel que $\pi_i \cdot t = s_i$ pour tout $i \in I$.

Puisque la négation linéaire $X \mapsto X^\perp$ est l'identité sur les objets, $\&_{i \in I} X_i$ est aussi le coproduit des X_i dans la catégorie **Rel**.

4.1.3 Exponentielles. Soit X un ensemble. On pose $!X = \mathcal{M}_{\mathrm{fin}}(X)$, l'ensemble des *multi-ensembles* finis d'éléments de X. Un élément de $\mathcal{M}_{\mathrm{fin}}(X)$ est donc une fonction $m : X \to \mathbb{N}$ telle que $m(a) = 0$ pour tous les éléments de X sauf un nombre fini d'entre eux. On note 0 le multi-ensemble vide (tel que $0(a) = 0$ pour tout $a \in X$). On note $m + m'$ la somme des multi-ensembles m et m', définie par $(m+m')(a) = m(a) + m'(a)$. Enfin, $|m|$ dénote l'ensemble des $a \in X$ tels que $m(a) \neq 0$, on appel cet ensemble le *support* de m, il est fini. On appelle *cardinal* de m le nombre d'éléments $\#m$ de m, en tenant compte des multiplicités. Autrement dit, $\#m = \sum_{a \in X} m(a) \in \mathbb{N}$.

Soit $x \subseteq X$. On note $x^!$ l'ensemble $\mathcal{M}_{\mathrm{fin}}(x) \subseteq\, !X$; c'est le *promu* de x. Si $s \in \mathbf{Rel}(X,Y)$, on pose

$$!s = \{([a_1,\dots,a_n],[b_1,\dots,b_n]) \mid n \in \mathbb{N} \text{ et } (a_i,b_i) \in s \text{ pour tout } i\}\,.$$

Autrement dit, un couple $(m,p) \in\, !X \times !Y$ appartient à $!s$ si les deux multi-ensembles m et p ont même cardinal n, et peuvent s'écrire $m = [a_1,\dots,a_n]$ et $p = [b_1,\dots,b_n]$ avec $(a_i,b_i) \in s$ pour tout i.

Lemme 4.1.1 *L'opération* $!\_$ *est un foncteur. De plus, si* $s \in \mathbf{Rel}(X,Y)$ *et* $x \subseteq X$, *on a* $!s \cdot x^! = (s \cdot x)^!$.

La déréliction et le digging sont définis par

$$\begin{aligned} \mathsf{d}_X &= \{([a], a) \mid a \in X\} \in \mathbf{Rel}(!X, X) \\ \mathsf{p}_X &= \{(m_1 + \cdots + m_n, [m_1, \ldots, m_n]) \mid m_1, \ldots, m_n \in !X\} \in \mathbf{Rel}(!X, !!X)\,. \end{aligned}$$

Lemme 4.1.2 *Ces deux morphismes sont des transformations naturelles, et font de* $!\_$ *une comonade. On rappelle que ça signifie que les trois équations suivantes sont satisfaites :*

$$\begin{aligned} \mathsf{d}_{!S} \cdot \mathsf{p}_S &= \mathsf{Id}_{!S} \\ !\mathsf{d}_S \cdot \mathsf{p}_S &= \mathsf{Id}_{!S} \\ \mathsf{p}_{!S} \cdot \mathsf{p}_S &= !\mathsf{p}_S \cdot \mathsf{p}_S\,. \end{aligned}$$

Exercice* **4.1.3** Prouver ces deux lemmes.

Soient X et Y deux ensembles. La fonction

$$\begin{aligned} !(X \mathbin{\&} Y) &\to !X \otimes !Y \\ [(1,a_1), \ldots, (1,a_p), (2,b_1), \ldots, (2,b_q)] &\mapsto ([a_1, \ldots, a_p], [b_1, \ldots, b_q]) \end{aligned}$$

définit une bijection, et donc un isomorphisme (dans **Rel**) de $!(X \mathbin{\&} Y)$ vers $!X \otimes !Y$.

