Preuves formelles (2/2)

1 Situation initiale

Dans l'épisode précédent, nous avions vu ce qu'était un arbre de preuve, et les règles d'inférences relatives aux symboles $\bot, \Rightarrow, \wedge, \vee$. En guise de rappel, de remise dans le bain, et pour les avoir sous la main, les voici en vrac :

$$\frac{}{\Gamma, A \vdash A}\ \texttt{ax} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ \bot - \text{elim} \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow - \text{intro} \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \texttt{Modus Ponens}$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge\texttt{-intro} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge - \text{elim}_{\text{g}} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge - \text{elim}_{\text{d}}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee - \text{intro}_{\text{g}} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee - \text{intro}_{\text{d}} \qquad \frac{\Gamma, A \vdash R \qquad \Gamma, B \vdash R \qquad \Gamma \vdash A \vee B}{\Gamma \vdash R}\ \vee - \text{elim}$$

2 Où l'on conte le constructivisme

2.1 L'élement pertubateur

L'épisode précédent s'était clos sur un petit exercice sur les lois dites de De Morgan, laissé en suspens. Lorsque l'on y réfléchit comme nous le ferions usuellement, ou avec des tables de vérité (le soin de la vérification est laissé au lecteur attentif et consciencieux), on établit assez aisément les relations suivantes :

$$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$$

$$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$$

Cependant, si l'on se lance dans les preuves, on est un petit peu plus embêté... on montre facilement $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ et $\neg(A \wedge B) \Leftarrow \neg A \vee \neg B$. Mais la dernière implication bloque : $\neg(A \wedge B) \not\Rightarrow \neg A \vee \neg B$. Regardons ce qu'il se passe, en applicant mécaniquement les règles :

$$\dfrac{\dfrac{\neg(A \wedge B) \vdash ?}{\neg(A \wedge B) \vdash \neg A \vee \neg B}\ \vee\texttt{-intro}}{\vdash \neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B}\ \Rightarrow - \text{intro}$$

On ne sait pas si l'on doit prouver $\neg A$ ou $\neg B$. Essayons avec l'un des deux (ce qui ne change rien), et continuons (on se souvient que $\neg A \equiv A \Rightarrow \bot$) :

$$\dfrac{\dfrac{\dfrac{?}{\neg(A \wedge B), A \vdash \bot}\ ?}{\neg(A \wedge B) \vdash \neg A}\ \Rightarrow - \text{intro}}{\vdots}\ \vee\texttt{-intro}$$

Cette fois, ça y est, on est coincé... notre seule possibilité de déduire $\bot$ serait de se servir de $\neg(A \wedge B)$, mais on ne pourra jamais prouver $A \wedge B$ avec la seule hypothèse A, ce n'est donc pas possible. Ce n'est pas à proprement parler une rigoureuse démonstration de l'impossibilité de la chose, mais celle-ci est vraie, et l'idée principale réside dans ce qui précède.

2.2 Péripéties

En fait, on vient de pointer du doigt une différence essentielle entre le modèle booléen (avec des *vrai* ou *faux*, des 1 ou des 0, ou ce qui vous fait plaisir), et la théorie que l'on s'est donnée avec les règles d'inférences. En fait, la logique que l'on s'est donnée, et qui s'appelle logique intuitionniste, est plus faible que notre logique usuelle (dite classique). Et le modèle booléen est en relation avec cette théorie-là [1].

1. *En fait, modèle n'est pas un mot anodin, et il y a tout un domaine d'études sur la question (la théorie des modèles). Et bien entendu, il existe d'autres modèles permettant de travailler en logique intuitionniste, notamment le modèle de Kripke.*

Cette logique ne permet pas de démontrer tout ce qu'on a l'habitude de connaître, mais possède une propriété extrêmement intéressante : elle est constructive. Ce qui signifie que chaque fois que l'on prouve l'existence de quelque chose, on est en fait capable de le construire. Ce qui n'est pas le cas usuellement, il suffit de regarder le résultat classique suivant :

Théorème 1. *Il existe $x, y \notin \mathbb{Q}$ tels que $x^y \in \mathbb{Q}$.*

Démonstration. Considérons $\sqrt{2}^{\sqrt{2}}$:
- Soit il est rationnel, auquel cas $x = y = \sqrt{2}$ conviennent
- Soit il ne l'est pas, et alors $x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$ convient $((\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$

