Université Paris VI - Pierre & Marie Curie
DEA Programmation : Sémantique, Preuves et Langages
Année 1999/2000

Rapport de stage

Exécution de termes de preuves

Une nouvelle méthode d'extraction pour le Calcul des Constuctions Inductives

présenté et soutenu par
Pierre Letouzey

Directeur de stage :
Christine Paulin-Mohring

Stage effectué dans le cadre du groupe Démons
Lri - Paris XI

Table des matières

1 Introduction

1.1 Présentation

Le Calcul des Constructions inductives (CIC) [15] est un calcul d'ordre supérieur qui permet d'exprimer dans un même formalisme à la fois des propositions mathématiques, des preuves ainsi que des fonctions et des types récursifs. Ce formalisme très riche sert de base au système d'aide à la preuve Coq [1, 7] développé à l'INRIA, qui peut être utilisé autant pour l'élaboration et la vérification de preuves mathématiques formelles que pour la conception de programmes certifiés conformes vis-à-vis de leur spécification.

Conformément à l'isomorphisme de Curry-De Bruijn-Howard [6], les preuves en CIC sont représentées comme des termes fonctionnels qui peuvent ensuite être exécutés. Ainsi une preuve intuitionniste d'une spécification de programme fournit directement ce programme.

Le système Coq comprend actuellement un système dit d'extraction qui fournit un programme ML (Ocaml ou Haskell) à partir d'un terme de preuve. Cette fonction d'extraction fait plus que traduire les termes de preuves en ML, elle extrait de ces termes de preuves les seules parties utiles pour le calcul.

Mais la méthode actuellement utilisée [9, 10, 11] dans l'assistant Coq pour traduire les preuves en programmes ML ne prend pas en compte de manière satisfaisante les définitions inductives et les univers. Il y a de fait un véritable problème car les fonctionalités avancées des définitions inductives et des univers sortent du cadre des programmes typables en ML. Le but du stage a donc été de proposer une méthode qui étende l'analyse actuelle des preuves et l'exécution des termes extraits à tout le Calcul des Constructions Inductives.

Un des problèmes majeurs lorsque l'on veut veut faire de l'extraction sur tous les univers de CIC, c'est qu'on doit prendre en compte des termes dont le statut est ambigu. Considérons par exemple le terme inductif suivant.

$$\begin{array}{rlcl} Cases\ b\ of & & & \\ & true & \Rightarrow & Prop \\ | & false & \Rightarrow & Set \\ end. & & & \end{array}$$

Ce terme est légal en Coq, et de type *Type*. Maintenant est-il informatif et doit-on le garder lors de l'extraction ? Ou au contraire est-ce un terme logique qui ne sert pas lors de l'exécution. Cela dépend de la valeur du b, qui n'est pas connue lors de l'extraction.

Dans l'extraction actuelle, on fait disparaître complètement les parties logiques, et obtenir un *sous-système* de CIC (en fait F_ω), quitte à échouer sur de tels termes ambigus. Si on veut maintenant les intégrer, il faut accepter que les termes extraits puissent avoir encore des traces de parties logiques, ces traces étant représentées par le symbole $\circ$. L'extraction du terme ci-dessus sera alors :

$$\begin{array}{rlcl} Cases\ b\ of & & & \\ & true & \Rightarrow & \circ \\ | & false & \Rightarrow & Set \\ end. & & & \end{array}$$

On va donc bâtir une *extension* de CIC, nommée CIC$\circ$, contenant le symbole $\circ$ et qui va servir d'intermédiaire entre CIC et ML. Les principales caractéristiques de ce système vont être les suivantes :

- Pour traiter fidèlement les univers de CIC, ce système garde les dépendances des termes par rapport à des types, contrairement à l'extraction actuelle. Ceci nous empêche de typer tous les termes extraits en ML, vu les incompatibilités de typage entre CIC et ML. La solution adoptée est *de ne pas typer* ce système CIC$\circ$. Si on part d'un terme t de CIC, on se sert de son typage pour assurer que le terme traduit $t_\circ$ de CIC$\circ$ est bien fortement normalisant (corollaire 5.37). Il est alors possible d'exécuter ce dernier terme comme un terme ML *non typé*.

- Notre mécanisme de remplacement des parties inutiles par $\circ$ s'inspire des techniques de "pruning" (élagage) mise au point par Berardi, Boerio et Prost. Ce mécanisme a déjà été étudié pour le λ-calcul simplement typé [2], pour le système F [3] et pour les systèmes du cube [14, 13]. Nous avons ici en plus à considérer la hiérarchie des univers de CIC, ainsi que les types inductifs. L'autre principale différence entre ces travaux et le nôtre tient en la différence d'approche : ici nous nous en tenons à une analyse *a priori* basée sur le clivage $Prop/Set$ fourni par l'utilisateur, alors que les travaux de Berardi, Boerio et Prost sont basés sur des analyses de dépendances *a posteriori*.

- Pour un terme, le fait d'être logique ou non dépend non seulement de sa syntaxe, mais aussi beaucoup de son type. Il suffit par exemple de considérer une variable pour s'en persuader. Mais dans CIC les types peuvent évoluer par β-conversion, et également changer d'univers. Il est alors délicat d'établir des propriétés sur la β-réduction des termes si leurs types mêmes varient par β. Ceci nous a amené pour des raisons de simplicité de preuves, à annoter les termes par un de leurs types. Ces marques, inspirées de [4], permettent alors de définir une relation de réduction $\rightarrow_\circ$ directement sur la syntaxe. Et cette relation va correspondre à une version "small-step" de l'extraction.

La principale difficulté , et dès lors le principal objet du stage a été d'étudier les interactions entre extraction et exécution, c'est à dire voir comment les relations $\rightarrow_\beta$ et $\rightarrow_\circ$ se comportaient l'une par rapport à l'autre. Et en particulier nous avons établi que la relation $\rightarrow_\beta \cup \rightarrow_\circ$ normalise fortement (théorème 5.39).

1.2 Plan

Ce rapport reprend la progression chronologique du stage. Dans un premier temps l'attention s'est portée sur le problème de la hiérarchie des univers dans le Calcul des Constructions (CC), système qui correspond au CIC moins les définitions inductives. Ce système CC est présenté dans le premier chapitre, et le système CC$\circ$ correspondant est décrit dans le deuxième chapitre.

Puis ce système CC$\circ$ a été étendu à CIC$\circ$, en intégrant les définitions récursives. Le chapitre 3 est consacré à une description de CIC, et le chapitre 4 présente et étudie CIC$\circ$.

2 Le Calcul des Constructions

2.1 Définition de CC

Notre présentation de CC s'inspire de [15, 1, 8]. Les trois principales caractéristiques de notre version de CC sont :

- la hiérarchie de types $Prop, Set, Type_i$
- la règle de conversion qui permet de monter dans la hiérarchie
- la présence de marques sur certains termes : ces termes sont annotés par leur type, dans une présentation hérité de [4].

Ces marques alourdissent les notations, mais vont permettre de construire la relation $\to_\circ$ de traduction de CC vers CC$\circ$ uniquement à partir de la syntaxe des termes.

Définition 2.1 (Syntaxe de CC) *Les sortes et les termes de CC sont donnés par les grammaires suivantes :*

$$\begin{array}{lcl} s & ::= & Prop \mid Set \mid Type_i \\ t & ::= & s \mid x^t \mid (t\ \ t)^t \mid (x : t)\ t \mid ([x : t]\ t)^t \end{array}$$

Comme d'habitude, $a \to b$ signifiera $(x : a)\ b$ avec x sans occurrence libre dans a et b.

Bien que les contextes et les marques de typage sur les variables fassent double emploi, nous utiliserons néanmois des contextes.

Définition 2.2 (Contextes)

$$\Gamma ::= \emptyset \mid \Gamma; x : t$$

La substitution doit tenir compte des marques

Définition 2.3 (Substitution) *On définit la substitution sur les termes marqués de la façon suivante :*

$$\begin{array}{lcl} s[x/u] & = & s \\ x^T[x/u] & = & u \\ y^T[x/u] & = & y^{T[x/u]} \\ etc... & & \end{array}$$

La β-réduction est définie comme d'habitude à partir de la substitution, elle peut s'effectuer dans les termes proprement dit ou dans les marques.

Définition 2.4 (β-réduction)

$$(([x : X]\ t)^T\ \ u)^U \ \to_\beta\ t[x/u]$$

Notations :

$\rightarrow_\beta$ désigne une étape de β-réduction.

$\rightarrow_\beta^?$ désigne zéro ou une étape de β-réduction.

$\rightarrow_\beta^*$ désigne un certain nombre ($n \geq 0$) d'étapes.

$\rightarrow_\beta^+$ désigne un nombre non nul d'étapes.

$=_\beta$ désigne l'équivalence modulo β-réduction.

L'ordre de conversion suivant va être utilisé par la règle de typage (Conv1).

Définition 2.5 (Ordre de conversion $\preceq$) *Il est défini inductivement par*

1. *si* $M =_\beta N$ *alors* $M \preceq N$
2. $Set \preceq Type_i$
3. $Prop \preceq Type_i$
4. *si* $i \leq j$ *alors* $Type_i \preceq Type_j$
5. *si* $X =_\beta Y$ *et* $M \preceq N$ *alors* $(x : X)\ M \preceq (x : Y)\ N$
6. *si* $M \preceq N$ *avec* $M' =_\beta M$ *et* $N' =_\beta N$ *alors* $M' \preceq N'$

2.2 Typage de CC

Les règles suivantes permettent de définir de façon mutuellement récursive le typage d'un terme $\Gamma \vdash t : T$ ainsi que la correction d'un contexte $\Gamma \vdash ok$.

Règles de formation d'environnements

(Vide)	$\emptyset \vdash ok$	
(Contexte)	$\dfrac{\Gamma \vdash T : s}{\Gamma; x : T \vdash ok}$	$x \notin \Gamma$, s sorte

Règles de typage des termes

(Ax-Prop)	$\dfrac{\Gamma \vdash ok}{\Gamma \vdash Prop : Type_i}$	
(Ax-Set)	$\dfrac{\Gamma \vdash ok}{\Gamma \vdash Set : Type_i}$	
(Ax-Type)	$\dfrac{\Gamma \vdash ok}{\Gamma \vdash Type_i : Type_j}$	$i < j$
(Var)	$\dfrac{\Gamma \vdash ok}{\Gamma \vdash x^T : T}$	$(x : T) \in \Gamma$
(Prod1)	$\dfrac{\Gamma \vdash X : s_1 \quad \Gamma; x : X \vdash T : s_2}{\Gamma \vdash (x : X)\ T : s_2}$	s_1 ou $s_2 \in \{Prop, Set\}$
(Prod2)	$\dfrac{\Gamma \vdash X : Type_i \quad \Gamma; x : X \vdash T : Type_j}{\Gamma \vdash (x : X)\ T : Type_k}$	$i \leq k\ ,\ j \leq k$
(Lamb)	$\dfrac{\Gamma; x : X \vdash t : T}{\Gamma \vdash ([x : X]\ t)^{(x : X)\ T} : (x : X)\ T}$	
(App)	$\dfrac{\Gamma \vdash t : (x : X)\ T \quad \Gamma \vdash u : X}{\Gamma \vdash (t\ \ u)^{T[x/u]} : T[x/u]}$	
(Conv1)	$\dfrac{\Gamma \vdash t : T \quad \Gamma \vdash U : s \quad T \preceq U}{\Gamma \vdash t : U}$	
(Conv2)	$\dfrac{\Gamma \vdash t^U : T \quad \Gamma \vdash V : s \quad U =_\beta V}{\Gamma \vdash t^V : T}$	

Dans la règle (Conv2), et par la suite, t^U est un abus de notation désignant en fait n'importe quel terme marqué, que ce soit un x^U, un $([x : X]\ t)^U$ ou un $(t\ \ u)^U$. En toute rigueur il faudrait écrire trois règles pour les trois catégories syntaxiques...

2.3 Propriétés de CC

Nous admettrons que cette présentation du Calcul des Constructions vérifie bien les propriétés habituelles : Church-Rosser, lemme de substitution, Subject Reduction, et surtout normalisation forte. Cf par exemple [15] ou [8] pour des preuves concernant des systèmes similaires. On notera M_β la forme β-normale d'un terme M.

En particulier, on aura besoin des lemmes suivants.

Lemme 2.6 *$\preceq$ est un préordre, la relation d'equivalence qui lui est associée est $=_\beta$. En particulier, $\preceq$ est transitif.*

$\Diamond$ La définition donnée de $\preceq$ est équivalente à celle donnée par Luo dans [8] page 51 (à ceci près qu'il faut rajouter une deuxième sorte de base Set). On peut alors utiliser le lemme 3.6 p.52. $\square$

Lemme 2.7 *On a la caractérisation suivante : $M \preceq M'$ ssi l'on est dans l'un des cas suivant :*

(i) $M =_\beta M'$

(ii) $M =_\beta Prop$ *ou* Set *ou* $Type_i$ *et* $M' =_\beta Type_j$ *avec* $i \leq j$

(iii) $M =_\beta (x : X)\ N$ *et* $M' =_\beta (x : X')\ N'$ *avec* $X =_\beta X'$ *et* $N \preceq N'$.

$\Diamond$ Cf. lemme 3.4 p.51 de Luo. $\square$

Lemme 2.8 *Une dernière caractérisation :*
$M \preceq M'$ *ssi* $M =_\beta M'$ *ou* $M =_\beta (x_1 : X_1) \ldots (x_n : X_n)s$ *et* $M' =_\beta (x_1 : X'_1) \ldots (x_n : X'_n)s'$ *avec* $\forall i, X_i =_\beta X'_i$ *et* $s \preceq s'$.

$\Diamond$ Il suffit d'utiliser récursivement le lemme précédent. $\square$

Lemme 2.9 *Si* $M \preceq M'$ *et* M,M' *β-normaux, alors soit* $M = M'$, *soit* $M = (x_1 : X_1) \ldots (x_n : X_n)s$, $M' = (x_1 : X'_1) \ldots (x_n : X'_n)s'$ *et* $s \preceq s'$.

$\Diamond$ Résulte de la combinaison du lemme précédent et du caractère β-normal de M et M'. $\square$

Lemme 2.10 *Si* $\Gamma \vdash t^T : U$ *alors* $T \preceq U$

$\Diamond$ Par récurrence sur le typage. Si la dernière règle utilisée est (Var), (Lamb) ou (App), on a directement $T = U$. Et si cette dernière règle est (Conv1) ou (Conv2), on utilise l'hypothèse de récurrence et le fait que $\preceq$ est transitif. $\square$

Lemme 2.11 *Si* $\Gamma \vdash t^T : U$ *alors on a aussi* $\Gamma \vdash t^T : T$

$\Diamond$ Toujours par récurrence sur le typage. Si la dernière règle utilisée est (Var), (Lamb) ou (App), on a directement $T = U$. Si cette dernière règle est (Conv1), on applique juste l'hypothèse de récurrence. Enfin il peut s'agir de (Conv2) :

$$\frac{\Gamma \vdash t^{T'} : U \quad \Gamma \vdash T : s \quad T =_\beta T'}{\Gamma \vdash t^T : U}$$

On déduit $\Gamma \vdash t^{T'} : T'$ de l'hypothèse de récurrence, puis $\Gamma \vdash t^{T'} : T$ par (Conv1) vu que $T =_\beta T' \Rightarrow T' \preceq T$, et enfin $\Gamma \vdash t^T : T$ par (Conv2). $\square$

Lemme 2.12 *On ne peut avoir à la fois* $\Gamma \vdash M : Prop$ *et* $\Gamma \vdash M : Set$.

