Lambda-calcul et domaines

Pierre-Louis Curien

November 12, 2001

Introduction

λ-calcul. Lorsqu'on écrit une fonction, par exemple

$$f(x) = 1 + x^2 e^{-2x} + \int x^{-1.5} dx \ ,$$

on peut s'intéresser au graphe de f, et voir $f(a) = b$ comme $(f(a), b) \in graph(f)$. On peut aussi voir $f(x)$ comme une expression formelle F, avec deux occurrences libres de x et une liée (sous le signe intégrale), et voir $f(a)$ comme le résultat d'une substitution formelle de x par a:

$$f(a) = 1 + a^2 e^{-2a} + \int x^{-1.5} dx$$

Ce sont les fonctions-algorithmes, ou fonctions - règles de calcul. Le λ-calcul formalise cette opération de substitution: On forme d'abord $\lambda x.F$, dans laquelle les deux occurrences libres de x deviennent liées (on peut représenter la liaison par des liens explicites, et supprimer le nom x, cf. théorie des ensembles de Bourbaki). Puis on forme $(\lambda x.F)a$, qui est "l'appel de procédure" en appel par nom (de a). Et enfin on applique la règle (unique!) de calcul:

$$(\beta) \qquad (\lambda x.F)a \ \rightarrow \ F[a/x]$$

Notons que cette substitution peut être coûteuse (duplication), ou au contraire génératrice d'économies (effacement).

Repères historiques: C'est d'abord la logique combinatoire qui est apparue (Schönfinkel, 1924), comme outil pour éliminer les variables liées dans les formules de logique d'ordre supérieur. Redécouverte de la logique combinatoire par Curry en 1928, et vers la même époque découverte et développements du λ-calcul par Church, Kleene et Rosser. Ces recherches mêlent pur formalisme de manipulation de fonctions et logique. Beaucoup d'incohérences (par exemple Kleene et Rosser prouvent en 1935 l'incohérence du premier système de Kleene, publié en 1932 et 1933). Mais le λ-calcul sert à formaliser la notion de fonction calculable, ou récursive, et mène Kleene au théorème de récursion (Kleene 1936, voir plus bas). (Ces références sont dans [Bare84].)

Plus tard, avec la déduction naturelle de Gentzen et Prawitz, on a réalisé que le λ-calcul typé décrivait exactement des preuves.

Domaines. Les structures de données de base de l'informatique sont les listes et les arbres. Ces structures sont naturellement ordonnées par l'accroissement de l'information. Par exemple, considérons l'insertion de 13 dans l'arbre binaire de recherche

$$12(5(2(\Omega,\Omega),9(\Omega,\Omega)),18(15(\underline{\Omega},17(\Omega,\Omega)),19(\Omega,\Omega)))$$

qui est obtenue en remplaçant le Ω souligné par $13(\Omega,\Omega)$:

$$12(5(2(\Omega,\Omega),9(\Omega,\Omega)),18(15(13(\Omega,\Omega),17(\Omega,\Omega)),19(\Omega,\Omega))).$$

Dans ce formalisme, continuité = préservation des sup de suites croissantes, et toute fonction continue f a un plus petit point fixe $\bigvee f^n(\perp)$, où $\perp$ est le plus petit élément (par exemple, l'arbre réduit à une racine indéfinie).

Le lien avec le λ-calcul pur est fourni par la résolution de l'équation $D = D \to D$, que permet le cadre de la théorie des domaines (et pas celui de la théorie des ensembles pour causes de cardinalité). On peut alors interpréter l'auto-application ff, considérant le premier f dans $D \to D$ et le second f dans D.

On trouve ce genre de relation d'ordre en mathématiques. En logique d'abord, avec les fonctions partielles récursives. Dans ce cadre, le théorème de point fixe ci-dessus donne (avec un peu de travail) le théorème de récursion de Kleene. Soit $f : \omega \to \omega$ récursive, totale, et extensionnelle, ce qui veut dire qu'en fait f est une endo-fonction sur l'ensemble des fonctions récursives partielles énumérées par $\phi_1, \ldots, \phi_n, \ldots$:

$$\forall\, m, n \;\; \phi_m = \phi_n \Rightarrow \phi_{f(m)} = \phi_{f(n)}.$$

Donc on peut définir $F(\phi_n) = \phi_{f(n)}$. Alors F a un point fixe, i.e. il existe n_0 tel que $\phi_{n_0} = \phi_{f(n_0)}$.

Et en analyse. Penser aux réels obtenus par encadrement d'intervalles de longueur tendant vers 0, fournis par exemple par les approximants d'une fraction continue. Pensez aussi aux points d'un espace métrique comme points maximaux d'un espace de boules (formelles), ordonnées par

$$(x,r) \leq (y,s) \Leftrightarrow d(x,y) \leq r - s$$

Alors le théorème de point fixe de Banach pour une application f c-contractante est obtenu comme corollaire du théorème de point fixe de Kleene, grâce à l'extension de f aux boules formelles donnée par

$$\tilde{f}(x,r) = (f(x), cr).$$

Ce point de vue peut être aussi appliqué à l'intégration. Une subdivision d'un intervalle en intervalles b_j de longueur r_j définit une combinaison élémentaire $\sum r_j \eta_{b_j}$ de "mesures de Dirac" sur l'espace des intervalles: $\eta_b(A) = 1$ si $b \in A$ et $\eta_b(A) = 0$ sinon. Les sommes de Riemann (disons inférieures) associées à une fonction f définissent une fonction $\hat{f}$ de ces mesures (ou valuations) élémentaires dans $\Re$:

$$\hat{f}(\sum r_j \eta_{b_j}) = \sum r_j inf f(b_j)$$

Enfin les mesures sur $\Re$ sont (en bijection avec) les éléments maximaux de l'espace des valuations sur l'espace des intervalles. Ce qui amène à définir $\int f d\mu = \hat{f}(\mu) = \bigvee_\nu \hat{f}(\nu)$, où ν parcourt l'ensemble des valuations élémentaires au-dessous de μ.

1 Lambda-calcul et logique

1.1 Paradoxes

Barendregt appendix B. Illative combinatory logic. Illatif veut dire "dont on peut inférer quelque chose". L'idée est de considérer les formules comme des λ-termes sans type. On obtient alors un paradoxe en prenant un point fixe. L'implication $\Rightarrow$ est une constante, et pour M fixé et arbitraire, on prend X tel que

$$X = (\Rightarrow XM) = (X \Rightarrow M).$$

Alors, partant de l'hypothèse X, on déduit X (axiome) et $X \Rightarrow M$ (égalité), puis M (modus ponens). Donc, par abstraction, on obtient une preuve sans hypothèse de $X \Rightarrow M$, donc de X (égalité). On a maintenant une preuve de X et une preuve de $X \Rightarrow M$, dont on obtient par modus ponens une preuve de M. Donc toute formule est prouvable, ce qui est tout de même gênant. Le terme sous-jacent à la preuve est $\Delta\Delta$, qui n'a pas de forme normale, ce qui est en accord avec le paradoxe: il ne peut y avoir de preuve sans coupure de l'absurdité.

Nous montrons que ce paradoxe "a pour instance" le paradoxe de Russell. Rappelons ce paradoxe. Soit $A = \{x \mid \neg(x \in x)\}$. Alors A est membre de A si et seulement si A n'est pas membre de A. Formellement A est une sorte de λ-abstraction, et on a la "β-réduction" $(a \in \{x \mid P(x)\}) \to P(a)$, qui donne ici, appliquée à $a = A$ et $P(x) = \neg(x \in x)$: $(A \in A) \to \neg(A \in A)$. En écrivant $\neg(A \in A) = (A \in A) \Rightarrow \bot$, on retrouve le paradoxe ci-dessus, en poseant $X = (A \in A)$ et $M = \bot$.

Malheureusement, même une fois le paradoxe soigné à l'aide du schéma de compréhension, on retrouve une preuve non normalisante, ce qui indique la difficulté à faire rentrer la théorie des ensembles dans le cadre de la théorie de la démonstration, où l'élimination des coupures joue un rôle central. On pose maintenant $A = \{x \in B \mid \neg(x \in x)\}$ – qui n'est plus un ensemble paradoxal si B est un ensemble–, ce qui conduit à $(A \in A) \to ((A \in B) \cap \neg(A \in A))$. En posant

$(A \in A) = X$, $(A \in B) = N$ et $M = \bot$, on retrouve un terme (du λ-calcul étendu avec des produits) prouvant l'absurdité sous l'hypothèse $y : N$, et qui n'a pas de forme normale ($x : X$):

$$(\lambda x.snd(x)x)(y, \lambda x.snd(x)x)$$

qui se réduit sur lui -même ($x : X$):

$$\begin{array}{rcl} (\lambda x.snd(x)x)(y, \lambda x.snd(x)x) & \to & snd((y, \lambda x.snd(x)x))(y, \lambda x.snd(x)x) \\ & \to & (\lambda x.snd(x)x)(y, \lambda x.snd(x)x) \end{array}$$

- déduction naturelle
- calcul LJT
- représentation des fonctions récursives
- consistence de l'arithmétique et Dialectica interpretation (Hindley-Seldin)

2 Les théorèmes syntaxiques

2.1 Exemples de λ-termes

Les entiers de Church:

$$\begin{array}{l} Succ = \lambda nfx.f(nfx) \\ 0 = \lambda fnx.x \end{array}$$

Deux manières différentes de programmer addition, multiplication et puissances:

$$\begin{array}{lll} m + n & m\ Succ\ n & \lambda fx.m(f(nfx)) \\ m \times n & m\ (\lambda x.n + x)\ n & \lambda f.m(nf) \\ n^m & m\ (\lambda x.n \times x)\ n & mn \end{array}$$

(Anticipant sur le système F, mn est en fait $\Lambda X.m(X \to X)(nX)$.)

2.2 Substitutions explicites

$(B ::= b \mid \Uparrow(B))$

$$\begin{array}{lcll}
(\lambda a)b & \rightarrow & a\{b\} & \\
 & & & \\
(a_1 a_2)\{B\} & \rightarrow & (a_1\{B\})(a_2\{B\}) & \\
(\lambda a)\{B\} & \rightarrow & \lambda(a\{\Uparrow(B)\}) & \\
1\{b\} & \rightarrow & b & \\
(m+1)\{b\} & \rightarrow & m & \\
1\{\Uparrow(B)\} & \rightarrow & 1 & \\
(m+1)\{\Uparrow(B)\} & \rightarrow & \tau_1(m\{B\}) & \\
 & & & \\
\tau_i(a_1 a_2) & \rightarrow & \tau_i(a_1)\tau_i(a_2) & \\
\tau_i(\lambda a) & \rightarrow & \lambda(\tau_{i+1}(a)) & \\
\tau_i(m) & \rightarrow & m+1 & (m \geq i) \\
\tau_i(m) & \rightarrow & m & (m < i)
\end{array}$$

2.3 Développements finis

Théorème 2.1 *Soit M un λ-terme et U un ensemble d'occurrences de radicaux dans M. Toutes les dérivations à partir de M qui ne dérivent que des radicaux résidus de U – on les appelle dérivations relatives à U – terminent, et terminent sur le même terme. Une telle dérivation est appelée un développement de U. De plus, si $v \notin U$, et si D_1 et D_2 sont deux développements de U, alors $v/D_1 = v/D_2$.*

Preuve. On considère l'ensemble $\underline{\Lambda}$ des λ-termes soulignés, defini comme suit:

$$M ::= x \mid MM \mid \lambda x.M \mid (\underline{\lambda} x.M)M\ .$$

muni de la règle de réécriture

$$(\underline{\beta}) \quad (\underline{\lambda} x.M)N \ \rightarrow\ M[x \leftarrow N]$$

Le lien entre ce caclul et le théorème que nous devons prouver est le suivant: on transforme le terme M de l'énoncé en un terme $M_U \in \underline{\Lambda}$, qui est obtenu en soulignant tous les λ qui apparaissent en occurrence $u1$, pour tous les $u \in U$. Il est facile de voir que si $M \rightarrow_\beta^\star N$ et si la dérivation D de M à N est relative à U, alors $M_U \rightarrow_{\underline{\beta}}^\star N_{U/D}$, et que réciproquement, pour toute dérivation $P \rightarrow_{\underline{\beta}}^\star Q$ dans $\underline{\Lambda}$, la β-dérivation sous-jacente obtenue en supprimant les soulignements est relative à U.

On est donc ramenés à prouver la terminaison de la $\underline{\beta}$-réduction. Soit $\mathcal{FD}$ le plus petit sous-ensemble de $\underline{\Lambda}$ contenant les variables, fermé par λ-abstraction et par application, et tel que, pour tous $M, N \in \underline{\Lambda}$.

$$(M[x \leftarrow N] \in \mathcal{FD} \text{ and } N \in \mathcal{FD}) \Rightarrow (\underline{\lambda} x.M)N \in \mathcal{FD}\ .$$

On a:

1. $M[x_1 \leftarrow N_1, \ldots x_n \leftarrow N_n] \in \mathcal{FD}$, pour tous $M \in \mathcal{FD}$ et $N_1, \ldots, N_n \in \mathcal{FD}$ (par récurrence sur la preuve de $M \in \mathcal{FD}$).

2. $\underline{\Lambda} = \mathcal{FD}$ (par récurrence sur la taille de $M \in \underline{\Lambda}$ et en utilisant (1) dans le cas $M = (\underline{\lambda} x.M_1)M_2$).

3. $\underline{\beta}$ est fortement normalisante. (par récurrence sur la d'efinition of $\mathcal{FD}$, et en utilisant le fait que si $M[x \leftarrow N]$ est fortement normalisable, alors M est fortement normalisable).

Par ailleurs, il est facile de voir que la $\underline{\beta}$ est localement confluente, donc confluente, d'où le résultat d'unicité de l'énoncé.

Enfin, pour obtenir le dernier résultat, on modifie le calcul comme suit. Il y a maintenant deux soulignements différents:

$$M ::= x \mid MM \mid \lambda x.M \mid (\underline{\lambda} x.M)M \mid (\underline{\underline{\lambda}} x.M)M \ .$$

La règle de calcul est toujours la $\underline{\beta}$-réduction (et elle seule). Ce calcul est toujours SN et confluent. On traduit maintenant M en le terme $M_{U,v}$ obtenu en soulignant les λ des radicaux de U comme ci-dessus et en soulignant doublement le λ du radical v. Les occurrences doublement soulignéss au cours des $\underline{\beta}$-dérivations repèrent les occurrences de radicaux résidus de v. La forme normale Q de $M_{U,v}$ contient donc cette information, indépendamment du chemin suivi. Ceci prouve la dernière partie de l'énoncé. CQFD

Le théorème des développements finis nous renseigne sur la nature de la non-terminaison dans le λ-calcul. Un radical qui n'est pas résidu d'un radical précédent au cours d'une dérivation est dit créé par la dérivation. Une dérivation ne peut être infinie que si elle procède à une infinité de contractions de radicaux créés. Par exemple, *chaque* étape de réduction $\Delta\Delta \rightarrow \Delta\Delta$ crèe le radical de droite. Il y a trois cas de création de radical:

1. $(\lambda y.C[xN])(\lambda x.M)$,

2. $(\lambda x_1 x.M)N_1 N$,

3. $(\lambda y.y)(\lambda x.M)N$.