□

Cette démonstration élémentaire ne choquera personne. Et pourtant, elle pose un problème : le jour où l'on aura réellement besoin des fameux x et y, on sera incapable de faire quoi que ce soit, on ne peut les construire. Cela vient du fait que l'on a raisonné par disjonction de cas : soit un nombre est rationel, soit il ne l'est pas. À l'inverse, en intuitionniste, si l'on arrive par exemple à prouver que pour tout entier a et b il existe q et $r < b$ tels que $a = b * q + r$, votre division euclidienne favorite, c'est que l'on est capable (voir par la suite), étant donnés deux entiers a et b de construire effectivement le quotient et le reste correspondant !

2.3 L'élément de résolution

Ce type de raisonnement s'appuie sur un axiome (i.e. qui ne peut être déduit des règles précédentes), le $tiers - exclus$: $\dfrac{}{\vdash A \vee \neg A}\,\mathtt{te}$. Celui-ci est équivalent à l'axiome de double-négation, que nous connaissons usuellement via le raisonnement par l'absurde : $\dfrac{}{\vdash \neg\neg A \Rightarrow A}\,\mathtt{abs}$. Un troisième axiome relativement classique est lui aussi équivalent aux précédents et mérite d'être mentionner à titre culturel, la loi de Peirce : $\dfrac{}{\vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A}\,\mathtt{peirce}$.

On peut prouver (en jouant sur les bons A et B) $te \Leftrightarrow abs \Leftrightarrow peirce$. Je vous donne l'équivalence la plus facile, comme ça vous pouvez essayer de faire l'autre si ça vous amuse :

• $te \Leftarrow abs$:

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\mathtt{ax} \qquad \dfrac{\dfrac{\dfrac{}{A, \neg\neg A \vdash \neg A \Rightarrow \bot}\,\mathtt{ax} \qquad \dfrac{}{A, \neg\neg A \vdash A}\,\mathtt{ax}}{\neg A, \neg\neg A \vdash \bot}\,\mathtt{MP}}{\neg A, \neg\neg A \vdash A}\,\bot - \mathrm{elim} \qquad A \vee \neg A \vdash \neg\neg A \vdash A \vee \neg A B}{A \vee \neg A, \neg\neg A \vdash A}\,\vee - \mathrm{elim}}{A \vee \neg A \vdash \neg\neg A \Rightarrow A}\,\Rightarrow - \mathrm{intro}}{\vdash A \vee \neg A \Rightarrow (\neg\neg A \Rightarrow A)}\,\Rightarrow - \mathrm{intro}$$

• $abs \Rightarrow te$:

$$\dfrac{\dfrac{[1]}{\vdash \neg\neg(A \vee \neg A)} \qquad \dfrac{}{\neg\neg P \Rightarrow P \vdash \neg\neg(A \vee \neg A) \Rightarrow (A \vee \neg A)}\,\mathtt{ax}}{\neg\neg P \Rightarrow P \vdash A \vee \neg A}\,\mathtt{MP}}{\vdash (\neg\neg P \Rightarrow P) \Rightarrow A \vee \neg A}\,\Rightarrow - \mathrm{intro}$$

[1] :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg(A \vee \neg A), A \vdash A}\,\mathtt{ax}}{\neg(A \vee \neg A), A \vdash (A \vee \neg A)}\,\vee - \mathrm{intro_g} \qquad \dfrac{}{\neg(A \vee \neg A), A \vdash \neg(A \vee \neg A)}\,\mathtt{ax}}{\neg(A \vee \neg A), A \vdash \bot}\,\mathtt{MP}}{\neg(A \vee \neg A) \vdash \neg A}\,\Rightarrow - \mathrm{intro}}{\neg(A \vee \neg A) \vdash (A \vee \neg A)}\,\vee - \mathrm{intro} \qquad \dfrac{}{\neg(A \vee \neg A) \vdash (A \vee \neg A) \Rightarrow \neg}\,\mathtt{ax}}{\neg(A \vee \neg A) \vdash \bot}\,\mathtt{MP}}{\vdash \neg\neg(A \vee \neg A)}\,\Rightarrow - \mathrm{intro}$$

Remarques
- Les preuves commencent à être longues, et on s'imagine assez aisément que ça ne peut qu'aller en s'empirant. Aussi, on peut s'autoriser à se servir de règles dites admissibles, notées $\dfrac{\text{Hyp1} \vdash \text{Res1}}{\text{Hyp2} \vdash \text{Res2}}$ qui signifient moralement qu'on peut passer de la ligne du dessus à celle du-dessous avec un arbre de preuve complet : $\dfrac{\text{Hyp1} \vdash \text{Res1}}{\vdots}$ $\dfrac{}{\text{Hyp2} \vdash \text{Res2}}$. En quelque sorte, on ne fait que le replier, mais c'est bien pratique. De façon générale, on peut couper des petits bouts pour les réécrire ailleurs, etc...

