

Proofs and Programs

Phillipe Audebaud *

ENS de Lyon

Contents

I	(Pure) λ-Calculus	2
1	Computing with functions ?	2
2	Church λ -calculus (informally)	2
3	A toolbox on λ -calculus	3
II	Calcul propositionnel et correspondance de Curry-Howard	6
1	Éléments de langage (informels)	6
2	Fragments λ_{\rightarrow}	7
3	Interprétation BHK	7
III	λ-calcul simplement typé	8
1	Quelques Lemmes	8

*<https://perso.ens-lyon.fr/philippe.audebaud/PnP/>

Basis

- Lecture: Tue 8h-10h (Philippe Audebaud)
- Tutorial: We 8h-10h (Aurore)

10 Weeks of courses (3x3), which is really low.

$$Final\ mark = 50\% \cdot CC + 50\% \cdot Exam$$

No mid-time exam, but weekly homework.

Warning Presence at the courses and tutorial will have an impact on the marks.

Prerequisites

- L2.2 \rightarrow Logical (Natacha P., Chapter 1 & 2):
 - Proof theory
 - Formal system for logic inference.
- λ -calculus
- Category theory

Part I

(Pure) λ -Calculus

1 Computing with functions ?

How do we do mathematics ?

- A Having *structures*: numbers, spaces (points, vectors, functions) \rightarrow Eilenberg-Mac Lane (\sim 1942) Category theory
- B Build, explore, transform structures \rightarrow Church (\sim 1930) λ -Calculus
- C Compare "stuff": *equality* \rightarrow Voevodski (\sim 2006) Algebraic topology \rightarrow search HoTT (Hight order Type Theory)
- D Provide a framework (*rules*) to reasoning on all that! \rightarrow 1st point

2 Church λ -calculus (informally)

$$\begin{array}{l} f : A \rightarrow B \\ x \mapsto e \end{array}$$

Given $a \in A$, $f(a)$ is the "replacement of the occurrence of x in e by a "

$$\begin{array}{ll} f \stackrel{\text{def}}{=} \lambda x. e & (\lambda\text{-abstraction}) \\ f\ a = (\lambda a. e)\ a & (\text{Application}) \end{array}$$

Notation

$$e\langle a/x \rangle$$

is the replacement in e of all the occurrences of a by x .

Example

1.

$$\begin{aligned} \lambda x.x \\ x \mapsto x \end{aligned}$$

is the identity function

2.

$$\begin{aligned} \lambda x.y \\ x \mapsto y \end{aligned}$$

Here x and y are variables, $x \neq y$. $(\lambda x.y) a$ leads to $y\langle a/x \rangle \equiv y$

$$(\lambda x.a) b \rightarrow_{\beta} a\langle b/x \rangle$$

\rightarrow_{β} is a binary relation on lambda-terms \Rightarrow idea of computation on terms.

Notion of α -equivalence

$$\lambda x.a \stackrel{?}{=}_{\alpha} \lambda y.b$$

Pick a *fresh* variable, let say z ,

$$a\langle z/x \rangle =_{\alpha} b\langle z/y \rangle$$

All the results and proofs will be done up to α -equivalence (no difference made between $\lambda x.x$ and $\lambda y.y$).

3 A toolbox on λ -calculus

λ -calculus: Syntax and Semantics, Herk Barendregt (1977)

Let \mathcal{X} be a measurable set of variables, ranged over by x, y, z, \dots

Definition 1. A λ -term e is generated by the grammar:

$$a, b, e \dots ::= x \in \mathcal{X} \mid \lambda x.e \mid a b$$

The set of λ -terms is denoted Λ .

Definition 2 (Free variable). The set of free variables in e , denoted $FV(e)$ is defined inductively:

- if $e \equiv x \in \mathcal{X}$, $FV(x) \equiv \{x\}$
- if $e \equiv \lambda x.a_0$, $FV(\lambda x.a_0) \equiv FV(a_0) \setminus \{x\}$
- if $e \equiv a_1 a_2$, $FV(a_1 a_2) \equiv FV(a_1) \cup FV(a_2)$

A term e is closed if $FV(e) = \emptyset$

Definition 3 (Substitution). Given $x \in \mathcal{X}$, $a \in \Lambda$, the substitution of (all the) occurrences of a in $e \in \Lambda$, denoted $e\langle a/x \rangle$ is:

