Histoire des algorithmes

version du 2 mai 2004 – 21 h 34

La correspondance de Curry-Howard

La mathématisation

L'histoire des sciences montre que tout ce qui est susceptible de se mathématiser se mathématise.

Au début, seuls les entiers sont des êtres mathématiques.

Puis les Anciens acceptent les rationnels.

Au début du dix-neuvième siècle, les relatifs et les complexes (ou imaginaires) deviennent eux-aussi des êtres mathématiques.

La mathématisation

Au cours du dix-neuf siècle

– les réels (Dedekind),
– puis les fonctions (en «extension»)
– et les ensembles (Cantor) deviennent des êtres mathématiques.

Au début du vingtième siècle, les fonctions (en «intention») (Church et Curry) et les théorèmes (Boole, Frege etc.) deviennent des êtres mathématiques.

Aujourd'hui (1980), les démonstrations deviennent des êtres mathématiques.

La mathématisation

Au cours du dix-neuf siècle

– les réels (Dedekind),
– puis les fonctions (en «extension»)
– et les ensembles (Cantor) deviennent des êtres mathématiques.

Au début du vingtième siècle, les fonctions (en «intention») (Church et Curry) et les théorèmes (Boole, Frege etc.) deviennent des êtres mathématiques.

Aujourd'hui (1980), les démonstrations deviennent des êtres mathématiques.

La déduction naturelle

Les séquents

La déduction naturelle est due à Gentzen et Prawitz.

En déduction naturelle, on raisonne avec des hypothèses.

On utilise des séquents $\Gamma \vdash p$

– où Γ est un ensemble de propositions (les hypothèses) appelé l'antécédent

– et où p est une proposition.

On écrit $\Gamma, p \vdash q$ au lieu de $\Gamma \cup \{p\} \vdash q$

et $\vdash p$ quand l'ensemble des hypothèses est vide.

$\Gamma \vdash p$ se lit «de Γ on déduit p»

$\vdash p$ se lit «p est un théorème».

Les démonstrations

Les démonstrations sont des arbres dont

– les noeuds sont les règles de déduction,

– les feuilles sont les axiomes

– et la racine est le séquent dont c'est la démonstration.

$$\dfrac{\dfrac{\dfrac{\cdots \quad \cdots}{}\,(foo_1) \qquad \dfrac{\cdots}{}\,(bar)}{\cdots \qquad \cdots}\,(foo_2)}{\dfrac{\cdots \qquad\qquad \cdots}{\Gamma \vdash \Delta}\,(foo_1)}$$

Les théorèmes

Les théorèmes sont les séquents de la forme $\vdash p$ qui peuvent être déduits des axiomes et des règles.

On trouvent donc le séquent $\vdash p$ à la racine d'un arbre de démonstration de p.

La logique propositionnelle minimale

Les propositions

C’est une logique très très simple.

Les propositions sont construites

– à partir des variables propositionnelles $p, q, r, \ldots$,

– et du connecteur $\Rightarrow$.

L’axiome

Il n’y a qu’un seul axiome,

$$\Gamma, p \vdash p$$

Les règles

Il y a deux règles : introduction et élimination :

$$\frac{\Gamma, p \vdash q}{\Gamma \vdash p \Rightarrow q} \Rightarrow I$$

$$\frac{\Gamma \vdash p \Rightarrow q \qquad \Gamma \vdash p}{\Gamma \vdash q} \Rightarrow E$$

Les règles

Il y a deux règles : introduction et élimination :

$$\frac{\Gamma, p \vdash q}{\Gamma \vdash p \Rightarrow q} \Rightarrow I$$

$$\frac{\Gamma \vdash p \Rightarrow q \qquad \Gamma \vdash p}{\Gamma \vdash q} \Rightarrow E$$

$\Rightarrow E$ est aussi appelé modus ponens.

Une démonstration

Je pose $\Gamma \equiv (p \Rightarrow q), (q \Rightarrow r), p$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \vdash p \Rightarrow q \qquad \Gamma \vdash p}{\Gamma \vdash q}\Rightarrow E \qquad \Gamma \vdash q \Rightarrow r}{\Gamma \vdash r}\Rightarrow E}{(p \Rightarrow q), (q \Rightarrow r) \vdash p \Rightarrow r}\Rightarrow I}{(p \Rightarrow q) \vdash (q \Rightarrow r) \Rightarrow p \Rightarrow r}\Rightarrow I}{\vdash (p \Rightarrow q) \Rightarrow (q \Rightarrow r) \Rightarrow p \Rightarrow r}\Rightarrow I$$

Le lambda calcul

Les fonctions comme citoyens de première classe

Les preuves ont été faites citoyens de première classe,

mais pourquoi pas les fonctions ?