4.1.4 Catégorie de Kleisli. Elle est défine comme en 2.6.5, on la note $\mathbf{Rel}_{\mathsf{K}}$. Un objet de $\mathbf{Rel}_{\mathsf{K}}$ est un ensemble, et $\mathbf{Rel}_{\mathsf{K}}(X,Y) = \mathbf{Rel}(!X,Y)$. Contrairement à ce qui se passait dans $\mathbf{PoLR}_{\mathsf{K}}$, il n'est pas possible de voir les éléments de $\mathbf{Rel}_{\mathsf{K}}(X,Y)$ comme des fonctions (du moins, pas directement). On rappelle que l'identité en X est $\mathsf{d}_X \in \mathbf{Rel}_{\mathsf{K}}(X,X)$ et que la composition de $s \in \mathbf{Rel}_{\mathsf{K}}(X,Y)$ et de $t \in \mathbf{Rel}_{\mathsf{K}}(Y,Z)$ est

$$t \circ^{\mathsf{K}} s = t \cdot !s \cdot \mathsf{p}_s\,.$$

Exercice* **4.1.4** Soient $m \in !X$ et $c \in Z$. Montrer que $(m,c) \in t \circ^{\mathsf{K}} s$ si et seulement si on peut trouver $(m_1,b_1), \ldots, (m_n,b_n) \in s$ tels que $m_1 + \cdots + m_n = m$ et $([b_1, \ldots, b_n], c) \in t$.

Comme en 2.6.5, on voit facilement que $\mathbf{Rel}_{\mathsf{K}}$ est cartésienne fermée. Le produit cartésien d'une famille $(X_i)_{i \in I}$ d'ensembles est $X = \&_{i \in I} X_i$, avec les projections $\pi_i \cdot \mathsf{d}_X \in \mathbf{Rel}_{\mathsf{K}}(\&_{i \in I} X_i, X_i)$. L'objet des morphismes de X vers Y est $X \Rightarrow Y = !X \multimap Y$, avec comme morphisme d'évaluation $\mathsf{Ev} \in \mathbf{Rel}(!(X \Rightarrow Y) \otimes !X, Y)$ (indentifiant $!((X \Rightarrow Y) \mathbin{\&} X)$ et $!(X \Rightarrow Y) \otimes !X$) est donné par

$$\mathsf{Ev} = \{((([(m,b)], m), b) \mid m \in !X \text{ et } b \in Y\}\,.$$

4.1.5 Um modèle du lambda-calcul pur. Il est très facile de construire un modèle du lambda-calcul pur (beta et eta) dans la catégorie $\mathbf{Rel}_{\mathsf{K}}$. On construit une suite d'ensembles $(D_n)_{n \in \mathbb{N}}$ en posant

$$\begin{aligned} D_0 &= \emptyset \\ D_{n+1} &= \mathcal{M}_{\mathrm{fin}}(\mathbb{N} \times D_n)\,. \end{aligned}$$

Cette suite d'ensembles est croissante, et on pose $D_\infty = \bigcup_{n=0}^{\infty} D_n$.

Autrement dit, D_∞ est le plus petit ensemble qui a la propriété suivante : pour toute famille $\vec{m} = (m_n)_{n \in \mathbb{N}}$ telle que $m_n \in \mathcal{M}_{\mathrm{fin}}(D_\infty)$ pour tout $n \in \mathbb{N}$ et $m_n = 0$ pour presque tout n, on a $\vec{m} \in D_\infty$. On a une bijection évidente entre $\mathcal{M}_{\mathrm{fin}}(D_\infty) \times D_\infty$ et D_∞ (qui envoie le couple $(p, \vec{m})$ sur $\vec{p} \in D_\infty$ donné par $p_0 = p$ et $p_{n+1} = m_n$). C'est un isomorphisme (dans $\mathbf{Rel}_{\mathsf{K}}$) de $D_\infty \Rightarrow D_\infty$ vers D_∞.

4.2 Calcul avec ressources

Puisque notre modèle tient compte des mutiplicités, il semble naturel de cherche une syntaxe dans laquelle les multiplicités soient également explicites. C'est le cas du *lambda-calcul avec ressources* que nous introduisons maintenant, et qui nous servira à «approximer» les lambda-termes ordinaires. C'est un langage qui se situe en quelque sorte à l'interface entre la syntaxe et la sémantique.

4.2.1 SYNTAXE. On travaille avec le même variables que pour le lambda-calcul pur. On définit les *termes simples* comme suit.

- Si x est une variable, x est un terme simple.
- Si x est une variable et s est un terme simple, $\lambda x\, s$ est un terme simple.
- Si s est un terme simple et si T est un multiensemble fini de termes simples, alors $\langle s\rangle\, T$ est un terme simple.

Les termes simples sont considérés systématiquement à alpha-conversion près.

On note Δ l'ensemble des termes simples et $\Delta^!$ l'ensemble des multi-sensembles de termes simples, qu'on appellera aussi *poly-termes*.