- if $y \in \mathcal{X} \setminus \{x\}$, $y\langle a/x \rangle \equiv y$ and $x\langle a/x \rangle \equiv a$
- $(\lambda y.e)\langle a/x \rangle = \lambda y.e\langle a/x \rangle$
- $(e f)\langle a/x \rangle = (e\langle a/x \rangle) f\langle a/x \rangle$

Definition 4 (\rightarrow_β reduction).

$$\rightarrow_\beta \subseteq \Lambda \times \Lambda$$

$$\left\{ \left(\underbrace{(\lambda x.a) b}_{\text{redex}}, \underbrace{a\langle b/x \rangle}_{\text{contraction}} \right) \mid x \in \mathcal{X}, a, v \in \Lambda \right\}$$

Example

1.

$$\underbrace{(\lambda x.(\lambda y.y) a) b}_{\rightarrow_\beta (\lambda y.y) b} \rightarrow_\beta ((\lambda y.y) a) \langle b/x \rangle \equiv ((\lambda y.y) \langle b/x \rangle) a \langle b/x \rangle$$

$$\equiv (\lambda y.y) a \langle b/x \rangle$$

2.

$$(\lambda x.y) a \rightarrow_\beta y$$

3.

$$(\lambda x.x x)(\lambda x.x x) \rightarrow_\beta (x x) \langle \lambda x.x x/x \rangle \text{ or } (x x) \langle \lambda y.y y/x \rangle$$

$$(\lambda x.x x)(\lambda x.x x)$$

Russell paradox: we get an infinite β -reduction!

$$\rightarrow_\beta \subseteq \beta_0 \subseteq \underbrace{\beta}_{\beta\text{-reduction}} = \beta_0^*$$

\rightarrow_β^* is the β -reduction, noted \rightarrow_β

Definition 5 (β_0 -contraction). Let $a, b \in \Lambda$. $a \beta_0 b$ is defined by cases:

- $x \beta_0 x$
- $(\lambda x.u)v \beta_0 u\langle v/x \rangle$
- $(\lambda x.u) \beta_0 (\lambda x.v)$ if $u \beta_0 v$
- $(u v) \beta_0 (u' v)$ if $u \beta_0 u'$
- $(u v) \beta_0 (u v')$ if $v \beta_0 v'$

Maintenant en français !

Remarque: β_0 est réflexive.

Definition 6. La β -réduction est la clôture transitive de β_0 :

$$\beta = \beta_0^*$$

Remarque Si $a, b \in \Lambda$, alors $a \beta b$ si il existe $n \geq 0$ et $(e_k)_{0 \leq k \leq n}$ λ -termes tels que :

- $a = e_0$ et $b = e_n$
- pour tout $k < n$, $e_k \beta_0 e_{k+1}$

Definition 7. Soit \mathcal{R} une relation binaire sur Λ . On dit que \mathcal{R} est λ -compatible si elle satisfait les propriétés suivantes :

- $x \mathcal{R} x$
- si $a \mathcal{R} b$ et $c \mathcal{R} d$ alors $a c \mathcal{R} b d$
- si $a \mathcal{R} b$ alors $\lambda x.a \mathcal{R} \lambda x.b$

Propriété 1. La β -réduction est la plus petite relation λ -compatible et transitive contenant \rightarrow_β

Proof. ★ On vérifie d'abord :

$$\rightarrow_\beta \subseteq \beta_0 \subseteq \beta_0^* = \beta$$

D'autre part, β_0 est λ -compatible :

- par réflexivité, $x \beta_0 x$
- soit $a \beta_0 b$; par définition, il existe $n \geq 0$, $(e_k)_{0 \leq k \leq n}$ tel que $a = e_0$, $b = e_n$ et pour tout $k < n$, $e_k \beta_0 e_{k+1}$. Du coup, par définition de β_0 , pour tout $k < n$, $\lambda x.e_k \beta_0 \lambda x.e_{k+1}$.
Ainsi, $\lambda x.a \beta_0 \lambda x.b$.

