Théorie des Types
III) L'isomorphisme de Curry-Howard

Joëlle Despeyroux

INRIA Sophia-Antipolis

Module
"Méthodes formelles et fiabilité du logiciel"
Dea d'informatique, Nice, automne 2000

Curry-Howard dans le λ-calcul simple

Logique propositionelle:

$$\Rightarrow_i: \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad \Rightarrow_e: \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

$$\wedge_i: \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \wedge_{e1}: \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \wedge_{e2}: \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\vee_{i1} \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \vee_{i2} \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \qquad \vee_e \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$$

λ-calcul simplement typé:

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x : A.\, t : A \to B} \qquad \frac{\Gamma \vdash t : A \to B \quad \Gamma \vdash a : A}{\Gamma \vdash (t\ a) : B}$$

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B}{\Gamma \vdash (a, b) : (A \times B)} \qquad \frac{\Gamma \vdash t : (A \times B)}{\Gamma \vdash \mathrm{fst}\ t : A} \qquad \frac{\Gamma \vdash t : (A \times B)}{\Gamma \vdash \mathrm{snd}\ t : B}$$

$$\frac{\Gamma \vdash a : A}{\Gamma \vdash \mathrm{inl}\ a : (A + B)} \qquad \frac{\Gamma \vdash b : B}{\Gamma \vdash \mathrm{inr}\ b : (A + B)}$$

$$\frac{\Gamma \vdash t : A + B \qquad \Gamma, a : A \vdash t_1 : C \qquad \Gamma, b : B \vdash t_2 : C}{\Gamma \vdash \mathsf{case}\ t\ \mathsf{of}\ \mathrm{inl}\ a \Rightarrow t_1 \mid \mathrm{inr}\ b \Rightarrow t_2 : C}$$

Règles de réduction:

correspondent aux éliminations des coupures dans la logique

$$\begin{array}{c} (\lambda x : A.M \quad N) \hookrightarrow_\beta M[N/x] \\ \mathrm{fst}(M, N) \hookrightarrow M \qquad \mathrm{snd}(M, N) \hookrightarrow N \\ \mathrm{case}\ \mathrm{inl}\ t\ \mathrm{of}\ \mathrm{inl}\ a \Rightarrow t_1 \mid \mathrm{inr}\ b \Rightarrow t_2 \hookrightarrow t_1[t/a] \\ \mathrm{case}\ \mathrm{inr}\ t\ \mathrm{of}\ \mathrm{inl}\ a \Rightarrow t_1 \mid \mathrm{inr}\ b \Rightarrow t_2 \hookrightarrow t_2[t/b] \\ (\mathrm{fst}(M), \mathrm{snd}(M)) \hookrightarrow_\eta M \end{array}$$

Les Systèmes de Types Purs (PTS)

termes $M \ ::= x \mid c \mid \lambda x : M.M' \mid (M \ M') \mid \Pi x : M.M'$

Un PTS est défini par la donnée d'un triplet $(\mathcal{S}, \mathcal{A}, \mathcal{R})$ où $\mathcal{S} \subset \mathcal{C}$, $\mathcal{A}$ est un ens d'axiomes $(c : s)$ où $c \in \mathcal{C}$ et $s \in \mathcal{S}$, et $\mathcal{R}$ est un ens de triplets (s_1, s_2, s_3) avec $s_i \in \mathcal{S}$.

$$ax \ \vdash c : s \quad (c : s) \in \mathcal{A}$$

$$var \ \frac{\Gamma \vdash A : s}{\Gamma, x : A \vdash x : A} \ x \notin \Gamma$$

$$aff \ \frac{\Gamma \vdash A : B \qquad \Gamma \vdash C : s}{\Gamma, x : C \vdash A : B} \ x \notin \Gamma$$

$$lam \ \frac{\Gamma, x : A \vdash M : B \qquad \Gamma \vdash (\Pi x : A.B) : s}{\Gamma \vdash \lambda x : A.M \ : \ \Pi x : A.B}$$

$$app \ \frac{\Gamma \vdash M : \Pi x : A.B \qquad \Gamma \vdash N : A}{\Gamma \vdash (M \ N) : B[N/x]}$$

$$prod \ \frac{\Gamma \vdash A \ : \ s_1 \qquad \Gamma \vdash B \ : \ s_2}{\Gamma \vdash \Pi x : A.B \ : \ s_3} \ (s_1, s_2, s_3) \in \mathcal{R}$$

$$conv \ \frac{\Gamma \vdash A \ : \ B \qquad \Gamma \vdash B' \ : \ s \qquad B =_\beta B'}{\Gamma \vdash A \ : \ B'}$$

Le λ-cube est un sous-ens des PTS, où $(s_1, s_2) = (s_1, s_2, s_2)$.

