Intuitionistic Model Constructions and Normalization Proofs

Thierry COQUAND et Peter DYBJER
Présenté par Chantal KELLER

Université Paris VII - MPRI

19 janvier 2009

Première partie I

Introduction

Présentation

Étant données `red` une règle de réduction, `conv` sa clôture reflexive, transitive et symétrique. Pour prouver que `red` est fortement normalisante, deux possibilités :

- prouver des propriétés de `red` (Church-Rosser...) ;
- fournir une **fonction de normalisation** : un algorithme qui choisit un représentant irréductible pour chaque classe d'équivalence de `conv`.

Originalité : manière **sémantique** d'obtenir cet algorithme.

Propriétés fondamentales

Theorem

Si a conv a', *alors* $\mathbf{nf}\ a = \mathbf{nf}\ a'$.

Theorem

a conv $\mathbf{nf}\ a$

Theorem

a conv a' *si et seulement si* $\mathbf{nf}\ a = \mathbf{nf}\ a'$.

Démonstration.

$\boxed{\Rightarrow}$: Théorème ci-dessus.

$\boxed{\Leftarrow}$: Si $\mathbf{nf}\ a = \mathbf{nf}\ a'$. Alors a conv $\mathbf{nf}\ a$ conv $\mathbf{nf}\ a'$ conv a'. □

Deuxième partie II

Système T de Gödel

Types

$$\mathtt{Type} : \mathit{Set}$$

$$\frac{}{\mathtt{N} \in \mathtt{Type}} \qquad \frac{A, B \in \mathtt{Type}}{A \Rightarrow B \in \mathtt{Type}}$$

Termes typés

$$\mathtt{T}(A) : \mathit{Set} \text{ pour } A \in \mathtt{Type}$$

$$\forall A, B, C \in \mathtt{Type} :$$

$$\frac{}{\mathtt{K} \in \mathtt{T}(A \Rightarrow B \Rightarrow A)} \qquad \frac{c \in \mathtt{T}(A \Rightarrow B) \qquad a \in \mathtt{T}(A)}{\mathtt{app}(a, c) \in \mathtt{T}(B)}$$

$$\frac{}{\mathtt{S} \in \mathtt{T}((A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C)} \qquad \frac{}{\mathtt{0} \in \mathtt{T}(\mathtt{N})}$$

$$\frac{a \in \mathtt{T}(\mathtt{N})}{\mathtt{s}(a) \in \mathtt{T}(\mathtt{N})} \qquad \frac{d \in \mathtt{T}(C) \qquad e \in \mathtt{T}(\mathtt{N} \Rightarrow C \Rightarrow C)}{\mathtt{rec}(d, e) \in \mathtt{T}(\mathtt{N} \Rightarrow C)}$$

Conversion

$$a \ \mathtt{conv}_A \ a' : \mathit{Set} \text{ si } a, a' \in \mathtt{T}(A)$$

- On notera simplement $\mathtt{conv}$
- Relation réflexive, symétrique et transitive
- Règles de congruence avec les constructeurs de termes :

$$\frac{a \ \mathtt{conv} \ a'}{\mathtt{s}(a) \ \mathtt{conv} \ \mathtt{s}(a')}$$

- Autres règles :

$$\begin{array}{rcl}
\mathtt{app}(\mathtt{app}(\mathtt{K}, a), b) & \mathtt{conv} & a \\
\mathtt{app}(\mathtt{app}(\mathtt{app}(\mathtt{S}, g), f), a) & \mathtt{conv} & \mathtt{app}(\mathtt{app}(g, a), \mathtt{app}(f, a)) \\
\mathtt{app}(\mathtt{rec}(d, e), 0) & \mathtt{conv} & d \\
\mathtt{app}(\mathtt{rec}(d, e), \mathtt{s}(a)) & \mathtt{conv} & \mathtt{app}(\mathtt{app}(e, a), \mathtt{app}(\mathtt{rec}(d, e), a))
\end{array}$$

Modèle standard

Interprétation des types :

$$\begin{aligned} [\![\mathtt{N}]\!] &= \mathbb{N} \\ [\![A \Rightarrow B]\!] &= [\![A]\!] \to [\![B]\!] \end{aligned}$$