2.4 Confluence

Un système de réécriture abstrait est la donnée d'un ensemble A muni d'une relation binaire notée $\rightarrow$. On note $\rightarrow^\star$ la clôture réflexive et transitive de $\rightarrow$. On note $\rightarrow^1$ la clôture éflexive de $\rightarrow$. Une forme normale est un élément a tel que $(\nexists b \;\; a \rightarrow b)$.

Définition 2.2 *On dit que* $\to$ *est* confluente *si*

$$\forall\, a_1, a_2, a_3 \ \ (a_1 \to^\star a_3 \ \ et \ a_2 \to^\star a_3 \Rightarrow \exists\, a_4 \ \ a_3 \to^\star a_4 \ \ et \ a_3 \to^\star a_4)\ .$$

On dit que $\to$ *est* localement confluente *si*

$$\forall\, a_1, a_2, a_3 \ \ (a_1 \to a_3 \ \ et \ a_2 \to a_3 \Rightarrow \exists\, a_4 \ \ a_3 \to^\star a_4 \ \ et \ a_3 \to^\star a_4)\ .$$

On dit que $\to$ *est* fortement confluente *si*

$$\forall\, a_1, a_2, a_3 \ \ (a_1 \to a_3 \ \ et \ a_2 \to a_3 \Rightarrow \exists\, a_4 \ \ a_3 \to^1 a_4 \ \ et \ a_3 \to^1 a_4)\ .$$

Définition 2.3 *On dit que* $\to$ *est* faiblement normalisante *, ou WN (pour "weakly normalizing"), si pour tout* a*, il existe une dérivation* $a \to a_1 \to \cdots \to a_n$*, avec* a_n *en forme normale.*

On dit que $\to$ *est* fortement normalisante *, ou SN (pour "strongly normalizing"), s'il n'existe aucune dérivation infinie* $a \to a_1 \to \cdots \to a_n \to \cdots$ *.*

On a les propriétés suivantes:

- La confluence locale n'implique pas la confluence. Voici deux contre-exemples:

  1. $A = \{a, b, c, d\}$, avec $b \to a$, $c \to d$, $b \to c$ et $c \to b$. Pour la non-confluence, remarquer que $b \to a$ et $b \to^\star d$. Pour la confluence locale, noter que l'on peut toujours revenir de c à b (ou de b à c). Cet exemple est une version finie du contre-exemple suivant.
  2. $A = \{a, d\} \cup \{b_n \mid n \in \omega\} \cup \{c_n \mid n \in \omega\}$, avec $b_n \to a$ et $c_n \to d$, $b_n \to c_n$ et $c_n \to b_{n+1}$ pour tout n. Cet exemple est une version acyclique du contre-exemple précédent.

- La confluence locale plus la propriété WN impliquent la confluence à partir de tout élément a (preuve par récurrence sur la profondeur de a, qui est la longueur de la plus longue dérivation à partir de a).

- La confluence forte implique la confluence (argument de pavage évident).

On s'intéresse maintenant à la confluence de la β-réduction. Il est facile de vérifier que β est localement confluente, mais non fortement confluente (cas typique: $M = (\lambda x.xx)R$, où R est un β-radical). On ne peut donc appliquer l'une des deux méthodes ci-dessus directement. Mais la relation $\to_U$ donnée par les développements finis est fortement confluente. Si en effet on a $M \to_U N$ et $M \to_V P$, alors si Q est le terme tel que $M \to_{U\cup V} Q$, en complétant le développement de $U \cup V$ à partir de N on a $N \to_{V/U} Q$, et de même $P \to_{U/V} Q$.

2.5 Standardisation

Référence: [AmaCur98, section 2.1].

On montre le théorème de standardization comme conséquence des développements finis, par une technique due a Curry. Soit

$$D : M_{00} \to_{u_0} M_{10} \to_{u_1} M_{20} \to^* M_{n0}$$

la dérivation à standardiser. On choisit une occurrence u^1 le plus à gauche parmi les occurrences de radicaux de M dont un résidu u_j $(= u^1)$ est réduit dans D. Soit $M_{00} \to_{u^1} M_{01}$; on construit la dérivation

$$D_1 : M_{01} \to^* M_{j1} = M_{(j+1)0} \to^* M_{n1} = M_{n0}$$

où chaque étape est un développement fini de $u_i/u^1 = U_i$ $(i < j)$ puis coïncide avec la dérivation précédente (on pose $U_i = \emptyset$ pour $i \geq j$):

$$\begin{array}{lllllllll}
M_{00} & \to_{u_0} & M_{10} & \to^* & M_{j0} & \to_{u_j} & M_{(j+1)0} & \to^* & M_{n0} \\
\downarrow_{u^1} & & \downarrow_{u^1} & & \downarrow_{u^1} & & \downarrow_{\emptyset} & & \downarrow_{\emptyset} \\
M_{01} & \to_{U_0} & M_{11} & \to^* & M_{j1} & = & M_{(j+1)1} & \to^* & M_{n1}
\end{array}$$

On continue ce processus, en construisant des dérivations $D_2, \ldots, D_n, \ldots$. On a par construction:

$$u^i/D_{i-1} = \emptyset \quad \text{and} \quad D_{i-1}/u^i = D_i$$

On dit qu'une colonne de la figure ci-dessous termine lorsqu'elle ne comporte qu'un nombre fini d'étapes non vides. La colonne de droite termine. Supposons par l'absurde que la colonne de gauche ne termine pas. Il existe donc deux colonnes successives, commençant par M_{k0} et $M_{(k+1)0}$ respectivement telle que la première ne termine pas et la seconde termine. On se place à la ligne commençant par M_{0m} où la seconde de ces colonnes termine. L'"étape" de M_{km} à $M_{(k+1)m}$ est un développement d'un ensemble U d'occurrences. Il est facile de voir que la dérivation verticale

$$M_{km} \to M_{k(m+1)} \to^* \cdots$$

est relative à ce développement, i.e. les radicaux réduits sont résidus de radicaux qui sont dans U. En effet, par construction on a $u^m \in U$ car on aurait sinon $M_{(k+1)m} \to_{\emptyset} M_{(k+1)(m+1)}$; puis $u^{m+1} \in (U/u^m)$, etc..; . Cette dérivation doit donc terminer, ce qui est une contradiction. La dérivation de gauche termine donc. La dernière ligne ne peut comporter que des étapes vides, sinon la dérivation verticale de gauche devrait continuer. Donc la dérivation verticale gauche s'achève en M_{n0}. Il reste à voir qu'elle est standard. Pour le voir, il faut utiliser la version forte des développements finis. Supposons que u^j soit résidu de u à gauche de u^i. On a $u/D_i = \{u\}$ par le lemme 2.4 et $u^j/D_j = \emptyset$. Or par équivalence de dérivations on devrait avoir $u/D_i = u^j/D_j$. Cette contradiction montre que la dérivation construite est bien standard.

Lemme 2.4 *Si D est une dérivation à partir d'un terme M et u est une occurrence de radical dans M à gauche de toutes les occurrences de radicaux de M dont un résidu est réduit au cours de la dérivation D – on dit que u est à gauche de D –, alors $D/u = \{u\}$.*

Preuve. Par récurrence sur la longueur de la dérivation. C'est clair pour une dérivation de longueur 1. Pour le pas de récurrence, soit $M \rightarrow_{u_0} M_1$ le premier pas de D et soit D_1 le reste de la dérivation à partir de M_1. Pour appliquer la récurrence à M_1, il suffit de vérifier que u satisfait les hypothèses du lemme par rapport à D_1. Il y a deux sortes de radicaux de M_1 parmi ceux dont un résidu est réduit par D_1: ceux qui sont résidus d'un radical déjà présent dans M, et ceux qui ont été créés par u_0. On est ainsi ramené à prouver les deux propriétés suivantes (pas de difficulté):

- Si u est à gauche de u_0 et v dans M, alors u est à gauche de v/u_0 dans M_1.
- Si u est à gauche de u_0 dans M et si w est créé par u_0 dans M_1, alors u est à gauche de w dans M_1. CQFD

$$
\begin{array}{lllllllll}
M_{00} & \rightarrow_{u_0} & M_{10} & \rightarrow^* & M_{k0} & \rightarrow_{u_k} & M_{(k+1)0} & \rightarrow^* & M_{n0} \\
\downarrow_{u^1} & & \downarrow & & \downarrow & & \downarrow & & \downarrow_{\emptyset} \\
M_{01} & \rightarrow_{u_0/u^1} & M_{11} & \rightarrow^* & M_{k1} & \rightarrow_{U_k} & M_{(k+1)1} & \rightarrow^* & M_{n1} \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
M_{0m} & \rightarrow & M_{1m} & \rightarrow^* & M_{km} & \rightarrow_{U} & M_{(k+1)m} & \rightarrow^* & M_{nm} \\
\downarrow_{u^{m+1}} & & \downarrow_{u^{m+1}} & & \downarrow_{u^{m+1}} & & \downarrow_{\emptyset} & & \downarrow_{\emptyset} \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow_{\emptyset} & & \downarrow_{\emptyset} \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}
$$

Corollaire 2.5 *Si M a une forme normale, la dérivation gauche à partir de M (qui consiste à réduire le radical le plus à gauche à chaque étape) l'atteint.*

Preuve. Soit D une dérivation standard de M à sa forme normale P. Supposons qu'elle n'est pas gauche. Il existe donc une étape $M_n \rightarrow_v M_{n+1}$ de D où v n'est pas le radical u le plus à gauche de M_n. Alors, par le lemme précédent, u a un résidu unique dans P, qui n'est donc pas normal: contradiction. CQFD

2.6 Le théorème de Böhm

On rappelle que $0 = \lambda xy.x$, et on pose $1 = \lambda xy.x$. On rappelle aussi le codage des paires: $(M, N) = \lambda z.zMN$ ($z \notin FV(M) \cup FV(N)$). On en donne ici une version avec paramètres:

$$(M, N)_n = \lambda x_1 \dots x_n z.z(Mx_1 \dots x_n)(Nx_1 \dots x_n)$$

(donc (M, N) est le cas particulier $(M, N)_0$). On a:

$$\begin{array}{l} (M,N)_0 1 \to M \\ (M,N)_0 0 \to N \\ (M,N)_{n+1} P \to (MP, NP)_n \end{array}$$

Dans ce qui suit, on utilise la notation MN^p pour $MN \dots N$ (n applications).

Lemme 2.6 *Si $P[x \leftarrow M] \to^\star y$ ($x \notin FV(M)$), alors pour tout entier k suffisamment grand, il existe des entiers l, l' tels que $P[x \leftarrow (M, N)_k]1^l \to^\star y1^{l'}$ (pour tout N).*

Preuve. On peut supposer que la dérivation $P[x \leftarrow M] \to^\star y$ est normale. On raisonne par ordre lexicographique sur la longueur de cette dérivation, puis sur les cas ci-dessous.

(A) Si P n'est pas en fnt, soit $P \to P'$. Il suffit d'appliquer la récurrence à P'.

(B) Si P est une fnt, alors P ne peut avoir de λ en tête, puisque $P[x \leftarrow M]$ se réduit sur une variable. Comme cette variable est y, P ne peut commencer que par x ou être égal à y. Le cas $P = y$ est trivial. Si $P = x$, l'hypothèse se reformule en $M \to^\star y$. Il suffit alors de prendre $l = k + 1$ et $l' = k$:

$$(M,N)_k 1^{k+1} \to^\star (M1^k, N1^k)_0 1 \to M1^k \to^\star y1^k \; .$$

Il reste le cas $P = xQ_1 \dots Q_n$ ($n \geq 1$). On pose $P^1 = MQ_1 \dots Q_n$. On a $P^1[x \leftarrow M] = P[x \leftarrow M]$. De plus, P^1 n'est pas en fnt, car s'il l'était ce ne pourrait être qu'une variable appliquée à au moins $n \geq 1$ arguments, ce qui contredit que $P^1[x \leftarrow M]$ se réduit sur y. Donc on peut appliquer la récurrence à P^1 (même longueur de dérivation, cas "inférieur"). On prend soin de choisir $k \geq n$ (d'où le "k assez grand"). Il existe donc l, l' tels que, pour tout N, $P^1[x \leftarrow (M, N)_k]1^l = MQ'_1 \dots Q'_n 1^l \to^\star y1^{l'}$ (Q'_i désignant $Q_i[x \leftarrow (M, N)_k]$). Alors $k + l + 1$ et $l' + k$ conviennent pour P:

$$\begin{array}{ll} P[x \leftarrow (M,N)_k]1^{k+l+1} = (M,N)_k Q'_1 \dots Q'_n & \\ \quad \to^\star (MQ'_1 \dots Q'_n 1^{k-n}, NQ'_1 \dots Q'_n 1^{k-n})_0 1^{n+l+1} & \text{(k assez grand)} \\ \quad \to MQ'_1 \dots Q'_n 1^{k-n} 1^{n+l} = MQ'_1 \dots Q'_n 1^{k+l} & \\ \quad \to^\star y1^{l'}1^k = y1^{l'+k} & \text{(récurrence)} \end{array}$$

CQFD

Théorème 2.7 *Soit P et Q deux termes β-normaux dont les variables libres sont parmi $x_1, \dots, x_r$, et tels que P et Q ne sont pas η-convertibles. Alors il existe des termes clos $M_1, \dots, M_p$, $N_1, \dots, N_q$ tels que $P[\vec{x} \leftarrow \vec{M}]\vec{N} \to^\star 1$ et $Q[\vec{x} \leftarrow \vec{M}]\vec{N} \to^\star 0$.*

Preuve. On raisonne par récurrence sur la somme des tailles de P et Q, la taille étant définie par: $taille(x) = 0$, $taille(xM_1 \dots M_n) = 1 + taille(M_1) + \dots + taille(M_n)$ $(n > 0)$, $taille(\lambda x.M) = taille(M) + 1$. Regardons par exemple le cas $P = x_1 P_1 \dots P_n$ et $Q = \lambda y.Q'$. On résout alors le problème avec Py et Q', ce qui donne $M_1, \dots, M_p$, et $\vec{N}$. Alors $M_2, \dots, M_p$, et $M_1, \vec{N}$ conviennent pour P et Q.

