ISOMORPHISME DE CURRY HOWARD

Patrick Bellot

Télécom Paris
Institut Polytechnique de Paris
bellot@telecom-paris.fr

MITRO 202

Citons :

TO H.B. CURRY : ESSAYS ON COMBINATORY LOGIC
J.R. Hindley & J.P. Seldin ed.
Academic Press, 1980

et

PROOFS AND TYPES
J.Y. Girard & Y. Lafont & P. Taylor
Cambridge Tracts in T.C.S., Cambridge, Angleterre, 1989

Introduction

Le résultat décrit dans cette section porte le nom d'isomorphisme mais ce n'est pas véritablement un isomorphisme car un isomorphisme suppose des structures de part et d'autre.

L'isomorphisme de Curry-Howard est une identité de fonctionnement entre la Logique Combinatoire typée de Curry et la logique intuitionniste.

L'isomorphisme de Curry-Howard concerne la logique intuitionniste en déduction naturelle.

Introduction

Il se traduit par des identifications :

- une *preuve* est identifiée à un *terme fortement normalisable* de la Logique Combinatoire typée ;
- une *formule* est identifiée à un *type* ;
- si une formule est un théorème, le terme associé à sa preuve est typable et son type est la formule ;
- le processus d'élimination des coupures procède par transformation de preuves, ces transformations de preuves se traduisent par des réductions sur les termes associées aux preuves ;
- et une preuve sans coupures correspond à un terme en forme normale.

Introduction

L'isomorphisme de Curry-Howard concerne la logique intuitionniste en déduction naturelle et non en calcul de séquents.

Et nous venons de parler de coupures...

Examinons tout d'abord comment une démonstration en calcul des séquents se traduit en déduction naturelle.

Puis voyons ce que l'application d'une règle de coupure devient lors de cette traduction.

Nous décrirons ensuite l'isomorphisme de Curry-Howard.

Introduction

Une preuve en calcul des séquents peut être traduite en preuve en déduction naturelle.

Inversement, une preuve en déduction naturelle peut être traduite en une preuve en calcul des séquents mais pas de manière unique.

Une preuve en déduction naturelle d'une formule B sous des hypothèses $A_1, \ldots, A_n$ est traduite en la preuve en calcul des séquents du séquent $A_1, \ldots, A_n \vdash B$.

Et réciproquement.

Calcul des séquents vers déduction naturelle

Examinons la traduction du calcul des séquents intuitionniste en déduction naturelle.

Cette traduction est définie par induction sur la hauteur de la preuve du séquent qui commence à 1, c'est-à-dire à l'application d'un axiome.

Il n'y a qu'un axiome en calcul des séquents.

L'axiome d'identité $A \vdash A$ est transforme en la déduction:

$$\frac{[A]}{A}$$

Calcul des séquents vers déduction naturelle

Si la dernière règle est une règle de coupure :

$$\frac{\Gamma \vdash A \quad \Delta, A \vdash B}{\Gamma, \Delta \vdash B}\,(cut)$$

Par hypothèse, il existe des preuves en déduction naturelle :

$$\frac{[\Gamma] \quad \vdots}{A} \qquad \frac{[\Delta] \quad \vdots \qquad [A] \quad \vdots}{B}$$

Il faut prendre la deuxième preuve et remplacer toutes les occurrences de $[A]$ par la première preuve :

$$\dfrac{[\Delta] \quad \vdots \qquad \dfrac{[\Gamma] \quad \vdots}{A} \quad \vdots}{B}$$

Calcul des séquents vers déduction naturelle

La règle d'échange ne correspond à rien de particulier en déduction naturelle car une preuve en déduction naturelle sous des hypothèses A et B est aussi une preuve en déduction naturelle sous des hypothèses B et A.

La règle d'affaiblissement à gauche se traduit en déduction naturelle par l'ajout d'une hypothèse inutile dans une déduction.

La règle de contraction à gauche ne correspond à rien de précis non plus car une preuve sous des hypothèses A et A est aussi une preuve sous l'hypothèse A.

Calcul des séquents vers déduction naturelle

On ne va faire que le connecteur $\wedge$.
Les autres sont similaires.