$\Diamond$ Déja, M ne peut être une sorte. Ensuite, si $M = t^T$, on a alors d'après un lemme précédent à la fois $T \preceq Prop$ et $T \preceq Set$, ce qui est impossible. Et pour les produits, on procède par récurrence sur la structure. Les deux typage doivent utiliser la règle (Prod1), ce qui donne un sous-terme de M qui est aussi de type $Prop$ et Set. $\square$

Lemme 2.13 (Type principal) *Si M est un terme bien typé de CC dans un contexte Γ, il existe un type T_0 tel que :*
- $\Gamma \vdash M : T_0$
- *si* $\Gamma \vdash M : T$, *alors* $T_0 \preceq T$

$\Diamond$ Pour les sortes, c'est clair. Pour les termes marqués, les lemmes précédents 2.10 et 2.11 montrent que la marque est un type principal. Reste le cas d'un produit M. Première remarque, tout type d'un produit est β-équivalent à une sorte (récurrence immédiate). Il suffit alors de regarder les sortes qui peuvent servir de type pour M, et de prendre la plus petite. Et "la" plus petite sorte existe bien vu le lemme précédent : $Prop$ et Set ne peuvent être deux types d'un même terme. $\square$

Lemme 2.14 *Si* $\Gamma \vdash x^T : T'$ *et* $(x : T'') \in \Gamma$ *alors* $T =_\beta T''$.

$\Diamond$ Encore une fois, par récurrence sur le typage. Si la dernière règle utilisée est (Conv2), alors on utilise directement l'hypothèse de récurrence. S'il s'agit de (Conv1), il faut utiliser la transitivité de β avec l'hypothèse de récurrence. Et si enfin il s'agit de (Var), c'est trivial. $\square$

Ce dernier lemme justifie la remarque introductive selon laquelle marques de typage et contextes font double-emploi : si un terme est typable dans un certain contexte, on peut reconstituer ce contexte à β-équivalence près grâce aux marques. Ce qui fait que dans la suite, on parlera souvent de termes typables dans CC, sans préciser le contexte.

3 Le système CC$\circ$

3.1 Présentation du système

Comme expliqué en introduction, on rajoute un symbole supplémentaire $\circ$ au système CC précédent.

Définition 3.1 (Syntaxe de CC$\circ$) *Les termes de CC$\circ$ sont donnés par la grammaire suivante :*

$$t \quad ::= \quad \circ \mid Prop \mid Set \mid Type_i \mid x^t \mid (t \;\; t)^t \mid (x:t)\; t \mid ([x:t]\; t)^t$$

Définition 3.2 (Réduction $\circ$) *La relation de réécriture $\rightarrow_\circ$ est définie à partir des règles suivantes :*

$$\begin{array}{lcll}
(0) & Prop & \rightarrow_\circ & \circ \\
(1) & t^\circ & \rightarrow_\circ & \circ \\
(2) & (\circ \;\; t)^T & \rightarrow_\circ & \circ \\
(3) & (x:X)\;\circ & \rightarrow_\circ & \circ \\
(4) & ([x:X]\;\circ)^T & \rightarrow_\circ & \circ
\end{array}$$

Et $\rightarrow_\circ^*$ sera la fermeture reflexive transitive de $\rightarrow_\circ$. De cette façon, tout ce qui est logique et non pas calculatoire disparait : $Prop$ ainsi que les termes de symbole de tête $Prop$, ou encore les termes dont la marque est deja logique, etc. Là encore, la β-réduction est définie de façon usuelle pour les termes de CC$\circ$.

3.2 Objectifs et obstacles

Le but du reste du chapitre est de prouver que la réduction $\rightarrow_\circ$ ne modifie pas (trop) l'exécution d'un terme, c'est à dire sa réduction par β. Grosso-modo on désire que si un terme de CC a une certaine β-réduction, alors son réduit par $\rightarrow_\circ$ peut subir une β-réduction similaire. Et réciproquement, que si le $\circ$-réduit peut se β-réduire, c'est que le terme initial pouvait également se β-réduire.

On peut voir le problème de façon duale : si on prend $M \rightarrow_\beta N$, quelle relation existe-t'il entre les $\circ$-réduits respectifs de M et N ?

Une situation idyllique serait la commutation des deux relations, quelque chose comme :

$$\begin{tikzcd}
M \arrow[r, "*", "\beta"'] \arrow[d, "\circ"', "*"] & N \arrow[d, "\circ"', "*"] \\
M' \arrow[r, "*", "\beta"'] & N'
\end{tikzcd}$$

Malheureusement, à première vue, $\to_\beta$ et $\to_\circ$ cohabitent mal. Prenons ainsi le terme :

$$Cex_1 = (([X : Type]\ X)^{Type \to Type}\ \ Prop)^{Type}$$

C'est un terme qui est moralement logique, vu qu'il peut se β-réduire en *Prop*. Mais il ne peut donner $\circ$ par $\to_\circ^*$. A l'inverse, si $Id_{Prop} = ([x : Prop]\ x)^{Prop \to Prop}$, le terme

$$Cex_2 = (Id_{Prop}\ \ y^{Cex_1})^{Prop}$$

peut se réduire vers $\circ$ grâce à sa marque *Prop*, alors que son réduit y^{Cex_1} ne le peut plus.

Une autre chose qu'on attend d'un bon système d'extraction, c'est qu'il soit cohérent avec le typage : si un type T est détecté comme étant logique (i.e $T \to_\circ^* \circ$), et $\Gamma \vdash M : T$, alors on veut que M soit aussi détecté comme logique. Malheureusement, si l'on s'en tient à ce critère, notre $\to_\circ$ n'est pas un bon système d'extraction. Le typage suivant est en effet correct :

$$x : Prop \vdash x^{Cex_1} : Prop$$

On a juste fait évoluer la marque de x par (Conv1). Mais maintenant cette nouvelle marque fait que x ne se réduit plus vers $\circ$!

On sent pourtant que tous ces problèmes peuvent être contournés à condition de faire ce qu'il faut de β-réduction avant de $\circ$-réduire, en particulier dans les marques. La façon la plus simple de régler le problème est ce qui est fait dans la section 3.4 : on réclame la β-normalité des termes ou des marques. Puis une solution plus satisfaisante est utilisée dans la section 3.5 : on utilise la relation $\to_{\beta m}$ de réduction dans les marques.

Un autre problème est celui de l'ordre dans lequel on effectue les preuves : Pour toute preuve concernant la β-réduction, on va utiliser de façon critique des résultats sur le typage. Or le typage utilise une relation de conversion définie à partir de la β-réduction... Il faut donc être soigneux pour éviter le cercle vicieux.

3.3 Premières propriétés de CC$\circ$

Commençons par quelques propriétés immédiates de $\to_\circ$.

Proposition 3.3 *La relation $\to_\circ$ termine.*

$\Diamond$ Il suffit d'associer à chaque terme de CC$\circ$ une valuation du genre :

$$\begin{array}{lcll}
\mu(\circ) & = & 1 & \\
\mu(s) & = & 2 & s \in \{Set, Prop, Type_i\} \\
\mu(x^T) & = & 1 + \mu(T) & \\
\mu((t\ \ u)^T) & = & \mu(t) + \mu(u) + \mu(T) & \\
\mu((x : X)\ t) & = & \mu(X) + \mu(t) & \\
\mu(([x : X]\ t)^T) & = & \mu(X) + \mu(t) + \mu(T) &
\end{array}$$

A chaque dérivation $\to_\circ$, cette valuation décroit strictement. $\Box$

Proposition 3.4 *La relation* $\rightarrow_\circ$ *est confluente.*

$\Diamond$ Comme $\rightarrow_\circ$ est noetherienne, il suffit de montrer la confluence locale (Lemme de Newmann). Pour cela regardons les paires critiques de $\rightarrow_\circ$:

- Règles (1) et (2) : Le terme $(\circ\ \ t)^\circ$ peut se réduire par la règle (1) ou la règle (2). Mais dans les deux cas on obtient $\circ$. La confluence de cette paire critique est donc triviale.
- Règles (1) et (4) : $([x : X]\ \circ)^\circ$ se réduit également de deux façons. Là encore on obtient toujours le même résultat : $\circ$.

$\square$

Corollaire 3.5 *Pour tout terme t de CC*$\circ$*, il y a existence et unicité d'une forme normale vis-à-vis de* $\rightarrow_\circ$ *. On la notera* $t_\circ$*.*

Et maintenant trois lemmes syntaxiques autour de $\rightarrow_\circ$. Ils expriment tous simplement le fait que $\rightarrow_\circ$ ne modifie pas le squelette des termes, et ne fait que des changements locaux.

Lemme 3.6 (Conservation de la structure) *Soit* $M \rightarrow_\circ^* N$ *avec* $N \neq \circ$.

(i) Si M est une sorte, alors M=N.

(ii) Si $M = x^X$*, alors il existe* X' *tel que* $N = x^{X'}$ *et* $X \rightarrow_\circ^* X'$.

(iii) Si $M = (a\ \ b)^T$*, alors il existe* a',b',T' *tels que* $N = (a'\ \ b')^{T'}$ *et* $a \rightarrow_\circ^* a'$, $b \rightarrow_\circ^* b'$, $T \rightarrow_\circ^* T'$.

(iv) Si $M = (x : X)\ t$*, alors il existe* X',t' *tels que* $N = (x : X')\ t'$ *et* $X \rightarrow_\circ^* X'$, $t \rightarrow_\circ^* t'$.

(v) Si $M = ([x : X]\ t)^T$*, alors il existe* X',t',T' *tels que* $N = ([x : X']\ t')^{T'}$ *et* $X \rightarrow_\circ^* X'$, $t \rightarrow_\circ^* t'$, $T \rightarrow_\circ^* T'$.

$\Diamond$ Dans chacun des cas, on procède par récurrence sur la longueur de la dérivation $M \rightarrow_\circ M_1 \rightarrow_\circ \ldots \rightarrow_\circ M_n = N$. Lors de la dérivation $M \rightarrow_\circ M_1$, le $\circ$-redex ne peut être en tête du terme M, sinon $M_1 = \circ = N$. La réduction est donc interne, M_1 a la même structure de tête que M, et on termine en utilisant l'hypothèse de récurrence entre M_1 et N.

$\square$

Lemme 3.7 (Réciproque de la conservation) *Soit* $M \rightarrow_\circ^* N$.

(i) Si $N = x^X$*, alors il existe* X_0 *tel que* $M = x^{X_0}$ *et* $X_0 \rightarrow_\circ^* X$.

(ii) Si $N = (a\ \ b)^T$*, alors il existe* a_0,b_0,T_0 *tels que* $M = (a_0\ \ b_0)^{T_0}$ *et* $a_0 \rightarrow_\circ^* a$, $b_0 \rightarrow_\circ^* b$, $T_0 \rightarrow_\circ^* T$.

(iii) Si $N = (x : X)\ t$*, alors il existe* X_0,t_0 *tels que* $M = (x : X_0)\ t_0$ *et* $X_0 \rightarrow_\circ^* X$, $t_0 \rightarrow_\circ^* t$.

(iv) Si $N = ([x : X]\ t)^T$*, alors il existe* X_0,t_0,T_0 *tels que* $M = ([x : X_0]\ t_0)^{T_0}$ *et* $X_0 \rightarrow_\circ^* X$, $t_0 \rightarrow_\circ^* t$, $T_0 \rightarrow_\circ^* T$.

$\diamondsuit$ Prouvons par exemple le premier cas, les autres sont similaires. On a $N \neq \circ$, et M différent d'une sorte. On est donc dans l'un des quatre cas de la proposition précédente. Et en fait on est dans le premier cas, vu que N ne peut être à la fois une variable et une autre catégorie syntaxique. Il existe donc X_0 tel que $M = x^{X_0}$, et la proposition précédente affirme l'existence d'un X' tel que $X_0 \ \to_\circ^* \ X'$ et $N = x^{X'}$. Forcement $X' = X$. $\square$

Lemme 3.8 (Inversion de $\circ$) *$M \ \to_\circ^* \ \circ$ ssi l'on est dans l'un des cas suivants :*

(i) $M = \circ$

(ii) $M = Prop$

(iii) $M = x^X$ *et il existe une réduction* $X \ \to_\circ^* \ \circ$

(iv) $M = (a \ \ b)^T$ *et* $a \ \to_\circ^* \ \circ$ *ou* $T \ \to_\circ^* \ \circ$

(v) $M = ([x : X] \ t)^T$ *et* $t \ \to_\circ^* \ \circ$ *ou* $T \ \to_\circ^* \ \circ$

(vi) $M = (x : X) \ t$ *et* $t \ \to_\circ^* \ \circ$

$\diamondsuit$ Le sens $\Leftarrow$ provient de la définition même de $\ \to_\circ$. Pour l'autre sens, si $M \neq \circ$, on a $M \ \to_\circ \ M_1 \ \to_\circ \ \dots \ \to_\circ \ M_n \ \to_\circ \ \circ$, avec $M_n \neq \circ$. Alors M_n est un $\circ$-redex :
- soit $M_n = Prop = M$.
- soit $M_n = x^\circ$ et alors d'après le lemme précédent M ne peut être que de la forme x^X avec $X \ \to_\circ^* \ \circ$
- soit $M_n = (a' \ \ b')^\circ$ et alors $M = (a \ \ b)^T$ avec $T \ \to_\circ^* \ \circ$
- soit $M_n = ([x : X'] \ t')^\circ$ et alors $M = ([x : X] \ t)^T$ avec $T \ \to_\circ^* \ \circ$
- soit $M_n = (\circ \ \ b')^{T'}$ et alors $M = (a \ \ b)^T$ avec $a \ \to_\circ^* \ \circ$
- soit $M_n = (x : X') \circ$ et alors $M = (x : X) \ t$ avec $t \ \to_\circ^* \ \circ$
- soit $M_n = ([x : X'] \circ)^{T'}$ et alors $M = ([x : X] \ t)^T$ avec $t \ \to_\circ^* \ \circ$

$\square$

3.4 CC$\circ$ et typage : les premiers lemmes

Voici maintenant une première série de lemmes ayant tous en commun de réclamer des hypothèses concernant le caractère β-normal des termes.

Théorème 3.9 *Si on a :*
- $\Gamma \vdash M : T$
- *T β-normal*
- *M n'a que des marques β-normales*
- $T \ \to_\circ^* \ \circ$

Alors $M \ \to_\circ^* \ \circ$.

$\diamondsuit$ Par récurrence sur la structure de M.
- M ne peut être une sorte sinon T serait une sorte plus grande que s, donc un $Type_i$ et ne pourrait se réduire vers $\circ$.

- $M = t^{T'}$. D'après le lemme 2.10, on a $T' \preceq T$. Ces deux termes sont β-normaux, on peut appliquer le lemme 2.9 : $T = (x_1 : X_1) \dots (x_n : X_n)s$, $T' = (x_1 : X'_1) \dots (x_n : X'_n)s'$ et $s' \preceq s$. Comme $T \rightarrow_\circ^* \circ$, le lemme d'inversion de $\circ$ nous dit que $s \rightarrow_\circ^* \circ$, i.e. $s = Prop$. D'où $s' = Prop$ également, et finalement $M \rightarrow_\circ^* \circ$.
- $M = (x : X)\ t$. On a alors le typage suivant : un certain nombre de (Conv1) avant un (Prod1) ou un (Prod2).

