Introduction à la théorie de la démonstration, Partie 1/2

Béranger Seguin

22 octobre 2022

Sommaire

Pourquoi ce cours ?

But

Faire un horizon panoramique de la théorie de la démonstration, comprendre ce qu'est une preuve et ce qu'on peut en faire ; comprendre les théorèmes d'incomplétude de Gödel et la correspondance de Curry-Howard (toute preuve est un programme informatique !).

... en évitant la formalisation lourde (plein de petits détails) et en essayant de mettre en avant les idées-clés !

Introduction

En maths : *objets*, *opérations*, *sous-classes particulières*

Objet	Opérations	Sous-classes
Nombres	Addition, multiplication	Nombres premiers, entiers pairs
Ensembles	Intersection, produit	Finis, indénombrables
Figures	Rotation, translation	Rectangles, losanges

Introduction

En maths : *objets*, *opérations*, *sous-classes particulières*

Objet	Opérations	Sous-classes
Nombres	Addition, multiplication	Nombres premiers, entiers pairs
Ensembles	Intersection, produit	Finis, indénombrables
Figures	Rotation, translation	Rectangles, losanges

Philosophie (Point de départ de la théorie de la démonstration)

Les démonstrations mathématiques sont des objets mathématiques à part entière, qu'on peut étudier de façon mathématique.

- **Opérations** : *règles de déduction*, la *normalisation*...
- **Classes particulières** : preuves *sans coupures*, preuves *intuitionnistes*...

Point Terminologie

Dans ce qui suit :

Preuve = Démonstration

Énoncé = Proposition

« A est faux » est une abréviation pour « $\mathrm{Non}(A)$ est vrai » : on ne suppose pas a priori que tout énoncé soit ou vrai ou faux (on en reparlera)

Les preuves « ordinaires »

Preuve

Montrons qu'il y a une infinité de nombres premiers. On raisonne par l'absurde en supposant qu'il y a un nombre fini de nombres premiers qu'on note $p_1, p_2, \ldots, p_r$. On considère l'entier $P := p_1 \times p_2 \times \ldots p_r + 1$, qui est supérieur à 2 puisqu'il existe au moins un nombre premier (par exemple, 2), et qui est donc divisible par un nombre premier, disons p_i. Cependant, le reste dans la division euclidienne de P par p_i est 1, donc P ne peut pas être divisible par p_i. Cette contradiction montre que notre hypothèse de départ est erronée.

Les preuves « ordinaires »

Preuve

Montrons qu'il y a une infinité de nombres premiers. On raisonne par l'absurde en supposant qu'il y a un nombre fini de nombres premiers qu'on note $p_1, p_2, \ldots, p_r$. On considère l'entier $P := p_1 \times p_2 \times \ldots p_r + 1$, qui est supérieur à 2 puisqu'il existe au moins un nombre premier (par exemple, 2), et qui est donc divisible par un nombre premier, disons p_i. Cependant, le reste dans la division euclidienne de P par p_i est 1, donc P ne peut pas être divisible par p_i. Cette contradiction montre que notre hypothèse de départ est erronée.

Problème : trop elliptique et peu structuré pour être étudié tel quel
$\rightsquigarrow$ on va redéfinir la notion de démonstration
Cependant : garder en tête que ce genre de preuves sont formalis**ables** !

Le langage

Il faut définir ce qu'est un *énoncé* avant d'essayer d'en démontrer...

Le langage

Il faut définir ce qu'est un *énoncé* avant d'essayer d'en démontrer...
Les énoncés sont construits à partir d'un *langage* :

Definition (Langage, à la louche)

Un *langage* est un ensemble de *symboles*, par exemple :

$$0, \emptyset, 1, \int, +, -, \times, \cap, \cup, =, \geq, \text{Successeur}, \mathbb{Z}, \ldots$$

munis de règles de « grammaire » : par exemple, le symbole $+$ prend un élément à gauche et un à droite. Les symboles représentent des éléments, des fonctions ou des relations...
En revanche, le langage n'attribue aucune propriété particulière ni *sens* à ces symboles : ils ne sont que des symboles.

Il y a aussi des *variables* : on utilisera typiquement x, y, etc.