Une règle à droite en calcul des séquents correspond à une règle d'introduction en déduction naturelle. Par exemple :

$$\frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B}$$

devient la déduction :

$$\dfrac{\dfrac{[\Gamma]}{\vdots}\,A \qquad \dfrac{[\Delta]}{\vdots}\,B}{A \wedge B}$$

Calcul des séquents vers déduction naturelle

Une règle à gauche en calcul des séquents se traduit en une règle d'élimination en déduction naturelle :

$$\frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}$$

Par hypothèse d'induction, il existe :

$$\frac{\begin{array}{cc}[\Gamma] & [A] \\ \vdots & \vdots \end{array}}{C}$$

On remplace cette preuve par :

$$\frac{\begin{array}{cc}[\Gamma] & \dfrac{[A \wedge B]}{A} \\ \vdots & \vdots \end{array}}{C}$$

Déduction naturelle vers calcul des séquents

Pour une preuve en déduction naturelle de B sous les hypothèses $A_1, \ldots, A_n$, il faut traduire cela en une preuve en calcul des séquents de $A_1, \ldots, A_n \vdash B$.

Pour une même preuve en déduction naturelle, on pourrait trouver plusieurs preuves en calcul des séquents.

Il n'y a pas correspondance bi-univoque entre le calcul des séquents et la déduction naturelle.

En un sens, on pourrait admettre que la déduction naturelle présente l'essence de la preuve alors que le calcul des séquents présente des preuves avec beaucoup de manipulations syntaxiques qui sont représentées par les règles structurelles et par l'ordre d'application des règles.

Déduction naturelle vers calcul des séquents

Exemple

$$\dfrac{\dfrac{\dfrac{A \vdash A \quad B \vdash B}{A, B \vdash A \wedge B}}{A \wedge C, B \vdash A \wedge B}}{A \wedge C, B \wedge D \vdash A \wedge B} \qquad \dfrac{\dfrac{\dfrac{A \vdash A \quad B \vdash B}{A, B \vdash A \wedge B}}{A, B \wedge D \vdash A \wedge B}}{A \wedge C, B \wedge D \vdash A \wedge B}$$

sont deux traductions possibles de :

$$\dfrac{\dfrac{[A \wedge C]}{A} \qquad \dfrac{[B \wedge D]}{B}}{A \wedge B}$$

La coupure en déduction naturelle

Lorsque nous parlons de preuves sans coupures, nous supposons que nous sommes en calcul des séquents puisque la règle du *cut* est une règle d'inférence de ce type de calcul.

L'équivalent de la coupure en déduction naturelle est un bout de preuve où une règle d'introduction introduit une formule qui est éliminée un peu plus bas.

En effet, la règle de coupure du calcul des séquents s'énonce :

$$\frac{\Gamma \vdash A \quad \Delta, A \vdash B}{\Gamma, \Delta \vdash B}$$

La coupure en déduction naturelle

Pour obtenir la preuve en déduction naturelle de B sous les hypothèses Γ, Δ :

- On traduit $\Gamma \vdash A$. À moins d'être une preuve triviale, celle-ci a utilisé une règle à droite qui a produit la formule A. Cette règle est éventuellement suivie de quelques règles structurelles qui ne sont que du *méta-sucre* pour un système de déduction naturelle.
- Puis on traduit $\Delta, A \vdash B$. Elle utilisera une règle à gauche qui fera apparaître A dans une séquent. Nous avons vu que les règles à gauche devenaient des règles d'élimination en déduction naturelle.
- La combinaison de ces deux preuves comme il a été expliqué plus haut fournit une preuve en déduction naturelle où une règle d'introduction fournissant la formule de la coupure est suivie d'une règle d'élimination.

L'isomorphisme

On considère une logique des proposition...

intuitionniste...

avec une axiomatisation hilbertienne.

On rappelle que l'axiomatisation hilbertienne est constitué de la seule règle d'inférence *Modus Ponens* et de nombreux axiomes.

Les démonstrations y sont plus difficiles à trouver mais ça colle très bien avec les axiomes de la théorie des types. On aurait pu prendre un système de déduction naturelle mais ça aurait été plus long à expliquer.

La version très simple avec uniquement $\Rightarrow$

Les axiomes concernant $\Rightarrow$:

$$\frac{A \Rightarrow B \quad A}{B}$$

$$A \Rightarrow (B \Rightarrow A)$$

$$(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C$$

C'est une des axiomatisations possibles mais rappelons qu'elles sont toutes équivalentes en ce sens qu'une démonstration avec une axiomatisation peut être refaite différemment avec une autre car les règles de l'une sont dérivables dans l'autre.