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash X : s_1 \quad \Gamma; x : X \vdash t : s_2}{\Gamma \vdash (x : X)\ t : s_3}}{\vdots}}{\Gamma \vdash (x : X)\ t : T}$$

Grâce à la transitivité de $\preceq$, on a $s_3 \preceq T$. Or $T \rightarrow_\circ^* \circ$, donc $s_3 \rightarrow_\circ^* \circ$, i.e. $s_3 = Prop$. La dernière règle utilisée est donc (Prod1), et $s_2 = s_3 = Prop$. On peut alors appliquer l'hypothèse de récurrence à t qui est typé de type $Prop$.

□

Remarquons que les deux hypothèses sur T et M concernant la β-réduction sont indispensable. Si l'on enlève celle sur M, il suffit de reprendre Cex_1 pour avoir un contre-exemple. Et si l'on enlève l'hypothèse sur T, on peut construire un contre-exemple à partir de Cex_1 et Cex_2 :

$$y : Prop, z : y^{Prop} \vdash z^{y^{Cex_1}} : Cex_2$$

Lemme 3.10 *Si on a :*
- $\Gamma; x : X \vdash t : T$
- $\Gamma \vdash u : X$
- *t et u n'ont que des marques β-normales*
- $t \rightarrow_\circ^* \circ$

Alors $t[x/u] \rightarrow_\circ^* \circ$.

◊ Par récurrence sur la structure de t. Le lemme 3.8 nous dit que nous sommes dans l'un des cas suivants :

(i) $t = \circ$ est impossible car t est un terme de CC.

(ii) $t = Prop$ et alors $t[x/u] = Prop$

(iii) $t = y^Y$ avec $Y \rightarrow_\circ^* \circ$.
  - Si $x \neq y$, Y est typable dans le contexte Γ, on lui applique l'hypothèse de récurrence, on obtient $Y[x/u] \rightarrow_\circ^* \circ$ et donc $[x/u] \rightarrow_\circ^* \circ$.
  - Si maintenant $x = y$, le lemme 2.14 affirme que $X =_\beta Y$. On a donc $\Gamma \vdash u : Y$ par (Conv1). Comme Y est une marque de t, il est β-normal, et on peut appliquer le théorème précédent à u, ce qui donne une dérivation $u \rightarrow_\circ^* \circ$. On a donc bien $t[x/u] \rightarrow_\circ^* \circ$.

(iv) $t = (a \ \ b)^C$ et $a \rightarrow_\circ^* \circ$ ou $C \rightarrow_\circ^* \circ$. Alors par hypothèse de récurrence on a soit $a[x/u] \rightarrow_\circ^* \circ$, soit $C[x/u] \rightarrow_\circ^* \circ$. De toute façon, $t[x/u] = (a[x/u] \ \ b[x/u])^{C[x/u]} \rightarrow_\circ^* \circ$.

(v) et (vi). Ces deux derniers cas $t = (x : X)\ v$ et $t = ([x : X]\ v)^V$ se traitent de la même façon que l'application.

$\square$

La encore, les hypothèses concernant le caractère β-normal sont essentielles.

Lemme 3.11 (lemme de substitution) *Si on a :*
- $\Gamma; x : X \vdash t : T$
- $\Gamma \vdash u : X$
- *t et u n'ont que des marques β-normales*
- $t\ \to_\circ^*\ t'$
- $u\ \to_\circ^*\ u'$

Alors $t[x/u]\ \to_\circ^*\ t'[x/u']$.

$\Diamond$ Si $t' = \circ$, c'est exactement le lemme précédent. Sinon on va procéder par récurrence sur la structure de t, en appliquant dans chaque cas le lemme 3.6 :

(i) si t est une sorte, il n'y a rien à remplacer

(ii) si $t = y^Y$, alors $t' = y^{Y'}$ avec $Y\ \to_\circ^*\ Y'$. On a deux sous-cas :
  - si $x = y$, le but à prouver se simplifie en $u\ \to_\circ^*\ u'$ qui est vrai par hypothèse
  - si $x \neq y$: Y a toutes les propriétés nécessaires pour lui appliquer l'hypothèse de récurrence, ce qui donne $Y[x/u]\ \to_\circ^*\ Y'[x/u']$, puis le résultat.

(iii) si $t = (a\ \ b)^C$, alors $t' = (a'\ \ b')^{C'}$, avec $a\ \to_\circ^*\ a'$, etc. Il ne reste plus qu'à appliquer trois fois l'hypothèse de récurrence.

(iv) et (v). Ces deux autres cas (produit et lambda) se traitent de la même façon que l'application.

$\square$

Lemme 3.12 (Raffinement du lemme d'inversion de $\circ$) *Si* $([x : X]\ t)^T\ \to_\circ^*\ \circ$*, avec* $([x : X]\ t)^T$ *typé dans un contexte Γ, et dont les marques sont β-normales, alors* $t\ \to_\circ^*\ \circ$.

$\Diamond$ Le lemme 3.8 dit que $T\ \to_\circ^*\ \circ$ ou $t\ \to_\circ^*\ \circ$. Dans le second cas, c'est gagné. Examinons le premier. On a $\Gamma \vdash ([x : X]\ t)^T\ : T$ par le lemme 2.11. L'arbre de typage de ce terme comprend forcement une utilisation de (Lamb) :

$$\frac{\Gamma; x : X \vdash t : V}{\Gamma \vdash ([x : X]\ t)^{(x : X)\ V} : (x : X)\ V}$$

Puis la marque peut évoluer par (Conv2) vers T. En tout cas $T =_\beta (x : X)\ V$. Or T est β-normal, donc aussi de la forme $(x : X')\ V'$, avec $V =_\beta V'$. Et si $T\ \to_\circ^*\ \circ$, c'est donc que $V'\ \to_\circ^*\ \circ$. On a enfin $\Gamma; x : X \vdash t : V'$ par (Conv1). Une application du théorème 3.9 donne $t\ \to_\circ^*\ \circ$. $\square$

3.5 La deuxième génération de lemmes

Le lemme suivant va régler le problème des différences de résultats de la $\circ$-réduction lorsqu'on l'applique à différents termes β-équivalents : il suffit de considérer la forme β-normale pour retrouver un résultat cohérent.

Lemme 3.13 (fondamental) *Soit M un terme de CC bien typé dans un contexte Γ, et tel que $M \rightarrow_\circ^* \circ$. Alors sa forme β-normale M_β se réduit aussi vers $\circ$ par $\rightarrow_\circ^*$.*

$$\begin{tikzcd}
M \arrow[r, "*", "\beta"'] \arrow[d, "\circ"', "*"] & M_\beta \arrow[d, dashed, "\circ"', "*"] \\
\circ & \circ
\end{tikzcd}$$

$\Diamond$ Pour tout M, soit $l(M)$ la longueur de la plus longue réduction de M par $\rightarrow_\beta$. On définit l'ordre de réduction $<_\beta$ par $M <_\beta N$ ssi $l(M) < l(N)$. Puis notons $\lhd$ l'ordre sous-terme strict. Soit ensuite $<_0$ l'ordre lexicographique $(<_\beta, \lhd)$. Quelques remarques :

- si $M \lhd N$ alors $l(M) \leq l(N)$. Donc $M \lhd N \implies M <_0 N$.
- cet ordre est bien fondé, vue la normalisation de CC, on va donc pouvoir s'en servir pour faire notre récurrence.

Utilisons maintenant le lemme 3.8 :

(i) M terme de CC ne peut être $\circ$

(ii) $M = Prop$, et alors c'est évident : $M_\beta = Prop$.

(iii) $M = x^T$, ou plus généralement M terme marqué t^T et $T \rightarrow_\circ^* \circ$. T est un sous-terme de M, on peut donc utiliser l'hypothèse de récurrence : $T_\beta \rightarrow_\circ^* \circ$. On se sert ensuite du typage : le lemme 2.11 donne $\Gamma \vdash M : T$. Puis la Subject Reduction de CC et la règle (Conv1) donne $\Gamma \vdash M_\beta : T_\beta$. On a maintenant tous les éléments pour conclure via le lemme 3.9.

(iv) $M = (a \;\; b)^C$ avec $a \rightarrow_\circ^* \circ$. Il y a 3 sous-cas :

- Si il existe une réduction interne dans a, b ou C, alors le terme $N = (a_\beta \;\; b_\beta)^{C_\beta}$ est strictement plus petit que M par l'ordre $<_0$. L'hypothèse de récurrence appliqué au sous-terme a de M donne que $a_\beta \rightarrow_\circ^* \circ$. Donc $N \rightarrow_\circ^* \circ$. Une nouvelle application de l'hypothèse de récurrence, à N cette fois-ci, donne $N_\beta \rightarrow_\circ^* \circ$. Or $M \rightarrow_\beta^* N$. Donc $M_\beta = N_\beta$.
- Si maintenant les sous-termes a, b et C sont déjà β-normaux, et que le terme M entier peut encore se réduire, c'est qu'il y a un β-rédex en tête : $a = ([x : X] \;\; t)^T$. Le lemme 3.12 dit alors que $t \rightarrow_\circ^* \circ$. Le réduit $t[x/b]$ de M se réduit alors vers $\circ$ grâce au lemme de substitution. Enfin on conclut en passant de $t[x/b]$ à M_β par hypothèse de récurrence.

– Enfin il y a encore le cas trivial où M ne peut plus se β-réduire.

(v) $M = ([x : X]\ t)^T$ avec $t \ \to_\circ^* \ \circ$. Alors $M_\beta = ([x : X_\beta]\ t_\beta)^{T_\beta}$. L'hypothèse de récurrence donne $t_\beta \ \to_\circ^* \ \circ$, et donc $M_\beta \ \to_\circ^* \ \circ$.

(vi) $M = (x : X)\ t$ avec $t \ \to_\circ^* \ \circ$. Ce cas se traite de façon similaire au cas précédent.

□

Rappelons que $\to_{\beta m}$ désigne la β-réduction dans les marques. On peut maintenant reprendre les lemmes précédents en remplaçant les hypothèses requises *a priori* concernant β par de la normalisation $\to_{\beta m}$ *a posteriori*.

Théorème 3.14 *Si on a* $\Gamma \vdash M : T$ *et* $T \ \to_\circ^* \ \circ$, *alors* $M \ \to_{\beta m}^* \to_\circ^* \ \circ$.

◊ Le théorème précédent affirme que $T_\beta \ \to_\circ^* \ \circ$. Il suffit maintenant de β-réduire les marques de M, ce qui donne un M' . On fait évoluer le typage par Subject Reduction et (Conv1) vers $\Gamma \vdash M' : T_\beta$, puis on utilise le théorème 3.9. □

Malheureusement, concernant le lemme de substitution, il ne semble pas possible de prouver aussi simplement la nouvelle version du lemme à partir de l'ancienne. Il faut donc reprendre les démonstrations en utilisant le théorème 3.14 à la place du théorème 3.9.

Lemme 3.15 *Si on a :*
- $\Gamma; x : X \vdash t : T$
- $\Gamma \vdash u : X$
- $t \ \to_\circ^* \ \circ$

Alors $t[x/u] \ \to_{\beta m}^* \to_\circ^* \ \circ$.

◊ Par récurrence sur la structure de t. Le lemme 3.8 nous dit que nous sommes dans l'un des cas suivants :

(i) $t = \circ$ est impossible car t est un terme de CC.

(ii) $t = Prop$ et alors $t[x/u] = Prop$

(iii) $t = y^Y$ avec $Y \ \to_\circ^* \ \circ$. Si $x \neq y$, on applique l'hypothèse de récurrence à Y, on obtient $Y[x/u] \ \to_{\beta m}^* \to_\circ^* \ \circ$ et donc $t[x/u] \ \to_{\beta m}^* \to_\circ^* \ \circ$. Si maintenant $x = y$, le lemme 2.14 affirme que $X =_\beta Y$. On a donc $\Gamma \vdash u : Y$ par (Conv1). On applique le théorème précédent à u, ce qui donne une dérivation $u \ \to_{\beta m}^* \to_\circ^* \ \circ$. On a donc bien $t[x/u] \ \to_{\beta m}^* \to_\circ^* \ \circ$.

(iv) $t = (a\ \ b)^C$ et $a \ \to_\circ^* \ \circ$ ou $C \ \to_\circ^* \ \circ$. Alors par hypothèse de récurrence on a soit $a[x/u] \ \to_{\beta m}^* \to_\circ^* \ \circ$, soit $C[x/u] \ \to_{\beta m}^* \to_\circ^* \ \circ$. De toute façon, $t[x/u] = (a[x/u]\ \ b[x/u])^{C[x/u]} \ \to_{\beta m}^* \to_\circ^* \ \circ$.

(v) et (vi). Ces deux derniers cas $t = (x : X)\ v$ et $t = ([x : X]\ v)^V$ se traitent de la même façon que l'application.

□

Lemme 3.16 (lemme de substitution 2) *Si on a :*

- $\Gamma; x : X \vdash t : T$
- $\Gamma \vdash u : X$
- $t \ \rightarrow_{\circ}^{*} \ t'$
- $u \ \rightarrow_{\circ}^{*} \ u'$

Alors $t[x/u] \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \ t'[x/u']$.

$\Diamond$ La encore il suffit de plagier la démonstration du lemme 3.11. $\square$

Lemme 3.17 (Raffinement 2 du lemme d'inversion de $\circ$) *Si* $([x : X] \ t)^{T} \ \rightarrow_{\circ}^{*} \circ$*, avec* $([x : X] \ t)^{T}$ *typé dans un contexte* Γ*, alors* $t \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \ \circ$.

$\Diamond$ Il suffit de réduire les marques de ce terme, puis d'utiliser le lemme 3.12. $\square$

Etudions maintenant le devenir d'un β-redex lors d'une $\circ$-réduction. Il peut soit disparaître complètement, soit à moitié, soit donner un nouveau β-redex.

Lemme 3.18 *Soit* M *un* β*-redex bien typé de CC, et soit* N *son réduit. Supposons* $M \ \rightarrow_{\circ}^{*} M'$*. Il y a alors trois cas :*

(i) $M' = \circ$ *et alors* $N \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \ \circ$

(ii) M' *est une application* $(\circ \ \ b')^{T'}$ *et alors* $N \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \ \circ$

(iii) M' *est encore un redex, de réduit* N'*, et alors* $N \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \ N'$

$\Diamond$ Notons $M = (([x : X] \ t)^{T} \ \ u)^{U}$ et $N = t[x/u]$. Il y a effectivement trois sorts possibles pour M' :

1. $M' = \circ$. Par le lemme d'inversion 3.8, cela signifie $U \ \rightarrow_{\circ}^{*} \ \circ$ ou $([x : X] \ t)^{T} \ \rightarrow_{\circ}^{*} \ \circ$, ce dernier cas impliquant $t \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \circ$ vu le lemme précédent. Examinons chacun de ces deux cas dans le détail :
   - $U \ \rightarrow_{\circ}^{*} \ \circ$. Alors $\Gamma \vdash M : U$ par le lemme 2.11. Puis $\Gamma \vdash N : U$ par Subject Reduction dans CC. Le théorème 3.9 peut alors s'appliquer, et nous donne $N \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \ \circ$.
   - $t \ \rightarrow_{\beta m}^{*} t_0 \ \ \rightarrow_{\circ}^{*} \ \circ$. Alors $t[x/u] \ \ \rightarrow_{\beta m}^{*} t_0[x/u]$. Puis le lemme de substitution 3.16 donne $t_0[x/u] \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \ \circ$. Au final on a bien $t[x/u] \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \ \circ$.
2. Si $M' \neq \circ$ alors on peut avoir $M' = (\circ \ \ u')^{U'}$ avec $u \ \rightarrow_{\circ}^{*} \ u'$ et $U \ \rightarrow_{\circ}^{*} \ U'$. Le lemme précédent affirme alors que $t \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \ \circ$. Encore une fois $t[x/u] \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \ \circ$.
3. L'autre cas de figure si $M' \neq \circ$ est que $M' = (([x : X'] \ t')^{T'} \ \ u')^{U'}$ avec toutes les sous-réductions $X \ \rightarrow_{\circ}^{*} \ X$, etc. M' est donc un redex qui se réduit en $N' = t'[x/u']$. Et le lemme de substitution 3.16 montre que $N \ \rightarrow_{\beta m}^{*} \rightarrow_{\circ}^{*} \ N'$.