Un *terme avec ressources* est alors un ensemble (fini ou non) de termes simples. On note ces termes $\overline{s}$, $\overline{t}$, etc.

4.2.2 NOTATION. On écrira parfois $t_1 \cdots t_n$ pour dénoter le poly-terme $[t_1, \ldots, t_n]$ et 1 pour dénoter le poly-terme vide $[]$.

4.2.3 CONVENTION. On considère implicitement tout terme simple s comme le terme avec ressources $\{s\}$. On étend aux termes avec ressources les constructions définies pour les termes simples, par «linéarité» :

$$\begin{aligned} \lambda x\, \overline{s} &= \{\lambda x\, s \mid s \in \overline{s}\} \\ \langle \overline{s}\rangle\, [\overline{t_1}, \ldots, \overline{t_n}] &= \{\langle s\rangle\, [t_1, \ldots, t_n] \mid s \in \overline{s} \text{ et } \forall i\, t_i \in \overline{t_i}\} \end{aligned}$$

4.2.4 SUBSTITUTION ATOMIQUE. On définit une notion de substitution atomique, qui remplace, dans un terme simple *une occurrence* de variable par un terme avec ressources. Comme il y a plusieurs façons de faire, le résultat est un ensemble, c'est-à-dire, un terme avec ressources. Soient $\overline{t}$ un terme avec ressources et x une variable. Alors $\frac{\partial s}{\partial x} \cdot \overline{t}$ est défini par récurrence sur s :

$$\begin{aligned} \frac{\partial y}{\partial x} \cdot \overline{t} &= \begin{cases} \overline{t} & \text{si } y = x \\ \emptyset & \text{sinon} \end{cases} \\ \frac{\partial \lambda y\, s}{\partial x} \cdot \overline{t} &= \lambda y \left(\frac{\partial s}{\partial x} \cdot \overline{t} \right) \\ \frac{\partial \langle s\rangle\, [s_1, \ldots, s_n]}{\partial x} \cdot \overline{t} &= \left\langle \frac{\partial s}{\partial x} \cdot \overline{t} \right\rangle [s_1, \ldots, s_n] \\ &\quad \cup \langle s\rangle\, [\frac{\partial s_1}{\partial x} \cdot \overline{t}, s_2, \ldots, s_n] \cup \cdots \cup \langle s\rangle\, [s_1, \ldots, s_{n-1}, \frac{\partial s_n}{\partial x} \cdot \overline{t}] \end{aligned}$$

Bien noter qu'on utilise fortement la convention 4.2.3 dans cette définition.

Autrement dit, et compte tenu de la convention 4.2.3, si $x_1, \ldots, x_n$ sont les différentes occurrences de x dans s, on a

$$\frac{\partial s}{\partial x} \cdot \overline{t} = \{s\, [t/x_i] \mid i = 1, \ldots, n \text{ et } t \in \overline{t}\}$$

et donc les éléments de $\frac{\partial s}{\partial x} \cdot t$ ont $n - 1$ occurrences de x (si on suppose que t n'a aucune occurrence libre de x).

On étend par linéarité cette opération à tous les termes avec ressources $\overline{s}$:

$$\frac{\partial \overline{s}}{\partial x} \cdot \overline{t} = \bigcup_{s \in \overline{s}} \frac{\partial s}{\partial x} \cdot \overline{t}\,.$$

Lemme 4.2.1 *La substitution atomique est bilinéaire, c'est-à-dire que*

$$\frac{\partial}{\partial x}\Big(\bigcup_{i\in I} \overline{u_i}\Big) \cdot \left(\bigcup_{j \in J} \overline{v_j}\right) = \bigcup_{(i,j)\in I\times J} \frac{\partial \overline{u_i}}{\partial x} \cdot \overline{v_j}$$

Démonstration. Il suffit de montrer que $\frac{\partial u}{\partial x} \cdot \left(\bigcup_{j\in J} \overline{v_j}\right) = \bigcup_{j\in J} \frac{\partial u}{\partial x} \cdot \overline{v_j}$, ce qui est immédiat, par récurrence sur u. □

Lemme 4.2.2 *Si x n'apparaît pas libre dans $\overline{u}$ (c'est-à-dire, dans aucun des éléments de $\overline{u}$), alors $\frac{\partial \overline{u}}{\partial x} \cdot \overline{v} = \emptyset$.*