On est ainsi ramené au cas où P et Q commencent par une variable, disons $P = xP_1 \dots P_m$ et $Q = yQ_1 \dots Q_n$. On distingue plusieurs cas:

- $x \neq y$: On peut supposer $x = x_1$, $y = x_2$. On prend $M_1 = \lambda z_1 \dots z_m.1$, $M_2 = \lambda z_1 \dots z_n.0$, et $\vec{N}$ vide.

- $x = y$ $(= x_1)$ et $m \neq n$; disons $m < n$. On prend $M_1 = \lambda z_1 \dots z_{n+1}.z_{n+1}$, $N_1 = \lambda z_1 \dots z_{n-m}.0$, $N_{n-m+1} = 1$ (les N intermédiaires sont quelconques). On a:
$$P[x_1 \leftarrow M_1]\vec{V} \rightarrow^\star N_{n-m+1} = 1$$
$$Q[x_1 \leftarrow M_1]\vec{V} \rightarrow^\star N_1 N_2 \cdots N_{n-m+1} \rightarrow^\star 0$$

- $x = y$ $(= x_1)$ et $m = n$. Il existe un j tel que P_j et Q_j ne sont pas η-convertibles. On peut leur appliquer la récurrence. Soit donc $\vec{M}$ et $\vec{N}$ convenant pour P_j et Q_j. On a:
$$P_j[\vec{x} \leftarrow \vec{M}]\vec{N} y_1 y_2 \rightarrow^\star y_1$$
$$Q_j[\vec{x} \leftarrow \vec{M}]\vec{N} y_1 y_2 \rightarrow^\star y_2$$

  L'idée est de combiner le terme M_1 obtenu par la récurrence avec la projection $\lambda z_1 \dots z_n.z_j$ qui permet de passer de P à P_j, et de Q à Q_j. C'est possible grâce au lemme précédent, qu'on applique deux fois, à
$$P_j[(x_2, \dots, x_p) \leftarrow (M_2, \dots, M_p)]\vec{N} y_1 y_2 \quad \text{et}$$
$$Q_j[(x_2, \dots, x_p) \leftarrow (M_2, \dots, M_p)]\vec{N} y_1 y_2$$
  respectivement, avec le même k, que l'on choisit de surcroît $\geq n + q + 2$. On obtient donc l_1, l'_1, et l_2, l'_2. On peut s'arranger pour que le $l_1 = l_2$, et $\geq k$ (car une fois qu'on a un couple l, l', n'importe quel translaté $l + s, l' + s$ convient). On note $l_1 = l_2 = l$. On pose $M'_1 = (M_1, \lambda z_1 \dots z_n.z_j)_k$ et $M'_i = M_i$ pour $i \geq 2$. On pose $P'_i = P_i[\vec{x} \leftarrow \vec{M}']$ et de même pour Q'_i. On

a:

$$
\begin{array}{ll}
P[\vec{x} \leftarrow \vec{M'}]\vec{N}RS1^a01^b & \\
\quad = (M_1, \lambda z_1 \ldots z_n.z_j)_k\vec{P'}\vec{N}RS1^a01^b & \\
\quad \rightarrow^\star (\_, (\lambda z_1 \ldots z_n.z_j)\vec{P'}\vec{N}RS1^a)_0 01^b & (a = k - n - q - 2) \\
\quad \rightarrow^\star P'_j\vec{N}RS1^a1^b = P'_j\vec{N}RS1^l & (b = l - k + n + q + 2) \\
\quad \rightarrow^\star R1^{l'_1} & (\text{récurrence et lemme}) \\
\quad \rightarrow^\star 1 & (R = \lambda z_1 \ldots z_{l'_1}.1)
\end{array}
$$

$$
\begin{array}{ll}
Q[\vec{x} \leftarrow \vec{M'}]\vec{N}RS1^a01^b & \\
\quad \rightarrow^\star (\_, (\lambda z_1 \ldots z_n.z_j)\vec{Q'}\vec{N}RS1^a)_0 01^b & \\
\quad \rightarrow^\star Q'_j\vec{N}RS1^a1^b = P'_j\vec{N}RS1^l & \\
\quad \rightarrow^\star S1^{l'_2} & \\
\quad \rightarrow^\star 0 & (S = \lambda z_1 \ldots z_{l'_2}.0)
\end{array}
$$

On a noté _ un sous-terme qui ne nous intéresse pas, et on a utilisé des "inconnues" a, b, R, S, instanciées au bon moment. On a montré que $\vec{M'}$, et $\vec{N}, R, S, 1, \ldots 1$ ($k - n - q - 2$ fois), $0, 1, \ldots, 1$ ($l - k + n + q + 2$ fois) conviennent pour P et Q. CQFD

2.7 La technique Böhm-out

Théorème 2.8 (Continuité syntaxique) *Pour tout contexte C et tout terme M, si $B \leq BT(C[M])$, il existe $A \leq BT(M)$ tel que $B \leq BT(C[A])$ (c'est-à-dire: il existe N tel que $C[A] \rightarrow^* N$ et $B \leq \omega(N)$).*

Preuve (indication). On peut montrer (procédé inside-out, un peu dual de la standardisation) que si $C[M] \rightarrow^* N$, alors il existe P tel que $C[M] \rightarrow^* C[P]$ et $C[P] \rightarrow^* N$ où la dernière réduction ne réduit jamais de (résidu de) radical de P. Donc cette réduction se fait essentiellement à partir de $C[\omega(P)]$. CQFD

On pose (fnt = forme normale de tête)

$$M \leq_{obs} N \Leftrightarrow \forall C \ \ ((C[M], C[N] \text{ clos et } C[M] \text{ a une fnt }) \Rightarrow C[N] \text{ a une fnt }).$$

On définit un préordre sur les Ω-formes normales:

$$\frac{}{\Omega \preceq A}$$

$$\frac{x = y \quad m = n \quad A_1 \preceq B_1, \ldots A_n \preceq B_n}{xA_1 \cdots A_m \preceq yB_1 \cdots B_n} \qquad \frac{A \preceq B}{\lambda x.A \preceq \lambda x.B}$$

$$\frac{A \preceq yB_1 \cdots B_n x}{\lambda x.A \preceq yB_1 \cdots B_n} \qquad \frac{yB_1 \cdots B_n x \preceq A}{yB_1 \cdots B_n \preceq \lambda x.A}$$

Si on a établi $A \preceq B$ sans l'aide des deux dernières règles, on écrit $A \leq B$. Si $A \leq B$, $A/u = \Omega$ et $B/u \neq \Omega$, on écrit $A <_u B$. On note $|u|$ la longueur d'une occurrence u.

Remarque 2.9 *Si l'on a établi $A \preceq B$ sans l'aide de la première règle, i.e., si $A \preceq B$ et A est un λ-terme (sans occurrences d'Ω), alors $A =_\eta B$, et B est aussi un λ-terme. Si $A = x$, on a même $B \rightarrow_\eta^\star x$.*

On définit un système formel $A\,, B \stackrel{u,\triangle}{\Longrightarrow} C$ qui construit un contexte C associé à deux Ω-formes normales A, B telles que $A \not\preceq B$. Les décorations u et f fournissent des indications utiles: u désigne l'occurrence commune à (l'expansion de) A et (l'expansion de) B où la différence est observée, et $\triangle \in \{r, f\}$ (voir remarque 2.10 pour la signification de ces lettres). On pose:

$$\pi_n^m = \lambda x_1 \cdots x_m.x_n \ \ (n \leq m) \quad \alpha_n = \lambda z_1 \cdots z_n z.z z_1 \cdots z_n$$

On utilise une syntaxe adaptée pour les contextes: ce sont des listes dont chaque élément est un terme M (en l'occurrence une variable), ou une substitution $[M/x]$. La correspondance avec les contextes habituels est donnée par:

$$\begin{array}{lll} xC & C[[\,]x] & (\text{“appliquer à } x, \text{ puis } C\text{”}) \\ [M/x]C & C[(\lambda x.[\,]] & (\text{“substituer } M \text{ à } x, \text{ puis } C\text{”})\ . \end{array}$$

$$\frac{}{\lambda x_1 \cdots x_n x.A_1 \cdots A_m \,,\, \Omega \stackrel{\epsilon,f}{\Longrightarrow} [\pi^{m+1}_{m+1}/x]x_1 \cdots x_n}$$

$$\frac{A \,,\, B \stackrel{u,\triangle}{\Longrightarrow} C}{\lambda x.A \,,\, \lambda x.B \stackrel{u,\triangle}{\Longrightarrow} xC}$$

$$\frac{A \,,\, yB_1 \cdots B_n x \stackrel{u,\triangle}{\Longrightarrow} C}{\lambda x.A \,,\, yB_1 \cdots B_n \stackrel{u,\triangle}{\Longrightarrow} xC}$$

$$\frac{yB_1 \cdots B_n x \,,\, A \stackrel{u,\triangle}{\Longrightarrow} C}{yB_1 \cdots B_n \,,\, \lambda x.A \stackrel{u,\triangle}{\Longrightarrow} xC}$$

$$(x \neq y) \quad \frac{}{xA_1 \cdots A_m \,,\, yB_1 \cdots B_n \stackrel{\epsilon,r}{\Longrightarrow} [\pi^{m+1}_{m+1}/x][\Omega/y]}$$

$$(m < n) \quad \frac{zA^*_1 \cdots A^*_m z_{m+1} \cdots z_n \,,\, z_{m+1} B^*_1 \cdots B^*_n z_{m+2} \cdots z_n z \stackrel{u,\triangle}{\Longrightarrow} C}{xA_1 \cdots A_m \,,\, xB_1 \cdots B_n \stackrel{u,\triangle}{\Longrightarrow} [\alpha_n/x] z_{m+1} \cdots z_n zC}$$

$$(m > n) \quad \frac{z_{n+1} A^*_1 \cdots A^*_m z_{n+2} \cdots z_m z \,,\, zB^*_1 \cdots B^*_n z_{n+1} \cdots z_m \stackrel{u,\triangle}{\Longrightarrow} C}{xA_1 \cdots A_m \,,\, xB_1 \cdots B_n \stackrel{u,\triangle}{\Longrightarrow} [\alpha_m/x] z_{n+1} \cdots z_m zC}$$

$$x \notin FV(A_j) \cup FV(B_j) \quad \frac{A_j \not\preceq B_j \quad A_j \,,\, B_j \stackrel{u,\triangle}{\Longrightarrow} C}{xA_1 \cdots A_m \,,\, xB_1 \cdots B_m \stackrel{uj,\triangle}{\Longrightarrow} [\pi^m_j/x]C}$$

$$x \in FV(A_j) \cup FV(B_j) \quad \frac{A_j \not\preceq B_j \quad A^*_j \,,\, B^*_j \stackrel{u,\triangle}{\Longrightarrow} C}{xA_1 \cdots A_m \,,\, xB_1 \cdots B_m \stackrel{uj,\triangle}{\Longrightarrow} [\alpha_q/x] z_{m+1} \cdots z_q z [\pi^q_j/z]C}$$

Lorsque l'on ne s'intéresse pas au contexte précis produit, on écrit simplement $A \,,\, B \stackrel{u,f}{\Longrightarrow} \_$. Dans la dernière règle, on choisit $q \geq m$ et $q \geq$ le maximum d'arguments que peut prendre x dans A_j et B_j. A^*_j désigne la forme normale de $A_j[x \leftarrow \alpha_q]$, qui est obtenue de manière "administrative" du fait que l'on a pris q assez grand. Il faut vérifier que $A_j \not\preceq B_j$ implique $A^*_j \not\preceq B^*_j$ ce qui est encore aisé à vérifier en utilisant de même le fait que q est assez grand. On fait aussi usage de la règle $\Omega M = \Omega$ (qui, avec $\lambda x.\Omega = \Omega$ est implicite dans la définition de $\omega(\lambda x_1 \cdots x_n.\Omega A_1 \cdots A_m) = \Omega$. [AmaCur98, définition 2.3.1]).

Remarque 2.10 *Il est facile de vérifier que si* $A\,, B \stackrel{u,r}{\Longrightarrow} \_$*, alors* $A\,, B' \stackrel{u,r}{\Longrightarrow} \_$ *pour tout* $B' \geq B$*, et que la même propriété est en général fausse si on remplace* r *par* f*. La terminologie employée est inspirée de cette observation:* r *comme rigide,* f *comme flexible.*

Lemme 2.11 *Pour tous* A, B*, si* $A\,, B \stackrel{u,\triangle}{\Longrightarrow} \_$*, alors* A/u *est défini ou* B/u *est défini.*

Preuve. Le passage de u à uj se fait via les deux dernières règles, précédées d'un nombre adéquat d'applications des deuxième, troisième et quatrième règles, qui permettent de passer d'un couple de termes

$$\lambda x_1 \cdots x_m.xA_1 \cdots A_n,\ \lambda x_1 \cdots x_p.xB_1 \cdots B_q$$

tels que $m-n = p-q$ et, disons $m \leq p$, au couple de termes $xA_1 \cdots A_n x_{m+1} \cdots x_p$, $xB_1 \cdots B_q$. On a alors $j \leq q$. Et symétriquement, si $p \leq m$, alors $j \leq n$. CQFD

Définition 2.12 *Si* u *est une occurrence, on définit la suite* $A\,|_u$ *de couples (variable , entier relatif) se terminant éventuellement par un* Ω *comme suit:*

$$\begin{array}{ll}
(A\,|_\epsilon) = (x,i) & (A = \lambda x_1 \cdots x_n.xA_1 \cdots A_m\ ,\ i = n-m) \\
(A\,|_{uj}) = (A\,|_u)(x,i) & (A/uj = \lambda x_1 \cdots x_n.xA_1 \cdots A_m\ ,\ i = n-m) \\
(A\,|_{uj}) = (A\,|_u)\Omega & (A/uj = \Omega) \\
(A\,|_{uj}) = (A\,|_u) & (A/uj \textit{ non défini})
\end{array}$$

On pose $A =_u A'$ *si* $A|_u = A|_u$*, et* $A <_u A'$ *s'il existe* S *et* (x,i) *tels que* $A|_u = S\Omega$ *et* $A'\,|_u = S(x,i)$*, et* $A \leq_u A'$ *si* $A =_u A'$ *ou* $A <_u A'$*, la structure des liaisons étant préservée (par exemple* $\lambda xy.xy \not\leq_{11} \lambda x.x(\lambda y.y)$*, car* y *n'est pas lié à la même hauteur dans les deux termes).*

Proposition 2.13 *Si* $A \not\leq B$*, alors il existe* $C, u, \triangle$ *tels que* $A\,, B \stackrel{u,\triangle}{\Longrightarrow} C$*, et l'on a* $C[A] \rightarrow^* I$ *et* $C[B] \rightarrow^* \Omega$*. De plus,*

1. *Si* $\triangle = r$*, alors* $C[B'] \rightarrow^* \Omega$ *pour tout* B' *tel que* $B \leq_u B'$*.*

2. *Si* $\triangle = f$*, alors* $C[B'] \rightarrow^* \Omega$ *pour tout* B' *tel que* $B =_u B'$*.*

Preuve (indication). On note que les règles qui font passer de u à uj procèdent essentiellement par extraction de sous-termes. Pour (1), noter de plus que le Ω vient du contexte. CQFD

On pose la définiton suivante. Un arbre de Böhm est appelé *expansion infinie* de x, et on note $x\,\infty\mathcal{A}$ si

$$\forall\, A \leq \mathcal{A}\ \ x \not\leq A \text{ et } \forall\, u\ \ (x\,, A \stackrel{u,\triangle}{\Longrightarrow} \_) \Rightarrow (\triangle = f \text{ et } \mathcal{A}/u \neq \Omega)\ .$$

On définit la relation $\preceq_\infty$ sur les arbres de Böhm comme suit: $\mathcal{A} \preceq_\infty \mathcal{B}$ si et seulement si pour tout approximant fini A de $\mathcal{A}$ il existe un approximant fini B de $\mathcal{B}$ tel que $A \preceq \hat{B}$, où $\hat{B}$ est un terme obtenu à partir de B en remplaçant éventuellement des occurrences u de Ω par une variable x si $\mathcal{B}/u$ est une expansion infinie de x. On dit que $\hat{B}$ est une variante de B.