Les termes

Les termes sont en quelque sorte les « objets décrits par une phrase grammaticalement valide » à partir de notre langage. Plus précisément :

Definition

- Les symboles de constante et de variables sont des termes ;
- Si f est un symbole de fonction prenant n paramètres, et que $T_1, T_2, \ldots, T_n$ sont des termes, alors $f(T_1, T_2, \ldots, T_n)$ est un terme.

Il ne faut pas s'offusquer de l'apparente circularité de la preuve : on peut définir des termes de « niveau » de plus en plus élevé (définition inductive).

Exemple

$2 + 2$; $4x - 2$; $(X \cap Y)^5 \cup (\mathbb{R} \setminus X)$; $\mathrm{Successeur}(n) - 1$; ...

Non-exemple

$4 + 2 = 4$; $5 \times (2+)$; $x(x)$; $\exp(a, b, c)$; ...

Les énoncés atomiques

Commençons par les plus simples des énoncés, les « briques élémentaires », les *énoncés atomiques* :

Definition (Énoncés atomiques, à la louche)

Les énoncés *atomiques* sont ceux de la forme :

$$R(T_1, T_2, \ldots, T_n)$$

où R est un symbole de relation à n paramètres, et les T_i sont des termes. De plus, on a un énoncé atomique particulier : $\bot$ (lu « Faux »).

Les énoncés atomiques

Commençons par les plus simples des énoncés, les « briques élémentaires », les *énoncés atomiques* :

Definition (Énoncés atomiques, à la louche)

Les énoncés *atomiques* sont ceux de la forme :

$$R(T_1, T_2, \ldots, T_n)$$

où R est un symbole de relation à n paramètres, et les T_i sont des termes. De plus, on a un énoncé atomique particulier : $\bot$ (lu « Faux »).

Exemple (Énoncés atomiques)

$2 + 2 = 4$; $4x - 2 \leq \pi$; $X \cap Y \subset \mathcal{P}(\mathbb{Z})$; $\mathrm{Successeur}(n) \geq n$; $\bot$; ...

Non-exemple (Pas des énoncés !)

$4 + 2$; $(2 \leq x) \geq 5$; $(9+)-$; $x \times x = \bot$; $\mathrm{Successeur} = 1+$; ...

Les énoncés

Enfin, on peut définir des énoncés plus complexes :

Les énoncés

Enfin, on peut définir des énoncés plus complexes :

Definition (Énoncé)

- Les énoncés atomiques sont des énoncés ;
- Si E et E' sont des énoncés, on définit les énoncés suivants :
  - « E et E' » ;
  - « E ou E' » ;
  - « Si E alors E'. », qu'on notera aussi « $E \Rightarrow E'$ ».

Les énoncés

Enfin, on peut définir des énoncés plus complexes :

Definition (Énoncé)

- Les énoncés atomiques sont des énoncés ;
- Si E et E' sont des énoncés, on définit les énoncés suivants :
  - « E et E' » ;
  - « E ou E' » ;
  - « Si E alors E'. », qu'on notera aussi « $E \Rightarrow E'$ ».
- Si E est un énoncé qui dépend d'une variable x (condition technique : la variable doit être libre), on définit :
  - « Pour tout x, E » (à interpréter comme « E est vrai quelle que soit la valeur prise par x ») ;
  - « Il existe x tel que E » (à interpréter comme « Il existe une valeur de x qui rende E vrai »).

(La définition des énoncés est également une définition inductive.)

La négation

Les plus attentifves auront remarqué qu'on n'a pas défini l'énoncé $\mathrm{Non}(P)$, lorsque P est un énoncé.
En fait, $\mathrm{Non}(P)$ n'est qu'une abréviation pour :

$$P \Rightarrow \bot.$$

Dire que P est faux revient donc à dire que, de P, je peux déduire une absurdité.
Ce choix permet d'avoir un système « parcimonieux » : plutôt que de formuler des règles concernant Non et des règles concernant $\Rightarrow$, on n'a qu'à traiter le cas de l'implication.

Syntaxe/sémantique, partie 1

- Attention ! Tant qu'on n'a pas de règles de déduction, les symboles et , ou , $\Rightarrow$ etc. sont **purement syntaxiques** !

Syntaxe/sémantique, partie 1

- Attention ! Tant qu'on n'a pas de règles de déduction, les symboles $\wedge$ et , $\vee$ ou , $\Rightarrow$ etc. sont **purement syntaxiques** !
- Les règles de déduction permettront d'assurer qu'ils se comportent à peu près comme on s'y attend, mais la démarche de démonstration reste **formelle**, c'est-à-dire qu'il s'agit de manipuler de la syntaxe.

