

Introduction à la théorie de la démonstration.

1 Formules et preuves.

Définition 1. On se donne un ensemble de *variables propositionnelles*, qui seront notées X, Y, Z , etc. L'ensemble des *formules* est défini par la grammaire :

$$A, B ::= X \mid A \Rightarrow B.$$

Cet ensemble de formules s'appelle le « *fragment implicatif de la logique propositionnelle intuitionniste* ».

Cela peut sembler inhabituel car, généralement, on commence par introduire \neg , \vee et \wedge , car on a en tête les booléens.

Définition 2. Les *séquents*, notés $\Gamma \vdash A$, un couple formé de Γ une *liste* de formules, et A une formule. La liste Γ est une *liste d'hypothèses*. On notera Γ, A la notation pour l'extension de la liste.

Définition 3. On *prouve* (*dérive*) les séquents à l'aides des *règles de déduction* (*d'inférence*) :

$$A \in \Gamma \quad \frac{}{\Gamma \vdash A} \text{Ax} \quad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow_I \quad \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \Rightarrow_E.$$

On les appelle, dans l'ordre, règle de l'*axiome*, règle de l'*introduction de \Rightarrow* et règle de l'*élimination de \Rightarrow* . Il s'agit des règles de déduction naturelle pour le fragment implicatif de la logique propositionnelle intuitionniste.

Définition 4. Le séquent $\Gamma \vdash A$ est *prouvable* s'il existe une *preuve (dérivation)* ayant $\Gamma \vdash A$ à la racine et des axiomes aux feuilles. La formule A est *prouvable* si $\vdash A$ l'est.

Exemple 1.

$$\frac{\frac{\frac{}{X \Rightarrow Y, X \vdash X \Rightarrow Y} \text{Ax} \quad \frac{}{X \Rightarrow Y, X \vdash X} \text{Ax}}{X \Rightarrow Y, X \vdash Y} \Rightarrow_E}{X \Rightarrow Y \vdash X \Rightarrow Y} \Rightarrow_I}{\vdash (X \Rightarrow Y) \Rightarrow (X \Rightarrow Y)} \Rightarrow_I .$$

On écrit généralement des « preuves génériques », en utilisant A, B plutôt que X, Y .

Exemple 2.

$$\frac{\frac{\frac{}{(A \Rightarrow A) \Rightarrow B \vdash (A \Rightarrow A) \Rightarrow B} \text{Ax} \quad \frac{\frac{}{(A \Rightarrow A) \Rightarrow B, A \vdash A} \text{Ax}}{(A \Rightarrow A) \Rightarrow B \vdash A \Rightarrow A} \Rightarrow_I}{(A \Rightarrow A) \Rightarrow B \vdash B} \Rightarrow_E}{\vdash ((A \Rightarrow A) \Rightarrow B) \Rightarrow B} \Rightarrow_I .$$

2 Et en Rocq ?

En Rocq, un objectif de preuve

$$\left. \begin{array}{l} H_1 : A_1 \\ H_2 : A_2 \\ H_3 : A_3 \\ \vdots \end{array} \right\} \Gamma$$

$$A$$

correspond au séquent

$$\Gamma \vdash A.$$

Chaque tactique correspond à des opérations sur l'arbre de preuve. On construit « au fur et à mesure » l'arbre de preuve montrant $\Gamma \vdash A$. Voici ce que quelques tactiques Rocq font.

$$\frac{??}{\Gamma, A, B, A \vdash A} \xrightarrow{\text{assumption}} \frac{}{\Gamma, A, B, A \vdash A} \text{Ax}$$

$$\frac{??}{\Gamma \vdash C} \xrightarrow{\text{assert } A} \frac{\frac{??}{\Gamma, A \vdash B} \quad \frac{??}{\Gamma \vdash A}}{\Gamma \vdash B} \Rightarrow_E$$

$$\frac{??}{\Gamma \vdash C} \xrightarrow{\text{cut } A} \frac{\frac{??}{\Gamma \vdash A \Rightarrow B} \quad \frac{??}{\Gamma \vdash A}}{\Gamma \vdash B} \Rightarrow_E$$

$$\frac{??}{\Gamma \vdash C} \xrightarrow{\text{apply } H} \frac{\frac{}{\Gamma, A \Rightarrow B \vdash A \Rightarrow B} \text{Ax} \quad \frac{??}{\Gamma, A \Rightarrow B \vdash A}}{\Gamma, \underbrace{A \Rightarrow B}_H \vdash B} \Rightarrow_E$$

$$\frac{??}{\Gamma \vdash B \Rightarrow C} \xrightarrow{\text{intro}} \frac{\frac{??}{\Gamma, B \vdash C}}{\Gamma \vdash B \Rightarrow C} \Rightarrow_I$$