★ Soit \mathcal{R} une autre relation λ -compatible et transitive contenant \rightarrow_β . Montrons que $\beta \subseteq \mathcal{R}$. Il "suffit" de vérifier que $\beta_0 \subseteq \mathcal{R}$ (laissé en exercice). \square

Propriétés essentielles de la β -réduction

Remarque (Λ, β_0) est un système de réduction abstrait¹.

Definition 8 (Forme normale, Relation normalisante). Soit \mathcal{R} une relation binaire sur Λ ,

- On dit que a est une forme normale (relativement à \mathcal{R}) s'il n'existe pas $b \in \Lambda$ tel que $a \mathcal{R} b$.
- On dit que a a une forme normale (relativement à \mathcal{R}) s'il existe $b \in \Lambda$ tel que b est une forme normale et $a \mathcal{R}^* b$
- On dit que \mathcal{R} est normalisante si tout $a \in \Lambda$ a une forme normale

Exemple

- $\lambda x.x$ est une forme normale relativement à β_0
- β_0 n'est pas normalisante !

$$\Omega \equiv (\lambda x.x x) (\lambda x.x x)$$

$$\Omega \rightarrow_\beta \Omega$$

Definition 9 (Confluence). Soit \mathcal{R} une relation binaire sur Λ . On dit que \mathcal{R} est confluente si pour tout $(a, b, c) \in \Lambda^3$ tel que

$$a \mathcal{R}^* b \text{ et } a \mathcal{R}^* c$$

alors il existe $d \in \Lambda$, tel que

$$b \mathcal{R}^* d \text{ et } c \mathcal{R}^* d$$

Theorem 1. La β_0 -réduction est confluente.

Proof. En semaine 3 ou 4. \square

Corollary 1. Tout λ -terme admet au plus une forme normale, relativement à β_0

¹Cf ThPr

Notion d'égalité sur les λ -termes

Definition 10. La β -équivalence sur Λ est la relation binaire notée $=_\beta$, définie comme la clôture réflexive symétrique transitive de β_0 :

$a =_\beta b$ s'il existe $n \geq 0$ et $(e_k)_{0 \leq k \leq n}$ tel que $a = e_0$ et $b = e_n$ et $\forall k < n$, soit $e_k \beta_0 e_{k+1}$ soit $e_{k+1} \beta_0 e_k$

Definition 11 (λ -congruence). Une relation binaire \mathcal{R} (sur Λ) est une λ -congruence si c'est une relation d'équivalence et qu'elle est λ -compatible.

Theorem 2 (Church-Rosser). Pour tout $(a, b) \in \Lambda^2$, $a =_\beta b$ si et seulement si il existe $c \in \Lambda$ tel que $a \beta b$ et $b \beta c$

Proof. La condition est suffisante

Réciproquement, pour la condition nécessaire, on introduit $R \subseteq \Lambda \times \Lambda$ défini par :
 $a R b$ s'il existe c tel que $a \beta c$ et $b \beta c$.

On remarque, par définition de \mathcal{R} ,

- \mathcal{R} est réflexive et symétrique
- \mathcal{R} est transitive

De plus, \mathcal{R} contient β (ou β_0). Donc, si $a =_\beta b$, alors $a R b$. □

Theorem 3. La relation d'équivalence $=_\beta$ est la plus petite λ -congruence contenant \rightarrow_β

Proof. En exo. □

Notation On note \equiv pour une définition ($\stackrel{\text{def}}{=}$), mais aussi pour l' α -équivalence ($=_\alpha$). On peut utiliser la notation de Bruijn (cf références).

Part II

Calcul propositionnel et correspondance de Curry-Howard

1 Éléments de langage (informels)

- Théorie de la *démonstration* (prouvabilité)
- Thème des modèles

Quelques "ingrédients" :

- *énoncés* (logiques) : ici les familles du calcul propositionnel:

$$A ::= x \mid \top \mid \perp \mid A \Rightarrow B \mid A \wedge B \mid A \vee B \mid \neg A^2 \quad (\star)$$

La notation " A propriété" signifie que A est engendrée par la grammaire (\star)

- On parle de *jugements* sur ces énoncés : " A true"
- On introduit aussi des jugements hypothétiques : $A_1 \text{ true}, A_2 \text{ true}, \dots, A_n \text{ true} \vdash B \text{ true}$

² $\neg A$ signifie en fait $A \Rightarrow \perp$

Commentaires sur les différentes règles de (NJ):