Interprétation des termes : si $a \in \mathtt{T}(A)$, alors $[\![a]\!] \in [\![A]\!]$

$$\begin{aligned} [\![\mathtt{K}]\!] &= \lambda xy.x \\ [\![\mathtt{S}]\!] &= \lambda gfx.g\ x\ (f\ x) \\ [\![\mathtt{app}(c,a)]\!] &= [\![c]\!]\ [\![a]\!] \\ [\![\mathtt{0}]\!] &= 0 \\ [\![\mathtt{s}(a)]\!] &= s\ [\![a]\!] \\ [\![\mathtt{rec}(d,e)]\!] &= rec\ [\![d]\!]\ [\![e]\!] \end{aligned}$$

Propriété

Theorem

Si a $\mathtt{conv}$ a', *alors* $[\![a]\!] = [\![a']\!]$.

Démonstration.

Par induction sur la preuve de a $\mathtt{conv}$ a'. □

Mais on n'a pas la possibilité d'inverser la fonction d'interprétation $[\![\bullet]\!] \in \mathtt{T}(A) \longrightarrow [\![A]\!]$.

Interprétation des types

Interprétation des types :

$$\begin{aligned} [\![\mathbb{N}]\!] &= \mathbb{N} \\ [\![A \Rightarrow B]\!] &= \mathtt{T}(A \Rightarrow B) \times ([\![A]\!] \to [\![B]\!]) \end{aligned}$$

Inverse de la fonction d'interprétation : $\mathbf{quote}_A \in [\![A]\!] \to \mathtt{T}(A)$

$$\begin{aligned} \mathbf{quote}_{A \Rightarrow B}\ \langle c, f \rangle &= c \\ \mathbf{quote}_{\mathbb{N}}\ 0 &= 0 \\ \mathbf{quote}_{\mathbb{N}}\ (s\ p) &= \mathtt{s}(\mathbf{quote}_{\mathbb{N}}\ p) \end{aligned}$$

Interprétation des termes

Interprétation des termes : si $a \in \mathtt{T}(A)$, alors $[\![a]\!] \in [\![A]\!]$

$$
\begin{array}{rcl}
[\![\mathtt{K}]\!] & = & \langle \mathtt{K}, \lambda p.\langle \mathtt{app}(\mathtt{K}, \mathbf{quote}\ p), \lambda q.p\rangle\rangle \\
[\![\mathtt{S}]\!] & = & \langle \mathtt{S}, \lambda p.\langle \mathtt{app}(\mathtt{S}, \mathbf{quote}\ p), \lambda q.\langle \mathtt{app}(\mathtt{app}(\mathtt{S}, \mathbf{quote} p), \\
 & & \mathbf{quote}\ q), \lambda r.app_M\ (app_M\ p\ r)\ (app_M\ q\ r)\rangle\rangle\rangle \\
[\![\mathtt{app}(c,a)]\!] & = & app_M\ [\![c]\!]\ [\![a]\!] \\
[\![\mathtt{0}]\!] & = & 0 \\
[\![\mathtt{s}(a)]\!] & = & s\ [\![a]\!] \\
[\![\mathtt{rec}(d,e)]\!] & = & \langle \mathtt{rec}(\mathbf{quote}\ [\![d]\!], \mathbf{quote}\ [\![e]\!]), \\
 & & rec\ [\![d]\!]\ (\lambda xy.app_M\ (app_M\ [\![e]\!]\ x)\ y)\rangle
\end{array}
$$

où l'application est ainsi définie :

$$app_M\ \langle c, f\rangle\ q = f\ q$$

Fonction de normalisation et propriété

Fonction de normalisation :

$$\mathbf{nf}\ a = \mathbf{quote}\ [\![a]\!]$$

Theorem

Si a conv a', *alors* $[\![a]\!] = [\![a']\!]$.

Démonstration.

Par induction sur la preuve de a conv a'. □

Theorem

Si a conv a', *alors* $\mathbf{nf}\ a = \mathbf{nf}\ a'$.

La forme normale d'un terme est équivalent à ce terme

Theorem

a conv ***nf*** a

Essayons de faire la preuve par induction sur a.
Dans le cas où $a = \mathrm{app}(a1, a2)$, on doit prouver que $\mathrm{app}(a1, a2)$ conv **nf** $\mathrm{app}(a1, a2)$, sachant que $a1$ conv **nf** $a1$ et $a2$ conv **nf** $a2$.

Rappel : **nf** $a =$ **quote** $[\![a]\!]$

Comment faire ?