3 Liens avec le λ -calcul simplement typé : *correspondance de Curry-Howard*.

Les règles de typage du λ -calcul correspondent aux règles d'inférences du fragment implicatif :

$$\begin{array}{ccc}
 \frac{x : A \in \Gamma \quad \overline{\Gamma \vdash x : A}}{\Gamma, x : A \vdash M : B} & \longleftrightarrow & \frac{A \in \Gamma \quad \overline{\Gamma \vdash A} \text{ Ax}}{\Gamma, A \vdash B} \\
 \frac{\Gamma \vdash \lambda x. M : A \rightarrow B}{\Gamma \vdash M N : B} & \longleftrightarrow & \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow_1 \\
 \frac{\Gamma \vdash M : A \rightarrow B \quad \Gamma \vdash N : A}{\Gamma \vdash M N : B} & \longleftrightarrow & \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow_1
 \end{array}$$

En retirant les λ -termes en bleu (incluant les « : »), et en changeant \rightarrow en \Rightarrow , on obtient exactement les mêmes règles.

Si on sait que $\Gamma \vdash x : A$ alors, en effaçant les parties en bleu, on obtient une preuve de $\hat{\Gamma} \vdash A$.

Inversement, on se donne une preuve de $\Gamma \vdash A$. On se donne des variables x_i pour transformer $\Gamma = A_1, \dots, A_k$ en $\hat{\Gamma} = x_1 : A_1, \dots, x_k : A_k$. Par induction sur $\Gamma \vdash A$, on montre qu'il existe un λ -terme tel que $\hat{\Gamma} \vdash M : A$. On a trois cas.

- ▷ Pour \Rightarrow_1 , par induction, si $\hat{\Gamma}, x = A \vdash M : B$, on déduit $\hat{\Gamma} \vdash \lambda x. M : A \rightarrow B$.
- ▷ Pour \Rightarrow_1 , par induction, si $\hat{\Gamma} \vdash M : A \rightarrow B$ et $\hat{\Gamma} \vdash N : A$, on déduit $\hat{\Gamma} \vdash M N : B$.
- ▷ Pour Ax, on sait $A \in \Gamma$ donc il existe x tel que $x : A \in \hat{\Gamma}$, et on conclut $\hat{\Gamma} \vdash x : A$.

On a les propriétés suivantes pour la relation de déduction :

- ▷ *affaiblissement* : si $\Gamma \vdash B$ (implicitement « est prouvable ») alors $\Gamma, A \vdash B$;
- ▷ *contraction* : si $\Gamma, A, A \vdash B$ alors $\Gamma, A \vdash B$;
- ▷ *renforcement* si $\Gamma, A \vdash B$ alors $\Gamma \vdash B$ à condition qu'on n'utilise pas l'axiome avec l'hypothèse A (celle là uniquement, les A intermédiaires ne posent pas de problèmes) pour déduire B .

▷ *échange* ; si $\Gamma, A, B, \Gamma' \vdash C$ alors $\Gamma, B, A, \Gamma' \vdash C$.

C'est analogue aux propriétés du typage en λ -calcul.

En effet, la propriété de renforcement, très imprécise dans sa formulation logique, est simplement : si $\hat{\Gamma}, x : A \vdash M : B$ alors $\hat{\Gamma} \vdash M : B$ à condition que $x \notin \mathcal{V}\ell(M)$.

Si on veut prouver ces propriétés (au lieu d'utiliser la correspondance de Curry-Howard), on ferait une induction sur la preuve du séquent qui est donné.

La règle

$$\frac{\Gamma \vdash B}{\Gamma, A \vdash B} \text{ aff}$$

est *admissible*. En effet, si on sait prouver les prémisses (ici, $\Gamma \vdash B$) alors on sait prouver la conclusion (ici, $\Gamma, A \vdash B$). Ceci dépend fortement de la logique que l'on utilise.

4 Curry-Howard du côté calcul : les coupures.

Typons un redex :

$$\frac{\frac{\Gamma, x : A \vdash M : B}{\lambda x. M : A \rightarrow B} \Rightarrow_1 \quad \Gamma \vdash N : A}{\Gamma \vdash (\lambda x. M) N : M} \Rightarrow_E.$$

Oui, c'est exactement la même chose que la tactique `assert` en Rocq.

Définition 5. Une *coupure* est un endroit dans la preuve où il y a un usage d'une règle d'élimination (\Rightarrow_E) dont la prémisses principale est déduite à l'aide d'une règle d'introduction (\Rightarrow_1) pour le même connecteur logique.