Démonstration. Il suffit de le montrer pour $\overline{u}$ simple, et on le fait par une récurrence immédiate sur u. □

Lemme 4.2.3 *Soient $\overline{s}$, $\overline{u}$ et $\overline{v}$ des termes avec ressources et soient x et y des variables (distinctes ou non). On suppose que x n'apparaît pas libre dans $\overline{v}$. On a*

$$\frac{\partial}{\partial y}\Big(\frac{\partial s}{\partial x} \cdot \overline{u}\Big) \cdot \overline{v} = \frac{\partial}{\partial x}\Big(\frac{\partial s}{\partial y} \cdot \overline{v}\Big) \cdot \overline{u} \cup \frac{\partial s}{\partial x} \cdot \left(\frac{\partial \overline{u}}{\partial y} \cdot \overline{v}\right)$$

Exercice* 4.2.1 Prouver ce lemme (récurrence sur s).

4.2.5 Réduction à petit pas. Soit s un terme simple et $\overline{u}$ un terme avec ressources. Par récurrence sur s, on décrit quand $s\ \beta_p\ \overline{u}$.

- Si s est une variable, on n'a jamais $s\ \beta_p\ \overline{u}$.
- Si $s = \lambda x\, t$, on a $s\ \beta_p\ \overline{u}$ si $\overline{u} = \lambda x\, \overline{v}$ et $t\ \beta_p\ \overline{v}$.
- Si $s = \langle t\rangle\, T$ (avec $T = [t_1, \ldots, t_n]$), on a $s\ \beta_p\ u$ dans l'un des cas suivants :
  - $\overline{u} = \langle \overline{v}\rangle\, T$ avec $t\ \beta_p\ \overline{v}$;
  - il existe $i \in \{1, \ldots, n\}$ tel que $\overline{u} = \langle t\rangle\, [t_1, \ldots, t_{i-1}, \overline{v_i}, t_{i+1}, \ldots, t_n]$ avec $t_i\ \beta_p\ \overline{v_i}$;
  - $t = \lambda x\, w$ et il existe $i \in \{1, \ldots, n\}$ tel que

$$\overline{u} = \left\langle \lambda x \left(\frac{\partial w}{\partial x} \cdot t_i\right)\right\rangle [t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n]$$

Dans le dernier cas, on dit que s est un *redex* et que $\overline{u}$ est l'un de ses réduits.

Autrement dit, $s\ \beta_p\ \overline{u}$ si s contient un rédex t (au sens ci-dessus), $\overline{v}$ est l'un des réduits de t, et $\overline{u}$ est l'ensemble des termes obtenus en remplaçant le redex t par les éléments de $\overline{v}$ dans s. Pour être très précis, t est une *occurrence de redex* dans s.

On a défini la réduction à petits pas sur les termes simples ; on l'étend maintenant aux termes avec ressources quelconques. On dira que $\overline{s}\ \beta_p\ \overline{u}$ si $\overline{s} = \{s_i \mid i \in I\}$ et $\overline{u} = \left(\bigcup_{i\in I} \overline{u_i}\right)$, avec $s_i\ \beta_p\ \overline{u_i}$ ou $u_i = \{s_i\}$ pour chaque $i \in I$ et si, pour au moins un i, on a $s_i\ \beta_p\ \overline{u_i}$.

Proposition 4.2.4 *La relation de réduction β_p^* (clôture transitive de β_p) est confluente sur les termes avec ressources.*

On ne donnera pas la preuve ici. Disons simplement qu'elle est basée sur la méthode classique de Tait et Martin-Löf.

Proposition 4.2.5 *Toute partie finie de Δ est fortement normalisante pour β_p.*

Démonstration. Utiliser le lemme de König, en observant que si $s\ \beta_p\ \overline{u}$, alors chaque élément de $\overline{u}$ a une occurrence de variable en moins. □

Exercice 4.2.2 Rédiger cette preuve.

4.2.6 Réduction à grand pas. Soit s un terme simple et T un poly-terme simple. On définit $\partial_x(s,T)$ comme suit. On écrit $T = [t_1, \dots, t_n]$ et on note $x_1, \dots, x_k$ les différentes occurrences libres de x dans s. On pose

$$\partial_x(s,T) = \begin{cases} \emptyset & \text{si } k \neq n \\ \{s[t_{f(1)}/x_1, \dots, t_{f(n)}/x_n] \mid f \in \mathfrak{S}_n\} & \text{sinon} \end{cases}$$

où $\mathfrak{S}_n$ est l'ensemble des permutations de $\{1, \dots, n\}$. Remarquer que cette définition ne dépend pas du choix de l'énumération $t_1, \dots, t_n$ des éléments de T.