Quelques dates

Fin du 19ème siècle la notion de fonction se précise en analyse[a] et en théorie des ensembles.

1920 Schönfinkel introduit les premiers concepts de logique combinatoire,

1925 Haskell Curry crée la logique combinatoire,

1936 Alonso Church crée le λ-calcul,

1970-... Explosion du λ-calcul due à l'informatique (Barendregt, Berry, Boehm, de Bruijn, Curien, Girard, Hindley, Klop, Krivine, Levy, Plotkin, Statmann, Scott etc.)

[a] En particulier Weierstrass exhibe une fonction continue nulle part dérivable.

Des notations différentes, un même concept

en maths	$x \mapsto x$	$f \mapsto (x \mapsto f(f(x)))$
en CAML	`fun x -> x`	`fun f -> (fun x -> (f (f x)))`
en λ-calcul	$\lambda x.x$	$\lambda f.(\lambda x.(f(fx)))$

La syntaxe

La classe Λ est la plus petite classe qui contient

1. x si x est une variable,
2. $\lambda x.M$ si $M \in \Lambda$,
3. $(M\,N)$ si $M \in \Lambda$ et $N \in \Lambda$.

La syntaxe

La classe Λ est la plus petite classe qui contient

1. x si x est une variable,
2. $\lambda x.M$ si $M \in \Lambda$, abstraction
3. $(M\,N)$ si $M \in \Lambda$ et $N \in \Lambda$. application

Qu'y a-t-il derrière la syntaxe ?

On peut voir les termes comme des abstractions des fonctions ou des programmes.

Dans $\lambda x.M$, on dit que M est le corps de la fonction ou du programme.

Dans (MN), on peut voir M comme une fonction que l'on applique au paramètre N. La valeur va s'obtenir par «réduction» (approche intentionnelle).

Le lambda-calcul décrit les fonctions par leur comportement.

La decription extensionnelle et la description intentionnelle

Dans l’approche extensionnelle, on décrit la fonction comme un ensemble de couples paramètre-résultat.

Dans l’approche intensionnelle, on décrit ce que fait la fonction, c’est-à-dire son calcul.

La β-contraction

Les fonctions sont faites pour calculer !

Les réductions d'un terme représentent son calcul.

La β-contraction en est l'étape élémentaire.

$$(\lambda x.M)P \to M[x := P]$$

On remplace tout occurrence de x dans M par P.

Un exemple

$$
\begin{array}{lcl}
(\lambda f.\lambda x(f\ (f\ x)))\ (\lambda f.\lambda x(f\ x)) & \equiv & (\lambda f.\lambda x(f\ (f\ x)))\ (\lambda g.\lambda y(g\ y)) \\
& \rightarrow & \lambda x.(\lambda g.\lambda y(g\ y))\ ((\lambda g.\lambda y(g\ y))\ x) \\
& = & \lambda x.(\lambda g.\lambda y(g\ y))\ ((\lambda g.\lambda y(g\ y))\ x) \\
& \rightarrow & \lambda x.(\lambda g.\lambda y(g\ y))\ (\lambda y(x\ y)) \\
& = & \lambda x.(\lambda g.\lambda y(g\ y))\ (\lambda y'(x\ y')) \\
& = & \lambda x.(\lambda g.\lambda y(g\ y))\ (\lambda y'(x\ y')) \\
& \rightarrow & \lambda x.\lambda y(\lambda y'(x\ y')\ y) \\
& = & \lambda x.\lambda y(\lambda y'(x\ y')\ y) \\
& \rightarrow & \lambda x.\lambda y.x\ y \\
& = & \lambda f.\lambda x.f\ x.
\end{array}
$$

Il y a plusieurs réduction possibles.

On peut montrer que le résultat ne dépend de la réduction suivie :

– confluence,
– ou propriété de Church-Rosser.