Syntaxe/sémantique, partie 1

- Attention ! Tant qu'on n'a pas de règles de déduction, les symboles $\wedge$ et , $\vee$ ou , $\Rightarrow$ etc. sont **purement syntaxiques** !
- Les règles de déduction permettront d'assurer qu'ils se comportent à peu près comme on s'y attend, mais la démarche de démonstration reste **formelle**, c'est-à-dire qu'il s'agit de manipuler de la syntaxe.
- La même chose est vraie pour les symboles quand on les compare aux objets qu'on essaie de leur faire signifier : le symbole 0 désigne le « vrai nombre zéro » avant tout dans la tête du mathématicien. Les axiomes essaieront de contraindre son comportement pour l'y faire ressembler autant que possible, mais on verra que c'est impossible.

Syntaxe/sémantique, partie 1

- Attention ! Tant qu'on n'a pas de règles de déduction, les symboles $\wedge$ et , $\vee$ ou , $\Rightarrow$ etc. sont **purement syntaxiques** !
- Les règles de déduction permettront d'assurer qu'ils se comportent à peu près comme on s'y attend, mais la démarche de démonstration reste **formelle**, c'est-à-dire qu'il s'agit de manipuler de la syntaxe.
- La même chose est vraie pour les symboles quand on les compare aux objets qu'on essaie de leur faire signifier : le symbole 0 désigne le « vrai nombre zéro » avant tout dans la tête du mathématicien. Les axiomes essaieront de contraindre son comportement pour l'y faire ressembler autant que possible, mais on verra que c'est impossible.
- On reparlera des liens syntaxe/sémantique, où la sémantique désigne la notion non-mathématique de *ce qui est vrai, qu'on arrive à le prouver ou non*. Dans certains contextes, on peut donner un sens au mot « vrai » (qui reste surtout une notion empirique).

Idée de la définition de preuve

On va commencer à définir la notion de preuve.
Dans l'idée, une preuve est toujours une preuve *de quelque chose* à partir *d'axiomes* : on ne peut pas déduire grand chose sans point de départ.

Idée de la définition de preuve

On va commencer à définir la notion de preuve.
Dans l'idée, une preuve est toujours une preuve *de quelque chose* à partir *d'axiomes* : on ne peut pas déduire grand chose sans point de départ.
Soit un ensemble d'énoncés $\mathcal{A}$ et un énoncé P. Démontrer P à partir (des axiomes) de $\mathcal{A}$, c'est faire des opérations sur les énoncés de $\mathcal{A}$ (parmi une liste d'opérations licites) et obtenir, à la fin, l'énoncé P.
Une telle série de déductions peut se noter sous la forme d'un arbre, qu'on lit « De $\mathcal{A}$, je déduis P » :

$$\frac{\mathcal{A}}{\begin{array}{c}\vdots\\ P\end{array}}$$

Idée de la définition de preuve

On va commencer à définir la notion de preuve.
Dans l'idée, une preuve est toujours une preuve *de quelque chose* à partir *d'axiomes* : on ne peut pas déduire grand chose sans point de départ.
Soit un ensemble d'énoncés $\mathcal{A}$ et un énoncé P. Démontrer P à partir (des axiomes) de $\mathcal{A}$, c'est faire des opérations sur les énoncés de $\mathcal{A}$ (parmi une liste d'opérations licites) et obtenir, à la fin, l'énoncé P.
Une telle série de déductions peut se noter sous la forme d'un arbre, qu'on lit « De $\mathcal{A}$, je déduis P » :

$$\begin{array}{c} \mathcal{A} \\ \hline \vdots \\ \hline P \end{array}$$

But

Préciser la forme de ces arbres et les opérations licites (les règles de déduction).

« Définition » de preuve

Definition (Preuve)

Une preuve (modulo un ensemble d'énoncés $\mathcal{A}$: les axiomes) est un arbre d'une des formes suivantes :

- Un axiome de $\mathcal{A}$;
- Un arbre de la forme :

$$\frac{P_1 \qquad \dots \qquad P_r}{Q}$$

où $P_1, \dots, P_r$ sont des preuves, où Q est un énoncé (qu'on appelle « *conclusion* » de la preuve), et où l'arbre obtenu en remplaçant les preuves $P_1, \dots, P_r$ par leurs conclusions appartient à la liste (qu'on va décrire) des règles de déduction.