$\square$

3.6 Le théorème de remontée de β

Le théorème qui va suivre répond à un des objectifs initiaux : étant donné une dérivation β dans CC$\circ$, on va pouvoir la “remonter” en une dérivation correspondante dans CC. Par rapport au théorème de “descente” qui va suivre, ici tout se passe bien : à un redex qui est arrivé “en bas” correspond bien un redex “en haut”.

Théorème 3.19 *Soit M un terme typable de CC. Si $M \ \to_\circ^* \ M' \ \to_\beta \ N'$, alors il existe N tel que $M \ \to_\beta \ N \ \to_{\beta m}^* \to_\circ^* \ N'$. En particulier, on a aussi $M \ \to_\beta^+ \to_\circ^* \ N'$*

$$\begin{tikzcd}
M \arrow[r, dashed, "\beta"] \arrow[dr, dashed, "+", "\beta"'] \arrow[dd, "\circ"', "*"] & N \arrow[d, dashed, "\beta m"', "*"] \\
& {} \arrow[d, dashed, "\circ"', "*"] \\
M' \arrow[r, "\beta"'] & N'
\end{tikzcd}$$

$\diamondsuit$ Remarquons tout d'abord que M', qui peut se β-réduire, est différent de $\circ$, ce qui va permettre d'utiliser le lemme de conservation de la structure 3.6. La preuve se fait récurrence sur la structure de M.

(i) M ne peut être une sorte puisque M' peut se β-réduire.

(ii) $M = x^X$. Alors $M' = x^{X'}$ avec $X \ \to_\circ^* \ X'$ et la β-réduction de M' se fait dans la marque : $X' \ \to_\beta \ Y'$. On utilise l'hypothèse de récurrence pour trouver un Y qui ferme le diagramme partant de X. Alors $N = x^Y$ convient.

(iii) $M = (a \ \ b)^T$. Alors $M' = (a' \ \ b')^{T'}$ avec $a \ \to_\circ \ a'$.

1. Si la β-réduction se fait en tête, $a' = ([x : X'] \ t')^{U'}$, $N' = t'[x/b']$, et du coup $a = ([x : X] \ t)^U$ avec $X \ \to_\circ^* \ X'$, etc. On est donc dans le cas (iii) du lemme précédent, ce qui montre que $N = t[x/b]$ convient.
2. Si la β-réduction est interne, par exemple $a' \ \to_\beta \ a'_0$, l'hypothèse de récurrence appliquée à a donne un a_0 fermant le diagramme. On prend alors $N = (a_0 \ \ b)^T$. On fait de même si la β-réduction a lieu dans b' ou dans T'.

(iv) $M = (x : X) \ t$. Alors $M' = (x : X') \ t'$ avec $X \ \to_\circ \ X'$, etc. Si c'est X' qui se β-réduit en X'_0, on utilise l'hypothèse de récurrence pour obtenir un X_0 qui ferme le diagramme correspondant à X. Et alors $N = (x : X_0) \ t$ convient. On fait de même si c'est t' qui se β-réduit.

(v) le cas du lambda se traite de la même façon que celui du produit.

$\square$

Corollaire 3.20 *La réduction $\ \to_\circ^* \ $ conserve le caractère β-normal : si M terme bien typé de CC est β-normal, alors tous ses réduits par $\ \to_\circ^* \ $ aussi.*

La version "duale" qui serait que $\to_\beta$ conserve le caractère $\circ$-normal est faux. Il suffit pour s'en convaincre de considérer Cex_1.

3.7 Le théorème de descente de β

Il s'agit de la réciproque du théorème précédent. On part maintenant d'une dérivation dans CC, et on souhaite la "descendre" dans CC$\circ$. Dans ce sens là, on doit tenir compte du fait que le redex peut disparaître en partie ou totalement (cf. lemme 3.18). D'où l'utilité de la relation qui suit :

Définition 3.21 *On dira que $M \to_{\beta 2} N$ ssi $M = N$ ou $M \to_\beta N$ ou $M \to_\circ N$ par la règle (2) de $\to_\circ$.*
Là encore, $\to^*_{\beta 2}$ sera la fermeture transitive de $\to_{\beta 2}$.

Cette règle (2) de la $\circ$-réduction $(\circ\ \ t)^T \to_\circ \circ$ correspond en effet à une β-réduction d'un redex dont la tête aurait disparu.

Commençons par le cas particulier où tout le monde se réduit vers $\circ$.

Théorème 3.22 *Soit M un terme bien typé de CC. Si $M \to_\beta N$ et $M \to^*_\circ \circ$, alors $N \to^*_{\beta m} \to^*_\circ \circ$.*

$\Diamond$ Par récurrence sur la structure de M, en utilisant le lemme 3.8

(i) M ne peut être $\circ$ car c'est un élément de CC.

(ii) M ne peut être une sorte puisque M peut se β-réduire.

(iii) $M = x^X$ avec $X \to^*_\circ \circ$, $N = x^Y$ et $X \to_\beta Y$. L'hypothèse de récurrence concernant X montre que $Y \to^*_{\beta m} \to^*_\circ \circ$, donc N aussi.

(iv) $M = (a\ \ b)^T$ avec $T \to^*_\circ \circ$ ou $a \to^*_\circ \circ$. Si M entier est le redex qui se réduit pour donner N, il suffit d'appliquer le lemme 3.18. Sinon la β-réduction est interne : $N = (a_0\ \ b_0)^{T_0}$ avec $a \to^?_\beta a_0$, $b \to^?_\beta b_0$ et $T \to^?_\beta T_0$.
 – Si $T \to^*_\circ \circ$, alors par hypothèse de récurrence $T_0 \to^*_{\beta m} \to^*_\circ \circ$, et N également.
 – Si $a \to^*_\circ \circ$, alors par hypothèse de récurrence $a_0 \to^*_{\beta m} \to^*_\circ \circ$, et N également.

(v) $M = (x : X)\ t$ avec $t \to^*_\circ \circ$. Alors $N = (x : X_0)\ t_0$ avec $X \to^?_\beta X_0$ et $t \to^?_\beta t_0$. Alors par hypothèse de récurrence $t_0 \to^*_{\beta m} \to^*_\circ \circ$, et N également.

(vi) Le cas du lambda se traite de façon similaire.

$\square$

Théorème 3.23 *Soit M un terme bien typé de CC. Si $M \to_\beta N$ et $M \to^*_\circ M'$, alors il existe N' tel que $M' \to_{\beta 2} N'$ et $N \to^*_{\beta m} \to^*_\circ N'$.*

$$
\begin{tikzcd}
M \arrow[r, "\beta"'] \arrow[dd, "\circ\ *"'] & N \arrow[d, dashed, "\beta m\ *"] \\
& {} \arrow[d, dashed, "\circ\ *"] \\
M' \arrow[r, dashed, "\beta 2"'] & N'
\end{tikzcd}
$$

◊ Si $M' = \circ$, on prend $N' = \circ$ et on applique le théorème précédent. Sinon on procède par récurrence sur la structure de M, en utilisant le lemme 3.6

(i) M ne peut être une sorte puisque M peut se β-réduire.

(ii) $M = x^X$ avec $M' = x^{X'}$ et $X \rightarrow_\circ^* X'$, et d'autre part $N = x^{X_0}$ et $X \rightarrow_\beta X_0$. L'hypothèse de récurrence concernant X determine un X'_0 fermant le diagramme. On prend alors $N' = x^{X'_0}$.

(iii) $M = (a\ \ b)^T$ avec $M' = (a'\ \ b')^{T'}$ et $a \rightarrow_\circ a'$, etc. Si M entier est le redex qui se réduit pour donner N, il suffit d'appliquer le lemme 3.18. Sinon la β-réduction est interne : $N = (a_0\ \ b_0)^{T_0}$ avec $a \rightarrow_\beta^? a_0$, $b \rightarrow_\beta^? b_0$ $T \rightarrow_\beta^? T_0$. On applique trois fois l'hypothèse de récurrence pour obtenir a'_0,b'_0 et T'_0 qui ferment les diagrammes respectifs de a,b et t. De cette façon, $N' = (a'_0\ \ b'_0)^{T'}$ convient.

(iv) et (v). Ces deux cas (lambda et produit) sont similaires.

□

3.8 Accessibilité

Les résultats établis jusqu'à présent utilisent tous au moins un terme de CC comme point de départ. Nous allons maintenant regarder ce qui se passe à l'intérieur de CC∘. Mais dans CC∘ il n'y a pas de typage qui permette d'écarter les termes incorrects. Il nous faut utiliser le bon typage d' "ancêtres" situés dans CC.

Définition 3.24 *On dira qu'un terme M de CC∘ est accessible ssi il existe M_0 de CC, typable, et tel que $M_0 \rightarrow_\circ^* M$.*
On notera $\mathcal{A}$ le sous-ensemble de CC∘ formé des termes accessibles.

Proposition 3.25 *$\mathcal{A}$ est clos par $\rightarrow_\circ$.*

◊ Soit M accessible à partir de M_0. Si $M \rightarrow_\circ N$, alors évidemment $M_0 \rightarrow_\circ^* N$, donc N accessible. □

Proposition 3.26 *$\mathcal{A}$ est clos par sous-terme.*

◊ Démontrons par récurrence sur la structure d'un terme M de $\mathcal{A}$ que tous ses sous-termes sont dans $\mathcal{A}$. Notons M_0 le terme de CC à partir duquel M est accessible.

- si M est une sorte, ou $\circ$, il n'a pas de sous-termes stricts.
- si $M = x^X$, alors $M_0 = x^{X_0}$ avec $X_0 \ \rightarrow^*_\circ\ X$, de par le lemme 3.7. X est alors dans $\mathcal{A}$, puisque X_0 convient comme "ancêtre". Et les sous-termes de X sont encore dans $\mathcal{A}$ par hypothèse de récurrence.
- Les autres cas se font de manière similaire.

$\square$

Théorème 3.27 *$\mathcal{A}$ est clos par β-réduction.*

$\lozenge$ Soit M dans $\mathcal{A}$, accessible à partir du terme typé de CC M_0. Si $M \ \rightarrow_\beta\ N$, alors le théorème 3.19 affirme l'existence d'un terme N_0 tels que $M_0 \ \rightarrow^+_\beta N_0 \ \rightarrow^*_\circ\ N$. Le terme N_0 convient donc comme "ancêtre" prouvant l'accessibilité de N. $\square$

Notons $\rightarrow_{\beta\circ}$ la relation $\rightarrow_\beta\ \cup \ \rightarrow_\circ$.

Théorème 3.28 *Toute réduction $\rightarrow^*_{\beta\circ}$ dans $\mathcal{A}$ termine.*

$\lozenge$ Soit $M \ \rightarrow_{\beta\circ} M_1 \ \rightarrow_{\beta\circ} \ldots \ \rightarrow_{\beta\circ} M_n \ \rightarrow_{\beta\circ} \ldots$ une réduction de M par $\rightarrow_{\beta\circ}$. On construit alors une suite dans CC $N_0 \ \rightarrow^*_\beta\ N_1 \ \rightarrow^*_\beta\ \ldots \ \rightarrow^*_\beta\ N_n \ \rightarrow^*_\beta\ \ldots$ avec $\forall i, N_i \ \rightarrow^*_\circ\ M_i$ de la façon suivante :
- pour N_0, on prend l' "ancêtre" de M fourni par l'accessibilité.
- pour définir N_{i+1} à partir de N_i :

  (i) si $M_i \ \rightarrow_\circ\ M_{i+1}$, alors on prend $N_{i+1} = N_i$.

  (ii) si $M_i \ \rightarrow_\beta\ M_{i+1}$, on utilise le théorème 3.19 pour créer N_{i+1} tel que $N_i \ \rightarrow^+_\beta N_{i+1}$.

Par exemple :

$$\begin{tikzcd}
N \arrow[r, dashed, "+", "\beta"'] \arrow[d, dashed, "\circ"', "*"] & N_1 = N_2 \arrow[r, dashed, "+", "\beta"'] \arrow[d, dashed, "\circ"', "*"] & N_3 \arrow[r, dashed, "+", "\beta"'] \arrow[dd, dashed, "\circ"', "*"] & \ldots \\
M \arrow[r, "\beta"'] & M_1 \arrow[d, "\circ"] & & \\
& M_2 \arrow[r, "\beta"'] & M_3 \arrow[r, "\beta"'] & \ldots
\end{tikzcd}$$

Or cette suite (N_i) stationne à partir d'un certain rang, vu la forte normalisation de CC. Ceci signifie qu'à partir d'un certain rang, la suite initiale ne fait plus que des $\circ$-réductions (cas (ii) précédent). Et à partir de là, ces $\circ$-réductions sont forcément en nombre fini (Cf. Prop. 3.3). $\square$

Corollaire 3.29 *Toute réduction $\rightarrow^*_\beta$ dans $\mathcal{A}$ termine.*

◊ Il suffit de voir la réduction $\to_\beta^*$ comme un cas particulier de réduction $\to_{\beta\circ}^*$. □

Corollaire 3.30 *Pour tout terme M de $\mathcal{A}$, il y a existence et unicité d'une forme normale vis-à-vis de $\to_\beta$. On la notera encore M_β.*

◊ Il suffit de relier la terminaison tout juste établie avec la propriété de Church-Rosser. Cette dernière, syntaxique, est vrai dans CC∘ en général : il suffit de regarder ∘ comme une simple constante, et de reprendre les preuves classiques, par exemple celle de Tait & Martin-Löf. □

Lemme 3.31 *Si M est un terme typé de CC, et N un terme $\beta\circ$-normal tel que $M \to_\circ^* N$, alors $M_\beta \to_\circ^* N$.*

$$\begin{tikzcd}
M \arrow[rr, "*", "\beta"'] \arrow[dr, "*", "\circ"'] & & M_\beta \arrow[dl, dashed, "*"', "\circ"] \\
& N &
\end{tikzcd}$$

◊ On va procéder par récurrence sur la taille de la plus longue dérivation β partant de M.

- Si la taille de cette plus longue dérivation vaut zéro, c'est que M est déjà β-normal, et alors $M = M_\beta$.
- Sinon M peut encore se β-réduire vers un terme P. Alors par le théorème 3.23, il existe Q, R tel que $P \to_{\beta m}^* Q \to_\circ^* R$ et $N \to_{\beta 2} R$, donc forcément $R = N$ vu que N est supposé $\beta\circ$-normal. On a donc $Q \to_\circ^* N$ et Q fait partie des β-réduits stricts de M. On peut donc utiliser l'hypothèse de récurrence pour Q et affirmer que $Q_\beta \to_\circ^* N$. Or enfin $Q_\beta = M_\beta$.