Définition 2.14 *Pour tous $A, \mathcal{B}$, la frontière $Fr(A, \mathcal{B})$ de A relativement à $\mathcal{B}$ est définie comme suit:*

$$\begin{aligned} Fr(A,\mathcal{B}) &= \{ui \mid A/u = \lambda x_1 \cdots x_m.xA_1 \cdots A_n,\ \mathcal{B}/u = \lambda x_1 \cdots x_p.x\mathcal{B}_1 \cdots \mathcal{B}_q, \\ &\quad m-n = p-q \text{ et } n < i \leq q\}\ . \end{aligned}$$

Il est facile de voir que si $B \leq \mathcal{B}$ et u sont tels que $A\,, B \stackrel{u,\triangle}{\Longrightarrow}$ _ et A/u n'est pas défini, alors u passe par la frontière, i.e., u a un préfixe v (unique) dans $Fr(A, \mathcal{B})$.

Lemme 2.15 *Si $\mathcal{A} \not\preceq_\infty \mathcal{B}$, alors il existe $A \leq \mathcal{A}$, $B \leq \mathcal{B}$ et une variante $\hat{B}$ de B tels que $A\,, \hat{B} \stackrel{u,\triangle}{\Longrightarrow}$ _ et, si $\triangle = f$, alors $\mathcal{B}/u = \Omega$.*

Preuve. On choisit A qui "témoigne" contre tous les $\hat{B}$. Supposons que l'on n'ait $A\,, \hat{B} \stackrel{u,r}{\Longrightarrow}$ _ pour aucun $\hat{B}$, et donc que pour tout $\hat{B}$ l'on a $A\,, \hat{B} \stackrel{u,f}{\Longrightarrow}$ _. Supposons que l'on ait de plus toujours $\mathcal{B}/u \neq \Omega$ (u dépend de $\hat{B}$). On définit deux suites infinies $B_1, \ldots, B_n, \ldots$ et $u_1, \ldots, u_n, \ldots$, telles que $B_n \leq \mathcal{B}$ et u_n est une occurrence dans $\mathcal{B}$ pour tout n. On choisit $B_1 \leq \mathcal{B}$ arbitrairement. Si B_n a été construit, on choisit u_n tel que $A\,, B_n \stackrel{u_n,f}{\Longrightarrow}$ _, puis on choisit B_{n+1} minimal tel que $B_n \leq B_{n+1} \leq \mathcal{B}$ et $B_n <_u B_{n+1}$ (ce qui est possible puisque par hypothèse $\mathcal{B}/u_n \neq \Omega$).. On note $U_n = \{u \mid B_n/u = \Omega\}$. On a donc $u_n \in U_n$. On note aussi que U_{n+1} est obtenu à partir de B_n en remplaçant un élément (en l'occurrence u_n) par un ensemble fini d'occurrences de longueur $> |u_n|$. On montre qu'il y a dans $\bigcup U_n$ des u arbitrairement longs. Supposons que non: alors la relation $u\,\mathcal{R}\,v$ si et seulement si $|u| > |v|$ est bien fondée (i.e., n'admet pas de suite infinie décroissante). Mais on a par construction $U_{n+1} < U_n$ pour l'extension multiset de la relation $\mathcal{R}$. Or l'extension multiset d'une relation bien fondée est bien fondée. Contradiction, puisque la suite U_n est infinie. On montre maintenant qu'il y a des u_n arbitrairement longs. Supposons que non, et soit L tel que $L \geq |u_n|$ pour tout n, et soit $L' = \max(\max\{|u| \mid u \in U_1\}, L+1)$. On montre par récurrence que ($u \in U_n \Rightarrow |u| \leq L'$), ce qui constituera une contradiction. L'implication est vraie pour $n = 1$ par définition de L'. Pour le pas de récurrence, il suffit d'observer que les éléments de U_{n+1} sont des éléments de U_n ou sont de longueur $|u_n| + 1$ (par minimalité de B_{n+1}).

L'arbre $\mathcal{T}$ formé par les u_n a donc des branches arbitrairement longues. Par ailleurs, le lemme 2.11 permet de conclure que $\mathcal{T}$ est aussi à branchement fini, car $\mathcal{B}$ est à branchement fini, et toute occurrence définie dans un $\hat{B}$ l'est dans $\mathcal{B}$. Par le lemme de König, l'arbre $\mathcal{T}$ possède alors une branche infinie. Soit u le préfixe de cette branche tel que $u \in Fr(A, \mathcal{B})$. En tronquant éventuellement la liste u_n de ses premiers éléments, on peut écrire $u_n = uv_n$, et il existe alors x tel que $x\,, B_n/u \stackrel{v_n,f}{\Longrightarrow} \_$, ce qui prouve $x \infty \mathcal{B}/u$. On reprend alors le raisonnement ci-dessus en partant cette fois de $\hat{B}_1$ tel que $\hat{B}_1/u = x$. On épuise ainsi progressivement tous les éléments de $Fr(A, \mathcal{B})$, qui est fini. Lorsque cela est fait, on a construit un terme $\hat{B}$ tel que $A'' \leq \hat{B}$, pour une η-expansion appropriée A'' de A. Ce qui contredit $A \not\preceq \hat{B}$. CQFD

Théorème 2.16 *Pour tous λ-termes M, N:*

$$M \leq_{obs} N \Rightarrow BT(M) \preceq_{\infty} BT(N).$$

Preuve. Supposons que $BT(M) \not\preceq_{\infty} BT(N)$, et soient $A \leq BT(M)$, $B \leq BT(N)$, $\hat{B}$, u, $\triangle$ et C donnés par le lemme 2.15. Nous allons montrer que $C[M] \to^* I$ (et a donc une fnt) et que $C[N]$ n'a pas de fnt. Soit M' tel que $M \to^* M'$ et $A \leq \omega(M')$. De $C[A] \to^* I$, on déduit $C[\omega(M')] \to^* I$, et donc $C[M] \to^* C[M'] \to^* I$. Pour N, on raisonne par l'absurde. Si $C[N]$ a une fnt, alors par continuité syntaxique il existe $B' \leq BT(N)$ (que l'on peut prendre assez grand pour que B'/u soit défini) tel que $C[B']$ a une fnt. Nous montrons qu'il ne peut exister de tel B'. Il y a deux cas: Si $\triangle = r$, on a $(B\,|_u) \leq (B'\,|_u)$ et on conclut que $C[B'] \to^* \Omega$ (proposition 2.13(1)). Si $\triangle = f$, on sait par le lemme 2.15 que $B'/u = \Omega$; donc $B =_u B'$, et $C[B']$ n'a pas de fnt (proposition 2.13(2)). CQFD

La réciproque est vraie. Plus précisément, on a la chaîne

$$(M \leq_{obs} N) \Rightarrow (BT(M) \preceq_{\infty} BT(N)) \Rightarrow (\llbracket M \rrbracket \leq \llbracket N \rrbracket) \Rightarrow (M \leq_{obs} N).$$

où la sémantique est relative au modèle D^{∞} et se présente aussi “en forme logique”: l'interprétation d'un terme est l'ensemble des types qu'il peut avoir dans un système de types avec intersections (voir [AmaCur98, section 3.4]). On suppose qu'il y a un type de base κ tel que $\kappa \leq \omega \to \kappa$ et $\omega \to \kappa \leq \kappa$. On esquisse la preuve des deux dernières implications. La première repose sur le théorème des approximations logiques, qui dit que si $\Gamma \vdash M : \sigma$, alors il existe $A \leq BT(M)$ tel que $\Gamma \vdash A : \sigma$. Ce théorème se montre par la technique de réalisabilité ou calculabilité [AmaCur98, Exercice 3.5.19]. Supposons que $BT(M) \preceq_{\infty} BT(N)$ et $\Gamma \vdash M : \sigma$. Soit $A \leq BT(M)$ tel que $\Gamma \vdash A : \sigma$. et soit $B \leq BT(N)$ et $\hat{B}$ tel que $A \preceq \hat{B}$. Alors $\Gamma \vdash \hat{B} : \sigma$, et pour ce faire on se sert de la stabilité du typage par η-expansion, que garantit pour les types de base l'égalité entre κ et $\omega \to \kappa$. L'objectif est de prouver qu'il existe $B' \leq BT(N)$ tel que $\Gamma \vdash B' : \sigma$, car alors $\Gamma \vdash N : \sigma$, grâce à la stabilité du typage (avec intersections!) par β-expansion. On ne peut pas forcément prendre B. Soit u telle que $B/u = \Omega$ et $\hat{B}/u = x$, et donc telle que $x \infty BT(N)/u$. C'est trop brutal de remplacer un x qui peut avoir un type précis par un Ω qui ne peut avoir que le type ω. Mais, comme

x remplace une η-expansion infinie dans $BT(N)$, on peut remplacer x par une approximation suffisante pour que lui soit attribué le type voulu. L'argument est formalisé par les lemmes suivants.

Lemme 2.17 *Si $x \infty \mathcal{B}$, alors $\mathcal{B} = \lambda y_1 \cdots y_n.x\mathcal{B}_1 \cdots \mathcal{B}_n$ $(n \geq 1)$, et $y_i \infty \mathcal{B}_i$, ou $\mathcal{B}_i$ est fini et $\mathcal{B}_i \rightarrow_\eta^\star y_i$, pour chaque i.*

PREUVE. Il est d'abord clair, par définition de ∞, que $\mathcal{B} \neq \Omega$. Donc $\mathcal{B}$ est de la forme $\lambda y_1 \cdots y_m.x\mathcal{B}_1 \cdots \mathcal{B}_n$. Si l'on avait $m \neq n$, on aurait

$$x\,,\lambda y_1 \cdots y_m.x\Omega \cdots \Omega \stackrel{\epsilon,r}{\Longrightarrow} \_\,,$$

mais ceci contredit $x \infty \mathcal{B}$. Donc $m = n$. Il faut ensuite montrer (cf. remarque 2.9) que $y_i \infty \mathcal{B}_i$ ou il existe une approximation finie B_i de $\mathcal{B}_i$ telle que $y_i \preceq B_i$, pour tout i, i.e., il suffit de prouver que si $y_i \not\infty \mathcal{B}_i$, alors il existe $B_i \leq \mathcal{B}_i$ tel que $y_i \preceq B_i$. Par définition de ∞, l'hypothèse $y_i \not\infty \mathcal{B}_i$ signifie qu'il existe $B_i \leq \mathcal{B}_i$ tel que $y_i \preceq \mathcal{B}_i$, ou $y_i\,, B_i \stackrel{u,r}{\Longrightarrow} \_$, ou $y_i\,, B_i \stackrel{u,f}{\Longrightarrow} \_$ et $\mathcal{B}_i/u = \Omega$. Mais $y_i\,, B_i \stackrel{u,r}{\Longrightarrow} \_$ est exclu car car on aurait alors $x\,, B \stackrel{iu,r}{\Longrightarrow} \_$, ce qui contredit $x \infty \mathcal{B}$. On exclut de même le dernier cas. il ne reste donc plus que le premier, i.e., $y_i \preceq B_i$. CQFD

Lemme 2.18 *Si $x \infty \mathcal{B}$, alors, pour tout σ, il existe $B \leq \mathcal{B}$ tel que $x : \sigma \vdash B : \sigma$*

PREUVE. On a $\mathcal{B} = \lambda y_1 \cdots y_n.x\mathcal{B}_1 \cdots \mathcal{B}_n$ (avec $n \geq 1$) par le lemme 2.17. On procède par récurrence sur la taille de σ. Si $\sigma = \omega$, $B = \Omega$ convient. Si $\sigma = \kappa$, alors $B = \lambda y_1 \cdots y_n.x\Omega \cdots \Omega$ convient, car on peut attribuer le type κ à $x\Omega \cdots \Omega$ grâce à l'inégalité $\kappa \leq \omega \rightarrow \kappa$, puis le type κ à B grâce à l'inégalité $\omega \rightarrow \kappa \leq \kappa$. Si $\sigma = \sigma_1 \rightarrow \cdots \rightarrow \sigma_m \rightarrow \kappa$, on peut écrire σ sous la forme $\sigma_1 \rightarrow \cdots \rightarrow \sigma_n \rightarrow \tau$, en utilisant le cas échéant $\kappa = \omega \rightarrow \kappa$. Chacun des σ_i $(i \leq n)$ est donc soit de taille plus petite que celle de σ, soit égal à ω. Il suffit de montrer que l'on peut donner le type σ_i à une approximation B_i de $\mathcal{B}_i$ (sous l'hypothèse $y_i : \sigma_i$), pour chaque i. Ceci est évident si $\sigma_i = \omega$. C'est également clair si $\mathcal{B}_i$ est une η-expansion finie de y_i. Il reste le cas où $\sigma_i \neq \omega$ et $y_i \infty \mathcal{B}_i$: alors on trouve B_i par hypothèse de récurrence. CQFD

Enfin, la dernière implication se montre par la caractérisation des termes qui ont une fnt comme ceux qui ont un type non trivial (livre de Krivine ou [AmaCur98, exercice 3.5.20]).