« Définition » de preuve

Definition (Preuve)

Une preuve (modulo un ensemble d'énoncés $\mathcal{A}$: les axiomes) est un arbre d'une des formes suivantes :

- Un axiome de $\mathcal{A}$;
- Un arbre de la forme :

$$\frac{P_1 \qquad \dots \qquad P_r}{Q}$$

où $P_1, \dots, P_r$ sont des preuves, où Q est un énoncé (qu'on appelle « *conclusion* » de la preuve), et où l'arbre obtenu en remplaçant les preuves $P_1, \dots, P_r$ par leurs conclusions appartient à la liste (qu'on va décrire) des règles de déduction.

La définition est un peu tarabiscotée... Des questions ?

« Définition » de preuve

Definition (Preuve)

Une preuve (modulo un ensemble d'énoncés $\mathcal{A}$: les axiomes) est un arbre d'une des formes suivantes :

- Un axiome de $\mathcal{A}$;
- Un arbre de la forme :

$$\frac{P_1 \qquad \dots \qquad P_r}{Q}$$

où $P_1, \dots, P_r$ sont des preuves, où Q est un énoncé (qu'on appelle « *conclusion* » de la preuve), et où l'arbre obtenu en remplaçant les preuves $P_1, \dots, P_r$ par leurs conclusions appartient à la liste (qu'on va décrire) des règles de déduction.

La définition est un peu tarabiscotée... Des questions ?
... Il reste à donner la liste des règles de déduction, pour compléter cette définition !

Premières règles de déduction

Les règles de déduction sont de « tout petits bouts d'arbres » qui permettent de passer d'un étage au suivant, comme des fragments insécables de raisonnement mathématique. C'est en les combinant qu'on fera des arbres plus compliqués.

Question

Voici trois règles de déduction, pour commencer. Comment les lit-on ? Que signifient-elles ?

$$\frac{A \qquad B}{A \text{ et } B}$$

$$\frac{A \text{ et } B}{A}$$

$$\frac{A \text{ et } B}{B}$$

Introduction et élimination du et

Félicitations à celleux qui auront trouvé : ces règles permettent d'introduire et d'éliminer le connecteur « et ».

Règle (Introduction et élimination du « et »)

$$\frac{A \qquad B}{A \text{ et } B}\ \text{(Iet) : Règle d'introduction du « et »}$$

$$\frac{A \text{ et } B}{A}\ \text{(Eet) : Règle d'élimination du « et » (à gauche)}$$

$$\frac{A \text{ et } B}{B}\ \text{(Eet) : Règle d'élimination du « et » (à droite)}$$

Une première preuve à faire

À l'aide de ces quelques règles, on peut faire une première preuve un peu plus compliquée.

Une première preuve à faire

À l'aide de ces quelques règles, on peut faire une première preuve un peu plus compliquée.

Exercice

Soit A et B des énoncés quelconques. De « A et B », déduisez « B et A » !

Je rappelle les règles :

Règle (Introduction et élimination du « et »)

$$\frac{A \qquad B}{A \text{ et } B}\ (\text{Iet}) : \text{Règle d'introduction du « et »}$$

$$\frac{A \text{ et } B}{A}\ (\text{Eet}) : \text{Règle d'élimination du « et » (à gauche)}$$

$$\frac{A \text{ et } B}{B}\ (\text{Eet}) : \text{Règle d'élimination du « et » (à droite)}$$

Une première preuve achevée !

Preuve (Déduisons « B et A » de « A et B »)

Voici l'arbre correspondant :

$$\dfrac{\dfrac{A \text{ et } B}{B}\,(\text{Eet}) \qquad \dfrac{A \text{ et } B}{A}\,(\text{Eet})}{B \text{ et } A}\,(\text{Iet})$$

Une première preuve achevée !

Preuve (Déduisons « B et A » de « A et B »)

Voici l'arbre correspondant :

$$\dfrac{\dfrac{A \text{ et } B}{B}\,(\text{Eet}) \qquad \dfrac{A \text{ et } B}{A}\,(\text{Eet})}{B \text{ et } A}\,(\text{Iet})$$

Remarque

On a implicitement utilisé le fait qu'on peut utiliser un axiome plusieurs fois (ou pas du tout !). Certaines logiques alternatives ne prennent pas pour acquis ce principe !