□

Théorème 3.32 *Tout terme M de $\mathcal{A}$ a une et une seule forme normale par $\to_{\beta\circ}$, qui est $(M_\beta)_\circ$, la forme ∘-normale de la forme β-normale de M.*

◊ Prouvons l'unicité. Soit N "l'ancêtre" de M dans CC. Supposons qu'il existe une réduction $M \to_{\beta\circ} M_1 \to_{\beta\circ} \ldots \to_{\beta\circ} M_n$ de M vers une forme $\beta\circ$-normale M_n. Reprenons alors la construction effectuée lors de la preuve du théorème 3.28. On obtient alors un N_n tel que $N \to_\beta^* N_n$, et $N_n \to_\circ^* M_n$. Le lemme précédent montre alors que $(N_n)_\beta \to_\circ^* N_n$, et donc que $N_\beta \to_\circ^* M_n$. Enfin, puisque M_n est en particulier ∘-normal, on obtient $(N_\beta)_\circ = M_n$. Et ceci est vrai quel que soit la forme $\beta\circ$-normale M_n choisie, d'où l'unicité.

Pour ce qui est de l'existence, il suffit de prendre le terme $(M_\beta)_\circ$. Ce terme est évidemment ∘-normal, et le corollaire 3.20 montre que c'est également un terme β-normal.

Et vu l'unicité, cet exemple de terme $\beta\circ$-normal est en fait le seul. □

L'ordre dans lequel on réduit vers les formes normales (β puis ∘) est essentiel. Si l'on procède dans l'autre sens, $(M_\circ)_\beta$ est certes β-normal, mais pas forcément ∘-normal. Cf. la remarque qui suit le corollaire 3.20.

Corollaire 3.33 $\rightarrow^*_{\beta\circ}$ *vérifie la Propriété de Church-Rosser.*

Corollaire 3.34 *Soit N un terme typé de CC, avec $N \rightarrow^*_\circ M$. On a $(N_\beta)_\circ = (M_\beta)_\circ$.*

Plus précisement, à partir des réductions $N \rightarrow^*_\beta N_\beta$ et $M \rightarrow^*_\beta M_\beta$, on a les relations suivantes :

$$
\begin{tikzcd}
N \arrow[r, "*", "\beta"'] \arrow[d, "\circ"', "*"] & {} \arrow[r, "*", "\beta"'] \arrow[d, dashed, "\circ"', "*"] & N_\beta \arrow[d, dashed, "\circ"', "*"] \\
M \arrow[r, "*", "\beta"'] & M_\beta \arrow[r, dashed, "*", "(2)"'] & {} \arrow[d, dashed, "\circ"', "*"] \\
& & (M_\beta)_\circ = (N_\beta)_\circ
\end{tikzcd}
$$

On peut donc très bien imaginer appliquer $\rightarrow^*_\circ$ une seule fois, au moment de l'extraction de N, et n'utiliser que β lors de l'exécution. La réduction s'arrête alors à M_β. Il est aussi possible (et même souhaitable) d'intégrer la règle (2) parmi les mécanismes de réduction post-extraction. Ceci permet de mimer plus fidèlement la réduction β de N. Enfin, si l'on désire une optimisation poussée, il peut être nécessaire de $\circ$-réduire de nouveau à la fin, afin d'aboutir à $(N_\beta)_\circ$.

4 Le Calcul des Constructions Inductives

Nous allons présenter CIC comme une extension de CC, en mettant l'accent sur les ajouts, toujours en s'inspirant de [1], [12] et [15]. Pour une présentation moins formelle, on pourra se reporter à [5].

4.1 Notation vectorielle

Comme dans [15], nous utiliserons des notations vectorielles pour élimininer tant que faire se peut les notations avec points de suspension. Ainsi nous parlerons d'une séquence de termes :

$$\overrightarrow{t_i} = t_1, t_2 \dots t_n$$

Il s'agit d'un abus de notation désignant en fait $(\overrightarrow{t_i})_{i=1..n}$. La longueur de la séquence sera notée $|\overrightarrow{t_i}|$. Par convention, si deux séquences portent le même index, alors elles ont même longueur.

Puis nous utiliserons des produits et des applications séquentiels. Soit $\overrightarrow{x_i}$ une séquence de variables, $\overrightarrow{u_i}$ et $\overrightarrow{U_i}$ deux séquences de termes. Alors :

$$\begin{array}{rcl} (\overrightarrow{x_i} : \overrightarrow{u_i})\ t & = & (x_1 : u_1)\ \dots (x_n : u_n)\ t \\ (t \quad \overrightarrow{u_i})^{\overrightarrow{U_i}} & = & ((t \quad u_1)^{U_1} \quad \dots \quad u_n)^{U_n} \end{array}$$

Si l'on prend un contexte Γ , on peut en extraire la séquence des variables que ce contexte introduit. Nous la noterons $Var(\Gamma)$, et elle est définie par :

$$Var(x_1 : T_1, \dots , x_n : T_n) = x_1, \dots , x_n$$

Nous utiliserons également des séquences de contextes $\overrightarrow{\Gamma_i} = \Gamma_1, \dots , \Gamma_n$

Définissons ensuite les substitutions séquentielles :

$$t[\overrightarrow{x_i}/\overrightarrow{u_i}] = t[x_1/u_1] \dots [x_n/u_n]$$

Pour décrire simplement les séquences de types utilisées lors d'applications séquentielles, nous définissons :

$$\begin{array}{rcl} seq((\overrightarrow{x_i} : \overrightarrow{U_i})\ V, \overrightarrow{u_i}) & = & ((\overrightarrow{x_i} : \overrightarrow{u_i})_{i=2..n} V)[x_1/u_1], \\ & & \dots \\ & & ((x_n : u_n)V)[x_1/u_1] \dots [x_{n-1}/u_{n-1}], \\ & & V[\overrightarrow{x_i}/\overrightarrow{u_i}] \end{array}$$

Ainsi pour un terme t de type $T = (\overrightarrow{x_i} : \overrightarrow{U_i})\ V$, nous pourrons écrire $(t \quad \overrightarrow{u_i})^{seq(T,\, \overrightarrow{u_i})}$, qui sera de type $V[\overrightarrow{x_i}/\overrightarrow{u_i}]$. Dans un dernier abus de notation, nous dirons $(t \quad \overrightarrow{u_i})^{seq(T)}$, vu que le deuxième argument du *seq* est déjà donné à l'intérieur de l'application.

4.2 Occurrences positives et constructeurs

Définition 4.1 (Occurrences positives) *Soit X une variable. On dira qu'un terme t est strictement positif en X si $t = (\overrightarrow{x_i} : \overrightarrow{u_i})\ (X \quad \overrightarrow{v_j})^{\overrightarrow{V_j}}$, si X n'à pas d'occurrences libres dans $\overrightarrow{u_i}$, $\overrightarrow{v_j}$ et $\overrightarrow{V_j}$, et aucune des composantes de $\overrightarrow{x_i}$ n'est égale à X. On notera $Pos(X, t)$.*

Définition 4.2 (Type de constructeur) *Un terme C est un type de constructeur en X, ce que l'on note $constr(C, X)$, si l'une des conditions suivantes est vérifiée :*

- *$C = (X \quad \overrightarrow{v_j})^{\overrightarrow{V_j}}$ sous la condition que X n'est pas libre dans $\overrightarrow{v_j}$ et $\overrightarrow{V_j}$.*
- *$C = (x : u)\ D$ sous les conditions : D est un type de constructeur en X, X n'a pas d'occurrences libres dans u et $X \neq x$.*
- *$C = P \to D$ sous les conditions : D est un type de constructeur en X et $Pos(X, P)$.*

Définition 4.3 (Petits et grands constructeurs) *Soit C un type de constructeur en X, que l'on peut écrire $C = (\overrightarrow{x_i} : \overrightarrow{t_i})\ (X \quad \overrightarrow{t_i'})^{\overrightarrow{T_i}}$. Si tous les $\overrightarrow{t_i}$ sont de types $Prop$ ou Set dans le système de typage qui va suivre, alors on dira que C est un petit constructeur. On notera $small(C)$. Et si un constructeur n'est pas petit, il est grand.*

4.3 Les définitions inductives

Définition 4.4 (Syntaxe de CIC) *On rajoute quatre constructions par rapport à la syntaxe de CC :*

$$t ::= \cdots \mid Ind(x)\{\overrightarrow{t_i}\}^t \mid Constr_n(t) \mid (Cases\ t\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^t \mid Fix(x,\ t)^t$$

Précisons le status des variables de ces nouvelles constructions, et en particulier quelles sont les variables libres :

$$\begin{array}{lcl}
FV(Ind(x)\{\overrightarrow{C_i}\}^A) & = & FV(A) \cup (\bigcup_i FV(C_i)\ \setminus \{x\}) \\
FV(Constr_n(I)) & = & FV(I) \\
FV((Cases\ c\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^T & = & FV(T) \cup (\bigcup_i (FV(\Gamma_i) \cup FV(t_i) \setminus Var(\Gamma_i))) \\
FV(Fix(f,\ t)^T & = & FV(T) \cup (FV(t) \setminus \{f\})
\end{array}$$

Par exemple, $nat = Ind(x)\{x^{Set},\ x^{Set} \to x^{Set}\}^{Set}$ nous donne les entiers naturels, et alors $O = Constr_1(nat)$ et $S = Constr_2(nat)$. Cette syntaxe ne permet pas les définitions mutuellement récursives.

La syntaxe $(Cases\ c\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^T$ est en fait une version abrégée de la construction Coq

$$\begin{array}{lllll} Cases\ c\ of & & & & \\ & & (Constr_1(I)\ Var(\Gamma_1)) & => & t_1 \\ & | & & \ldots & \\ & | & (Constr_n(I)\ Var(\Gamma_n)) & => & t_n \\ end. & & & & \end{array}$$

La fonction *prédécesseur* peut ainsi s'écrire

$$(Cases\ n\ of\ \{\emptyset, m : nat\}\{O, m^{nat}\})^{nat}$$

Donnons également un exemple de point-fixe. Si $N = nat \to nat$, la fonction *double* vaut :

$$Fix(f, ([n : nat]\ Cases\ n\ of\{\emptyset, m : nat\}\{0, (S(S(f^N\ m^{nat})))\})^N)^N$$

En plus de la β-réduction, on définit également une ι-réduction spécifique aux termes inductifs.

Définition 4.5 (ι-réduction) *Si $I = Ind(X)\{\overrightarrow{C_i}\}^A$, alors*

$$(Cases\ (Constr_n(I)\ \ \overrightarrow{m_j})^{\overrightarrow{T_j}}\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^T\ \to_\iota t_n[Var(\Gamma_n)/\overrightarrow{m_j}]$$

Et pour le point-fixe :

$$(Fix(f,\ t)^T\ \ c)^U\ \to_\iota (t[f/Fix(f,\ t)^T]\ \ c)^U$$

à condition qu'il y ait un $Constr_n$ en tête de c.

Cette dernière condition sur la réduction du point-fixe permet d'éviter que cette réduction ne diverge. Il s'agit en fait d'une version simplifiée du point-fixe de Coq, puisque dans Coq l'argument inductif qui contrôle la terminaison n'est pas forecement le premier.

Par rapport à CC, nous allons maintenant utiliser $\to_{\beta\iota} = \to_\beta\ \cup\ \to_\iota$ par défaut au lieu de $\to_\beta$. Par exemple nous allons reprendre la définition 2.5 de l'ordre de conversion, à ceci près qu'on utilise la $\beta\iota$-équivalence au lieu de la β-équivalence comme base de la construction. Pareil pour la règle de typage (Conv2).

4.4 Typage de CIC

Les nouvelles règles de typages correspondantes aux nouveaux constructeurs sont données ci-dessous. On y utilise les notations suivantes :

$$\begin{array}{l}
A = (\overrightarrow{x_i} : \overrightarrow{A_i})\ s \\
I = Ind(X)\{\overrightarrow{C_j(X)}\}^A \\
\forall j,\ C_j = (\overrightarrow{y_{k_j}} : \overrightarrow{Y_{k_j}})\ (X\ \ \overrightarrow{\tau_{p_j}})^{seq(A)} \\
\forall j, \Gamma_j = \overrightarrow{y_{k_j}} : \overrightarrow{Y_{k_j}} \\
B = (\overrightarrow{x_i} : \overrightarrow{A_i})(I\ \ \overrightarrow{x_i}) \to s'
\end{array}$$

Règles de typage des termes

$$\text{(Ind)} \qquad \frac{\Gamma \vdash A : Type \quad \forall j,\ \Gamma; X : A \vdash C_j : s \quad \forall j,\ constr(C_j, X)}{\Gamma \vdash I : A}$$

$$\text{(Constr)} \quad \forall j \in [1..|I|],\ \frac{\Gamma \vdash I : A'}{Constr_j(I) : C_j[X/I]}$$

$$\text{(Cases)} \qquad \frac{\begin{array}{c}\Gamma \vdash \overrightarrow{u_i} : (\overrightarrow{x_i} : \overrightarrow{A_i}) \qquad \Gamma \vdash c : (I\ \ \overrightarrow{u_i})^{seq(A)} \qquad Conditions(I, s, s') \\ \forall j,\ \Gamma; \Gamma_j[X/I] \vdash t_j : (Q\ \overrightarrow{\tau_{p_j}}\ (Constr_j(I)\ \overrightarrow{y_{k_j}})^{seq(C_j[X/I])})^{seq(B)} \qquad \Gamma \vdash Q : B\end{array}}{\Gamma \vdash (Cases\ c\ of\ \{\overrightarrow{\Gamma_j}\}\{\overrightarrow{t_j}\})^{(Q\ \overrightarrow{u_i}\ c)^{seq(B)}} : (Q\ \overrightarrow{u_i}\ c)^{seq(B)}}$$

$$\text{(Fix)} \qquad \frac{\Gamma \vdash T : s \qquad \Gamma; f : T \vdash t : T \qquad Convenable(t, T)}{\Gamma \vdash Fix(f,\ t)^T : T}$$

Dans la règle de typage (Cases), le prédicat $Condition(I, s, s')$ impose des restrictions sur les sortes utilisées : on doit avoir $s' \leq s$ dans l'ordre définit par $Prop \leq Set \leq Type$, ou alors $s = Set$ et $s' = Type$ et tous les constructeurs de I sont petits.

Concernant la règle (Fix), on se reportera à [1] pour ce qui est des conditions $Convenable(t, T)$ (conditions de garde, etc). Dans notre présentation, nous réclamerons en particulier que T soit de la forme $T = (I\ \ \overrightarrow{u_i})^{\overrightarrow{A_i}} \to T'$ avec T' de même sorte s que I.

4.5 Propriétés de CIC

Nous admettrons que cette présentation du Calcul des Constructions Inductives vérifie bien les propriétés habituelles. En particulier les lemmes de la section 2.3 concernant CC ont des analogues dans CIC, où on a remplacé β-équivalence par $\beta\iota$-équivalence.

Nous aurons en plus besoin de lemmes précisant la forme des sequences de marques $\overrightarrow{U_i}$ utilisé pour une application séquentielle $(t\ \ \overrightarrow{u_i})^{\overrightarrow{U_i}}$.

Lemme 4.6 (application séquentielle 1) *Soit t un terme de CIC dont le type principal est de la forme suivante :*

$$\Gamma \vdash t : (\overrightarrow{x_i} : \dots)\ s$$

Alors :

(i) si $\Gamma \vdash (t\ \ u)^U : V$ avec U $\beta\iota$-normal, alors U est de la forme $(\overrightarrow{x_i} : \dots)_{i=2..n} s'$ avec $s \preceq s'$.