2.8 λ-calcul simplement typé

Normalisation

On commence par une preuve de la propriété de faible normalisation WN. On pose:

$$O = WN, \quad \text{l'ensemble des termes non typés qui ont une forme normale}$$
$$V = \{xM_1 \cdots M_n \mid M_1, \ldots, M_n \in O\}$$

Si E, F sont deux ensembles de termes non typés, on pose $E \to F = \{M \mid (\forall N \in E\ \ MN \in F)\}$ Les types simples sont construits comme suit:

$$\sigma ::= \kappa \mid \sigma \to \sigma$$

(où κ est un type de base). On interprète les types comme suit:

$$|\kappa| = O \qquad |\sigma \to \tau| = |\sigma| \to |\tau|$$

(On peut ajouter d'autres types de base, et poser $|\kappa| = 0$ pour chaque type de base κ.) On montre

(A) $V \subseteq O$, $V \subseteq O \to V$, et $V \to O \subseteq O$.

(B) Pour tout type σ, $|\sigma|$ est clos par β-expansion: si $M \in |\sigma|$ et $M' \to M$, alors $M' \in |\sigma|$.

Pour (A), $V \subseteq O$ résulte de ce que les réductions à partir d'un terme de la forme $xM_1 \cdots M_n$ les réductions sont indépendantes:

$$xM_1 \cdots M_n \to^\star P \Rightarrow (P = xN_1 \cdots N_n \text{ et } M_1 \to^\star N_1, \ldots, M_n \to^\star N_n)$$

La définition de V a été faite pour avoir (B) (ce qui compte dans V, c'est que V contient les variables). Enfin, si $M \in V \to O$, on a en particulier $Mx \in O$. Il faut déduire $M \in O$, ce qui demande un peu de travail. Soit $Mx \to^\star P$ une dérivation de M vers P normal. On distinque deux cas:

- La réduction ne fait pas interagir M et x. Alors $P = Qx$ (donc Q est normal) et $M \to^\star Q$.

- $M \to^\star \lambda x.R$ (par α-conversion, on peut choisir x comme nom de variable liée) et $R \to^\star P$. Alors $M \to^\star \lambda x.R \to^\star \lambda x.P$.

Dans les deux cas, on conclut $M \in O$.

Pour (B), si $\sigma = \kappa$, c'est évident, car si P est une forme normale de M et $M' \to M$, alors $M' \to M \to^\star P$. Pour $\sigma \to \tau$, c'est évident aussi, car si $M' \to M$, alors $M'N \to MN$.

On prouve maintenant deux autres propriétés:

1. (Lemme fondamental): Si $x_1 : \sigma_1, \ldots, x_n : \sigma_n \vdash M : \tau$, et si $N_1 \in |\sigma_1|, \ldots, N_n \in |\sigma_n|$, alors $M[\vec{x} \leftarrow \vec{N}] \in |\tau|$.

2. Pour tout type σ: $V \subseteq |\sigma| \subseteq O$.

La seconde propriété est une conséquence immédiate de (A), par récurrence sur la taille de σ. Pour le lemme fondamental, les cas variable et application sont évidents, et le cas abstraction est conséquence de la propriété (B).

Comment faut-il adapter cette preuve pour avoir la propriété de forte normalisation SN? On indique ci-dessous les modifications à faire, et on laisse les détails au lecteur:

- Maintenant $|\kappa| = SN$, l'ensemble des termes fortement normalisables. La définition de V ne change pas (mais naturellement l'ensemble V change, puisque O a changé).

- La dernière propriété de (A) est plus facile à prouver, car si Mx est SN, alors M est SN (tous sous-terme d'un terme SN est SN).

- La propriété (B) est fausse, il faut la remplacer par quelque chose de plus prudent:

  $$(M[x \leftarrow N]N_1 \cdots N_n \in |\sigma| \text{ et } N \in \mathrm{SN}) \Rightarrow (\lambda x.M)NN_1 \cdots N_n \in |\sigma|$$

  et la preuve de ce que cette propriété est vraie pour $|\kappa| = SN$ demande un peu de travail (regarder tous les cas de réduction possibles à partir de $M[x \leftarrow N]\vec{N}$.

- Dans la preuve du lemme fondamental, le cas de l'abstraction est encore conséquence de (B) modifié, mais il faut prouver la propriété 2 d'abord.

On considère maintenant les types simples et les λ-termes simplement typés comme les traces propositionnelles de formules et preuves, respectivement, du calcul des prédicats bâti sur deux prédicats de base $V(M)$ et $O(M)$. On va s'intéresser à la trace propositionnelle des preuves propriétés (1) et (2) ci-dessus. La trace propositionnelle $|A|$ d'une formule A est définie comme suit

$$\begin{array}{l} [V(M)] = v \text{ et } [O(M)] = o \\ [A \Rightarrow B] = [A] \to [B] \\ [\forall x \ \ A] = [A] \end{array}$$

(on suppose donc qu'il y a deux types de base v et o). On "escamote" la propriété (B) en prenant comme individus (sujets des prédicats) les *classes d'équivalence* de λ-termes non typés modulo $\beta\eta$. Et on prend les inégalités de la propriété (A) comme axiomes:

$$\begin{array}{ll} (c) & \forall x\ \ V(x) \Rightarrow O(x) \\ (a) & \forall x\ \ V(x) \Rightarrow (\forall y\ \ O(y) \Rightarrow V(xy)) \\ (l) & \forall x\ \ (\forall y\ \ V(y) \Rightarrow O(xy)) \Rightarrow O(x) \end{array}$$

(Notons que e.g. $V(xy)$ est ici un abus de notation pour $V([xy])$, où $[xy]$ est la classe d'équivalence modulo $\beta\eta$ de $[xy]$). On choisit trois variables pour représenter ces hypothèses:

$$\begin{array}{l} c : [\forall x\ \ V(x) \Rightarrow O(x)] = v \to o \\ a : v \to o \to v \\ l : (v \to o) \to o\ . \end{array}$$

Pour commencer, on exprime logiquement la définition de $|\sigma|$, en écrivant maintenant $\sigma^\star(M)$ au lieu de $M \in |\sigma|$:

$$\begin{array}{l} \kappa^\star(M) = O(M) \\ (\sigma \to \tau)^\star(M) = (\forall x\ \ \sigma^\star(x) \Rightarrow \tau^\star(Mx)) \end{array}$$

On vérifie immédiatement que $[\sigma^\star(M)] = \sigma$.

Pour la propriété (2), on construit des preuves $\pi_{V\sigma}$ et $\pi_{\sigma O}$ des inclusions, par récurrence sur σ. Par exemple, la trace propositionnelle, ou *terme extrait* de la preuve de $(\forall x\ \ (\sigma \to \tau)^\star(x) \Rightarrow O(x))$, est $\lambda x.l(\lambda y.Q(x(Py)))$, où P et Q sont les termes extraits des preuves de $(\forall y\ \ (V(y) \Rightarrow \sigma^\star(y)))$ et de $(\forall z\ \ (\tau^\star(z) \Rightarrow O(z)))$. En effet, il s'agit de prouver $(\sigma \to \tau)^\star(x) \Rightarrow O(x)$, ou encore $O(x)$ sous l'hypothèse $(\sigma \to \tau)^\star(x)$, d'où une variable $x : \sigma \to \tau$. Il suffit de prouver $\forall y\ \ V(y) \Rightarrow O(xy)$, grâce à l'axiome l. On cherche donc à prouver $O(xy)$ sous l'hypothèse $V(y)$, d'où une variable $y : V$. Par instanciations correspondant à P, x et Q, nous avons des preuves de $V(y) \Rightarrow \sigma^\star(y)$, $\sigma^\star(y) \Rightarrow \tau^\star(xy)$ et $\tau^\star(xy) \Rightarrow O(xy)$, respectivement, ce qui permet de conclure. Pour l'autre moitié "$V \subseteq |\sigma \to \tau|$" de la propriété (2), le terme suivant fait l'affaire, si P et Q sont extraits des preuves appropriées par récurrence: $\lambda xy.Q(ax(Py))$, où $x : V$ et $y : \sigma$. Le cas de base de la récurrence se règle avec la constante c.

On passe maintenant au lemme fondamental, dont la formalisation est donnée par la formule

$$\forall x_1, \ldots, x_n\ \ \sigma_1^\star(x_1), \ldots, \sigma_n^\star(x_n) \Rightarrow \tau^\star(M) \quad (FV(M) \subseteq \{x_1, \ldots, x_n\})\ .$$

Le terme extrait de la preuve π de $\sigma_1^\star(x_1), \ldots, \sigma_n^\star(x_n) \vdash \tau^\star(M)$ est M lui-même (si l'on choisit de nommer x_i la variable correspondant à l'hypothèse $\sigma_i = |\sigma_i^\star(x_i)|$. Autrement dit, on peut dire que *le typage est la trace propositionnelle de la preuve qu'un terme est réalisable.* Montrons-le par récurrence sur la taille de M. Il s'agit de montrer $\tau^\star(M)$ sous les hypothèses $\sigma_1^\star(x_1), \ldots, \sigma_n^\star(x_n)$, d'où des variables $x_1 : \sigma_1, \ldots, x_n : \sigma_n$. Si $M = x_i$, la preuve est l'axiome, ainsi que sa trace propositionnelle, i.e. $[\pi] = x_i$. Si $M = M_1 M_2$, la preuve de $\tau^\star(M)$ est obtenue en instanciant la preuve de $(\sigma \to \tau)^\star(M_1)$ en M_2, et on a $[\pi] = [\pi_1][\pi_2]$, où π_1 et π_2 sont les preuves pour M_1 et M_2. Donc, par récurrence $[\pi] = M_1 M_2 = M$. Enfin, si $M = \lambda x.P$, on recherche une preuve de $\tau^\star((\lambda x.M)x)$ sous l'hypothèse supplémentaire $\sigma^\star(x)$, d'où une variable $x : \sigma$. Or par récurrence, on a une preuve de $\tau^\star(M)$. Mais comme nos prédicats varient sur des classes déquivalence, $\tau^\star(M)$ et $\tau^\star((\lambda x.M)x)$ sont la même formule, toutes deux abus de langage pour $\tau^\star([M])$.

Si l'on combine maintenant les propriétés (1) et (2), pour $M : \tau$ clos, la trace de la preuve que M est normalisable, i.e., $O(M)$, est le terme $[\pi_{\tau O}]M : o$, dont les seules variables libres sont parmi c, a, l. On examine maintenant la structure des termes de ce type, avec ces variables libres, et *en forme normale*.

Lemme 2.19 *Les termes normaux $x_1 : v, \ldots, x_n : v \vdash N : o$ et $x_1 : v, \ldots, x_n : v \vdash Q : v$ écrits avec $c : v \to o$, $a : v, o \to v$ et $l : (v \to o) \to o$ sont donnés par la syntaxe suivante (où $x : v$):*

$$\begin{aligned} N &::= cQ \mid l(\lambda x.N) \mid lc \\ Q &::= x \mid aQN \end{aligned}$$

De plus, au cas lc près, ces termes sont en bijection avec les formes normales du λ-calcul sans types.

Preuve. La preuve se fait par examen des cas. Si N et Q sont comme dans l'énoncé, ils ne peuvent commencer par λ, puisque leur type est de base. Donc ils sont de la forme $y\vec{M}$, avec $y \in \{c, a, l\}$ ou $y : v$. On en déduit que les seuls termes possibles pour N (Q) sont cQ, lR (x, aQN), avec $R : v \to o$. Il reste donc à analyser les termes $R : v \to o$ possibles (mêmes variables libres). Un tel terme est soit de la forme $\lambda x.N$, soit de la forme $x\vec{N}$, mais l'examen des types possibles de y donne lc comme seule possibilité (par exemple, aQ est de type $o \to v$, et non $v \to o$).

La seconde partie de l'énoncé est conséquence immédiate de l'écriture des termes M en forme normale du λ-calcul sous la forme suivante (noter qu'au passage cette présentation enlève les … de la présentation compacte habituelle $M ::= \lambda x_1 \ldots c_m..yM_1 \ldots M_n$):

$$\begin{aligned} M &::= \lambda x.M \mid P \\ P &::= x \mid PM \end{aligned}$$

CQFD

Mais on peut pousser le bouchon un peu plus loin. Le lemme précédent suggère de définir un codage des β-formes normales non typées par des termes normaux typés comme suit.

Définition 2.20 *On définit deux fonctions de codage comme suit:*

$$\begin{array}{ll} |\lambda x.M| = l(\lambda x.|M|) & |P| = c|P|' \\ |x|' = x & |PM|' = a|P|'|M| \end{array}$$

Si $FV(M) \subseteq \{x_1, \ldots, x_n\}$), on a

$$c : v \to o, a : v \to o \to v, l : (v \to o) \to o, x_1 : v, \ldots, x_n : v \vdash |M| : o$$

et de même $\ldots \vdash |P|' : v$ (quelque soit les types des variables x dans les termes sources).

On pose

$$\mathbf{N} = (v \to o) \to (v \to o \to v) \to ((v \to o) \to o) \to o$$

$\mathbf{N}$ peut être considéré comme le *type des* (codages des) λ-*termes non typés en forme normale.*

Lemme 2.21 *Si π est une preuve de $O(M)$ sous les hypothèses $(c), (a)$ et (l), et $[\pi]$ est β-normal, alors il existe un (unique) terme β-normal $M^\dagger$ tel que $M =_{\beta\eta} M^\dagger$ et $[\pi] = |M^\dagger|$.*

Preuve. Pour dérouler la récurrence, il faut étendre l'énoncé d'une part à des preuves qui ont aussi des hypothèses de la forme $V(x)$ (qui deviennent des hypothèse $x : v$ dans l'extraction, avec le *même* x), et d'autre part aux preuves π' de $V(P)$: on montre alors qu'il existe un terme normal $P^\dagger$ tel que $P =_{\beta\eta} P^\dagger$ et $[\pi] = |P^\dagger|'$. L'existence (et l'unicité) de $M^\dagger$ ($P^\dagger$) sont garanties par le lemme précédent (le cas lc peut être simulé par $l(\lambda x.cx)$). L'enjeu est donc de vérifier la relation entre M et $M^\dagger$ (P et $P^\dagger$). On procède par récurrence sur la taille.