Une parenthèse... pleine de conséquences

Si, à partir des axiomes de $\mathcal{A}$, on a des preuves de P_1 et de P_2, on peut utiliser (Iet) pour former l'arbre :

$$\dfrac{\dfrac{\mathcal{A}}{\vdots}\quad\dfrac{\mathcal{A}}{\vdots}}{\dfrac{P_1 \qquad P_2}{P_2 \text{ et } P_2}\,(\text{Iet})}$$

Autrement dit, on peut voir (Iet) comme une opération sur les preuves, plus précisément une opération qui prend une preuve de P_1 et une preuve de P_2 et qui renvoie une preuve de « P_1 et P_2 ».

Philosophie

Les règles de déduction sont des opérations sur les preuves.

Question

Comment faut-il voir (Eet) selon cette philosophie ? Et les axiomes ?

Le cas de la disjonction

Règle (Introduction du ou)

$$\frac{A}{A \text{ ou } B}\ (\text{Iou})$$

$$\frac{B}{A \text{ ou } B}\ (\text{Iou})$$

Question

Comment éliminer ce connecteur ?

Le cas de la disjonction

Règle (Introduction du ou)

$$\frac{A}{A \text{ ou } B}\ (\text{Iou})$$

$$\frac{B}{A \text{ ou } B}\ (\text{Iou})$$

Question

Comment éliminer ce connecteur ?

Règle (Disjonction de cas : élimination de « ou » , mais aussi de l'implication)

$$\frac{A \text{ ou } B \qquad \text{Si } A \text{ alors } C \qquad \text{Si } B \text{ alors } C}{C}\ (\text{DC})$$

Le cas de l'implication 1/2

Règle (Modus ponens : élimination de l'implication)

$$\frac{A \qquad \text{Si } A \text{ alors } B}{B} \text{ (MP)}$$

Exercice

En fait, cette règle se déduit de (DC) et de (Iou)... Le montrer !

Question

Comment introduire une implication ?

Le cas de l'implication 1/2

Règle (Modus ponens : élimination de l'implication)

$$\frac{A \qquad \text{Si } A \text{ alors } B}{B} \text{ (MP)}$$

Exercice

En fait, cette règle se déduit de (DC) et de (Iou)... Le montrer !

Question

Comment introduire une implication ?

L'idée est la suivante : si d'un ensemble d'axiomes $\mathcal{A}$ auquel j'ajoute l'énoncé P, je peux démontrer Q, alors $\mathcal{A}$ démontre $P \Rightarrow Q$...

Le cas de l'implication 2/2

On notera la règle correspondante de la manière suivante (qui n'est pas la plus fréquente, mais que je trouve pédagogique ici) :

Règle (Introduction de l'implication)

$$\dfrac{\mathcal{A} \quad \boxed{\begin{array}{c} \mathcal{A} \quad B \\ \hline \vdots \\ \hline C \end{array}}}{\text{Si } B \text{ alors } C}\ (\mathrm{I}\Rightarrow)$$

Attention : l'arbre suivant n'est *pas* un énoncé : $\boxed{\begin{array}{c} \mathcal{A} \qquad B \\ \hline \vdots \\ \hline C \end{array}}$

En effet, c'est bien de $\mathcal{A}$ qu'on déduit « Si B alors C » : l'ajout de ce « faux énoncé » n'est qu'une manière de préciser *pourquoi* on peut utiliser la règle (I⇒).

Parenthèse 2.1

Question

Comment (I⇒) s'inscrit-elle dans la philosophie « Les règles de déduction sont des opérations ? » ?

Parenthèse 2.1

Question

Comment (I⇒) s'inscrit-elle dans la philosophie « Les règles de déduction sont des opérations ? » ?

Réponse

C'est la plus subtile des règles ! En fait, (I⇒) peut être vue comme une opération :

- Qui prend en entrée une preuve de $\mathcal{A}$ et une **fonction** qui transforme une preuve de $\mathcal{A}$ et de B en preuve de C
- Qui renvoie une preuve de $B \Rightarrow C$.

Comprenez-vous pourquoi ?