(ii) si $\Gamma \vdash (t\ \ \overrightarrow{u_j})^{\overrightarrow{U_j}} : V$ avec tous les U_j $\beta\iota$-normaux, alors pour tout j, U_j est de la forme $(\overrightarrow{x_i} : \dots)_{i=j..n} s_j$ avec $s \preceq s_j$.

$\Diamond$ Prouvons tout d'abord le point (i). On a le typage suivant pour $(t\ \ u)^U$: un certain nombre de (Conv1) ou (Conv2) avant un (App) :

$$\cfrac{\cfrac{\Gamma \vdash t : (x : X)W \qquad \Gamma \vdash u : X}{\Gamma \vdash (t\ \ u)^{W[x/u]} : W[x/u]}}{\cfrac{\vdots}{\Gamma \vdash (t\ \ u)^U : V}}$$

Vu la définition du type principal, on a $(\overrightarrow{x_i} : \dots)\ s \preceq (x : X)W$. Donc W est $\beta\iota$-équivalent à un terme de la forme $(\overrightarrow{x_i} : \dots)_{i=2..n} s'$, avec $s \preceq s'$. Donc $W[x/u]$ est aussi $\beta\iota$-équivalent à un terme de la même forme. Enfin U, $\beta\iota$-normal, est donc la forme $\beta\iota$-normale de $W[x/u]$, et s'écrit donc aussi $(\overrightarrow{x_i} : \dots)_{i=2..n} s'$.

Et pour prouver le point (ii), on utilise par récurrence le point (i). $\square$

Lemme 4.7 (application séquentielle 2) *Soit t un terme de CIC typable de la façon suivante :*

$$\Gamma \vdash t : (\overrightarrow{x_i} : \dots)\ (M_0\ \ \dots)^{\dots}$$

avec M_0 $\beta\iota$-normal, différent d'une sorte et d'un lambda, et dont les variables libres sont distinctes des $\overrightarrow{x_i}$. Alors :

(i) si $\Gamma \vdash (t\ \ u)^U : V$ avec U $\beta\iota$-normal, alors U est de la forme $(\overrightarrow{x_i} : \dots)_{i=2..n}(M_0\ \ \dots)^{\dots}$

(ii) si $\Gamma \vdash (t\ \ \overrightarrow{u_j})^{\overrightarrow{U_j}} : V$ avec tous les U_j $\beta\iota$-normaux, alors pour tout j, U_j est de la forme $(\overrightarrow{x_i} : \dots)_{i=j..n}(M_0\ \ \dots)^{\dots}$

$\Diamond$ Prouvons tout d'abord le point (i). On a le typage suivant pour $(t\ \ u)^U$: un certain nombre de (Conv1) ou (Conv2) avant un (App) :

$$\cfrac{\cfrac{\Gamma \vdash t : (x : X)W \qquad \Gamma \vdash u : X}{\Gamma \vdash (t\ \ u)^{W[x/u]} : W[x/u]}}{\cfrac{\vdots}{\Gamma \vdash (t\ \ u)^U : V}}$$

En utilisant un type principal T de t, on a $T \preceq (\overrightarrow{x_i} : \dots)\ (M_0\ \ \dots)^{\dots}$ et $T \preceq (x : X)W$. le lemme 2.8 permet de voir que T est $\beta\iota$-équivalent à $(\overrightarrow{x_i} : \dots)\ (M_0\ \ \dots)^{\dots}$, puis que

$(x : X)W$ également. D'où $x = x_1$, et $W[x/u]$ est $\beta\iota$-équivalent à un terme de la forme $(\overrightarrow{x_i} : \dots)_{i=2..n}(M_0 \quad \dots)^{\cdots}[x_1/u]$. Et vu les hypothèses sur les variables libres de M_0, ce dernier terme est encore de la forme $(\overrightarrow{x_i} : \dots)_{i=2..n}(M_0 \quad \dots)^{\cdots}$. Enfin U est la forme $\beta\iota$-normale de $U[x/u]$, donc encore de la forme $(\overrightarrow{x_i} : \dots)_{i=2..n}(M_0 \quad \dots)^{\cdots}$.

Et pour prouver le point (ii), on utilise par récurrence le point (i). $\square$

5 Le système CIC∘

Nous allons ici reprendre le canevas du chapitre 3, en essayant de ne pas reprendre les parties strictement “CC” des preuves, et au contraire de voir les changements dûs à la présence des Inductifs.

5.1 Présentation du système

On rajoute un symbole supplémentaire $\circ$ au système CIC précédent.

Définition 5.1 (Syntaxe de CIC∘) *Les termes de CIC∘ sont donnés par la grammaire suivante :*

$$\begin{array}{rcl} t & ::= & \circ \mid Prop \mid Set \mid Type_i \mid x^t \mid (t\ \ t)^t \mid (x:t)\ t \mid ([x:t]\ t)^t \\ & & \mid Ind(x)\{\overrightarrow{t_i}\}^t \mid Constr_n(t) \mid (Cases\ t\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^t \mid Fix(x,\ t)^t \end{array}$$

La relation $\rightarrow_\circ$ comprend deux règles supplémentaires propres aux inductifs.

Définition 5.2 (Réduction ∘) *La relation de réécriture $\rightarrow_\circ$ est définie à partir des règles suivantes :*

$$\begin{array}{lccc} (0) & Prop & \rightarrow_\circ & \circ \\ (1) & t^\circ & \rightarrow_\circ & \circ \\ (2) & (\circ\ \ t)^T & \rightarrow_\circ & \circ \\ (3) & (x:X)\ \circ & \rightarrow_\circ & \circ \\ (4) & ([x:X]\ \circ)^T & \rightarrow_\circ & \circ \\ (5) & Constr_n(\circ) & \rightarrow_\circ & \circ \\ (6) & (Cases\ \ \circ\ \ of\ \ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^T & \rightarrow_\circ & \circ \end{array}$$

Remarquons que maintenant la pseudo-syntaxe t° de la règle (1) englobe aussi les nouveaux termes avec marques que sont Ind, $Cases$ et Fix.

5.2 Premières propriétés de CC∘

Proposition 5.3 *La relation $\rightarrow_\circ$ termine.*

◊ cf. Prop. 3.3 □

Proposition 5.4 *La relation $\rightarrow_\circ$ est confluente.*

◊ Une paire critique de plus par rapport à la Prop. 3.4, celle formée à partir des règles (1) et (6), ce qui donne $(Cases\ \ \circ\ \ of\ \ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^\circ$, qui se réduit de toute façon vers $\circ$. □

Corollaire 5.5 *Pour tout terme t de CIC$\circ$, il y a existence et unicité d'une forme normale vis-à-vis de $\to_\circ$. On la notera $t_\circ$.*

Concernant les trois lemmes syntaxiques de conservation/inversion, nous ne donnerons que les cas nouveaux.

Lemme 5.6 (Conservation de la structure) *Soit $M \to_\circ^* N$ avec $N \neq \circ$.*

(i) à (v) : cf lemme 3.6.

(vi) Si $M = Ind(x)\{\overrightarrow{t_i}\}^A$, alors il existe A' et des $\overrightarrow{t'_i}$ tels que $N = Ind(x)\{\overrightarrow{t'_i}\}^{A'}$, $A \to_\circ^* A'$ et $\forall i, t_i \to_\circ^* t'_i$.

(vii) Si $M = Constr_n(I)$, alors il existe I' tel que $N = Constr_n(I')$ et $I \to_\circ^* I'$.

(viii) Si $M = (Cases\ c\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^T$, alors il existe $c', \overrightarrow{\Gamma'_i}$, $\overrightarrow{t'_i}$ et T' tels que $N = (Cases\ c'\ of\ \{\overrightarrow{\Gamma'_i}\}\{\overrightarrow{t'_i}\})^{T'}$ et $c \to_\circ^* c'$, etc.

(ix) Si $M = Fix(f,\ t)^T$, alors il existe t' et T' tels que $N = Fix(f,\ t')^{T'}$ avec $t \to_\circ^* t'$ et $T \to_\circ^* T'$.

Lemme 5.7 (Réciproque de la conservation) *Soit $M \to_\circ^* N$.*

(i) à (iv) : cf lemme 3.7

(v) Si $N = Ind(x)\{\overrightarrow{t_i}\}^A$, alors il existe A_0 et des $\overrightarrow{t^0_i}$ tels que $M = Ind(x)\{\overrightarrow{t^0_i}\}^{A_0}$, $A \to_\circ^* A_0$ et $\forall i, t^0_i \to_\circ^* t_i$.

(vi) Si $N = Constr_n(I)$, alors il existe I_0 tel que $M = Constr_n(I_0)$ et $I_0 \to_\circ^* I$.

(vii) Si $N = (Cases\ c\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^T$, alors il existe $c_0, \overrightarrow{\Gamma^0_i}$, $\overrightarrow{t^0_i}$ et T_0 tels que $M = (Cases\ c_0\ of\ \{\overrightarrow{\Gamma^0_i}\}\{\overrightarrow{t^0_i}\})^{T_0}$ et $c_0 \to_\circ^* c$, etc.

(viii) Si $N = Fix(f,\ t)^T$, alors il existe t_0 et T_0 tels que $M = Fix(f,\ t_0)^{T_0}$ avec $t_0 \to_\circ^* t$ et $T_0 \to_\circ^* T$.

Lemme 5.8 (Inversion de $\circ$) $M \to_\circ^* \circ$ *ssi l'on est dans l'un des cas suivants :*

(i) à (vi) : cf lemme 3.8

(vii) $M = Ind(x)\{\overrightarrow{t_i}\}^A$, et il existe une réduction $A \to_\circ^* \circ$

(viii) $M = Constr_n(I)$, et $I \to_\circ^* \circ$

(ix) Si $M = (Cases\ c\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^T$, et $c \to_\circ^* \circ$ ou $T \to_\circ^* \circ$

(x) Si $M = Fix(f,\ t)^T$, et $T \to_\circ^* \circ$

5.3 Types inductifs et $\circ$-réductions

Nous aurons besoin de quelques résultats basiques sur les types inductifs.

Définition 5.9 *Un terme t est une arité de sorte s, noté $Ar(t, s)$, si t est de la forme $t = (\overrightarrow{x_i} : \overrightarrow{X_i})s$*

Proposition 5.10 *Tous les types inductifs $I = Ind(x)\{\overrightarrow{C_j}\}^A$ bien typés de CIC ont une marque A qui est $\beta\iota$-équivalent à une arité sur une sorte s Nous noterons $sorte(I)$ cette sorte s relatif au type I. Et cette sorte est invariante par $\beta\iota$-réduction.*

$\diamondsuit$ Par récurrence sur le typage de I : c'est immédiat pour la règle (Ind). Quant à la règle (Conv2), la seule modifiant la marque A, elle le fait par $\beta\iota$-équivalence. En particulier une modification de la marque A par $\beta\iota$-réduction ne modifie pas la sorte s. $\square$

Proposition 5.11 *Un type inductif I bien typé de CIC vérifie $I \to_\circ^* \circ$ ssi $sorte(I) = Prop$.*

$\diamondsuit$ D'après la règle (1) de la $\circ$-réduction, $I \to_\circ^* \circ$ ssi sa marque $A \to_\circ^* \circ$. Et vu la forme de A donnée par la proposition précédente, $A \to_\circ^* \circ$ ssi $sorte(I) \to_\circ^* \circ$. $\square$

Proposition 5.12 *Soit $I = Ind(x)\{\overrightarrow{C_j}\}^A$ un type inductif bien typé de CIC. Alors pour tout j, on a $C_j[x/I]$ ssi $sorte(I) = Prop$.*

$\diamondsuit$ D'après la règle (Ind), $C_j[x/I]$ est de la forme $C_j[x/I] = (\overrightarrow{y_{k_j}} : \overrightarrow{Y_{k_j}}[x/I])\ (I\ \ \overrightarrow{\tau_{p_j}})^{seq(A)}$, avec $A = (\overrightarrow{x_i} : \overrightarrow{A_i})\ s$, et $s = sorte(I)$. Or tous les éléments de la séquence $seq(A, \overrightarrow{\tau_{p_j}})$ sont des arités sur s, et en particulier le dernier élément est s lui-même. Donc si $sorte(I) = Prop$, $C_j[x/I] \to_\circ^* \circ$. Et réciproquement, si $C_j[x/I] \to_\circ^* \circ$, c'est que soit I, soit l'un des éléments de la séquence $seq(A, \overrightarrow{\tau_{p_j}})$ peut se réduire vers $\circ$ (utilisation répété du lemme d'inversion), ce qui dans tous les cas donne $sorte(I) = Prop$. $\square$

Proposition 5.13 *Si $M = (Constr_n(I)\ \ \overrightarrow{m_i})^{\overrightarrow{T_i}}$ est un terme bien typé de CIC, avec les $\overrightarrow{T_i}$ tous $\beta\iota$ normaux, alors $M \to_\circ^* \circ$ ssi $sorte(I) = Prop$.*

$\diamondsuit$ Déjà, si $sorte(I) = Prop$, on a $Constr_n(I) \to_\circ^* \circ$, et donc $M \to_\circ^* \circ$. Réciproquement, supposons que $M \to_\circ^* \circ$. Une utilisation répétée du lemme d'inversion nous montre que soit $Constr_n(I) \to_\circ^* \circ$, et c'est alors gagné, soit il existe i tel que $T_i \to_\circ^* \circ$. Etudions maintenant la forme de ces marques $\overrightarrow{T_i}$. Ecrivons $I = Ind(x)\{\overrightarrow{C_j}\}^A$ et $I_0 = Ind(x)\{\overrightarrow{C_j^0}\}^{A_0}$ sa forme $\beta\iota$-normale. On a alors le typage $\Gamma \vdash Constr_n(I) : C_n^0[x/I_0]$. et $C_n^0[x/I_0]$ est de la forme $(\overrightarrow{y_k} : \dots)(I_0\ \dots)^{\cdots}$ On peut donc appliquer le lemme 4.7 : pour tout i, T_i est de la forme $(\overrightarrow{y_k} : \dots)_{k=i..}(I_0\ \dots)^{\cdots}$ Appelons maintenant V_i la partie de T_i de forme $(I_0\ \dots)^{\cdots}$. Un type principal de I_0 est $A_0 = (\overrightarrow{x_l} : \dots)s$ avec $s = sorte(I_0) = sorte(I)$. D'autre part V_i est $\beta\iota$-normale car sous-terme de T_i. On peut donc appliquer le lemme 4.6 : les marques de V_i sont des arités sur des sortes plus grandes ou égale à s. Finalement $T_i \to_\circ^* \circ$ ssi $V_i \to_\circ^* \circ$ ssi $I_0 \to_\circ^* \circ$ ou l'une des marques de V_i se réduit vers $\circ$, i.e. l'une des sortes plus grandes ou égale à s vaut $Prop$. Dans tout les cas on arrive à $sorte(I) = Prop$. $\square$

5.4 CIC$\circ$ et typage : les premiers lemmes

Théorème 5.14 *Si on a :*
- $\Gamma \vdash M : T$
- T *$\beta\iota$-normal*
- M *n'a que des marques $\beta\iota$-normales*
- $T \rightarrow_\circ^* \circ$

Alors $M \rightarrow_\circ^* \circ$.