La version très simple avec uniquement $\Rightarrow$

Considérons à présent la Logique Combinatoire typée avec une présentation à la Curry :

$$\frac{\vdash M : \alpha \to \beta \qquad \vdash N : \alpha}{\vdash (M\ N) : \beta}$$

$$\vdash K : \alpha \to (\beta \to \alpha)$$

$$\vdash S : (\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to \alpha \to \gamma$$

Correspondance formule-type avec $\Rightarrow$ et $\rightarrow$

On peut établir de manière triviale une fonction bijective Π des formules vers les types :

- à chaque variable propositionnelle on associe une variable de type distincte ;

  ex. : $\Pi(A) \equiv_{def} \alpha$, $\Pi(B) \equiv_{def} \beta$, $\Pi(C) \equiv_{def} \gamma$, etc.

- puis $\Pi(A \Rightarrow B) \equiv_{def} \Pi(A) \rightarrow \Pi(B)$.

Correspondance preuve et inférence de type

On procède avec une définition par induction sur la hauteur de la preuve.

On commence avec les preuves de hauteur 1 :

- $A \Rightarrow (B \Rightarrow A)$

  devient

  $\vdash K : \alpha \to (\beta \to \alpha)$

- $(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C$

  devient

  $\vdash S : (\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to \alpha \to \gamma$

Correspondance preuve et inférence de type

Puis, si une preuve est de hauteur supérieure à2, elle se termine forcément par une application de la règle du *modus ponens* :

$$\frac{A \Rightarrow B \quad A}{B}$$

Par hypothèse, il existe un terme M et une inférence de $\vdash M : \Pi(A \Rightarrow B)$, c'est-à-dire une inférence de $\vdash M : \Pi(A) \to \Pi(B)$.
Toujours par hypothèse d'induction, il existe aussi une terme N et une inférence de $\vdash N : \Pi(A)$.
On prolonge ces deux inférences par :

$$\frac{\vdash M : \Pi(A) \to \Pi(B) \quad \vdash N : \Pi(A)}{\vdash (M\ N) : \Pi(B)}$$

pour obtenir une inférence de $\vdash (M\ N) : \Pi(B)$.

Correspondance preuve et inférence de type

La correspondance inverse est triviale.

Si l'on possède une inférence de type :

$$\vdash M : \alpha$$

il suffit de remplacer toutes les expressions de la forme $\vdash X : T$ figurant dans cette inférence par $\Pi^{-1}(T)$ pour obtenir une preuve en déduction naturelle de $\Pi^{-1}(\alpha)$.

Exemple

Voici la preuve de $A \Rightarrow A$:

$$\dfrac{\dfrac{(A \Rightarrow (A \Rightarrow A) \Rightarrow A) \Rightarrow (A \Rightarrow A \Rightarrow A) \Rightarrow A \Rightarrow A \quad A \Rightarrow (A \Rightarrow A) \Rightarrow A}{(A \Rightarrow A \Rightarrow A) \Rightarrow A \Rightarrow A} \qquad A \Rightarrow A \Rightarrow A}{A \Rightarrow A}$$

Exemple

Et voici sa traduction en inférence de type :

$$\dfrac{\dfrac{\vdash S : (\rho \to (\rho \to \rho) \to \rho) \to (\rho \to \rho \to \rho) \to \rho \to \rho \quad \vdash K : \rho \to (\rho \to \rho) \to \rho}{\vdash S\ K : (\rho \to \rho \to \rho) \to \rho \to \rho} \quad \vdash K : \rho \to \rho \to \rho}{\dfrac{\vdash S\ K\ K : \rho \to \rho}{\vdash I : \rho \to \rho}}$$

Quels conséquences ?

À toute preuve en déduction naturelle correspond de manière bijective un terme typable de la Logique Combinatoire.

Ce terme caractérise la preuve, il peut être considéré comme étant la preuve tout autant que la preuve elle-même.

On peut reconstruire la preuve en inférant le type du terme.

Si je vous donne I, je peux inférer le type de I :

$$\vdash I : \rho \to \rho$$

qui me donne la démonstration de

$$A \Rightarrow A$$

par la transformation inverse.

Le terme est une syntaxe particulière de la preuve.

Comme ce terme est typable, il est fortement normalisable.

Étendons l'isomorphisme à la conjonction

Considérons à présent la conjonction déterminée par les axiomes suivants que nous ajoutons à notre système hilbertien :

$$A \Rightarrow B \Rightarrow (A \wedge B)$$
$$(A \wedge B) \Rightarrow A$$
$$(A \wedge B) \Rightarrow B$$

Étendons l'isomorphisme à la conjonction

Notre Logique Combinatoire est étendu avec un combinateur de formation de paires π tel que $(\pi\ A\ B)$ représente la paire des deux éléments A et B. Ajoutons également les deux combinateurs projections $\pi_k, k \in \{1, 2\}$ tels que $\pi_1(\pi\ A\ B) = A$ et $\pi_2(\pi\ A\ B) = B$. Cela ne pose aucun problème puisque nous savons modéliser ces trois nouveaux combinateurs.