- Si $[\pi] = cQ$, π a instancié c en M (soit par instanciation directe, soit par une suite d'instanciations et de généralisations dont le détail n'importe pas), et Q est la trace d'une preuve π' de $V(M)$. Donc, par récurrence, $Q = |M^\dagger|'$ avec $M =_{\beta\eta} M^\dagger$, On a bien ce qu'il faut, puisque $[\pi] = cQ = |M^\dagger|$.

- Si $[\pi] = l(\lambda x.N)$, π a instancié l en M, tandis que la preuve dont $\lambda x.N$ est est l'extraction est une preuve de $O(Mx)$ sous l'hypothèse supplémentaire $V(x)$, suivie d'une décharge et d'une généralisation. Par récurrence, il existe $N^\dagger$ tel que $N = |N^\dagger|$ et $Mx =_{\beta\eta} N^\dagger$. On a bien ce qu'il faut en prenant $M^\dagger = \lambda x.N^\dagger$, car $[\pi] = l(\lambda x.|N^\dagger|) = |\lambda x.N^\dagger|$, et $\lambda x.N^\dagger =_{\beta\eta} \lambda x.Mx =_\eta M$ (c'est ici qu'intervient la règle η).

- Si $P = x$, il n'y a rien à faire: la preuve π ne peut être que l'axiome qui dérive $V(x)$.

- Si $[\pi] = aQN'$, π a instancié a avec un terme P, la preuve π_1 dont Q est extrait est une preuve de $V(P)$, la preuve dont aP' est extrait se termine par une instanciation avec un terme M', et la preuve π_2 dont N' est extrait est une preuve de $O(M')$. De plus, $M = PM'$. Par récurrence, il existe $P^\dagger$ et $M'^\dagger$ tels que $[\pi_1] = |P^\dagger|'$, $P =_{\beta\eta} P^\dagger$, $[\pi_2] = |M'^\dagger|$ et $M' =_{\beta\eta} M'^\dagger$. On prend $M^\dagger = P^\dagger M'^\dagger$. Cela convient, car $[\pi] = a|P^\dagger|'|M'^\dagger| = |P^\dagger M'^\dagger|$ et $P^\dagger M'^\dagger =_{\beta\eta} PM' = M$. CQFD

Théorème 2.22 *Soit σ un type quelconque. Il existe un terme $\Theta : \sigma \to \mathbf{N}$ (ne dépendant que de σ) tel que pour tout terme clos $M : \sigma$ il existe un terme N β-normal et $\beta\eta$-équivalent à M tel que $\Theta M \to_\beta^\star \lambda cal.|N|$.*

Preuve. On peut reformuler l'énoncé en: il existe un terme $\theta : \sigma \to o$ de variables libres parmi c, a, l, tel que $\theta M \to_\beta^\star |N|$. On prend $\theta = [\pi_{\sigma O}]$. Il résulte des considérations ci-dessus sur la formalisation des propriétés (1) et (2) que θM est la trace propositionnelle d'une preuve de $O(M)$. On conclut donc grâce au lemme 2.21, et grâce à la propriété suivante:

- Si $M = [\pi]$ et $M \to M'$, alors il existe une preuve π' de mêmes hypothèses et de même conclusion que π telle que $M' = [\pi']$. (En fait, la manière propre de faire est de définir une notion de réduction entre preuves, et de monter qu'on a en réalité $\pi \to^\star \pi'$.) CQFD

Ce théorème va nous servir à montrer un théorème de complétude. Mais on montre d'abord que ce théorème est lui-même équivalent à d'autres énoncés purement syntaxiques. Un modèle plein du λ-calcul simplement typé est donné par une interprétation arbitraire $[\![\kappa]\!]$ de chaque type de base κ, qui détermine le reste de l'interprétation: $[\![\sigma \to \tau]\!] = [\![\tau]\!]^{[\![\sigma]\!]}$ (l'ensemble de *toutes* les fonctions de $[\![\sigma]\!]$ dans $[\![\tau]\!]$ – d'où le qualificatif “plein”). Le modèle est dit fini si les types de base sont interprétés par des ensembles finis. Dans ce qui suit, on suppose pour simplifier qu'il y a un seul type de base κ.

Théorème 2.23 *Les trois énoncés suivants sont vrais et équivalents:*

1. *(Théorème de complétude de Statman) Si $[\![M]\!] = [\![N]\!]$ dans tous les modèles pleins finis, alors $M =_{\beta\eta} N$.*

2. *(Théorème de Böhm typé) Si M et N sont non $\beta\eta$-équivalents et de même type $\sigma_1 \to \cdots \to \sigma_r \to \kappa$, alors il existe n et $P_1 : \sigma_1[\kappa \leftarrow (\kappa^n \to \kappa)], \ldots, P_r : \sigma_r[\kappa \leftarrow (\kappa^n \to \kappa)]$ tels que*

$$\begin{array}{l} M[\kappa \leftarrow (\kappa^n \to \kappa)]P_1 \cdots P_r \to^\star \lambda x_1 \ldots x_n.x_1 \\ N[\kappa \leftarrow (\kappa^n \to \kappa)]P_1 \cdots P_r \to^\star \lambda x_1 \ldots x_n.x_2\ . \end{array}$$

3. *La $\beta\eta$-conversion est une relation maximale parmi les relations non triviales $\sim$ qui sont closes par les deux règles suivantes:*

$$\textit{(congruence)}\ \frac{M \sim M'}{MN \sim M'N} \qquad \textit{(instantiation)}\ \frac{M \sim M'}{M[\kappa \leftarrow \sigma] \sim M'[\kappa \leftarrow \sigma]}$$

Preuve. On montre d'abord leur équivalence.

(1) $\Rightarrow$ (2) On passe par l'intermédiaire d'une extension de la syntaxe (pour chaque $n \geq 2$). Λ_n est défini par:

$$M ::= x \mid MN \mid \lambda x.M \mid c_1 \| \cdots \mid c_n \mid cond_n$$

avec $c_1, \ldots, c_n : \kappa$ and $cond_n : \kappa^{n+1} \to \kappa$, et les règles additionnelles suivantes, pour tout i:

$$cond_n c_i M_1 \ldots M_n \ \to\ M_i\ .$$

Soit $\mathcal{M}_n$ le modèle plein défini par $[\![\kappa]\!] = \{c_1, \ldots, c_n\}$. On a les propriétés suivantes (on interprète de la manière évidente les constantes de Λ_n):

(A) Λ_n, muni de β et de la règle ci-dessus est confluent et SN.

(B) Tout point de $\mathcal{M}_n$ est définissable, i.e., pour tout σ et $a \in [\![\sigma]\!]$, il existe un terme $\vdash M : \sigma$ de Λ_n tel que $[\![M]\!] = a$.

On omet la preuve de la première propriété (la preuve de SN est une adaptation mineure de la preuve donnée plus haut), la confluence locale est aisée à vérifier).

Preuve de (B) On construit de tels termes, notés M_a, par récurrence sur les types; on prouve en fait simultanément que de plus il existe un terme $\vdash \delta_a : \sigma \to \kappa$ tel que, pour tout M:

$$([\![M]\!] = a \Rightarrow \delta_a M \to^\star c_1) \quad \text{et} \quad ([\![M]\!] \neq a \Rightarrow \delta_a M \to^\star c_2)\ .$$

Ceci est clair pour κ: on prend $\delta_{c_i} = \lambda x.cond_n x \underbrace{c_2 \ldots c_2}_{i-1} c_1 \underbrace{c_2 \ldots c_2}_{n-i}$. Pour $\sigma \to \tau$ et $f \in [\![\sigma \to \tau]\!]$, on définit (si $[\![\sigma]\!] = \{\alpha_1, \ldots, \alpha_k\}$):

$$\begin{array}{l} M_f = \lambda x.\mathit{If}(\delta_{\alpha_1}(x))(M_{f(\alpha_1)})(\delta_{\alpha_2}(x)\ldots) \\ \delta_f = \lambda x.\mathit{And}\ (\delta_{f(\alpha_1)}(xM_{\alpha_1}))(\mathit{And}\ (\delta_{f(\alpha_2)}(xM_{\alpha_2}))\ldots) \end{array}$$

où les ... sont faciles à remplir. En termes plus informels, M_a teste la valeur de son argument x et si cette dernière est α_i, alors le programme rend $f(\alpha_i)$. Le test que x est f consiste à tester leur égalité sur tous les points $\alpha_1, \ldots, \alpha_k$ (d'où la conjonction). Il reste à montrer que $\mathit{And} : \kappa^2 \to \kappa$ et $\mathit{If} : \kappa \to \sigma \to \sigma \to \sigma$ sont définissables, ce qui est aisé (le contenu des ... est indifférent):

$$\begin{array}{l} \mathit{If} = \lambda x y_1 y_2 \vec{z}.cond_n x(y_1\vec{z})(y_2\vec{z})\ldots \\ \mathit{And} = \lambda x_1 x_2.cond_n x_1 x_2 c_2 \ldots \end{array}$$

Retour à la preuve de (1) $\Rightarrow$ (2) Si M, N sont deux λ-termes de type $\sigma_1 \to \cdots \to \sigma_r \to \kappa$ tels que $M \neq_{\beta\eta} N$, on a par (1) qu'il existe un modèle fini, disons (sans perte de généralité) $\mathcal{M}_n$, tel que $[\![M]\!] \neq [\![N]\!]$ dans ce modèle. Il existe donc $\alpha_1, \ldots, \alpha_r$ tels que $[\![M]\!]\alpha_1 \ldots \alpha_r \neq [\![N]\!]\alpha_1 \ldots \alpha_r$, ce que l'on peut reformuler, grâce à la propriété (B), en: $[\![MM_{\alpha_1} \ldots M_{\alpha_r}]\!] \neq [\![NM_{\alpha_1} \ldots M_{\alpha_r}]\!]$. Les deux termes $MM_{\alpha_1} \ldots M_{\alpha_r}$ et $NM_{\alpha_1} \ldots M_{\alpha_r}$ ont une forme normale, par la propriété (A). Une forme normale close de type κ ne peut être qu'une constante c_i. Donc, ces formes normales sont c_i et c_j respectivement, et on a $i \neq j$, car

$$c_i = [\![c_i]\!] = [\![MM_{\alpha_1} \ldots M_{\alpha_r}]\!] \neq [\![NM_{\alpha_1} \ldots M_{\alpha_r} = [\![c_j]\!] = c_j$$

On peut, par exemple, supposer que $i = 1$ et $j = 2$. En résumé, nous avons obtenu:

$$\begin{array}{l} MM_{\alpha_1} \ldots M_{\alpha_r} \to^\star c_1 \\ NM_{\alpha_1} \ldots M_{\alpha_r} \to^\star c_2 \end{array}$$

Ce résultat a un "air" de théorème de Böhm. Il ne reste plus qu'à se débarrasser des constantes de Λ_n et des règles de calcul additionnelles. Ceci est possible en codant les c_i par les projections $\lambda x_1 \ldots x_n.x_i$ et $cond_n$ par $\lambda z x_1 \ldots x_n.z x_1 \ldots x_n$. Il suffit au préalable de remplacer partout le type κ par le type $\kappa^n \to \kappa$. Si l'on pose

$$P_i = M_{\alpha_i}[\kappa \leftarrow \kappa^n \to \kappa][c_1 \leftarrow \lambda x_1 \ldots x_n.x_1] \ldots [c_n \leftarrow \lambda x_1 \ldots x_n.x_n] \ ,$$

on obtient bien

$$\begin{array}{l} M[\kappa \leftarrow (\kappa^n \to \kappa)]P_1 \cdots P_r \to^\star \lambda x_1 \ldots x_n.x_1 \\ N[\kappa \leftarrow (\kappa^n \to \kappa)]P_1 \cdots P_r \to^\star \lambda x_1 \ldots x_n.x_2 \ . \end{array}$$

(2) $\Rightarrow$ (3) Soit en effet $\sim$ une telle relation, et supposons que $M \sim N$, mais $M \neq_{\beta\eta} N$. Alors, en utilisant les termes $P_1, \ldots, P_r$ de l'énoncé de (2), et les règles (*congurence*) et (*instantiation*), on obtient $\lambda x_1 \ldots x_n.x_1 \sim \lambda x_1 \ldots x_n.x_2$. Donc, par congruence encore, pour *tous* P, Q:

$$P \sim (\lambda x_1 \ldots x_n.x_1)PQ \ldots \sim (\lambda x_1 \ldots x_n.x_2)PQ \ldots \sim Q \ .$$

(3) $\Rightarrow$ (1) On pose $M \sim N$ ssi M et N ont la même interprétation dans tous les modèles finis (cette relation est non triviale, car par exemple $\lambda x_1 x_2.x_1$ et $\lambda x_1 x_2.x_2$ ont des intrprétations differéntes dés que $[\![\kappa]\!]$ a au moins deux éléments). La relation $\sim$ contient $\beta\eta$ puisque par définition les modèles valident tous β et η; elle satisfait la règle *(congruence)* parce que l'interprétation est compositionnelle; enfin la propriété *(instantiation)* est conséquence de la remarque suivante: l'interprétation de $M[\kappa \leftarrow \sigma]$ dans le modèle $\mathcal{M}$ est l'interprétation de M dans le modèle $\mathcal{M}'$ tel que $[\![\kappa]\!]' = [\![\sigma]\!]$.