$\Diamond$ Par récurrence sur la structure de M. Le seul cas nouveau par rapport au lemme 3.9 est celui où $M = Constr_n(I)$. Son typage est alors constitué d'un certain nombre de (Conv1) avant un (Constr).

$$\cfrac{\cfrac{\cfrac{\Gamma \vdash I : A'}{\Gamma \vdash Constr_n(I) : C_n[x/I]}}{\vdots}}{\Gamma \vdash Constr_n(I) : T}$$

Grâce à la transitivité de $\preceq$, on a $C_n[x/I] \preceq T$. Donc d'après l'adaptation pour CIC du lemme 2.8, on a soit $C_n[x/I] =_{\beta\iota} T$, soit $C_n[x/I]$ et T sont $\beta\iota$-équivalents à deux arités de sortes respectives s et s', avec $s \preceq s'$. Ce deuxième cas est impossible vu que C_n a x comme symbole de tête, tout comme ses $\beta\iota$-réduits. $C_n[x/I]$ ne peut donc être une arité. On est donc dans le premier cas, et on peut même dire que T est la forme $\beta\iota$-normale de $C_n[x/I]$. Maintenant, si l'on considère $I' = Ind(x)\{\overrightarrow{C_i'}\}^{A'}$ la forme $\beta\iota$-normale de I, alors $T = C_n'[x/I']$. Enfin vu que $T \rightarrow_\circ^* \circ$, les résultats du paragraphe précédent donne que $sorte(I') = sorte(I) = Prop$, d'où $I \rightarrow_\circ^* \circ$ et donc $Constr_n(I) \rightarrow_\circ^* \circ$. $\square$

Rien à signaler concernant les deux lemmes suivants.

Lemme 5.15 (lemme de substitution) *Si on a :*
- $\Gamma; x : X \vdash t : T$
- $\Gamma \vdash u : X$
- t *et* u *n'ont que des marques $\beta\iota$-normales*
- $t \rightarrow_\circ^* t'$
- $u \rightarrow_\circ^* u'$

Alors $t[x/u] \rightarrow_\circ^* t'[x/u']$.

$\Diamond$ Cf. la démonstration du lemme 3.11. $\square$

Lemme 5.16 (Raffinement du lemme d'inversion de $\circ$) *Si* $([x : X]\ t)^T \rightarrow_\circ^* \circ$, *avec* $([x : X]\ t)^T$ *typé dans un contexte* Γ, *et dont les marques sont $\beta\iota$-normales, alors* $t \rightarrow_\circ^* \circ$.

$\Diamond$ Cf. la démonstration du lemme 3.12. $\square$

5.5 La deuxième génération de lemmes

Lemme 5.17 (fondamental) *Soit M un terme de CIC bien typé dans un contexte Γ, et tel que $M \rightarrow_\circ^* \circ$. Alors sa forme $\beta\iota$-normale $M_{\beta\iota}$ se réduit aussi vers $\circ$ par $\rightarrow_\circ^*$.*

$$\begin{tikzcd} M \arrow[r, "*", "\beta\iota"'] \arrow[d, "\circ"', "*"] & M_\beta \arrow[d, dashed, "\circ"', "*"] \\ \circ & \circ \end{tikzcd}$$

$\Diamond$ On reprend le même schéma de preuve que pour le lemme 3.13, sauf que l'ordre bien fondé qui nous sert à faire la récurrence est maintenant défini par rapport à la réduction $\rightarrow_{\beta\iota}$, et non $\rightarrow_\beta$. Parmi les nouveaux cas, les seuls intéressants sont ceux concernant les deux ι-redex possibles.

- $M = (Fix(f,\ t)^T\ \ c)^U$, sans $\beta\iota$-réductions internes possibles. Alors $T \rightarrow_\circ^* \circ$ ou $U \rightarrow_\circ^* \circ$. Or à partir du typage de M, on peut obtenir $\Gamma; f : T \vdash t : T$, et donc $\Gamma \vdash t[f/Fix(f,\ t)^T] : T$. On peut alors utiliser le théorème 5.14 : si $T \rightarrow_\circ^* \circ$, alors $t[f/Fix(f,\ t)^T] \rightarrow_\circ^* \circ$. Bref, dans tous les cas le ι-réduit $(t[f/Fix(f,\ t)^T]\ \ c)^U$ peut encore se réduire vers $\circ$. Et on obtient alors $M_{\beta\iota} \rightarrow_\circ^* \circ$ par hypothèse de récurrence.
- $M = (Cases\ (Constr_n(I)\ \ \overrightarrow{m_j})^{\overrightarrow{T_j}}\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^T$, sans $\beta\iota$-réductions internes possibles. Le cas $T \rightarrow_\circ^* \circ$ se traite comme dans la preuve du lemme 3.13. Reste le cas $(Constr_n(I)\ \ \overrightarrow{m_j})^{\overrightarrow{T_j}} \rightarrow_\circ^* \circ$. La proposition 5.13 montre qu'on a alors $sorte(I) = Prop$. Or la règle de typage (Cases) montre que T est $\beta\iota$-équivalent à un terme de la forme $(Q\ \ \ldots)^{seq(B)}$. Et le dernier terme de la séquence $seq(B)$ est forcement s', et vu que $s = sorte(I) = Prop$, alors $s' = Prop$ également. On obtient finalement que T est de type $Prop$, donc se réduit vers $\circ$. On est en fait dans le premier cas...

$\square$

Soit $\rightarrow_{\beta\iota m}$ la $\beta\iota$-réduction dans les marques. On peut maintenant reprendre les lemmes précédents en remplaçant les hypothèses requises *a priori* concernant $\beta\iota$ par de la normalisation $\rightarrow_{\beta\iota m}$ *a posteriori.*

Théorème 5.18 *Si on a $\Gamma \vdash M : T$ et $T \rightarrow_\circ^* \circ$, alors $M \rightarrow_{\beta\iota m}^* \rightarrow_\circ^* \circ$.*

$\Diamond$ Cf. la démonstration du lemme 3.14 $\square$

Lemme 5.19 (lemme de substitution 2) *Si on a :*

- $\Gamma; x : X \vdash t : T$
- $\Gamma \vdash u : X$
- $t \rightarrow_\circ^* t'$
- $u \rightarrow_\circ^* u'$

Alors $t[x/u] \rightarrow_{\beta\iota m}^* \rightarrow_\circ^* t'[x/u']$.

$\Diamond$ Cf la démonstration des lemmes 3.15 et 3.16. $\square$

Lemme 5.20 (lemme de substitution 3) *Si on a :*

- $\Gamma; x : X \vdash t : T$
- $\Gamma \vdash u : X$
- $t \;\to^*_{\beta\iota m} \to^*_\circ\; t'$
- $u \;\to^*_\circ\; u'$

Alors $t[x/u] \;\to^*_{\beta\iota m} \to^*_\circ\; t'[x/u']$.

$\Diamond$ Notons $t \;\to^*_{\beta\iota m}\; t_0 \;\to^*_\circ\; t'$. Alors $t[x/u] \;\to^*_{\beta\iota m}\; t_0[x/u]$. Puis on utilise le lemme de substitution précédent avec t_0, ce qui nous donne $t_0[x/u] \;\to^*_{\beta\iota m} \to^*_\circ\; t'[x/u']$. D'où le résultat. $\square$

Lemme 5.21 (substitution séquentielle) *Si on a*

- $\Gamma; \overrightarrow{x_i} : \overrightarrow{X_i} \vdash t : T$
- $\Gamma \vdash \overrightarrow{u_i} : (\overrightarrow{x_i} : \overrightarrow{X_i})$
- $t \;\to^*_{\beta\iota m} \to^*_\circ\; t'$
- $\forall i, u_i \;\to^*_\circ\; u'_i$

Alors $t[\overrightarrow{x_i}/\overrightarrow{u_i}] \;\to^*_{\beta\iota m} \to^*_\circ\; t'[\overrightarrow{x_i}/\overrightarrow{u'_i}]$.

$\Diamond$ On utilise de façon répétée le lemme précédent. $\square$

Lemme 5.22 (Raffinement 2 du lemme d'inversion de $\circ$) *Si* $([x : X]\; t)^T \;\to^*_\circ\; \circ$, *avec* $([x : X]\; t)^T$ *typé dans un contexte* Γ, *alors* $t \;\to^*_{\beta\iota m} \to^*_\circ\; \circ$.

$\Diamond$ Il suffit de réduire les marques de ce terme, puis d'utiliser le lemme 5.16. $\square$

Lemme 5.23 *Soit M un β-redex bien typé de CIC, et soit N son réduit. Supposons $M \;\to^*_\circ\; M'$. Il y a alors trois cas :*

(i) $M' = \circ$ *et alors* $N \;\to^*_{\beta\iota m} \to^*_\circ\; \circ$

(ii) M' *est une application* $(\circ\;\; b')^{T'}$ *et alors* $N \;\to^*_{\beta\iota m} \to^*_\circ\; \circ$

(iii) M' *est encore un redex, de réduit* N', *et alors* $N \;\to^*_{\beta\iota m} \to^*_\circ\; N'$

$\Diamond$ Cf. la démonstration du lemme 3.18 $\square$

5.6 Les théorèmes de remontée de β et ι

Les deux théorèmes qui va suivre répond à un des objectifs initiaux : étant donné une dérivation $\beta\iota$ dans CIC$\circ$, on va pouvoir la “remonter” en une dérivation correspondante dans CIC.

Théorème 5.24 *Soit M un terme typable de CIC. Si* $M \;\to^*_\circ\; M' \;\to_\beta\; N'$, *alors il existe* N *tel que* $M \;\to_\beta\; N \;\to^*_{\beta\iota m} \to^*_\circ\; N'$.

$$
\begin{tikzcd}
M \arrow[r, dashed, "\beta"] \arrow[dr, dashed, "+", "\beta_\iota"'] \arrow[dd, "\circ"', "*"] & N \arrow[d, dashed, "\beta\iota m"', "*"] \\
 & {} \arrow[d, dashed, "\circ"', "*"] \\
M' \arrow[r, "\beta"'] & N'
\end{tikzcd}
$$

$\Diamond$ Cf. la démonstration du théorème 3.19.

$\square$

Théorème 5.25 *Soit M un terme typable de CIC. Si $M \rightarrow_\circ^* M' \rightarrow_\iota N'$, alors il existe N tel que $M \rightarrow_\iota N \rightarrow_{\beta\iota m}^* \rightarrow_\circ^* N'$.*

$$
\begin{tikzcd}
M \arrow[r, dashed, "\iota"] \arrow[dr, dashed, "+", "\beta_\iota"'] \arrow[dd, "\circ"', "*"] & N \arrow[d, dashed, "\beta\iota m"', "*"] \\
 & {} \arrow[d, dashed, "\circ"', "*"] \\
M' \arrow[r, "\iota"'] & N'
\end{tikzcd}
$$

$\Diamond$ On s'inspire de la démonstration du théorème 3.19. Une fois écartés les cas résolus directement par hypothèse de récurrence, il reste les deux cas où M' est un ι-redex qui se réduit en N'.

- $M = (Cases\ (Constr_n(I)\ \overrightarrow{m_j})^{\overrightarrow{T_j}}\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^T$ et
  $M' = (Cases\ (Constr_n(I')\ \overrightarrow{m'_j})^{\overrightarrow{T'_j}}\ of\ \{\overrightarrow{\Gamma'_i}\}\{\overrightarrow{t'_i}\})^{T'}$ et
  $N' = t'_n[Var(\Gamma'_n)/\overrightarrow{m'_j}]$. On prend alors $N = t_n[Var(\Gamma_n)/\overrightarrow{m_j}]$ et le lemme 5.21 montre que $N \rightarrow_{\beta\iota m}^* \rightarrow_\circ^* N'$.
- $M = (Fix(f,\ t)^T\ \ c)^U$ et $M' = (Fix(f,\ t')^{T'}\ \ c')^{U'}$ et $N' = (t'[f/Fix(f,\ t')^{T'}]\ \ c')^{U'}$. On prend alors $N = (t[f/Fix(f,\ t)^T]\ \ c)^U$ et une utilisation du lemme de substitution 5.19 montre que $N \rightarrow_{\beta\iota m}^* \rightarrow_\circ^* N'$.

$\square$

Corollaire 5.26 *La réduction $\rightarrow_\circ^*$ conserve le caractère $\beta\iota$-normal : si M terme bien typé de CIC est $\beta\iota$-normal, alors tous ses réduits par $\rightarrow_\circ^*$ aussi.*

5.7 Les théorème de descente de β et ι

Il s'agit de la réciproque du théorème précédent. On part maintenant d'une dérivation dans CIC, et on souhaite la "descendre" dans CIC$\circ$.

Définition 5.27 *On dira que* $M \rightarrow_{\beta 2} N$ *ssi* $M = N$ *ou* $M \rightarrow_{\beta} N$ *ou* $M \rightarrow_{\circ} N$ *par la règle (2) de* $\rightarrow_{\circ}$ *.*

Cette règle (2) de la $\circ$-réduction $(\circ\ \ t)^T \rightarrow_{\circ} \circ$ correspond en effet à une β-réduction d'un redex dont la tête aurait disparu.

Théorème 5.28 *Soit* M *un terme bien typé de CIC. Si* $M \rightarrow_{\beta} N$ *et* $M \rightarrow_{\circ}^{*} M'$*, alors il existe* N' *tel que* $M' \rightarrow_{\beta 2} N'$ *et* $N \rightarrow_{\beta\iota m}^{*} \rightarrow_{\circ}^{*} N'$*.*

$$\begin{tikzcd}
M \arrow[r, "\beta"'] \arrow[dd, "\circ" ', "*"] & N \arrow[d, dashed, "\beta\iota m" ', "*"] \\
 & {} \arrow[d, dashed, "\circ" ', "*"] \\
M' \arrow[r, dashed, "\beta 2"'] & N'
\end{tikzcd}$$

$\Diamond$ Cf. la démonstration des théorèmes 3.22 et 3.23. $\square$

Théorème 5.29 *Soit* M *un terme bien typé de CIC. Si* $M \rightarrow_{\iota} N$ *et* $M \rightarrow_{\circ}^{*} \circ$*, alors* $N \rightarrow_{\beta\iota m}^{*} \rightarrow_{\circ}^{*} \circ$*.*

$\Diamond$ Les deux seuls cas qui ne se démontrent pas par une utilisation immédiate de l'hypothèse de récurrence sont les cas où M est un ι-redex.

- $M = (Cases\ (Constr_n(I)\ \ \overrightarrow{m_j})^{\overrightarrow{T_j}}\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^T$. Si $T \rightarrow_{\circ}^{*} \circ$ c'est une affaire de Subject Reduction. Si maintenant $(Constr_n(I)\ \ \overrightarrow{m_j})^{\overrightarrow{T_j}} \rightarrow_{\circ}^{*} \circ$, alors par le lemme fondamental 3.13, la forme $\beta\iota$-normale de ce terme se réduit aussi vers $\circ$. La proposition 5.13 montre qu'alors $sorte(I) = Prop$. Par la règle de typage (Cases), t_n est typable de type $(Q\ \ldots)^{seq(B)}$ et le dernier terme de la séquence $seq(B)$ est un s' valant également $Prop$. Par le théorème 5.18, on a $t_n \rightarrow_{\beta\iota m}^{*} \rightarrow_{\circ}^{*} \circ$ et donc $N = t_n[Var(\Gamma_n)/\overrightarrow{m_j}] \rightarrow_{\circ}^{*} \circ$ (lemme 5.21).
- $M = (Fix(f,\ t)^T\ \ c)^U$, avec $U \rightarrow_{\circ}^{*} \circ$ ou $T \rightarrow_{\circ}^{*} \circ$. On procède comme lors de la démonstration du lemme 3.13.