Étendons aussi la théorie des types avec une nouvelle opération de construction de types : si α et β sont des schémas de types alors $(\alpha \times \beta)$ est un schéma de types. Intuitivement, $(\alpha \times \beta)$ est le produit cartésien de α et β, c'est-à-dire l'ensemble des paires formées d'un élément de type α et d'un élément de type β.

Étendons l'isomorphisme à la conjonction

On se donne également les règles concernant ce nouveau schéma de types :

$$\vdash \pi : \alpha \to \beta \to (\alpha \times \beta)$$
$$\vdash \pi_1 : (\alpha \times \beta) \to \alpha$$
$$\vdash \pi_2 : (\alpha \times \beta) \to \beta$$

Ces règles sont intuitivement évidentes si l'on considère les significations intuitives des éléments qu'elles contiennent.

On peut ainsi étendre de manière évidente l'isomorphisme de Curry-Howard.

Étendons l'isomorphisme à la disjonction

Les axiomes de la disjonction sont :

$$A \Rightarrow (A \vee B)$$
$$B \Rightarrow (A \vee B)$$
$$(A \Rightarrow C) \Rightarrow (B \Rightarrow C) \Rightarrow (A \vee B) \Rightarrow C$$

On appelle *union disjointe* de deux ensembles, un ensemble contenant à la fois les éléments des deux ensembles mais en gardant artificiellement les duplicatas générés par cette union. On pose en général la définition :

$$A \oplus B \equiv_{def} \{[0, a], a \in A\} \cup \{[1, b], b \in B\}$$

qui permet de représenter l'union disjointe de deux ensembles A et B.

Étendons l'isomorphisme à la disjonction

Alors soit $[x, y] \in A \oplus B$, si $x = 0$ alors $y \in A$ et si $x \neq 0$ alors $y \in B$. Les entiers 0 et 1 sont modélisés en Logique Combinatoire par les numéraux de Church $\underline{0}$ et $\underline{1}$. Le test d'égalité à zéro est modélisé par le terme $\underline{z}$. On peut modéliser l'opération in_l telle que $in_l(x) = [0, x]$ et l'opération $in_r(y) = [1, y]$. On peut aussi modéliser l'opération *choice* telle que :

$$choice(f)(g)(x) = \begin{cases} f(a) & \text{si} \quad x = [0, a] \\ g(b) & \text{si} \quad x = [1, b] \end{cases}$$

Ces trois fonctions étant modélisables en Logique Combinatoire, on les ajoute à l'ensemble des constantes.

Étendons l'isomorphisme à la disjonction

On ajoute également le schéma de types $\alpha \oplus \beta$ où α et β sont des schémas de types. Et on ajoute les trois règles de typage suivantes :

$$\vdash \mathit{in}_l : \alpha \to (\alpha \oplus \beta)$$
$$\vdash \mathit{in}_r : \beta \to (\alpha \oplus \beta)$$
$$\vdash \mathit{choice} : (\alpha \to \gamma) \to (\beta \to \gamma) \to (\alpha \oplus \beta) \to \gamma$$

Ici aussi la justification de ces règles est relativement évidentes si l'on en a compris les éléments constituants.

On prolonge ainsi l'isomorphisme de Curry-Howard à une logique intuitionniste pour les connecteurs $\Rightarrow$, $\wedge$ et $\vee$.

Étendons l'isomorphisme à la négation

On a choisi la négation définie par $\neg A \equiv_{def} A \Rightarrow \bot$.

L'axiome intuitionniste Hilbertien de la négation peut être choisi comme étant : $\bot \Rightarrow A$ mais nous lui préférerons la règle :

$$\frac{\bot}{A}$$

On introduit en Logique Combinatoire le type ϵ qui est le type vide. Aucun terme ne peut posséder le type ϵ. On ajoute alors la règle de typage :

$$\frac{\vdash M : \epsilon}{\vdash M : \alpha}$$

On voit que l'isomorphisme de Curry-Howard se prolonge à la logique intuitionniste propositionnelle tout entière.