(1) On prouve maintenant le théorème de complétude de Statman. On construit un modèle $\mathcal{M}$ sur deux (nouveaux) types de base v et o comme suit: $[\![o]\!]$ ($[\![v]\!]$) est l'union de l'ensemble des termes en forme normale de la forme M (P) (cf. preuve du lemme 2.19), de taille $\leq n$, et de $\{\perp\}$. On choisit n "assez grand" (on précisera plus tard). Si κ est le type (ou un type) de base, on les interprète comme on veut. On interprète c, a, l comme suit: $[\![c]\!]$ est l'inclusion de $[\![v]\!]$ dans $[\![o]\!]$, et

$$[\![a]\!]PM = \begin{cases} PM & \text{si } \mathit{taille}(MN) \leq n \\ \perp & \text{sinon} \end{cases}$$

$$[\![l]\!](f) = \begin{cases} \lambda x.M & \text{si } f(z_1) = M[x \leftarrow z_1] \\ & \text{et } f(z_2) = M[x \leftarrow z_2] \;\; (\text{et } FV(M) \subseteq \{x, z_1, z_2\}) \\ \perp & \text{sinon} \end{cases}$$

La raison de *deux* variables z_1 et z_2 ci-dessus tient au fait que $f(z_1) = M[x \leftarrow z_1]$ seule ne suffit pas à identifier M: on a par exemple $z_1[x \leftarrow z_1] = z_1 = x[x \leftarrow z_1]$. Par contre, on peut montrer facilement que si M et N sont tels que $M[x \leftarrow z_1] = N[x \leftarrow z_1]$ et $M[x \leftarrow z_2] = N[x \leftarrow z_2]$, alors $M = N$: la définition ci-dessus n'est donc pas ambigüe. On montre ensuite que pour tout terme M (P) (normal) clos de taille $\leq n$, on a (ρ étant l'environnement qui interprète c, a, l comme indiqué ci-dessus):

$$[\![|M|]\!]\rho = M \quad \text{et} \quad [\![|P|']\!]\rho = P\ .$$

Ceci se montre de manière routinière par récurrence sur la taille de M (P). Il faut étendre ρ à toutes les variables libres $x_1, \ldots, x_n$ de $|M|$ ($|P|'$), qui sont de type v. Il faut prendre tous les ρ tels que $\rho(x_i) \in \{z_1, z_2\}$ pour tout i (cf. la définition de $[\![l]\!]$), et montrer (détails omis):

$$\begin{array}{l} [\![|M|]\!]\rho = M[x_1 \leftarrow \rho(x_1)] \ldots [x_n \leftarrow \rho(x_n)] \\ [\![|P|']\!]\rho = P[x_1 \leftarrow \rho(x_1)] \ldots [x_n \leftarrow \rho(x_n)] \end{array}$$

La fin de l'argument est simple. Puisque $[\![M]\!] = [\![N]\!]$ dans tous les modèles, par le théorème 2.22, il existe deux formes β-normales $M^\dagger$ et $N^\dagger$ telles que $M^\dagger =_{\beta\eta} M$ et $N^\dagger =_{\beta\eta} N$ et $[\![|M^\dagger|]\!]\rho = [\![|N^\dagger|]\!]\rho$ dans tous les modèles et pour tous les ρ, donc en particulier dans le modèle ci-dessus (en prenant soin que $n \geq \mathit{taille}(M^\dagger), \mathit{taille}(N^\dagger)$) et pour le ρ ci-dessus. Donc $M^\dagger = [\![|M^\dagger|]\!]\rho = [\![|N^\dagger|]\!]\rho = N^\dagger$, i.e., $M^\dagger$ et $N^\dagger$ *coïncident*, et l'on peut conclure que $M =_{\beta\eta} N$. CQFD

3 Un peu de logique linéaire

La logique intuitionniste est constructive, ce qui s'exprime le plus souvent par l'interdiction du tiers exclu $\vdash$ (A ou (non A)), mais en fait plus emblématiquement par la propriété de disjonction: si on a une preuve de $\vdash (A \text{ ou } B)$, alors c'est que l'on a une preuve de $\vdash A$ ou une preuve de $\vdash B$. Cette propriété dépend crucialement du fait que la contraction n'est pas autorisée à droite de $\vdash$, ce qui fait que les preuves sans coupure de $\vdash (A \text{ ou } B)$ se terminent forcément par une introduction du connecteur "ou". Le fait que la contraction n'est pas autorisée est une conséquence de la limitation à une seule formule de la partie droite des séquents intuitionnistes. En fait, Girard a observé que cette limitation n'est là que pour cela. Il est impossible d'écrire en logique intuitionniste $\vdash A, (\text{non } A)$. Mais on pourrait l'accepter, et tout de même refuser $\vdash (A \text{ ou } (\text{non } A))$, en remarquant que pour passer de $\vdash A, (\text{non } A)$ à $\vdash (A \text{ ou } (\text{non } A))$, on utilise implicitement une contraction à droite. Si en effet les règles pour l'introduction à droite de la disjonction sont

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash (A \text{ ou } B), \Delta} \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash (A \text{ ou } B), \Delta}$$

(et ce sont en effet ces règles qui permettent de conclure à la propriété de disjonction ci-dessus), alors la règle

$$\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash (A \text{ ou } B), \Delta}$$

qui permet de conclure au tiers exclu se dérive des deux règles ci-dessus en utilisant la contraction:

$$\cfrac{\cfrac{\cfrac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash (A \text{ ou } B), B, \Delta}}{\Gamma \vdash (A \text{ ou } B), (A \text{ ou } B), \Delta}}{\Gamma \vdash (A \text{ ou } B), \Delta}$$

En logique linéaire, les contractions sont aussi contraintes, mais la restriction, au lieu d'être placée sur une zone spéciale du séquent, est internalisée dans la syntaxe même des formules: la contraction à droite ne peut s'effectuer que sur des formules de la forme $?A$. Donc les règles d'introduction de la disjonction ci-dessus ne sont plus inter-définissables, ce qui conduit à deux connecteurs distincts: $\oplus$ et $\wp$, appelés respectivement additif et multiplicatif (et en effet, dans leur interprétation en termes d'espaces de cohérence, on voit apparaître naturellement un cardinal somme et un cardinal produit):

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash (A \oplus B), \Delta} \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash (A \oplus B), \Delta} \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash (A \wp B), \Delta}$$

En logique linéaire, on aura donc le "tiers exclu" *et* la propriété de disjonction, mais avec deux connecteurs *différents*:

- $\vdash A \wp (A^\perp)$.
- Si $\vdash (A \oplus B)$, alors $\vdash A$ ou $\vdash B$.

(Notons qu'il est incompatible d'avoir ces deux propriétés à la fois pour un seul connecteur: si A est un atome, on ne peut pas le prouver, ni prouver sa négation – dans un modèle, A ((non A)) n'est pas vrai pour l'interprétation qui affecte la valeur faux (vrai) à A.)

Il reste cependant une trace de l'interdéfinissabilité des deux connecteurs, obtenue en insérant des modalités. Dans un premier temps, on se contente de nommer les deux disjonctions différemment. Pour prouver $(A \wp B) \vdash (A \oplus B)$, on doit utiliser la contraction:

$$\dfrac{\dfrac{\dfrac{\vdash A^\perp, A}{\vdash A^\perp, (A \oplus B)} \qquad \dfrac{\vdash B^\perp, B}{\vdash B^\perp, (A \oplus B)}}{\vdash (A^\perp \otimes B^\perp), (A \oplus B), (A \oplus B)}}{\vdash (A^\perp \otimes B^\perp), (A \oplus B)}$$

Il conviendra donc de faire deux dérélictions sur $A \oplus B$. Dans l'autre sens, on doit utiliser l'affaiblissement:

$$\dfrac{\dfrac{\dfrac{\vdash A^\perp, A}{\vdash A^\perp, A, B} \qquad \dfrac{\vdash B^\perp, B}{\vdash B^\perp, A, B}}{\vdash (A^\perp \& B^\perp), A, B}}{\vdash (A^\perp \& B^\perp), (A \wp B)}$$

Il faut donc une déréliction sur A et une déréliction sur B. On aura donc $?(A \oplus B)$ et $(?A \wp ?B)$ dans les séquents finaux des deux preuves. Par dualité, ceci nous conduit à remplacer $(A^\perp \& B^\perp)$ et $(A^\perp \otimes B^\perp)$ par $!(A^\perp \& B^\perp)$ et $(!A^\perp \otimes !B^\perp)$. Ces ! sont introduits par promotion. Voici les preuves ainsi "décorées linéairement":

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdash A^\perp, A}{\vdash A^\perp, (A \oplus B)}}{\vdash A^\perp, ?(A \oplus B)}}{\vdash !A^\perp, ?(A \oplus B)} \qquad \dfrac{\dfrac{\dfrac{\vdash B^\perp, B}{\vdash B^\perp, (A \oplus B)}}{B^\perp, ?(A \oplus B)}}{!B^\perp, ?(A \oplus B)}}{\vdash (!A^\perp \otimes !B^\perp), ?(A \oplus B), ?(A \oplus B)}}{\vdash (!A^\perp \otimes !B^\perp), ?(A \oplus B)}$$

REGLES LOGIQUES

$$(Axiome)\quad \frac{}{\vdash A, A^{\perp}} \qquad (Coupure)\quad \frac{\vdash A, \Gamma \quad \vdash A^{\perp}, \Delta}{\vdash \Gamma, \Delta} \qquad (Echange)\quad \frac{\vdash \Gamma}{\vdash \sigma(\Gamma)}$$

CONNECTEURS MULTIPLICATIFS

$$(I)\quad \vdash I \qquad\qquad (\perp)\quad \frac{\vdash \Gamma}{\vdash \perp, \Gamma}$$

$$(\otimes)\quad \frac{\vdash A, \Gamma \quad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta} \qquad (\wp)\quad \frac{\vdash A, B, \Gamma}{\vdash A \wp B, \Gamma}$$

CONNECTEURS ADDITIFS

$$(1)\quad \vdash 1, \Gamma \qquad (\times)\quad \frac{\vdash A, \Gamma \quad \vdash B, \Gamma}{\vdash A \times B, \Gamma} \qquad (\oplus)\quad \frac{\vdash A, \Gamma}{\vdash A \oplus B, \Gamma} \quad \frac{\vdash B, \Gamma}{\vdash A \oplus B, \Gamma}$$

CONNECTEURS EXPONENTIELS

$$(Promotion)\quad \frac{\vdash A, ?B_1, \ldots, ?B_n}{\vdash !A, ?B_1, \ldots, ?B_n} \qquad (D\acute{e}r\acute{e}liction)\quad \frac{\vdash A, \Gamma}{\vdash ?A, \Gamma}$$

$$(Contraction)\quad \frac{\vdash ?A, ?A, \Gamma}{\vdash ?A, \Gamma} \qquad (Affaiblissement)\quad \frac{\vdash \Gamma}{\vdash ?A, \Gamma}$$

Figure 1: Règles de la logique linéaire

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\vdash A^{\perp}, A}{\vdash A^{\perp}, ?A}}{\vdash A^{\perp}, ?A, ?B} \qquad \cfrac{\cfrac{\vdash B^{\perp}, B}{\vdash B^{\perp}, ?B}}{\vdash B^{\perp}, ?A, ?B}}{\vdash (A^{\perp} \& B^{\perp}), ?A, ?B}}{\vdash !(A^{\perp} \& B^{\perp}), ?A, ?B}}{\vdash !(A^{\perp} \& B^{\perp}), (?A \wp ?B)}$$

4 Variables locales

On s'intéresse à la sémantique des commandes impératives suivantes, que l'on combine avec la programmation fonctionnelle, i.e. le λ-calcul.

- affectation: $X := e$
- accès au contenu d'une variable: $\mathit{deref}\ X$
- déclaration de variable locale: $\mathit{new}\, X.C$ (allocation d'un emplacement pour x, initialisation à 0, exécution de C et désallocation).

Les types sont: **int**, **var** , **comm**.

$$\frac{\Gamma \vdash X : \mathbf{var} \quad \Gamma \vdash E : \mathbf{int}}{\Gamma \vdash (X := e) : \mathbf{comm}} \qquad \frac{\Gamma \vdash X : \mathbf{var}}{\Gamma \vdash \mathit{deref}\ X : \mathbf{int}}$$

$$\frac{\Gamma, X : \mathbf{var} \vdash C : \mathbf{comm}}{\Gamma \vdash (\mathit{new}\ X.C) : \mathbf{comm}}$$

On commence par une sémantique naïve, que l'on va critiquer. On suppose donné un ensemble L d'adresses mémoire (locations en anglais). On définit l'ensemble S des états par:

$$S \;=\; L \;\rightarrow\; (V + \{\mathit{unused}\})$$

Puis, en ignorant la divergence, on pose:

$$[\![\mathbf{comm}]\!] = S \rightarrow S \quad [\![\sigma \rightarrow \tau]\!] = [\![\sigma]\!] \rightarrow [\![\tau]\!]$$

$$[\![\mathbf{int}]\!] = S \rightarrow V \qquad [\![\mathbf{var}\ ]\!] = L\ ,$$

où V est l'ensemble des valeurs (ici les entiers). Et on interprète les nouvelles primitives comme suit:

$$\begin{array}{lcl}
[\![X := e]\!]\rho s & = & s[\rho(X) \leftarrow [\![e]\!]\rho] \\
[\![\mathit{deref}\ X]\!]\rho s & = & s(\rho(X)) \\
[\![\mathit{new}\ X.C]\!]\rho s & = & ([\![C]\!]\rho[X \leftarrow l]s[l \leftarrow 0])[l \leftarrow \mathit{unused}] \quad (s(l) = \mathit{unused})\ .
\end{array}$$

Cette sémantique n'est pas satisfaisante, car on n'a pas nécessairement

$$[\![(\mathit{new}\ X.C)]\!] = [\![C]\!]$$

lorsque X n'est pas libre dans C. L'interprétation de C à gauche et à droite se fait dans un état où $s(l) = 0$ et $s(l) = \mathit{unused}$, respectivement, et rien ne garantit que $[\![C]\!]$ soit insensible à cette différence sur l, l'hypothèse concernant C portant sur X.

Une meilleure sémantique, qui soigne ce défaut, et qui permet aussi de valider bien d'autres équivalences, est fournie par une paramétrisation par rapport aux supports mémoire utilisés. On explique d'abord cette idée dans un cadre concret. On se donne une catégorie $\mathbf{W}$ dont les objets sont les ensembles finis $w = \{0, \ldots, w-1\}$ et dont les flèches sont les injections. On relativise tout à ces mondes: les types sont des foncteurs de $\mathbf{W}$ dans la catégorie des ensembles (ou une catégorie de domaines), et les termes sont interprétés comme des transformations naturelles:

$$[\![\mathbf{comm}]\!]w = S(w) \to S(w)$$

$$[\![\mathbf{int}]\!]w = S(w) \to V \qquad\qquad [\![\mathbf{var}\,]\!]w = w\ ,$$

où $S(w) = w \to V$.

$$[\![\mathbf{comm}]\!]fcsl = \begin{cases} c(s \circ f)(l') & \text{si } f(l') = l \\ s(l) & \text{si } l \notin im(f) \end{cases}$$

$$[\![\mathbf{int}]\!]fes = e(s \circ f) \qquad\qquad\qquad [\![\mathbf{var}\,]\!]f = f\ ,$$

$$[\![new\ X.C]\!]w\rho s \quad = \quad ([\![C]\!](w+1)\overline{\rho}[X \leftarrow l]s[l \leftarrow 0]) \mid_w\ .$$

où $|_w=$ dénote la restriction à w, et où $\overline{\rho}$ est l'image composante par composante de ρ dans le monde $w+1$. Voici façon plus catégorique de dire les choses: si f est l'inclusion de w dans $w+1$, $s' \mid_w = s' \circ f$ $(s' : (w+1) \to V)$ et $\overline{\rho} = [\![\Gamma]\!]f\rho$.

Si on veut prouver que $[\![new\ X.C]\!]$ est naturelle, on doit passer des inclusions aux injections.