$\hookrightarrow$ Prouver que cette propriété est vraie. Mais pour cela, il faut prouver une propriété plus forte.
$Gl_A\ p$ pour $p \in [\![A]\!]$ est la propriété ainsi définie (par induction sur A) :

- $Gl_{\mathbb{N}}\ n$ pour tout $n \in \mathbb{N}$
- $Gl_{A \Rightarrow B}\ q$ si et seulement si pour tout p tel que $Gl_A\ p$, alors :
  1. $Gl_B\ (app_M\ q\ p)$
  2. $\mathtt{app}(\mathbf{quote}\ q, \mathbf{quote}\ p)\ \mathtt{conv}\ \mathbf{quote}\ (app_M\ q\ p)$

Propriétés (1/2)

Theorem

Pour tout $a \in \mathtt{T}(A)$, $Gl_A\ [\![a]\!]$.

Démonstration.

Par induction sur a. □

Propriétés (2/2)

Theorem

a conv $\boldsymbol{nf}\ a$

Démonstration.

Par induction sur a :

- le cas de l'application est maintenant géré en utilisant le fait que $Gl_A\ [\![a]\!]$;
- les autres cas sont triviaux.

□

On en déduit un algorithme de décision pour conv.

Troisième partie III

Interprétation catégorique

Algèbre combinatoire typée stricte

C'est la donnée de :

$$
\begin{array}{rcl}
[M & : & (A : \mathtt{Type})Set; \\
K_M & : & (A, B : \mathtt{Type})M(A \Rightarrow B \Rightarrow A); \\
S_M & : & (A, V, C : \mathtt{Type})M((A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C); \\
app_M & : & (A, B : \mathtt{Type}; M(A \Rightarrow B); M(A))M(B); \\
K_M axiom & : & (A, B : \mathtt{Type}; a : M(A); b : M(B)) \\
 & & I(app_M(app_M(K_M, a), b), a); \\
S_M axiom & : & (A, B, C : \mathtt{Type}; g : M(A \Rightarrow B \Rightarrow C); f : M(A \Rightarrow B); \\
 & & a : M(A))I(app_M(app_M(app_M(S_M, g), f), a), \\
 & & app_M(app_M(g, a), app_M(f, a)))]
\end{array}
$$

I est l'identité propositionnelle (un seul constructeur : ref).

Exemple du modèle standard

C'est une algèbre combinatoire typée (stricte) :

$$\begin{aligned}
\{M &:= \mathtt{T};\\
K_M &:= \lambda xy.x;\\
S_M &:= \lambda gfx.g\ x\ (f\ x);\\
app_M &:= app_M;\\
K_M axiom &:= ref;\\
S_M axiom &:= ref\}
\end{aligned}$$

avec des opérations permettant d'interpréter `0`, `s` et `rec`, en respectant les axiomes pour `rec`.

Modèles du système T (1/2)

Definition

Un modèle du système T est une algèbre combinatoire typée avec des opérations permettant d'interpréter 0, `s` et `rec`, en respectant les axiomes pour `rec`.

Nous avons deux modèles :

- $\mathtt{T}(A)$ avec `conv` comme relation d'équivalence (modèle initial) ;
- le modèle non standard $([\![A \Rightarrow B]\!] = \mathtt{T}(A \Rightarrow B) \times ([\![A]\!] \to [\![B]\!]))$.

Modèles du système T (2/2)

$[\![\bullet]\!]_A : \mathtt{T}(A) \to [\![A]\!]$ est un homomorphisme de modèles.

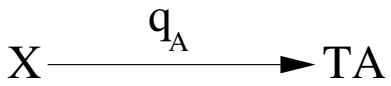
Mais $\mathbf{quote}_A : [\![A]\!] \to \mathtt{T}(A)$ n'est pas un homomorphisme de modèles car **quote** ne préserve pas l'application.
En définissant Gl_A, on construit un sous-modèle du modèle non standard. La restriction de **quote** à ce sous-modèle est un homomorphisme.

Donc $\mathbf{nf}_A : \mathtt{T}(A) \to \mathtt{T}(A)$ est un homomorphisme, donc l'identité, donc a conv **nf** a.