Isomorphisme de Curry-Howard étendu

Logique propositionelle:

$$\Rightarrow_i: \ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad \Rightarrow_e: \ \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x : A.\ t : A \to B} \qquad \frac{\Gamma \vdash t : A \to B \quad \Gamma \vdash a : A}{\Gamma \vdash (t \ a) : B}$$

Calcul des prédicats ($\Rightarrow$ **et** $\forall$)**:**

$$\forall_I : \ \frac{\Gamma \vdash B}{\Gamma \vdash \forall x.\ B} \ (x \notin \Gamma) \qquad \forall_E : \ \frac{\Gamma \vdash \forall x.\ B}{\Gamma \vdash B[t/x]}$$

$\Rightarrow$ et $\forall$ sont représentés par le même opérateur Π, où on étend le type de la variable x à tout type A:

$$\frac{\Gamma, x : A \vdash M : B \qquad \Gamma \vdash (\Pi x : A.B) : s}{\Gamma \vdash \lambda x : A.M \ : \ \Pi x : A.B} \qquad \frac{\Gamma \vdash M : \Pi x : A.B \qquad \Gamma \vdash N : A}{\Gamma \vdash (M \ N) : B[N/x]}$$

Règle de réduction:

$$(\lambda x : A.M \ \ N) \hookrightarrow_\beta M[N/x]$$

Curry-Howard étendu (suite)

Logique propositionelle:

$$\wedge_i : \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \wedge_{e1} : \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \wedge_{e2} : \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\vee_{i1} \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \vee_{i2} \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \qquad \vee_e \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$$

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B}{\Gamma \vdash (a, b) : (A \times B)} \qquad \frac{\Gamma \vdash t : (A \times B)}{\Gamma \vdash \text{fst } t : A} \qquad \frac{\Gamma \vdash t : (A \times B)}{\Gamma \vdash \text{snd } t : B}$$

$$\frac{\Gamma \vdash a : A}{\Gamma \vdash \text{inl } a : (A + B)} \qquad \frac{\Gamma \vdash b : B}{\Gamma \vdash \text{inr } b : (A + B)}$$

$$\frac{\Gamma \vdash t : A + B \qquad \Gamma, a : A \vdash t_1 : C \qquad \Gamma, b : B \vdash t_2 : C}{\Gamma \vdash \text{case } t \text{ of inl } a \Rightarrow t_1 \mid \text{inr } b \Rightarrow t_2 : C}$$

Calcul des prédicats ($\wedge$, $\vee$ **et** $\exists$)**:**

$$\exists_I : \frac{\Gamma \vdash B[a/x]}{\Gamma \vdash \exists x.\ B} \qquad \exists_E : \frac{\Gamma \vdash \exists x.\ B \qquad \Gamma, B[a/x] \vdash C}{\Gamma \vdash C} (x \notin \Gamma, C)$$

$\wedge$ et $\exists$ sont représentés par le même opérateur Σ:

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B[a/x]}{\Gamma \vdash (a, b) : \Sigma x : A.B} \qquad \frac{\Gamma \vdash t : \Sigma x : A.B \qquad \Gamma, u : B[a/x] \vdash t'[a/x] : C}{\Gamma \vdash \text{case } t \text{ of } (x, u) \Rightarrow t' : C}$$

Note: fst et snd ne sont pas des cas particuliers du case.
Σ n'existe pas dans certaines théories typées.

Règle de réduction:

$\text{case } (a, b) \text{ of } (x, u) \Rightarrow t' \hookrightarrow t'[a/x][b/u]$

Curry-Howard sur les données

formule de $L \rightarrow$ un type d'un λ-calcul (spécification),
preuve (dérivation) dans $L \rightarrow$ un terme de ce λ-calcul.

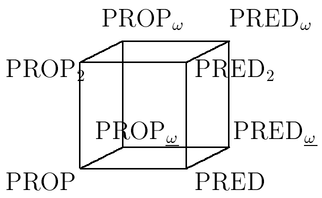
Exemples.

- $(even\ 0)$ est un type, ou spécification: "0 est pair."
- $even_S$ est un terme de type $\forall n : nat.(even\ n) \rightarrow (even\ (S\ (S\ n)))$, permettant de construire des preuves
- $\lambda n : nat.\lambda p : (even\ n) \rightarrow (even\ (S(S\ n)))$ est une fonction qui prend un entier n et une preuve p du fait que $(even\ n)$ et rend une preuve de $(even\ (S(S\ n)))$, donnée par le terme: $(even_S\ n\ p)$, et correspondant à la dérivation:

$$\frac{\stackrel{p}{(even\ n)}}{(even\ (S(S\ n)))}\ even_S$$

Isomorphisme de Curry-Howard - Le cube logique

PROP: logique propositionnelle / PRED: logique des prédicats.



Le cube logique est isomorphe au λ-cube:
T: formule de $L_i \rightarrow$ un type de λ_i.

Thm *(Iso. de Curry-Howard)* Le terme t de λ_i représente une preuve de la formule f de L_i ssi t est de type $T(f)$ dans λ_i.

Exemple. F, langage fonctionnel typé polymorphe $(\square, *)$, correspond à PROP$_2$, logique propositionelle étendue par une quantification sur les var. de proposition $(\forall A, B : (A \wedge B) \Rightarrow A)$.

Bibliographie

References

[Bar91] Henk Barendregt. Lambda calculi with types. In Samson Abramsky, D. M. Gabbai, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 2. Oxford University Press, 1991.

[GLT89] Jean-Yves Girard, Yves Lafont, and Paul Taylor. *Proofs and Types*. Cambridge University Press, 1989.

[Pfe92] Frank Pfenning. Computation and deduction. Unpublished lecture notes, 277 pp. Revised May 1994, April 1996, May 1992.