Un autre exemple

$$
\begin{aligned}
(\lambda x.x\ x)\ (\lambda x.x\ x) &= (\lambda x.x\ x)\ (\lambda y.y\ y) \\
&\rightarrow (x\ x)\ [x := (\lambda y.y\ y)] \\
&= (\lambda y.y\ y)\ (\lambda y.y\ y) \\
&= (\lambda x.x\ x)\ (\lambda x.x\ x)
\end{aligned}
$$

Le lambda calcul simplement typé

Le paradoxe du barbier

$\Omega \equiv (\lambda x.x\ x)(\lambda x.x\ x)$ et $\mathsf{Y} \equiv \lambda f.(\lambda x f(x\ x))\ (\lambda x f(x\ x))$ contiennent des termes qui s'appliquent à eux-mêmes.

Le paradoxe du barbier est :

> Le barbier rase tous ceux qui ne se rasent pas eux-mêmes.

Qui rase le barbier ?

Le paradoxe du barbier

$\Omega \equiv (\lambda x.x\ x)(\lambda x.x\ x)$ et $\mathsf{Y} \equiv \lambda f.(\lambda x f(x\ x))\ (\lambda x f(x\ x))$ contiennent des termes qui s'appliquent à eux-mêmes.

Le paradoxe du barbier est :

> Le barbier rase tous ceux qui ne se rasent pas eux-mêmes.
>
> Qui rase le barbier ?

Quelle est l'«intension» d'un terme comme Ω qui se réduit en lui-même ?

La thérapie

Pour éviter les paradoxes, on cherche à éviter de tels termes.

On va donc typer les termes.

≪Typer≫ est aussi apprécié en programmation.

Plusieurs langages de programmation s'appuient sur le typage, dont JAVA.

Les objectifs du typage

Le typage a donc deux objectifs :

– préserver la correction, rien de mauvais ne peut arriver,

– préserver la terminaison, toutes les réductions se terminent.

En λ-calcul la terminaison s'appelle la normalisation forte.

Les environnements

Il faut typer les variables libres, il faut donc faire des hypothèses sur les types de ces variables.

D'où la notion d'environnement.

Un environnement est un ensemble d'association de types à des variables.

$$\Gamma \equiv x_1 : \sigma_1, ..., x_n : \sigma_n$$

Les types

Un jugement est l'affirmation du type σ d'un terme M sous un certain environnement Γ :

$$\Gamma \vdash M : \sigma$$

Les types sont

– soit des types de base o,

– soit des types applications $\sigma \longrightarrow \tau$.

Les règles

$$\Gamma, x : \sigma \vdash x : \sigma \; (Var)$$

$$\frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash \lambda x.M : \sigma \to \tau} \; (Abs)$$

$$\frac{\Gamma \vdash M : \sigma \to \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash M \; N : \tau} \; (App)$$

La correspondance de Curry-Howard

La mathématique c’est l’art de donner le même nom à des choses différentes.

Henri Poincaré

La correspondance de Curry-Howard

$$\text{(Var)}\quad \Gamma, x : \sigma \vdash x : \sigma$$

$$\text{(Abs)}\quad \frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash \lambda x.M : \sigma \to \tau}$$

$$\text{(App)}\quad \frac{\Gamma \vdash M : \sigma \to \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash MN : \tau}$$

$$\Gamma, p \vdash p$$

$$\Rightarrow I\quad \frac{\Gamma, p \vdash q}{\Gamma \vdash p \Rightarrow q}$$

$$\Rightarrow E\quad \frac{\Gamma \vdash p \Rightarrow q \qquad \Gamma \vdash p}{\Gamma \vdash q}$$

La correspondance de Curry-Howard

Dans $\Gamma \vdash M : \sigma$,

– M : est une annotation qui est le «terme de preuve»,

– σ peut-être vu comme un type ou comme une proposition.

La preuve précédente

$$\dfrac{\dfrac{\dfrac{\dfrac{(p \Rightarrow q),\ (r \Rightarrow p), r \vdash p \Rightarrow q \quad \mathcal{D}}{(p \Rightarrow q),\ (r \Rightarrow p), r \vdash q}\ \Rightarrow E}{(p \Rightarrow q),\ (r \Rightarrow p) \vdash r \Rightarrow q}\ \Rightarrow I}{(p \Rightarrow q) \vdash (r \Rightarrow p) \Rightarrow r \Rightarrow q}\ \Rightarrow I}{\vdash (p \Rightarrow q) \Rightarrow (r \Rightarrow p) \Rightarrow r \Rightarrow q}\ \Rightarrow I$$

où $\mathcal{D}$ est

$$\dfrac{(p \Rightarrow q),\ (r \Rightarrow p), r \vdash r \Rightarrow p \quad (p \Rightarrow q),\ (r \Rightarrow p), r \vdash r}{(p \Rightarrow q),\ (r \Rightarrow p), r \vdash p}\ \Rightarrow E$$