- Le vrai
- L'implication ($/!\backslash$: $A \Rightarrow B \neq \neg A \vee B$ dans (NJ))
- Le faux
- La négation
- La disjonction

2 Fragments λ_{\rightarrow}

On peut associer des règles au typage de λ -termes en raisonnant sur $\lambda x.t : T$

Theorem 4 (Curry-Howard). *Le fragment NJ_{\rightarrow} et λ_{\rightarrow} sont en correspondance via:*

1. Si $\Delta \vdash t : T$ dans λ_{\rightarrow}

λ_{\rightarrow}	NJ_{\rightarrow}
<i>type</i>	<i>proposition</i>
variable de type	proposition atomique
type flèche	implication
<i>terme</i>	<i>dérivation</i>
variable de terme	hypothèse
λ -abstraction	règle d'introduction
application	règle d'élimination
β -redex	coupure
β -réduction	transformation sur les dérivations
<i>forme normale</i>	<i>dérivation sans coupure</i>

Figure 1: Correspondance de Curry-Howard

3 Interprétation BHK

L'interprétation de Brouwer-Heyting-Kolmogorov consiste à construire un témoin (une preuve) d'une proposition selon le protocole suivant :

- Un témoin pour $A \wedge B$ est une paire formée par un témoin pour A et un témoin pour B
- Il y a un témoin unique pour \top
- Un témoin pour $A \vee B$ est soit un témoin pour A , soit un témoin pour B
- Il n'y a pas de témoin pour \perp
- Un témoin pour $A \Rightarrow B$ est une application de témoins pour A vers des témoins pour B
- Un témoin pour $\neg A$ est un témoin de $A \Rightarrow \perp$

Avec A, B engendrés par la grammaire

$$A ::= X \mid A \Rightarrow A \mid A \vee A \mid A \wedge A \mid \top \mid \perp$$

Definition 12 (Produit (paire)). Soit A, B . Le produit de A par B est le damier de $A \times B$, et de la propriété universelle suivante :

Pour tout $f : D \rightarrow A$ et $g : D \rightarrow B$, il existe $h : D \rightarrow A \times B$ tel que $\pi_1 \circ h = f$ et $\pi_2 \circ h = g$ ³.

De plus, h est unique et ne dépend que de f et de g ,

$$h = \langle f, g \rangle$$

Par ailleurs, si $e : D \rightarrow A \times B$, alors

$$\begin{cases} \pi_1 \circ e : D \rightarrow A \\ \pi_2 \circ e : D \rightarrow B \end{cases}$$

Pour ce couple, il existe $\langle \pi_1 \circ e, \pi_2 \circ e \rangle : D \rightarrow A \times B$

Du coup, par unicité, on a nécessairement

$$\langle \pi_1 \circ e, \pi_2 \circ e \rangle = e$$

Cette observation donne lieu à :

- une transformation sur les dérivations
- une autre forme de réduction sur les λ -termes

On parle alors d' η -réduction.

On rajoute alors les règles de typage du produit (\times_i) et ($\times_{E,k}$) pour $k \in \{1, 2\}$.

Definition 13 (Somme (coproduit)). Soit A, B . C'est la donnée de $A + B$ avec la propriété universelle suivante :

Si $f : A \rightarrow C$, et $g : B \rightarrow C$, il existe $k : A + B \rightarrow C$ unique, ne dépendant que de f et de g noté $\{f, g\}$, tel que

$$\begin{cases} k \circ in_l = f \\ k \circ in_r = g \end{cases}$$

Par ailleurs, si on se donne

$$e : A + B \rightarrow C$$

Alors

$$\begin{cases} e \circ in_l : A \rightarrow C \\ e \circ in_r : B \rightarrow C \end{cases}$$

Donc

$$\{e \circ in_l, e \circ in_r\} = e$$

On rajoute alors trois règles : (+Ig), (+Id) et (+E)

Part III

λ -calcul simplement typé

1 Quelques Lemmes

Lemma 1. Si $\Delta \vdash t : T$ clos, $FV(t) \subseteq FV(\Delta)$, où $FV(\emptyset) = \emptyset$, et $FV(\Delta, x : S) = FV(\Delta) \cup \{x\}$.