– Dans la deuxième preuve, on constate que j'ai allègrement remplacé P par $A \vee \neg A$, en décrétant que c'était vrai pour tout P. On va voir par la suite comment formaliser ce genre de chose.

2.4 Situation Finale

On dispose donc de deux niveaux de logique : la logique classique, qui porte bien son nom, et qui n'est pas constructive, mais permet de prouver plus de choses que la logique intuitionniste, qui elle est constructive, ce qui offre des perspectives intéressantes (comme vous allez le constater par la suite). Vous pouvez aussi vérifier que l'implication qui nous manquait est facile à prouver en disposant du tiers-exclu, et est donc vraie en logique classique (ce que l'on savait un petit peu grâce au modèle booléen).

3 Où tout n'est qu'histoire de quantité

En maths, dès lors que l'on cherche à formaliser des propriétés un tant soit peu intéressante, on a besoin d'expliciter quand celle-ci est valable : tout le temps, pour certaine bonne valeurs, jamais. Pour cela, on dispose de deux notions, qui vous sont peut-être déjà familières : *il existe* x (notée $\exists x.$) et *pour tout* x (notée $\forall x$). Les grandes choses à savoir sont que ces quantificateurs ne commutent pas, c'est-à-dire qu'on ne peut pas les inverser (par exemple, on a facilement que $\forall m \in \mathbb{N}, \exists n \in \mathbb{N}, n > m$, alors que $\exists n \in \mathbb{N}, \forall m \in \mathbb{N}, n > m$ est très très faux). Et la deuxième chose, c'est que le contraire de *il fait beau tous les jours* est *il existe un jour où il ne fait pas beau* et non *il ne fait jamais beau.*

3.1 Les règles d'inférences

Maintenant que vous êtes rodés, vous pouvez appréhender les quantificateurs directement par les règles d'inférences qui leur sont liées.

$$\exists - \text{intro}: \quad \frac{\Gamma \vdash A\{x := t\}}{\Gamma \vdash \exists x.A} \qquad \exists - \text{elim}: \quad \frac{\Gamma, A\{x := t\} \vdash B}{\Gamma, \exists x.A \vdash B}$$

$$\forall - \text{intro}: \quad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}\ x \notin \Gamma \qquad \forall - \text{elim}: \quad \frac{\Gamma, A\{x := t\} \vdash B}{\Gamma, \forall x.A \vdash B}$$

L'idée pour l'introduction du $\exists$ est un petit peu la même que pour l'introduction du $\vee$: on dispose d'un témoin, et on dit juste qu'on sait qu'il en existe un, tout comme l'on disposait de A pour introduire $A \vee B$. Cette quantification est donc constructive (rien de surprenant), puisque pour dire qu'il existe x vérifiant une certaine propriété, il faut d'abord en disposer d'un de façon effective (c'est le t). Et l'élimination est aussi dans le même esprit que pour le *ou*. Pour le pour tout, on remarque qu'il ne faut pas que le x sur lequel on quantifie soit présent dans le contexte, en effet, sinon on généraliserait sur quelqu'un de particulier dont on sait des choses dans les hypothèses.

Exercice 1. *De même, essayez de trouver un lien entre :*

- $\neg(\exists x.A)$
- $\neg(\forall x.A)$
- $\exists x.(\neg A)$
- $\forall x.(\neg A)$

Et de même, si l'on n'admet pas le tiers-exclu dans nos axiomes, l'une des quatre implications, ne sera pas prouvable, laquelle ?

3.2 Où l'on voit les effets du non-constructivisme

Le paradoxe suivant, dû à Raymond Smullyan, montre que notre esprit n'est pas non plus complètement formé aux conséquences du non-constructivisme.