Parenthèse 2.2

Explication : L'arbre de preuve $\boxed{\begin{array}{c} \mathcal{A} \qquad B \\ \hline \vdots \\ \hline C \end{array}}$ peut être vu comme une fonction qui à une preuve de $\mathcal{A}$ et de B associe une preuve de C (en ajoutant toutes les étapes de déduction contenues dans la boîte).

On peut être plus radical en disant qu'une preuve de $B \Rightarrow C$ **est** une fonction qui à toute preuve de B associe une preuve de C ! (ce point de vue sera important quand on parlera des liens avec l'informatique)

Une règle de plus : le principe d'explosion

Règle (Ex Falso Quodlibet)

$$\frac{\bot}{A}\ (\text{EFQ})$$

De $\bot$, on peut déduire n'importe quel énoncé !

Si on montre P et $\mathrm{Non}(P)$ pour un énoncé P, on en déduit $\bot$ et donc n'importe quel énoncé : une incohérence dans les axiomes entraîne l'inutilité complète du système !
Cette règle est utile pour manipuler les négations (on rappelle que $\mathrm{Non}(A) = (A \Rightarrow \bot)$). Par exemple :

Exercice

Montrer (sans axiomes, pour un énoncé A quelconque) que $A \Rightarrow \mathrm{Non}(\mathrm{Non}(A))$?

Une règle de plus : le principe d'explosion

Règle (Ex Falso Quodlibet)

$$\frac{\bot}{A}\ (\text{EFQ})$$

De $\bot$, on peut déduire n'importe quel énoncé !

Si on montre P et $\mathrm{Non}(P)$ pour un énoncé P, on en déduit $\bot$ et donc n'importe quel énoncé : une incohérence dans les axiomes entraîne l'inutilité complète du système !
Cette règle est utile pour manipuler les négations (on rappelle que $\mathrm{Non}(A) = (A \Rightarrow \bot)$). Par exemple :

Exercice

Montrer (sans axiomes, pour un énoncé A quelconque) que $A \Rightarrow \mathrm{Non}(\mathrm{Non}(A))$?

Indication : Vu ce qu'on a dit sur l'implication, cela revient à montrer $\mathrm{Non}(\mathrm{Non}(A))(= \mathrm{Non}(A) \Rightarrow \bot)$ sous l'hypothèse A ; et donc, cela revient à montrer $\bot$ sous les hypothèses A et $\mathrm{Non}(A)$ (càd $A \Rightarrow \bot$).

Preuve de $A \Rightarrow \mathrm{Non}(\mathrm{Non}(A))$

La preuve tient dans cet arbre :

$$\dfrac{\dfrac{\dfrac{\dfrac{A \quad A \Rightarrow \bot}{\bot}\,(\mathrm{MP})}{(A \Rightarrow \bot) \Rightarrow \bot}\,(\mathrm{I}\Rightarrow)}{A \Rightarrow ((A \Rightarrow \bot) \Rightarrow \bot)}\,(\mathrm{I}\Rightarrow)}$$

Là encore, il faut se rappeler que $\mathrm{Non}(A)$ signifie $A \Rightarrow \bot$, et donc $\mathrm{Non}(\mathrm{Non}(A))$ n'est rien d'autre que $(A \Rightarrow \bot) \Rightarrow \bot$.

Exercice

Montrer les énoncés suivants (sans axiomes, A est un énoncé quelconque) :

- $\mathrm{Non}(\mathrm{Non}(A \text{ ou } \mathrm{Non}(A)))$
- $\mathrm{Non}(\mathrm{Non}(\mathrm{Non}(A))) \Rightarrow \mathrm{Non}(A)$

Preuve de Non(Non(A ou Non(A)))

L'énoncé se réécrit $((A \text{ ou } (A \Rightarrow \bot)) \Rightarrow \bot) \Rightarrow \bot$. Commençons par un lemme :

$$\dfrac{(A \text{ ou } (A \Rightarrow \bot)) \Rightarrow \bot \qquad \boxed{\dfrac{\dfrac{A}{A \text{ ou } (A \Rightarrow \bot)} \qquad (A \text{ ou } (A \Rightarrow \bot)) \Rightarrow \bot}{\bot}}}{A \Rightarrow \bot}\,(\mathrm{I}\Rightarrow)$$