Remarque 1. Ici, on n'a qu'un seul connecteur logique, \Rightarrow , mais

cela s'étend aux autres connecteurs que l'on pourrait ajouter. La *prémisse principale* est, par convention, la première.

On peut *éliminer une coupure* pour \Rightarrow , c'est-à-dire transformer une preuve (c.f. contracter un β -redex) en passant de

$$\frac{\frac{\delta}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B} \Rightarrow_I \quad \frac{\delta'}{\Gamma \vdash A}}{\Gamma \vdash B} \Rightarrow_E$$

à

$$\frac{\delta[\delta'/A]}{\Gamma \vdash B}$$

où l'on note $\delta[\delta'/A]$ la preuve obtenue en remplaçant dans δ chaque usage de l'axiome avec A par δ' .

On a le même séquent en conclusion (c.f. préservation du typage en λ -calcul simplement typé).

La correspondance de Curry-Howard c'est donc :

$$\begin{array}{lcl} \text{Types} & \longleftrightarrow & \text{Formules} \\ \text{Programmes} & \longleftrightarrow & \text{Preuves} \\ \beta\text{-réduction} & \longleftrightarrow & \text{Élimination d'une coupure} \\ \textit{Programmation} & \longleftrightarrow & \textit{Logique} \end{array}$$

5 Faux, négation, consistance.

On modifie nos formules :

$$A, B ::= X \mid A \Rightarrow B \mid \perp$$

et on ajoute la règle d'élimination du \perp (il n'y a pas de règle d'introduction) :

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A} \perp_E.$$

La négation $\neg A$ est une notation pour $A \Rightarrow \perp$. On peut donc prouver le séquent $\vdash A \Rightarrow \neg\neg A$:

$$\frac{\frac{\frac{\overline{A, \neg A \vdash \neg A} \text{Ax}}{A, \neg A \vdash \perp} \Rightarrow_1}{A \vdash \neg\neg A} \Rightarrow_1}{\vdash A \Rightarrow \neg\neg A} \Rightarrow_E .$$

Théorème 1 (Élimination des coupures). Si $\Gamma \vdash A$ (est prouvable) alors il existe une preuve *sans coupure* de $\Gamma \vdash A$.

Preuve. *c.f.* TD. □

Remarque 2 (Lien avec normalisation forte en λ -calcul simplement typé). Ici, on veut la normalisation faible (« il existe une forme normale ... »). On ne peut pas appliquer *stricto sensu* la normalisation forte pour le λ -calcul simplement typé car le système de type contient \perp .

Lemme 1. Une preuve sans coupure de $\vdash A$ en logique intuitionniste se termine (à la racine) nécessairement par une règle d'introduction.

Preuve. Par induction sur $\vdash A$. Il y a 4 cas.

- ▷ **Ax** : Absurde car $\Gamma = \emptyset$.
- ▷ \Rightarrow_1 : OK
- ▷ \Rightarrow_E : On récupère une preuve de $\vdash B \Rightarrow A$ qui termine (par induction) par une introduction \Rightarrow_1 . Absurde car c'est une coupure.
- ▷ \perp_E : On récupère une preuve de \perp qui termine par une règle d'induction : impossible.

□

Corollaire 1 (Consistance de la logique). Il n’y a pas de preuve de \vdash en logique propositionnelle intuitionniste dans le fragment avec \Rightarrow et \perp .

Preuve. S’il y en avait une, il y en aurait une sans coupure, qui se termine par une règle d’introduction, impossible. \square

6 Et en Rocq ? (partie 2)

On étend les formules avec $\forall, \exists, \neg, \vee, \wedge$, etc. Les preuves sont des λ -termes. En effet, dans une preuve de $\vdash X \rightarrow X \rightarrow X$ on peut écrire

$$\text{exact } (\text{fun } x y \rightarrow x),$$

pour démontrer le séquent.

Le mot clé **Qed** prend le λ -terme construit par la preuve et calcule M' sous forme normale tel que $M \rightarrow_{\beta}^* M'$. La logique de Rocq est *constructive*. C’est-à-dire qu’une preuve de $A \Rightarrow B$ c’est une fonction qui transforme une preuve de A en une preuve de B . Après avoir appelé **Qed**, il est possible d’extraire le λ -terme construit en un programme OCaml, Haskell, etc.

7 Logique intuitionniste vs logique classique.

Dans la logique que l’on a considérée (TD), on a deux règles d’introduction pour \vee :

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee_1^g \quad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee_1^g.$$

Lorsqu’on a une preuve de $A \vee B$, on a, soit une preuve de A , soit une preuve de B . Ce n’est pas une preuve « il est impossible de ne pas avoir A et B ». La logique est *constructive*.