Dans tout bar, il existe quelqu'un tel que lorsqu'il boit, tout le monde boit

Ce qui peut se formaliser comme suit, pour toute propriété P :

$$\exists y, (P(y) \Rightarrow \forall x.P(x))$$

Surprenant et même difficile à admettre à première vue... et pourtant ! L'idée est la suivante (je ferai peut-être une fiche d'exercice détaillée pour une vraie preuve formelle) :

– soit tout le monde boit, et dans ce cas qui que l'on prenne, il ne saurait invalider la propriété : il boit, et tout le monde boit.
– soit tout le monde ne boit pas, et il existe au moins une personne ne buvant pas dans le bar. Si l'on considère cette personne, elle vérifie bien la propriété, puisqu'elle invalide le prémisse de l'implication, et donc valide l'implication tout entière.

4 La correspondance de Curry-Howard

Je ne rentrerai pas ici dans les détails, et l'on en restera donc à une logique assez minimaliste (avec seulement des $\Rightarrow$). L'intérêt principale de la logique intuitionniste, vous disais-je, est son caractère constructif, et que lorsque l'on prouve un résultat, c'est qu'on est capable de construire les objets correspondants. Une façon naturelle de le faire est de se servir... du λ-calcul !

En effet, comparez les règles suivantes, les unes sont relatives au typage d'un λ-terme, les autres sont des règles d'inférences :

$$\frac{}{\Gamma, A \vdash A}\ \texttt{ax} \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \texttt{Modus Ponens} \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow -\text{intro}$$

$$\frac{}{\Gamma \vdash x : A}\ (x : A) \in \Gamma \qquad \frac{\Gamma \vdash T : A \to B \qquad \Gamma \vdash U : A}{\Gamma \vdash TU : B}\ @ \qquad \frac{\Gamma, x : A \vdash T : B}{\Gamma \vdash \lambda x.T : A \to B}\ \lambda$$

À la tête de la flèche près, on a quand même envie de dire que c'est la même chose. C'est le principe de la correspondance de Curry-Howard. De fait, désormais, pour prouver un résultat, on pourra aussi bien en donner une preuve sous forme d'arbre d'inférence qu'un λ-terme dont le type est le résultat demandé, puisqu'au final l'arbre de typage et celui de preuve serait les mêmes. Par exemple,

- $\lambda x.x$ est un terme de preuve de $A \Rightarrow A$
- une preuve de $A \Rightarrow (A \Rightarrow B) \Rightarrow B$ est fournie par $\lambda x f.f(x)$

Exercice 2. *Sauriez-vous donnez des termes de preuves pour les résultats suivants :*

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

Pour les autres règles d'inférences, on a besoin en fait de typage et de structures un tout petit peu plus compliquées (comme la paire), mais cela ne change rien sur l'idée générale. Le tout étant d'avoir pour chaque règle d'inférence une règle de typage correspondante. Et puis après, pour changer, on fait une preuve par induction.

5 En guise de conclusion

Tout d'abord, si par hasard ce genre de choses vous amuse follement (ça peut arriver, j'en sais quelque chose), il y a un logiciel pour faire des preuves formelles qui est complètement dans l'esprit de ce que je vous ai présenté. Ça s'appelle Coq, ça ne sert globalement qu'aux chercheurs, mais c'est plutôt marrant. On peut le télécharger à l'adresse suivante : http://coq.inria.fr/download. On trouve au même endroit la documentation officielle, qui est par contre en anglais. Si vous avez la moindre envie d'essayer, n'hésitez pas à me le dire, je me ferais un plaisir de vous faire un mini-tutorial de prise en main.

En dehors de ça, vous avez découvert les deux logiques principales. Il en existe quelques autres, mais à ma connaissance, soit elles sont trop exotiques, inutilisables et sans grand intérêt, soit elles sont proches de celle-ci. L'autre logique qui est très utilisée est la logique linéaire, qui est exactement aussi "puissante" que la logique intuitionniste, mais est plus expressive. Et il y a aussi une version du λ-calcul qui lui est directement liée.

Enfin, depuis peu, on sait aussi faire Curry-Howard en logique classique [2]. On se sert pour ça d'un opérateur qu'on rajoute aux termes de base et qui a le type de la loi de Peirce. Mais c'est une autre histoire...

The end.

2. *Pour ne rien vous cacher, on savait plus ou moins faire, en reposant sur le fait que $\neg\neg te$ est vrai en intuitionniste, mais c'était très pénible...*