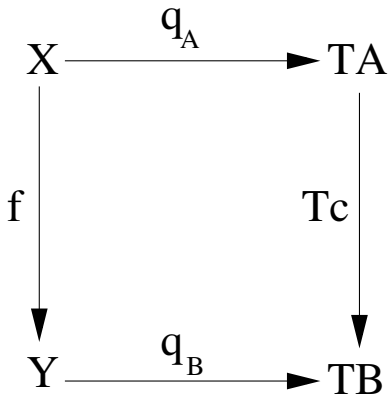
Glueing (cas de la catégorie des ensembles)

Étant donné un foncteur $T : \mathcal{C} \longrightarrow Set$, on construit la catégorie $\hat{\mathcal{C}}$ ainsi :

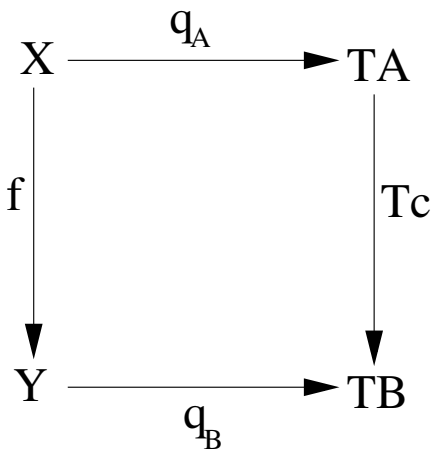
- objets : fonctions de Set :

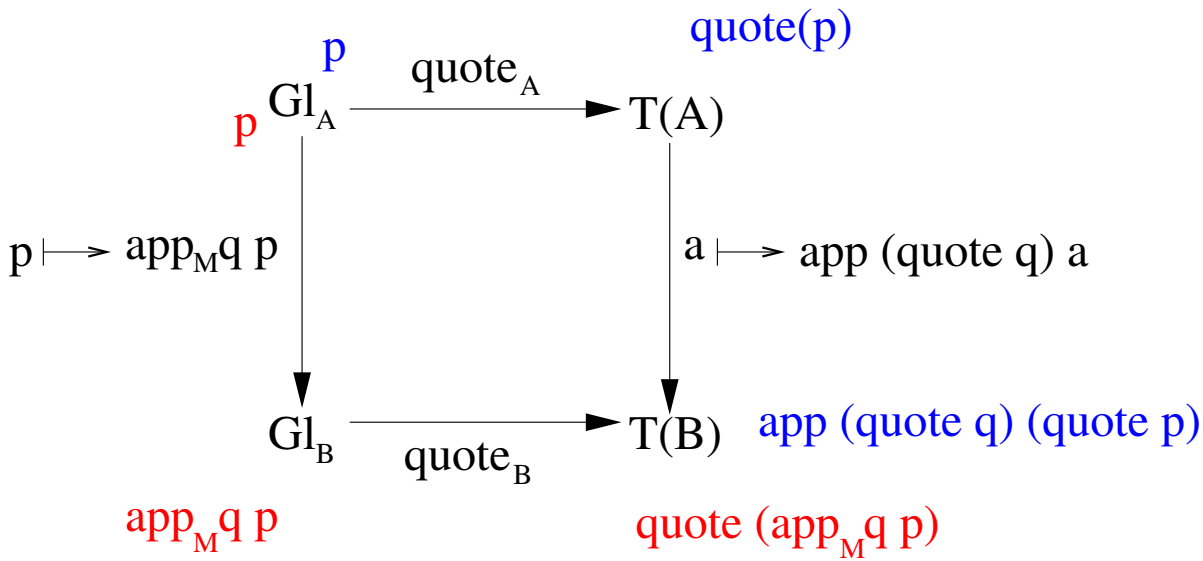


- morphismes : paires de morphismes $\langle c, f \rangle$ (c un morphisme de $\mathcal{C}$, f une fonction) tel que le diagramme suivant commute (dans Set) :



Dans notre cas





Quatrième partie IV

Extensions

Types

On ajoute aux types :

$$\frac{}{\bot \in \mathtt{Type}} \qquad \frac{}{\top \in \mathtt{Type}} \qquad \frac{A, B \in \mathtt{Type}}{A \wedge B \in \mathtt{Type}} \qquad \frac{A, B \in \mathtt{Type}}{A \vee B \in \mathtt{Type}}$$