On passe ensuite à un point de vue plus abstrait, où l'on ne rentre pas dans le détail de la structuration de la mémoire. Les mondes sont maintenant des ensembles d'états possibles, chaque monde correspondant à une structuration de la mémoire (store shape). On passe de w à $W = w \to V$, en oubliant w. Les variables sont maintenant interprétées comme un type de donnée abstrait: une variable est un objet qui peut être affecté (écriture) et déréférencée (lecture). Ceci mène à:

$$[\![\mathbf{comm}]\!]W = W \to W$$

$$[\![\mathbf{int}]\!]W = W \to V \qquad [\![\mathbf{var}\,]\!]W = (V \to [\![\mathbf{comm}]\!]W) \times [\![\mathbf{int}]\!]\ ,$$

$$\begin{array}{lcl} [\![X := e]\!]W\rho w & = & fst([\![X]\!]W\rho)([\![e]\!]W\rho w)w \\ [\![deref\ X]\!]W\rho & = & snd([\![X]\!]W\rho) \\ [\![new\ X.C]\!]W\rho w & = & fst([\![C]\!](W \times V)(\overline{\rho},(a,e))(w,0)). \end{array}$$

où $\overline{\rho}$ est comme ci-dessus l'image de ρ: $\overline{\rho} = expand\rho$, et où $(a,e) \in [\![var]\!](W \times V)$ est défini par:

$$a(v)(w,v') = (w,v) \qquad e(w,v) = v\ .$$

On est resté discret, depuis le passage aux mondes (concrets puis abstraits) sur l'interprétation des types fonctionnels: lemme de Yoneda.

Paramétricité.

$$[\![(new\ X.P(X := X + 1))]\!] = [\![P(skip)]\!]$$

Une approche différente est offerte par la sémantique des jeux: les états sont dilués dans l'histoire des variables impératives.

Le type **int** est interprété par le jeu qui a un mouvement opposant ? et les mouvements joueurs n. Le type **comm** est interprété par le jeu qui a deux mouvements: *run* et *done*, qui sont respectivement opposant et joueur. Le type **var** est interprété par le jeu qui a pour mouvements opposants *read* et $write(n)$ et pour mouvements joueurs n et OK.

- Séquencement de type $\mathbf{comm}_1 \times \mathbf{comm}_2 \rightarrow \mathbf{comm}_\epsilon$):

$$run_\epsilon\ run_1\ done_1\ run_2\ done_2\ done_\epsilon\ .$$

- Séquencement de type $\mathbf{comm}_1 \times \mathbf{int}_2 \rightarrow \mathbf{int}$ (c; *return* e):

$$?_\epsilon\ run_1\ done_1\ ?_2\ n_2\ n_1\ .$$

- *deref* : $\mathbf{var}_1 \rightarrow \mathbf{int}_\epsilon$:

$$?_\epsilon\ read_1\ n_1\ n_\epsilon\ .$$

- Affectation de type $\mathbf{var}_1 \times \mathbf{int}_2 \rightarrow \mathbf{comm}_\epsilon$:

$$run_\epsilon\ ?_2\ n_2\ write(n)_1\ OK_1\ done_\epsilon\ .$$

- *new* : $(\mathbf{var}_{11} \rightarrow \mathbf{comm}_1) \rightarrow \mathbf{comm}_\epsilon$ (initialisation de la variable non comprise):

$$\mathit{run}_\epsilon\ \mathit{run}_1 \begin{cases} \mathit{done}_1\ \mathit{done}_\epsilon \\ \vdots \\ \mathit{write}(m)_{11}\ OK_{11} \begin{cases} \mathit{done}_1\ \mathit{done}_\epsilon \\ \vdots \\ \mathit{write}(n)_{11}\ OK_{11} \begin{cases} \mathit{done}_1\ \mathit{done}_\epsilon \\ \vdots \\ \mathit{write}(p)_{11}\ OK_{11}\ \cdots \\ \vdots \\ \mathit{read}_{11}\ n_{11}\ \cdots \end{cases} \\ \vdots \\ \mathit{read}_{11}\ m_{11} \begin{cases} \mathit{done}_1\ \mathit{done}_\epsilon \\ \vdots \\ \mathit{write}(p)_{11}\ OK_{11} \\ \vdots \\ \mathit{read}_{11}\ m_{11}\ \cdots \end{cases} \end{cases} \\ \vdots \end{cases}$$

Voici quelques exemples

- $c : \mathbf{comm}_1 \vdash c; c : \mathbf{comm}_\epsilon$:

  $$\mathit{run}_\epsilon\ \mathit{run}_1\ OK_1\ \mathit{run}_1\ OK_1\ OK_\epsilon\ .$$

  (Noter la répétition des mouvements dans $\mathbf{comm}_1$, qui est nécessaire pour rendre compte de la dynamique de l'état.)

- $x : \mathbf{var}_1 \vdash (x := 0)\,;\,(x := x+1)\,;\,(x := x+1) : \mathbf{comm}_\epsilon$:

  $\mathit{run}_\epsilon\ \mathit{write}(0)_1\ OK_1\ \mathit{read}_1\ m_1\ \mathit{write}(m{+}1)_1\ \mathit{read}_1\ n_1\ \mathit{write}(n{+}1)_1\ OK_2\ \mathit{done}_\epsilon$.

- $\vdash \mathit{new}\ (\lambda x.(x := 0)\,;\,(x := x+1)\,;\,(x := x+1)) : \mathbf{comm}_\epsilon$: Le dialogue résultant sur le type **var** est celui qui est attendu, i.e., celui qui impose ci-dessus $m = 0$ et $n = m + 1$.

5 Construction du glueing et applications

Théorème 5.1 *Soit* $\mathbf{C}$ *une catégorie. Le plongement de* $\mathbf{C}$ *dans* $CCC(\mathbf{C})$*, la catégorie cartésienne fermée libre engendrée par* $\mathbf{C}$ *est plein et fidèle.*

PREUVE. Le plongement de Yoneda $Y : \mathbf{C} \to \mathbf{Set}^{\mathbf{C}^{op}}$ factorise à travers le plongement de $\mathbf{C}$ dans $CCC(\mathbf{C})$, qui est donc fidèle puisque Y est fidèle. La plénitude de Y ne se transfère pas aussi facilement. On construit une nouvelle catégorie, qui juxtapose $CCC(\mathbf{C})$ et $\mathbf{Set}^{\mathbf{C}^{op}}$, mondes respectivement “syntaxique” et “sémantique”. On considère le foncteur $G : CCC(\mathbf{C}) \to \mathbf{Set}^{\mathbf{C}^{op}}$ défini par

$$G\sigma a = CCC(\mathbf{C})[a, \sigma] \quad (a \in \mathbf{C}, \sigma \in CCC(\mathbf{C}))\ .$$

On construit la catégorie $Gl(G)$ (Gl pour “glue”) comme suit

- Les objets sont des triplets $(\sigma, F, \mu : F \to G\sigma)$, et
- $Gl(G)[(\sigma, F, \mu), (\sigma', F', \mu')]$ est l'ensemble des paires $(f : \sigma \to \sigma', \alpha : F \to F'$ telles que $Gf \circ \mu = \mu' \circ \alpha$. Cette condition est appelée *condition de cohérence.*

On a le lemme suivant

Lemme 5.2 *$Gl(G)$ est une CCC, et la projection évidente $\Pi : Gl(G) \to CCC(\mathbf{C})$ est un foncteur de CCC (i.e., $\Pi(A \times B) = \Pi(A) \times \Pi(B)$ et idem pour $\to$).*

(Voir plus loin pour une construction concrète qui retient l'essence de ce lemme.). Le lemme va nous permettre de construire un morphisme H de $CCC(\mathbf{C})$ dans $Gl(G)$ en nous contentant de définir ce morphisme sur $\mathbf{C}$ comme suit:

$$Ha = (a, Ya, \subseteq) \qquad (\subseteq \text{ est la transformation naturelle d'inclusion})\ .$$

Soit $a, b \in \mathbf{C}$ et $\phi \in CCC(\mathbf{C})[a, b]$. On pose $H\phi = (\phi, |\phi|)$. Par plénitude de Y, il existe $f : a \to b$ dans $\mathbf{C}$ tel que $|\phi| = Yf$, i.e. $|\phi|g = f \circ g$. Alors, par la condition de cohérence, on a:

$$\begin{array}{l} G\phi \circ \subseteq\ = \ \subseteq \circ |\phi| = \subseteq \circ Y \\ \quad \text{soit, en } a : G\phi a = Yfa \\ \quad \text{soit, appliqué à } Id : a \to a : \phi = \phi \circ Id = f \circ Id = f \end{array}$$

Plutôt que de montrer le lemme, on fournit maintenant explicitement une construction (optimisée) de H. On suppose pour simplifier que $\mathbf{C}$ a un seul objet 1 et une seule flèche $Id : 1 \to 1$. On construit $H\sigma = (\sigma, Val(\sigma), ')$ $(' : Val(\sigma) \to CCC(\mathbf{C}[1, \sigma])$ et $H\phi = (\phi, |\phi|)$, non par récurrence sur la formation des objets, mais par l'intermédiaire d'un système formel qui permet d'établir des jugements $u \in Val(\sigma)$, $'u = \phi$, et $|\phi|u = v$:

$$\frac{}{* \in Val(1) \qquad '* = Id}$$

$$\frac{u \in Val(\sigma) \quad v \in Val(\tau)}{(u, v) \in Val(\sigma \times \tau) \qquad '(u, v) = \langle 'u, 'v \rangle}$$

$$\frac{\phi : \sigma' \times \sigma \to \tau \quad u \in \mathit{Val}(\sigma')}{\phi[u] \in \mathit{Val}(\sigma \to \tau) \qquad {}'(\phi[u]) = \Lambda(\phi) \circ {}'u}$$

On peut voir le jugement $u \in \mathit{Val}(\sigma)$ comme un jugement de typage "$u : \sigma$". La récurrence qui est sous-jacente est alors la récurrence sur la syntaxe de u:

$$u ::= * \parallel (u, v) \parallel \phi[u]$$

On spécifie $|\phi|u = v$ comme suit:

$$\frac{}{|\mathit{Id}|u = u} \qquad \frac{|\phi|u = v \quad |\psi|v = w}{|\psi \circ \phi|u = w}$$

$$\frac{}{|\mathit{Fst}|(u, v) = u} \qquad \frac{}{|\mathit{Snd}|(u, v) = v}$$

$$\frac{|\phi|u = v \quad |\psi|u = w}{|\langle \phi, \psi \rangle|u = (v, w)}$$

$$\frac{|\phi|(u, v) = w}{|\mathit{App}|(\phi[u], v) = w} \qquad \frac{}{|\Lambda(\phi)|u = \phi[u]}$$

Ici, il n'y a pas de récurrence structurelle sous-jacente, car la règle pour App fait passer de App à ϕ (de taille inconnue). Le système est néanmoins déterministe (une seule règle par construction). On est donc assurés que l'on ne peut pas prouver $|\phi|u = v_1$ et $|\phi|u = v_2$ avec $v_1 \neq v_2$, i.e. $|\phi|$ est une fonction partielle. Il nous faut montrer qu'elle est en fait totale, i.e., que le système ci-dessus, qui spécifie une sémantique opérationnelle, termine. On pose $|\phi|u \downarrow$ s'il existe v tel que $|\phi|u = v$. On utilise une technique de réalisabilité. On définit le prédicat $u \Vdash \sigma$ (u réalise σ) comme suit:

$$\frac{}{\star \Vdash 1} \qquad \frac{u \Vdash \sigma \quad v \Vdash \tau}{(u, v) \Vdash \sigma \times \tau} \qquad \frac{\forall v \;\; (v \Vdash \sigma \Rightarrow |\phi|(u, v) \downarrow)}{\phi[u] \Vdash \sigma \to \tau}$$

La terminaison est conséquence immédiate des propriétés suivantes:

(A) Si $\phi : \sigma \to \tau$ et $u \Vdash \sigma$, alors il existe v tel que $|\phi|u = v$, et de plus $v \Vdash \tau$.

(B) Si $u \in \mathit{Val}(\sigma)$, alors $u \Vdash \sigma$.

(A) Par récurrence sur ϕ. Dans le cas de la composition, on se sert de la clause "de plus $v \Vdash \ldots$". La définition de $\phi[u] \Vdash \sigma \to \tau$ est précisément conçue pour faire passer le cas *App*. Tous les autres cas sont évidents.

(B) Par récurrence sur u. Le seul cas non trivial est $\phi[u]$. Par récurrence, on a $u \Vdash \sigma'$. Soit $v \Vdash \sigma$ (quelconque). On a $(u, v) \Vdash \sigma' \times \sigma$, donc par la propriété (A) (qui a été prouvée indépendamment), on a $|\phi|(u, v) \downarrow$. Donc $\phi[u] \Vdash \sigma \to \tau$. Ceci achève la preuve que ϕ est une fonction totale.

On vérifie enfin que $H\phi = (\phi, |\phi|)$ vérifie bien la condition de cohérence, i.e. $G\phi \circ ' = ' \circ |\phi|$, soit, pour tout u:

$$\phi \circ 'u = '(v) \quad (|\phi|u = v) .$$

Ceci se vérifie par récurrence sur la preuve de $|\phi|u = v$. On indique ci-dessous précisément les équations des CCC qui sont utilisées:

Id	$Id \circ f = f$
$\circ$	$(h \circ g) \circ f = h \circ (g \circ f)$
Fst	$Fst \circ \langle f, g \rangle = f$
Snd	$Snd \circ \langle f, g \rangle = g$
$\langle \_, \_ \rangle$	$\langle g, h \rangle \circ f = \langle f \circ f, h \circ f \rangle$
App	$App \circ \langle \Lambda(h) \circ f, g \rangle = h \circ \langle f, g \rangle$
Λ	(rien, c'est la raison même de la définition de $'(\phi[u])$)

References

[AmaCur98] R. Amadio, and Pierre-Louis Curien, Domains and Lambda-calculi, Cambridge University Press (1998).

[Bare84] Barendregt, H., The lambda calculus; its syntax and semantics, North-Holland, (1984).

[Church41] Church, A., The calculi of lambda-conversion, Princeton University Press (1941).

[Curry58] Curry, H. and Feys, R., Combinatory Logic, vol. 1, North Holland, (1958).

[CurryHinSel72] Curry, H. and Hindley, R. and Seldin, J., Combinatory Logic, vol. 2, North Holland (1972),

[HinSel86] Hindley, R. and Seldin, J., Introduction to combinators and lambda-calculus, Cambridge University Press (1986).

[Huet93] G. Huet, An analysis of Böhm's theorem, TCS 121, 145–167 (1993).