La preuve tient alors dans l'arbre suivant :

$$\dfrac{\boxed{\dfrac{\dfrac{\dfrac{(A \text{ ou } (A \Rightarrow \bot)) \Rightarrow \bot}{A \Rightarrow \bot}\,\text{Lemme}}{A \text{ ou } (A \Rightarrow \bot)}\,(\mathrm{I}\text{ou}) \qquad (A \text{ ou } (A \Rightarrow \bot)) \Rightarrow \bot}{\bot}}}{((A \text{ ou } (A \Rightarrow \bot)) \Rightarrow \bot) \Rightarrow \bot}\,(\mathrm{I}\Rightarrow)$$

Preuve de $\mathrm{Non}(\mathrm{Non}(\mathrm{Non}(A))) \Rightarrow \mathrm{Non}(A)$

L'énoncé se réécrit : $(((A \Rightarrow \bot) \Rightarrow \bot) \Rightarrow \bot) \Rightarrow (A \Rightarrow \bot)$.
L'arbre suivant montre le résultat :

$$\dfrac{\dfrac{\dfrac{[A]}{(A \Rightarrow \bot) \Rightarrow \bot}\ \text{Vu précédemment} \qquad ((A \Rightarrow \bot) \Rightarrow \bot) \Rightarrow \bot}{\bot}\ (\text{MP})}$$

Exercice (Adjonction tenseur-hom)

Montrer les deux implications suivantes :

- $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \text{ et } B) \Rightarrow C)$
- $((A \text{ et } B) \Rightarrow C) \Rightarrow (A \Rightarrow (B \Rightarrow C))$

puis les interpréter en prenant le point de vue « fonctions » !

Exercice (Preuve par contraposée)

Démontrer, en n'utilisant que les règles qu'on a vues :

$$\dfrac{\dfrac{A \Rightarrow B}{\vdots}}{\mathrm{Non}(B) \Rightarrow \mathrm{Non}(A)}$$

Remarque (Preuve de la négation)

Pour montrer un énoncé de la forme $\mathrm{Non}(A)$, on n'a pas (pour l'instant) d'autre possibilité que d'appliquer $(I \Rightarrow)$ après avoir démontré $\perp$ à partir de A.

Exercice (Preuve par contraposée)

Démontrer, en n'utilisant que les règles qu'on a vues :

$$\dfrac{\dfrac{A \Rightarrow B}{\vdots}}{\mathrm{Non}(B) \Rightarrow \mathrm{Non}(A)}$$

Remarque (Preuve de la négation)

Pour montrer un énoncé de la forme $\mathrm{Non}(A)$, on n'a pas (pour l'instant) d'autre possibilité que d'appliquer $(I \Rightarrow)$ après avoir démontré $\perp$ à partir de A.
Il ne s'agit *pas* d'un raisonnement par l'absurde : il est valide avec les règles qu'on a, tandis que le raisonnement par l'absurde (montrer A en montrant que $\mathrm{Non}(A)$ est faux) n'est pas encore à notre portée !

Cas de « Il existe »

« Il existe » est une généralisation de « ou ». Ses règles d'introduction et d'élimination sont donc proches :

Règle (Introduction et élimination de « Il existe »)

- Si A est un énoncé ayant x pour variable libre, si y est un terme dans lequel x n'intervient pas, et si $A[y/x]$ désigne A dans lequel on a remplacé les occurrences de x par le terme y :

$$\frac{A[y/x]}{\text{Il existe } x \text{ tel que } A}\ (\mathrm{I}\exists)$$

- Si A est un énoncé ayant x pour variable libre, B un énoncé ne faisant pas intervenir x, alors :

$$\frac{\text{Il existe } x \text{ tel que } A \qquad \text{Si } A \text{ alors } B}{B}\ (\mathrm{DC}^*)$$

Exercice

Montrer que si $A \Rightarrow B$ et qu'il existe x tel que A, alors il existe x tel que B.

Cas de « Pour tout »

« Pour tout » est une généralisation de « et ». Ses règles d'introduction et d'élimination sont donc proches :

Règle (Introduction et élimination de « Pour tout »)

- Si A est un énoncé ayant x pour variable libre, si y est un terme quelconque, et si $A[y/x]$ désigne A dans lequel on a remplacé les occurrences de x par le terme y :

$$\frac{\text{Pour tout } x,\ A}{A[y/x]}\ (\mathrm{E}\forall)$$

- Si A est un énoncé ayant x pour variable libre :

$$\frac{A}{\text{Pour tout } x,\ A}\ (\mathrm{I}\forall)$$

Exercice

Montrer que si $A \Rightarrow B$ et que « Pour tout x, A », alors « Pour tout x, B ».