La preuve précédente annotée

$$\dfrac{\dfrac{\dfrac{\dfrac{x : (p \Rightarrow q),\ y : (r \Rightarrow p), z : r \vdash x : p \Rightarrow q \quad \mathcal{D}}{x : (p \Rightarrow q),\ y : (r \Rightarrow p), z : r \vdash x\ (y\ z) : q}\ \Rightarrow E}{x : (p \Rightarrow q),\ y : (r \Rightarrow p) \vdash \lambda z.x\ (y\ z) : r \Rightarrow q}\ \Rightarrow I}{x : (p \Rightarrow q) \vdash \lambda yz.x\ (y\ z) : (r \Rightarrow p) \Rightarrow r \Rightarrow q}\ \Rightarrow I}{\vdash \lambda xyz.x\ (y\ z) : (p \Rightarrow q) \Rightarrow (r \Rightarrow p) \Rightarrow r \Rightarrow q}\ \Rightarrow I$$

où $\mathcal{D}$ est

$$\dfrac{x : (p \Rightarrow q),\ y : (r \Rightarrow p), z : r \vdash y : (r \Rightarrow p) \qquad x : (p \Rightarrow q),\ y : (r \Rightarrow p), z : r \vdash z : r}{(p \Rightarrow q),\ (r \Rightarrow p), r \vdash y\ z : p}\ \Rightarrow E$$

La preuve précédente annotée

$$\dfrac{\dfrac{\dfrac{\dfrac{x : (p \Rightarrow q),\ y : (r \Rightarrow p), z : r \vdash x : p \Rightarrow q \quad \mathcal{D}}{x : (p \Rightarrow q),\ y : (r \Rightarrow p), z : r \vdash x\ (y\ z) : q}\ (App)}{x : (p \Rightarrow q),\ y : (r \Rightarrow p) \vdash \lambda z.x\ (y\ z) : r \Rightarrow q}\ (Abs)}{x : (p \Rightarrow q) \vdash \lambda yz.x\ (y\ z) : (r \Rightarrow p) \Rightarrow r \Rightarrow q}\ (Abs)}{\vdash \lambda xyz.x\ (y\ z) : (p \Rightarrow q) \Rightarrow (r \Rightarrow p) \Rightarrow r \Rightarrow q}\ (Abs)$$

où $\mathcal{D}$ est

$$\dfrac{x : (p \Rightarrow q),\ y : (r \Rightarrow p), z : r \vdash y : (r \Rightarrow p) \qquad x : (p \Rightarrow q),\ y : (r \Rightarrow p), z : r \vdash z : r}{(p \Rightarrow q),\ (r \Rightarrow p), r \vdash y\ z : p}\ (App$$

La preuve du lemme est le typage du terme !

Simplification de preuves

La preuve

$$\dfrac{\dfrac{\dfrac{(p \Rightarrow p), q \vdash p \Rightarrow p}{(p \Rightarrow p) \vdash q \Rightarrow p \Rightarrow p}(\Rightarrow I)}{\vdash (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p}(\Rightarrow I) \qquad \dfrac{\dfrac{p \vdash p}{\vdash p \Rightarrow p}(\Rightarrow I)}{\vdash q \Rightarrow p \Rightarrow p}(\Rightarrow E)$$

peut être réduite

Simplification de preuves

En effet, on fait une introduction immédiatement suivie d'une élimination :

$$\dfrac{\dfrac{\dfrac{(p \Rightarrow p), q \vdash p \Rightarrow p}{(p \Rightarrow p) \vdash q \Rightarrow p \Rightarrow p}(\Rightarrow I)}{\vdash (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p}(\Rightarrow I) \qquad \dfrac{p \vdash p}{\vdash p \Rightarrow p}(\Rightarrow I)}{\vdash q \Rightarrow p \Rightarrow p}(\Rightarrow E)$$

On peut obtenir une preuve de $\vdash q \Rightarrow p \Rightarrow p$ à partir de la preuve de $(p \Rightarrow p) \vdash q \Rightarrow p \Rightarrow p$.

Pour cela, il suffit de remplacer chaque occurrence de l'utilisation de l'hypothèse $(p \Rightarrow p)$ par sa preuve.