Attention : Un contexte de typage $\Delta \equiv x_1 : S, \dots, x_p : S_p$ où $p \geq 0$ est valide si les variables x_1, \dots, x_p sont distinctes deux à deux.

³Ces égalité correspondent à des β -réduction dans le λ -calcul

On peut rajouter des règles sur la validité de Δ en tant que contexte.

$$\frac{}{\emptyset \text{ contexte valide}}$$

$$\frac{\Delta \text{ contexte valide} \quad T \text{ type} \quad x \notin FV(\Delta)}{\Delta, x : T \text{ contexte valide}}$$

Et on augmente (Hyp).

$$\frac{\Delta \text{ contexte valide} \quad x : T \in \Delta}{\Delta, x : T \text{ contexte valide}} \text{ (Hyp)}$$

Lemma 2 (Affaiblissement). *Si $\Delta \vdash t : T$ et si $\Delta \subseteq \Delta'$, avec Δ' contexte valide, alors $\Delta' \vdash t : T$.*

Proof. Par induction sur la dérivation principale, c'est-à-dire $\Delta \vdash t : T$. Le seul cas “délicat” est lorsque

$$\frac{\Delta, x : U \vdash a : V}{\rightarrow_I}$$

□

Theorem 5. *Si $\Delta \vdash t : T$, alors t est fortement normalisant.*

Proof. Deux parties : poser la notation générale, puis l'adapter à \rightarrow_λ .

1. *Définition générale* : Si $e \in \Lambda$, $e \equiv \lambda \bar{x}. \Delta \bar{u}$ avec $|\bar{x}| > 0$, $|\bar{u}| > 0$ et $\Delta \in \mathcal{X}$ ou bien Δ est un β -redex

- e est en forme normale si $\Delta \in \mathcal{X}$ et chaque u_i est en forme normale
- e est une forme normale de tête (HNF) si $\Delta \in \mathcal{X}$
- si e n'est pas en HNF, c'est-à-dire Δ est un β -redex, Δ est appelé *redex de tête*.

Definition 14. $e \in \Lambda$ est fortement normalisant (SN) s'il n'existe pas de β -réduction infinie issue de e

Exemple

- Ω n'est pas SN
- $(\lambda x. \lambda y. y \Omega)$ n'est pas SN (il existe une dérivation infinie) \rightarrow *attention* : la β -équivalence n'est pas compatible avec la propriété d'être fortement normalisant.

Par contre, si $a =_\beta b$ et b a une NF (resp HNF), alors a a une NF (resp HNF)

De plus :

- Si e a une NF (resp HNF), $\lambda x. e$ a une NF (resp HNF)
- Si e est SN, $\lambda x. e$ est SN

Soit \mathcal{N} l'ensemble des termes SN, et $\mathcal{N}_0 \equiv \{x\bar{u} \mid x\bar{u} \in \mathcal{N}\} \subseteq \mathcal{N}$

Notation

- $e \in \Lambda$, $Succ(e) = \{e' \in \Lambda \mid e\beta_0 e'\}$, et cet ensemble est *fini* (réduction à branchements fini)
- Lemme de Koenig : si un arbre est infini et que cet arbre est a branchement fini, alors il existe un chemin infini

Si $e \in \mathcal{N}$, $\bigcup_{p \geq 0} Succ^p(e)$ est *fini*, de sorte que la définition suivante est bien fondée :

Definition 15. Pour $e \in \mathcal{N}$, $\ell(e)$ désigne la somme des longueurs des chemins de tout réduction issue de e .

Lemma 3. Sont immédiats :

- Si $e \in \mathcal{N}$, alors $\lambda x.e \in \mathcal{N}$
- Si de plus $e' \in \mathcal{N}$ et $e\beta e'$, alors $e' \in \mathcal{N}$
- Si $e \in \Lambda$ tel que $Succ(e) \subseteq \mathcal{N}$, alors $e \in \mathcal{N}$

Proof. Pour le troisième point, soit $e \in \Lambda$ tel que $Succ(e) \subseteq \mathcal{N}$, pour tout $e' \in Succ(e)$, $\ell(e') < \ell(e) \rightarrow$ une récurrence simple sur $\ell(e)$ permet d'établir $\mathcal{P}(e) \equiv "Succ(e) \subseteq \mathcal{N} \text{ implique } e \in \mathcal{N}"$ □

□