Les types dépendants

Afin de pouvoir étendre l'isomorphisme à la logique du premier ordre, il faut introduire des types dépendants.

Un type dépendant est un type paramétré par une donnée, par exemple un terme de la Logique Combinatoire.

Ainsi, un type « tableau » est au moins paramétré par un entier qui est leur longueur. Un type tableau est aussi paramétré par un autre type : on dit un tableau de longueur N contenant des objets de types T. On entre alors dans le domaine des types polymorphes. Les types polymorphes peuvent aussi être formalisés.

On peut bien entendu formaliser la notion de type dépendant en donnant des règles de formation de type et des règles de typage mais cela nous entraînerait trop loin. Nous nous contenterons d'une approche informelle.

L'isomorphisme et la quantification universelle

Cette section reste informelle.

Soit $\beta(x)$ un type dépendant, on introduit $\prod_{x:\alpha} \beta(x)$ le type des fonctions qui ont un résultat de type $\beta(x)$ lorsque leur argument x est de type α.

N.B. Alors $\alpha \to \beta$ est équivalent à $\prod_{x:\alpha} \beta$ où x n'apparaît pas dans β.

Il est alors possible de trouver des règles logiques pour $\forall x \cdot A(x)$ et des règles de typages pour $\prod_{x:\alpha} \beta(x)$ qui prolonge l'isomorphisme de Curry-Howard à la quantification universelle.

L'isomorphisme et la quantification existentielle

Cette section reste informelle.

Soit $\beta(x)$ un type dépendant, on introduit $\sum_{x:\alpha} \beta(x)$ le type des couples formés d'un élément x de type α et d'un élément y de type $\beta(x)$.

N.B. Alors $\alpha \times \beta$ est équivalent à $\sum_{x:\alpha} \beta$ où x n'apparaît pas dans β.

Il est alors possible de trouver des règles logiques pour $\exists x \cdot \alpha(x)$ et des règles de typages pour $\sum_{x:\alpha} \beta(x)$ qui prolonge l'isomorphisme de Curry-Howard à la quantification existentielle.

Utilisation informelle

Imaginons que l'on prouve en déduction naturelle une formule de la forme :

$$\forall x \cdot (P(x) \Rightarrow \exists y \cdot Q(x, y))$$

Cette formule est identifiée au type :

$$\prod_{x:\alpha} \left(P'(x) \to \sum_{y:\alpha} Q'(x, y) \right)$$

où $P'(x)$ et $Q'(x, y)$ sont les types correspondant respectivement à $P(x)$ et $Q(x, y)$.

Le terme F associé à la preuve de la formule par l'isomorphisme de Curry-Howard possède ce type.

Utilisation informelle

Soit :

$$F : \prod_{x:\alpha} \left(P'(x) \to \sum_{y:\alpha} Q'(x,y) \right)$$

Donnons-nous un $x : \alpha$ normalisable tel alors :

$$\vdash F(x) : P'(x) \to \sum_{y:\alpha} Q'(x,y)$$

Si z est le terme associé à une preuve de $P(x)$, on a $\vdash z : P'(x)$ et :

$$\vdash F(x)(z) : \sum_{y:\alpha} Q'(x,y)$$

Donc $F(x)(z)$ est un couple $(\pi y p)$ où p est un terme associé à une preuve de $Q(x,y)$. On peut donc calculer le y associé à un x tel que $P(x)$ par $\pi_1(F(x)(z))$.

Côté logique	Côté fonctionnel	Côté informatique
preuve	terme fortement normalisable	programme qui se termine
coupure	réduction	étape d'exécution
preuve sans coupures	forme normale	valeur
formule	type	spécification
conjonction ($\wedge$)	produit cartésien ($\times$)	enregistrement (*record*)
disjonction ($\vee$)	union disjointe ($\oplus$)	type variant (*union*)
implication ($\Rightarrow$)	type fonctionnel ($\rightarrow$)	
quant. universelle ($\forall$)	produit dépendant ($\prod$)	
quant. existentielle ($\exists$)	somme dépendante ($\sum$)	
contradiction ($\bot$)	type vide (ϵ)	

Conclusions

Nous vous avons présenter l'isomorphisme de Curry-Howard de manière très informelle.

Pour exploiter cette isomorphisme, il faut une théorie complète et bien ficelée.

La théorie EON de M.J. Beeson que nous verrons au prochain cours.

La théorie AF_2 de J-L. Krivine que nous ne verrons pas. Elle fait appel à une logique d'ordre 2, c'est-à-dire que l'on peut quantifier les prédicats.