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*) :

$$_{A \in \Gamma}\frac{}{\Gamma \vdash A}\,\mathsf{Ax} \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\,\Rightarrow_{\mathsf{I}} \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\,\Rightarrow_{\mathsf{E}}.$$

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.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{X \Rightarrow Y, X \vdash X \Rightarrow Y}\,\mathsf{Ax} \quad \dfrac{}{X \Rightarrow Y, X \vdash X}\,\mathsf{Ax}}{X \Rightarrow Y, X \vdash Y}\,\Rightarrow_{\mathsf{E}}}{X \Rightarrow Y \vdash X \Rightarrow Y}\,\Rightarrow_{\mathsf{I}}}{\vdash (X \Rightarrow Y) \Rightarrow (X \Rightarrow Y)}\,\Rightarrow_{\mathsf{I}} .$$

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

Exemple 2.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{(A \Rightarrow A) \Rightarrow B \vdash (A \Rightarrow A) \Rightarrow B}\,\mathsf{Ax} \quad \dfrac{\dfrac{}{(A \Rightarrow A) \Rightarrow B, A \vdash A}\,\mathsf{Ax}}{(A \Rightarrow A) \Rightarrow B \vdash A \Rightarrow A}\,\Rightarrow_{\mathsf{I}}}{(A \Rightarrow A) \Rightarrow B \vdash B}\,\Rightarrow_{\mathsf{E}}}{\vdash ((A \Rightarrow A) \Rightarrow B) \Rightarrow B}\,\Rightarrow_{\mathsf{I}} .$$

2 Et en Rocq ?

En Rocq, un objectif de preuve

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

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.

$$\frac{??}{\Gamma, A, B, A \vdash A} \xrightarrow[\texttt{assumption}]{} \frac{}{\Gamma, A, B, A \vdash A}\,\mathsf{Ax}$$

$$\frac{??}{\Gamma \vdash C} \xrightarrow[\texttt{assert } A]{} \frac{\dfrac{??}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B} \quad \frac{??}{\Gamma \vdash A}\,\Rightarrow_{\mathsf{E}}$$

$$\frac{??}{\Gamma \vdash C} \xrightarrow[\texttt{cut } A]{} \frac{??}{\Gamma \vdash A \Rightarrow B} \quad \frac{??}{\Gamma \vdash A}\,\Rightarrow_{\mathsf{E}}$$

$$\frac{??}{\Gamma \vdash C} \xrightarrow[\texttt{apply } H]{} \frac{\dfrac{}{\Gamma, A \Rightarrow B \vdash A \Rightarrow B}\,\mathsf{Ax} \quad \dfrac{??}{\Gamma, A \Rightarrow B \vdash A}}{\Gamma, \underbrace{A \Rightarrow B}_{H} \vdash B}\,\Rightarrow_{\mathsf{E}}$$

$$\frac{??}{\Gamma \vdash B \Rightarrow C} \xrightarrow[\texttt{intro}]{} \frac{\dfrac{??}{\Gamma, B \vdash C}}{\Gamma \vdash B \Rightarrow C}\,\Rightarrow_{\mathsf{I}}$$

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

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

$$\frac{x : A \in \Gamma}{\Gamma \vdash x : A} \quad \longleftrightarrow \quad \frac{A \in \Gamma}{\Gamma \vdash A}\ \mathsf{Ax}$$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.\, M : A \to B} \quad \longleftrightarrow \quad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow_{\mathsf{I}}$$

$$\frac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash M\ N : B} \quad \longleftrightarrow \quad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow_{\mathsf{I}}$$

.

En retirant les λ-termes en bleu (incluant les « : »), et en changeant $\to$ 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 $\tilde{\Gamma} \vdash A$.

Inversement, on se donne une preuve de $\Gamma \vdash A$. On se donne des variables x_i pour transformer $\Gamma = A_1, \ldots, A_k$ en $\hat{\Gamma} = x_1 : A_1, \ldots, x_k : A_k$. 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 $\Rightarrow_{\mathsf{I}}$, par induction, si $\hat{\Gamma}, x = A \vdash M : B$, on déduit $\hat{\Gamma} \vdash \lambda x.\, M : A \to B$.
- Pour $\Rightarrow_{\mathsf{I}}$, par induction, si $\hat{\Gamma} \vdash M : A \to B$ 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 $\hat{\Gamma} \vdash x_i : A$.

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* ; su $\Gamma, A, B, \Gamma' \vdash C$ 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

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

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 :

$$\frac{\dfrac{\Gamma, x : A \vdash M : B}{\lambda x.\, M : A \to B}\Rightarrow_{\mathsf{I}} \qquad \Gamma \vdash N : A}{\Gamma \vdash (\lambda x.\, M)\, N : M}\Rightarrow_{\mathsf{E}}.$$

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 ($\Rightarrow_{\mathsf{E}}$) dont la prémisse principale est déduite à l'aide d'une règle d'introduction ($\Rightarrow_{\mathsf{I}}$) 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

$$\dfrac{\dfrac{\dfrac{\delta}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\Rightarrow_{\mathsf{I}} \qquad \dfrac{\delta'}{\Gamma \vdash A}}{\Gamma \vdash B}\Rightarrow_{\mathsf{E}}$$

à

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

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 :

Types	$\longleftrightarrow$	Formules
Programmes	$\longleftrightarrow$	Preuves
β-réduction	$\longleftrightarrow$	Élimination d'une coupure
Programmation	$\longleftrightarrow$	***Logique***

5 Faux, négation, consistance.

On modifie nos formules :

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

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

$$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}\bot_{\mathsf{E}}.$$

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

$$\dfrac{\dfrac{\dfrac{}{A, \neg A \vdash \neg A}\,\mathsf{Ax} \qquad \dfrac{}{A, \neg A \vdash A}\,\mathsf{Ax}}{A, \neg A \vdash \bot}\,\Rightarrow_{\mathsf{E}}}{A \vdash \neg\neg A}\,\Rightarrow_{\mathsf{I}}}{\vdash A \Rightarrow \neg\neg A}\,\Rightarrow_{\mathsf{I}} .$$

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 $\bot$.

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 $\Gamma = \emptyset$.
- ▷ $\Rightarrow_{\mathsf{I}}$: OK
- ▷ $\Rightarrow_{\mathsf{E}}$: on récupère une preuve de $\vdash B \Rightarrow A$ qui termine (par induction) par une introduction $\Rightarrow_{\mathsf{I}}$. Absurde car c'est une coupure.
- ▷ $\bot_{\mathsf{E}}$: On récupère une preuve de $\bot$ 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 $\bot$.

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

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 $\vdash X \to X \to X$ on peut écrire

$$\texttt{exact}\ (\texttt{fun}\ x\ y \texttt{ => } x),$$

pour démontrer le séquent.

Le mot clé `Qed` prend le λ-terme construit par la preuve et calcule M' sous forme normale tel que $M \to_\beta^\star M'$. 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.*