On rappelle que $\neg A := A \rightarrow \perp$, et que l’on se donne la règle d’élimination de \perp :

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A} \perp_E.$$

La *logique classique* est la logique obtenue à l'aide de l'ajout d'une des règles suivantes :

Tiers exclu. $\frac{}{\Gamma \vdash A \vee \neg A}$ tiers exclu

Ce n'est pas constructif : on ne sait pas si l'on a une preuve de $\Gamma \vdash A$ ou de $\Gamma \vdash \neg A$.

Absurde. $\frac{}{\Gamma \vdash (\neg \neg A) \Rightarrow A}$ absurde

C'est mieux : ici, on n'a pas de \vee .

Loi de Peirce. $\frac{}{\Gamma \vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A}$ peirce

C'est encore mieux : ici, on n'a pas de \vee , ni de \perp , mais c'est plus subtil.

En choisissant un de ces axiomes, on a la même notion de prouvabilité.

Exercice 1. Montrons que **absurde** implique **tiers exclu** (au sens de « on peut dériver l'un dans le système incluant l'autre »).

$$\frac{\frac{\frac{\frac{\frac{\frac{\Gamma, \neg(A \vee \neg A), A \vdash A}{\Gamma, \neg(A \vee \neg A), A \vdash A} \text{ax}}{\Gamma, \neg(A \vee \neg A), A \vdash A \vee \neg A} \vee^f}{\Gamma, \neg(A \vee \neg A), A \vdash \neg(A \vee \neg A)} \Rightarrow^f}{\Gamma, \neg(A \vee \neg A), A \vdash \perp} \Rightarrow^i}{\Gamma, \neg(A \vee \neg A) \vdash \neg A} \vee^d}{\Gamma, \neg(A \vee \neg A) \vdash A \vee \neg A} \Rightarrow^E}{\Gamma, \neg(A \vee \neg A) \vdash A \vee \neg A} \Rightarrow^i}{\Gamma, \neg(A \vee \neg A) \vdash \neg(A \vee \neg A)} \text{ax}}{\Gamma \vdash (A \vee \neg A)} \text{absurde}}{\Gamma \vdash A \vee \neg A} \Rightarrow^E$$

Théorème 2 (Glivenko). Une formule A est prouvable en logique classique si et seulement si $\neg \neg A$ est prouvable en logique intuitionniste.

Preuve. Ressemble un peu à la traduction par continuation des programmes **fouine**. □

Corollaire 2. La logique classique est consistante ssi la logique intuitionniste est consistante.

Preuve. Si $\vdash \perp$ en logique intuitionniste alors $\vdash \perp$ en logique classique. Si $\vdash \perp$ en logique classique, alors $\neg \neg \perp$ en intuitionniste,

et on peut en déduire une preuve de $\vdash \perp$ en intuitionniste :

$$\frac{\frac{\text{par hyp.}}{\vdash (\perp \rightarrow \perp) \rightarrow \perp} \quad \frac{\frac{\perp \vdash \perp}{\vdash \perp \rightarrow \perp} \text{ ax}}{\vdash \perp} \Rightarrow_I}{\vdash \perp} \Rightarrow_E .$$

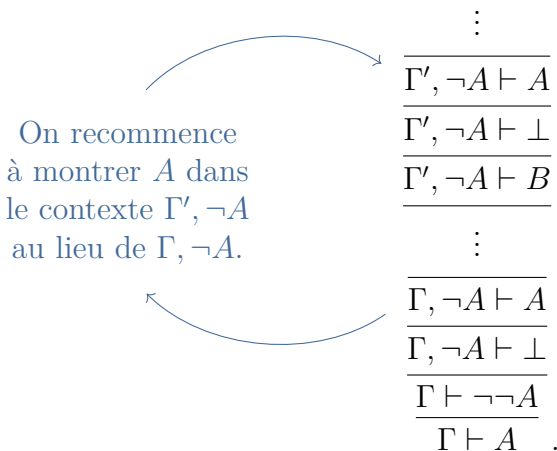
□

8 Logique classique et Curry-Howard : intuition opérationnelle.

On cherche à compléter la correspondance de Curry-Howard :

Types	\longleftrightarrow	Formules
Programmes	\longleftrightarrow	Preuves
β -réduction	\longleftrightarrow	Élimination d'une coupure
Principes classiques	\longleftrightarrow	???
Programmation	\longleftrightarrow	Logique

Avec la preuve par l'absurde, on peut « recommencer dans un contexte différent ».



S'autoriser les principes classiques, c'est savoir utiliser les exceptions : si ça explose, je peux le rattraper. En effet, l'élimination du \perp fait penser à un opérateur comme `raise` : `exn -> 'a`, et la construction `try...with...` pour pouvoir « sauter » à des endroits du programme, et dévier le flot du programme.