Termes

On ajoute aux termes, pour tout $A, B, C \in \mathtt{Type}$:

$$\frac{}{\mathtt{case0}(C) \in \mathtt{T}(\bot \Rightarrow C)} \qquad \frac{}{<> \in \mathtt{T}(\top)} \qquad \frac{a \in \mathtt{T}(A)}{\mathtt{inl}(a) \in \mathtt{T}(A \vee B)}$$

$$\frac{b \in \mathtt{T}(B)}{\mathtt{inr}(b) \in \mathtt{T}(A \vee B)} \qquad \frac{d \in \mathtt{T}(A \Rightarrow C) \qquad e \in \mathtt{T}(B \Rightarrow C)}{\mathtt{case}(d, e) \in \mathtt{T}(A \vee B \Rightarrow C)}$$

$$\frac{a \in \mathtt{T}(A) \qquad b \in \mathtt{T}(B)}{<a, b> \in \mathtt{T}(A \wedge B)} \qquad \frac{c \in \mathtt{T}(A \wedge B)}{\mathtt{fst}(c) \in \mathtt{T}(A)} \qquad \frac{c \in \mathtt{T}(A \wedge B)}{\mathtt{snd}(c) \in \mathtt{T}(B)}$$

Conversion

On ajoute aux règles de conversion :

- les congruences avec les nouveaux constructeurs de termes ;
- les règles suivantes :

$$\begin{aligned} \mathtt{app}(\mathtt{case}(d,e),\mathtt{inl}(a)) &\ \mathtt{conv}\ d\,a \\ \mathtt{app}(\mathtt{case}(d,e),\mathtt{inr}(b)) &\ \mathtt{conv}\ e\,b \\ \mathtt{fst}(<a,b>) &\ \mathtt{conv}\ a \\ \mathtt{snd}(<a,b>) &\ \mathtt{conv}\ b \end{aligned}$$

Normalisation

$\hookrightarrow$ Comme précédemment.

Types et termes

On ajoute aux types :

$$\frac{}{\mathtt{Ord} \in \mathtt{Type}}$$

On ajoute aux termes, pour tout $C \in \mathtt{Type}$:

$$\frac{}{0 \in \mathtt{T}(\mathtt{Ord})} \qquad \frac{b \in \mathtt{T}(\mathtt{N} \Rightarrow \mathtt{Ord})}{\mathtt{sup}(b) \in \mathtt{T}(\mathtt{Ord})}$$

$$\frac{d \in \mathtt{T}(C) \qquad e \in \mathtt{T}((\mathtt{N} \Rightarrow \mathtt{Ord}) \Rightarrow (\mathtt{N} \Rightarrow C) \Rightarrow C)}{\mathtt{ordrec}(d, e) \in \mathtt{T}(\mathtt{Ord} \Rightarrow C)}$$

Conversion

On ajoute aux règles de conversion :

- les congruences avec les nouveaux constructeurs de termes ;
- les règles suivantes :

$$\begin{array}{rcl} \mathtt{app}(\mathtt{ordrec}(d,e),0) & \mathtt{conv} & d \\ \mathtt{app}(\mathtt{ordrec}(d,e),\mathtt{sup}(b)) & \mathtt{conv} & \mathtt{app}(\mathtt{app}(e,b),\mathtt{ordrec}(d,e)\circ b) \end{array}$$

Normalisation

- Introduire un nouveau modèle des ordinaux de Brouwer $\mathcal{O}_M$.
- $[\![\mathtt{Ord}]\!] = \mathcal{O}_M$
- Étendre la définition de Gl pour $\mathcal{O}_M$ de sorte que :

$$\mathrm{app}(c, \mathbf{quote}\ p)\ \mathtt{conv}\ \mathbf{quote}\ (f\ p)$$

Cinquième partie V

Conclusion

Conclusion

But double :

- algorithme de décision pour la conversion ;
- preuve de la forte normalisation de la réduction.

Un système et plusieurs extensions :

- système T de Gödel ;
- calcul propositionnel ;
- ordinaux de Brouwer ;
- ...

Autres propriétés

- Consistance des différents systèmes
- Constructeurs : si $C(x_1, \ldots, x_n) = C(y_1, \ldots, y_n)$ alors $x_i = y_i$ pour $i \in [\![1, n]\!]$
- Normalisation faible

Implantation

- Un normaliseur en SML (article)
- Les définitions et les théorèmes en Coq :

`http://perso.ens-lyon.fr/chantal.keller/etudes.html`

Merci !

Des questions ?