On défint alors la réduction à grands pas comme on l'a fait pour la réduction à petit pas, sauf dans le cas «redex». Soit s un terme simple et $\overline{u}$ un terme avec ressources. Par récurrence sur s, on décrit quand $s\ \beta_g\ \overline{u}$.

- Si s est une variable, on n'a jamais $s\ \beta_g\ \overline{u}$.
- Si $s = \lambda x\, t$, on a $s\ \beta_g\ \overline{u}$ si $\overline{u} = \lambda x\, \overline{v}$ et $t\ \beta_g\ \overline{v}$.
- Si $s = \langle t\rangle\, T$ (avec $T = [t_1, \dots, t_n]$), on a $s\ \beta_g\ u$ dans l'un des cas suivants :
  - $\overline{u} = \langle \overline{v}\rangle\, T$ avec $t\ \beta_g\ \overline{v}$;
  - il existe $i \in \{1, \dots, n\}$ tel que $\overline{u} = \langle t\rangle\, [t_1, \dots, t_{i-1}, \overline{v_i}, t_{i+1}, \dots, t_n]$ avec $t_i\ \beta_g\ \overline{v_i}$;
  - $t = \lambda x\, w$ et $\overline{u} = \partial_x(w, T)$.

On étend β_g aux termes avec ressources comme on l'a fait pour β_p.

Lemme 4.2.6 *Si $\overline{s}\ \beta_g\ \overline{s'}$, alors $\overline{s}\ \beta_p^*\ \overline{s'}$. De plus, un terme simple est normal pour β_g si et seulement si il est normal pour β_p.*

Par suite, si s est un terme simple, on atteint sa forme normale (au sens de β_p) en itérant la réduction β_g.

4.3 Typage et sémantique relationnelle

4.3.1 Typage simple. On considère un système de types simples, défini comme en 1.1.3, avec les quantificateurs en moins (il ne serait pas difficile de les considérer aussi mais cela ne nous servirait pas ici). Les règles de typage sont les suivantes.

$$\frac{}{\Gamma, x : A \vdash x : A}$$

$$\frac{\Gamma, x : A \vdash s : B}{\Gamma \vdash \lambda x^A\, s : A \Rightarrow B}$$

$$\frac{\Gamma \vdash s : A \Rightarrow B \qquad \Gamma \vdash t_i : A \text{ (pour } i = 1, \dots, n)}{\Gamma \vdash \langle s\rangle\, t_1 \cdots t_n : B}$$

Enfin, si $\overline{s}$ est un terme avec ressources, on écrira $\Gamma \vdash \overline{s} : A$ si on a $\Gamma \vdash s : A$ pour tout $s \in \overline{s}$. En particulier, on a toujours $\Gamma \vdash \emptyset : A$, et si $\Gamma \vdash \overline{s} : A$ et $\Gamma \vdash \overline{t} : A$, alors $\Gamma \vdash \overline{s} \cup \overline{t} : A$.

Lemme 4.3.1 (substitution) *Si $\Gamma, x : A \vdash s : B$ et si $\Gamma \vdash t : A$, alors $\Gamma, x : A \vdash \frac{\partial s}{\partial x} \cdot t : B$.*

La preuve est une simple récurrence sur s. On en déduit facilement le résultat suivant.

Proposition 4.3.2 (réduction du sujet) *Si* $\Gamma \vdash \overline{s} : A$ *et si* $\overline{s}\ \beta_p\ \overline{s'}$*, alors* $\Gamma \vdash \overline{s'} : A$*. Si* $\Gamma \vdash \overline{s} : A$ *et si* $\overline{s}\ \beta_g\ \overline{s'}$*, alors* $\Gamma \vdash \overline{s'} : A$*.*

4.3.2 Sémantique relationnelle : cas simplement typé.

À SUIVRE...

Index

Bibliographie

[AC98] Roberto Amadio and Pierre-Louis Curien. *Domains and lambda-calculi*, volume 46 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1998.

[GLT89] Jean-Yves Girard, Yves Lafont, and Paul Taylor. *Proofs and types*, volume 7 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1989.

[Kri90] Jean-Louis Krivine. *Lambda-Calcul : Types et Modèles*. Études et Recherches en Informatique. Masson, 1990.