Simplification de preuves

En utilisant cette remarque

$$\dfrac{\dfrac{\dfrac{(p \Rightarrow p), q \vdash p \Rightarrow p}{(\Rightarrow I)}}{(p \Rightarrow p) \vdash q \Rightarrow p \Rightarrow p}(\Rightarrow I) \qquad \dfrac{p \vdash p}{\vdash p \Rightarrow p}(\Rightarrow I)}{\vdash (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p}(\Rightarrow E)$$

$$\vdash q \Rightarrow p \Rightarrow p$$

donne

$$\dfrac{\dfrac{q, p \vdash p}{(\Rightarrow I)}}{q \vdash p \Rightarrow p}(\Rightarrow I)$$

$$\vdash q \Rightarrow p \Rightarrow p$$

Simplification de preuves

Donc avec les annotations par les termes de preuve

$$\dfrac{\dfrac{\dfrac{x : (p \Rightarrow p), y : q \vdash p \Rightarrow p}{x : (p \Rightarrow p) \vdash \lambda y.x : q \Rightarrow p \Rightarrow p}(Abs)}{\vdash \lambda xy.x : (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p}(Abs) \qquad \dfrac{z : p \vdash z : p}{\vdash \lambda z.z : p \Rightarrow p}(Abs)}{\vdash (\lambda xy.x)\ (\lambda z.z) : q \Rightarrow p \Rightarrow p}(App)$$

donne

$$\dfrac{\dfrac{y : q, z : p \vdash p}{y : q \vdash \lambda z.z : p \Rightarrow p}(Abs)}{\vdash \lambda yz.z : q \Rightarrow p \Rightarrow p}(Abs)$$

Simplification de preuves

Donc avec les annotations par les termes de preuve

$$\dfrac{\dfrac{\dfrac{x : (p \Rightarrow p), y : q \vdash p \Rightarrow p}{x : (p \Rightarrow p) \vdash \lambda y.x : q \Rightarrow p \Rightarrow p}(Abs)}{\vdash \lambda xy.x : (p \Rightarrow p) \Rightarrow q \Rightarrow p \Rightarrow p}(Abs) \qquad \dfrac{z : p \vdash z : p}{\vdash \lambda z.z : p \Rightarrow p}(Abs)}{\vdash (\lambda xy.x)\ (\lambda z.z) : q \Rightarrow p \Rightarrow p}(App)$$

donne

$$\dfrac{\dfrac{y : q, z : p \vdash p}{y : q \vdash \lambda z.z : p \Rightarrow p}(Abs)}{\vdash (\lambda y.x)[x := \lambda z.z] \equiv \lambda yz.z : q \Rightarrow p \Rightarrow p}(Abs)$$

La β-réduction correspond à la simplification des preuves.

Simplification de preuves

$$\dfrac{\dfrac{\dfrac{\mathcal{D}}{\varphi, \Gamma \vdash \psi}}{\Gamma \vdash \varphi \Rightarrow \psi}(\Rightarrow I) \qquad \dfrac{\mathcal{D}'}{\Gamma \vdash \varphi}}{\Gamma \vdash \psi}(\Rightarrow E)$$

se transforme en

$$\dfrac{\mathcal{D}''}{\Gamma \vdash \psi}$$

$\mathcal{D}''$ est la preuve $\mathcal{D}$ dans laquelle toutes les utilisations de l'hypothèse φ sont remplacées par la preuve $\mathcal{D}$ de φ.

Simplification de preuves

$$\dfrac{\dfrac{\dfrac{\mathcal{D}}{x : \varphi, \Gamma \vdash M : \psi}}{\Gamma \vdash (\lambda x.M) : \varphi \Rightarrow \psi}(Abs) \qquad \dfrac{\mathcal{D}'}{\Gamma \vdash N : \varphi}}{\Gamma \vdash (\lambda x.M)\ N : \psi}(App)$$

se transforme en

$$\dfrac{\mathcal{D}''}{\Gamma \vdash M[x := N] : \psi}$$

$\mathcal{D}''$ est la preuve $\mathcal{D}$ (qui se note M) dans laquelle toutes les utilisations de l'hypothèse $x : \varphi$ sont remplacées par la preuve $\mathcal{D}$ de φ (qui se note N).

La correspondance complète de Curry-Howard

On obtient le tableau de correspondance :

types	propositions
termes	preuves
réduction	simplification des preuves

Philip Wadler

La correspondance de Curry-Howard est aussi importante pour les sciences de l'information que la relativité d'Einstein et la mécanique quantique de Dirac pour la physique.