$\square$

Théorème 5.30 *Soit* M *un terme bien typé de CIC. Si* $M \rightarrow_{\iota} N$ *et* $M \rightarrow_{\circ}^{*} M'$*, alors il existe* N' *tel que* $M' \rightarrow_{\beta\iota\circ}^{*} N'$ *et* $N \rightarrow_{\beta\iota m}^{*} \rightarrow_{\circ}^{*} N'$*.*

$$\begin{tikzcd} M \arrow[r, "\iota"'] \arrow[dd, "\circ\,*"'] & N \arrow[d, dashed, "\beta\iota m\,*"] \\ & {} \arrow[d, dashed, "\circ\,*"] \\ M' \arrow[r, dashed, "*", "\beta\iota\circ"'] & N' \end{tikzcd}$$

$\Diamond$ Là encore on ne s'intéresse qu'aux ι-redex, les autres cas se traitant par hypothèse de récurrence. On suppose $M' \neq \circ$.

- $M = (Cases\ (Constr_n(I)\ \overrightarrow{m_j})^{\overrightarrow{T_j}}\ of\ \{\overrightarrow{\Gamma_i}\}\{\overrightarrow{t_i}\})^T$ et $N = t_n[Var(\Gamma_n)/\overrightarrow{m_j}]$. Deux sous-cas :
  - $M' = (Cases\ \circ\ of\ \{\overrightarrow{\Gamma'_i}\}\{\overrightarrow{t'_i}\})^{T'}$. Alors $M \ \to_\circ^* \ \circ$ donc le théorème précédent donne $N \ \to_{\beta\iota m}^* \to_\circ^* \ \circ$. Et on a bien $M' \ \to_{\beta\iota\circ}^* \circ$.
  - $M' = (Cases\ (Constr_n(I')\ \overrightarrow{m'_j})^{\overrightarrow{T'_j}}\ of\ \{\overrightarrow{\Gamma'_i}\}\{\overrightarrow{t'_i}\})^{T'}$.
    On prend alors $N' = t'_n[Var(\Gamma'_n)/\overrightarrow{m'_j}]$, et on utilise le lemme 5.21.
- $M = (Fix(f,\ t)^T\ \ c)^U$ et $N = (t[f/Fix(f,\ t)^T]\ \ c)^U$. Trois sous-cas :
  - $M' = (\circ\ \ c')^{U'}$. Alors on a $M \ \to_\circ^* \ \circ$ donc $N' \ \to_{\beta\iota m}^* \to_\circ^* \ \circ$ et $M' \ \to_{\beta\iota\circ}^* \circ$.
  - $M' = (Fix(f,\ t')^{T'}\ \ \circ)^{U'}$. Dans ce cas on ne peut pas ι-réduire M'... Mais en fait si l'argument inductif $c = (Constr_n(I)\ \ldots)^{\cdots}$ se réduit vers $\circ$, c'est encore une fois que $sorte(I) = Prop$. Et alors les conditions sur le type d'un point-fixe font que T est $\beta\iota$-équivalent à un terme se réduisant vers $\circ$. Donc $M' \ \to_{\beta\iota\circ}^* \circ$ et on a également $N \ \to_{\beta\iota m}^* \to_\circ^* \ \circ$ (Subject Reduction + théorème 5.18).
  - $M' = (Fix(f,\ t')^{T'}\ \ c')^{U'}$ avec c' commençant bien par un constructeur. Dans ce cas-là, il n'y a plus de problème, on prend $N' = (t'[f/Fix(f,\ t')^{T'}]\ \ c')^{U'}$, et une utilisation du lemme de substitution 5.19 montre que $N \ \to_{\beta\iota m}^* \to_\circ^* \ N'$.

$\square$

5.8 Accessibilité

Tous les résultats concernant l'accessibilité dans CC se traduisent dans CIC, avec des preuves quasi-identiques.

Définition 5.31 *On dira qu'un terme M de CIC$\circ$ est accessible ssi il existe M_0 de CIC, typable, et tel que $M_0 \ \to_\circ^* \ M$.*
On notera $\mathcal{A}$ le sous-ensemble de CIC$\circ$ formé des termes accessibles.

Proposition 5.32 *$\mathcal{A}$ est clos par $\to_\circ$.*

Proposition 5.33 *$\mathcal{A}$ est clos par sous-terme.*

Théorème 5.34 *$\mathcal{A}$ est clos par $\beta\iota$-réduction.*

Théorème 5.35 *Toute réduction $\rightarrow^*_{\beta\iota\circ}$ dans $\mathcal{A}$ termine.*

Corollaire 5.36 *Toute réduction $\rightarrow^*_{\beta\iota}$ dans $\mathcal{A}$ termine.*

Corollaire 5.37 *Pour tout terme M de $\mathcal{A}$, il y a existence et unicité d'une forme normale vis-à-vis de $\rightarrow_{\beta\iota}$. On la notera encore $M_{\beta\iota}$.*

Lemme 5.38 *Si M est un terme typé de CIC, et N un terme $\beta\iota\circ$-normal tel que $M \rightarrow^*_\circ N$, alors $M_{\beta\iota} \rightarrow^*_\circ N$.*

$$
\begin{tikzcd}
M \arrow[rr, "*", "\beta\iota"'] \arrow[dr, "*", "\circ"'] & & M_{\beta\iota} \arrow[dl, dashed, "\circ", "*"'] \\
& N &
\end{tikzcd}
$$

Théorème 5.39 *Tout terme M de $\mathcal{A}$ a une et une seule forme normale par $\rightarrow^*_{\beta\iota\circ}$, qui est $(M_{\beta\iota})_\circ$, la forme $\circ$-normale de la forme $\beta\iota$-normale de M.*

Corollaire 5.40 *$\rightarrow^*_{\beta\iota\circ}$ vérifie la Propriété de Church-Rosser.*

Corollaire 5.41 *Soit N un terme typé de CIC, avec $N \rightarrow^*_\circ M$. On a $(N_{\beta\iota})_\circ = (M_{\beta\iota})_\circ$.*

On a maintenant le diagramme suivant :

$$
\begin{tikzcd}
N \arrow[r, "*", "\beta\iota"'] \arrow[d, "\circ"', "*"] & {} \arrow[r, "*", "\beta\iota"'] \arrow[d, dashed, "\circ"', "*"] & N_{\beta\iota} \arrow[dd, dashed, "\circ"', "*"] \\
M \arrow[r, "*", "\beta\iota"'] & M_{\beta\iota} \arrow[dr, dashed, "*", "\circ"'] & \\
& & (M_{\beta\iota})_\circ = (N_{\beta\iota})_\circ
\end{tikzcd}
$$

Par rapport à CC, on ne peut plus mimer exactement la β-réduction initiale avec β plus la règle (2) de $\rightarrow_\circ$. On peut s'en approcher, par exemple avec $\beta\iota$ plus les règles (2) et (6) de $\rightarrow_\circ$. Mais la réduction du point-fixe peut exiger l'utilisation de toutes les règles de $\rightarrow_\circ$ (Cf. la preuve de 5.28).

5.9 Equivalence observationnelle

Heureusement, on n'a pas toujours besoin de $\circ$-réduire après l'exécution (i.e. la $\beta\iota$-réduction).

Lemme 5.42 *Si $M \to_\circ N$, alors N contient des symboles $\circ$.*

$\Diamond$ Il suffit de regarder le $\circ$-redex dans M qui va se contracter en un $\circ$ dans N. $\square$

Lemme 5.43 *Soit N un terme typé de CIC, avec $N \to_\circ^* M$. Si $N_{\beta\iota}$ ne contient plus de $\circ$ ni de $Prop$, alors $M_{\beta\iota} = N_{\beta\iota}$.*

$\Diamond$ On a alors $(N_{\beta\iota})_\circ = N_{\beta\iota}$. Et le lemme précédent montre que dans la réduction $M_{\beta\iota} \to_\circ^* (M_{\beta\iota})_\circ$, il ne peut y avoir de réduction $\to_\circ$. Les deux termes sont donc égaux, et finalement $M_{\beta\iota} = N_{\beta\iota}$ vu le corollaire 5.41. $\square$

Et cette situation arrive lorsqu'on considère des termes clos sur un type de base du genre de *bool*. Au passage les booléens sont définis par :

$$\begin{array}{lcl} bool & = & Ind(x)\{x, x\}^{Set} \\ true & = & Constr_1(bool) \\ false & = & Constr_2(bool) \end{array}$$

Ce qui nous amène à l'équivalence observationnelle.

Définition 5.44 *Un contexte à trou $C[-^A]$ est un terme de CIC n'ayant qu'une seule variable libre $-^A$, et cette variable libre n'a qu'une seule occurence.*

Définition 5.45 (équivalence observationnelle pour CIC) *On dit que deux termes clos t et u de CIC sont observationnellement équivalents par rapport à un type A ssi t et u sont typables de type A, et si pour tout contexte à trou $C[-^A]$ de type bool, on a $C[t] =_{\beta\iota} C[u]$.*

Adaptons cette définition aux termes de CIC$\circ$.

Définition 5.46 (équivalence observationnelle pour CIC$\circ$) *On dit que deux termes clos t et u de CIC$\circ$ sont observationnellement équivalents par rapport à un type A ssi il existe t_0 et u_0 termes de CIC de type A tels que $t_0 \to_\circ^* t$ et $u_0 \to_\circ^* u$, et si pour tout contexte à trou $C[-^A]$ de type bool, on a $C[t] =_{\beta\iota} C[u]$.*

On notera $t \approx_A u$. Et le résultat principal est alors qu'un terme M de CIC et le terme extrait M' associé sont observationnellement équivalents par rapport au type de M.

Théorème 5.47 *Soit M un terme clos de CIC de type A, et tel que $M \to_\circ^* M'$. Alors $M \approx_A M'$.*

$\Diamond$ La forme $\beta\iota$-normale du terme clos $C[M]$ est forcément $true$ ou $false$, et en tout cas ne contient plus de $\circ$ ni de $Prop$. Vu que $C[M] \to_\circ^* C[M']$, on obtient par le lemme précédent $(C[M])_{\beta\iota} = (C[M'])_{\beta\iota}$. $\square$

6 Conclusion

Nous avons donc proposé un mécanisme d'extraction des termes de CIC vers un système CIC$\circ$. Puis nous avons défini une notion d'exécution des termes de CIC$\circ$ basée sur la réduction $\beta\iota$ de CIC. Enfin nous avons prouvé que ces deux notions d'exécution, dans CC et dans CIC, sont compatibles.

L'étape suivante serait alors de proposer une implémentation de ce système CC$\circ$, qui fournisse réellement un programme ML à partir d'un terme de CIC. Ceci n'a malheureusement pu être fait faute de temps.

En vu de cette implémentation, un certain nombre de points théoriques restent encore à étudier, afin de rendre notre système CIC le plus proche possible de celui implémenté dans l'assistant Coq. Mais notre système s'est déjà révélé assez modulaire pour permettre le passage de CC à CIC. Il a suffit de rajouter les deux règles de la $\circ$-réduction propres aux types inductifs, et d'adapter les preuves. Les extensions évoquées ci-dessous devraient donc également pouvoir être intégrées à l'ensemble de façon modulaire.

– Il faudra à un moment ou à un autre prendre en compte les définitions mutuellement inductives, mais ceci ne semble pas poser de difficultés théoriques majeures.

– Il est aussi question de passer à une relation de conversion qui vérifierait $Prop \preceq Set$, et non pas $Prop$ incomparable avec Set comme actuellement.

– Autre aspect de Coq non encore intégré, les types inductifs singletons violent le principe $sorte(Cases\ \ldots) \leq sorte(I)$. Il faut donc leur réserver un traitement particulier.

– Enfin nos exigences sur le type des points-fixes sont plus strites que celles de Coq. En effet dans Coq il est légal d'utiliser un inductif sur $Prop$ dans un $Fixpoint$ afin d'obtenir un résultat dans Set par exemple. De tous les points évoqués ici, c'est sans doute le plus délicat, vu qu'autoriser de tels point-fixes dans CIC$\circ$ entrainera la perte de la forte normalisation. Il faudra alors étudier de près les stratégies possibles d'évaluation.

Une autre extension possible serait d'étudier cette procédure d'extraction du point de vue réalisabilité. En effet la procédure d'extraction actuelle est batie sur un principe théorique de réalisibilité (cf. [11]). Cette vision a quelque peu cédé le pas à un vision plus procédurale lors de ce stage. Il serait sans doute intéressant de voir quelle réalisabilité correspond à cette nouvelle extraction.

Références

[1] B. Barras, S. Boutin, C. Cornes, J. Courant, Y. Coscoy, D. Delahaye, D. de Rauglaudre, J.C. Filliâtre, E. Giménez, H. Herbelin, G. Huet, H. Laulhère, P. Loiseleur, C. Muñoz, C. Murthy, C. Parent, C. Paulin, A. Saïbi, and B. Werner. *The Coq Proof Assistant Reference Manual – Version V6.3*, July 1999.

[2] S. Berardi. Pruning simply typed λ-calculi. *Journal of Logic and Computation*, 1996.

[3] L. Boerio. Extending pruning techniques to polymorphic second order λ-calculus. In D. Sannella, editor, *Proceedings ESOP'94*, volume 788, 1994.

[4] G. Dowek, G. Huet, and B. Werner. On the definition of the eta-long normal form in the type systems of the cube. Informal Proceedings of the Workshop "Types", Nijmegen, 1993.

[5] E. Giménez. A tutorial on recursive types in coq. Technical report, INRIA, 1998. à paraitre.

[6] W.A. Howard. The formulae-as-types notion of constructions. In J.P. Seldin and J.R. Hindley, editors, *to H.B. Curry : Essays on Combinatory Logic, Lambda Calculus and Formalism.* Academic Press, 1980. Unpublished 1969 Manuscript.

[7] G. Huet, G. Kahn, and Ch. Paulin-Mohring. *The* Coq *Proof Assistant - A tutorial - Version 6.3*, July 1999.

[8] Z. Luo. *Computation and Reasoning ; a type theory for Computer Science*, volume 11 of *International Series of Monographs in Computer Science.* Oxford Science Publication, 1994.

[9] C. Paulin-Mohring. Extracting F_ω's programs from proofs in the Calculus of Constructions. In *Sixteenth Annual ACM Symposium on Principles of Programming Languages*, Austin, January 1989. ACM.

[10] C. Paulin-Mohring. *Extraction de programmes dans le Calcul des Constructions.* Thèse d'université, Paris 7, January 1989.

[11] C. Paulin-Mohring. Réalisabilité et extraction de programmes. In B. Courcelle, editor, *Logique et Informatique : une introduction*, volume 8 of *Collection Didactique*, pages 163–180. INRIA, 1991.

[12] C. Paulin-Mohring. *Définitions Inductives en Théorie des Types d'Ordre Supérieur.* Habilitation à diriger les recherches, Université Claude Bernard Lyon I, December 1996.

[13] F. Prost. *Interprétation de l'analyse statique en théorie des types.* Thèse d'université, École Normale Supérieure de Lyon, december 1999.

[14] F. Prost. A static calculus of dependencies for the λ-cube. In *Proc. of IEEE 15th Ann. Symp. on Logic in Computer Science (LICS'2000).* IEEE Computer Society Press, 2000. To appear.

[15] Benjamin Werner. *Méta-théorie du Calcul des Constructions Inductives.* Thèse de doctorat, Univ. Paris VII, 1994.