Le tiers exclu

Jusque ici, on a fait de la logique *intuitionniste*. Pour retrouver la logique classique habituelle, il faut une dernière règle de déduction :

Règle (Tiers exclu)

Pour tout énoncé A :

$$\frac{}{A \text{ ou } \mathrm{Non}(A)} \text{ (LEM)}$$

Le tiers exclu

Jusque ici, on a fait de la logique *intuitionniste*. Pour retrouver la logique classique habituelle, il faut une dernière règle de déduction :

Règle (Tiers exclu)

Pour tout énoncé A :

$$\frac{}{A \text{ ou } \mathrm{Non}(A)} \text{ (LEM)}$$

Cette règle dit que tout énoncé est soit vrai soit faux. En quelque sorte, on « force » la logique à choisir. Cela a des conséquences :

Le tiers exclu

Jusque ici, on a fait de la logique *intuitionniste*. Pour retrouver la logique classique habituelle, il faut une dernière règle de déduction :

Règle (Tiers exclu)

Pour tout énoncé A :

$$\frac{}{A \text{ ou } \mathrm{Non}(A)}\ (\mathrm{LEM})$$

Cette règle dit que tout énoncé est soit vrai soit faux. En quelque sorte, on « force » la logique à choisir. Cela a des conséquences :

- **En logique intuitionniste :** une preuve de « A ou B » peut être « normalisée » : on obtient soit une preuve de A, soit une preuve de B.
  Plus généralement, toute preuve d'existence peut être transformée en algorithme pour calculer l'objet dont on a montré l'existence ($\rightsquigarrow$ mathématiques constructives)

Le tiers exclu

Jusque ici, on a fait de la logique *intuitionniste*. Pour retrouver la logique classique habituelle, il faut une dernière règle de déduction :

Règle (Tiers exclu)

Pour tout énoncé A :

$$\frac{}{A \text{ ou } \mathrm{Non}(A)}\ (\mathrm{LEM})$$

Cette règle dit que tout énoncé est soit vrai soit faux. En quelque sorte, on « force » la logique à choisir. Cela a des conséquences :

- **En logique intuitionniste :** une preuve de « A ou B » peut être « normalisée » : on obtient soit une preuve de A, soit une preuve de B.
  Plus généralement, toute preuve d'existence peut être transformée en algorithme pour calculer l'objet dont on a montré l'existence ($\rightsquigarrow$ mathématiques constructives)
- **En logique classique :** On peut montrer qu'un objet existe sans savoir le construire !

Logique classique et intuitionniste

Exercice

Montrer que le tiers exclu est équivalent (on peut montrer l'un à partir de l'autre) à la règle suivante, dite « d'élimination des doubles négations » :

$$\frac{\mathrm{Non}(\mathrm{Non}(A))}{A}$$

Bien sûr, un énoncé qui a une preuve intuitionniste a aussi une preuve classique. La réciproque est fausse, mais :

Théorème

S'il existe une preuve classique de P, alors il existe une preuve intuitionniste de $\mathrm{Non}(\mathrm{Non}(P))$.

On en a vu un exemple plus tôt, avec $\mathrm{Non}(\mathrm{Non}(A \text{ ou } \mathrm{Non}(A)))$ (autrement dit, le tiers exclu n'est pas faux en logique intuitionniste)

Raisonnement par l'absurde 1/3

La logique classique permet le *raisonnement par l'absurde* : pour montrer A, on peut supposer $\mathrm{Non}(A)$ et arriver à une absurdité :

$$\dfrac{\dfrac{\boxed{\dfrac{\mathrm{Non}(A)}{\begin{array}{c}\vdots\\ \bot\end{array}}}}{\mathrm{Non}(\mathrm{Non}(A))}\,(\mathrm{I}\Rightarrow)}{A}\ \text{Élimination de la double-négation}$$

Proposition (Lois de De Morgan)

En logique classique, sont équivalents (deux par deux) :

- « A *et* B » *et* « $\mathrm{Non}(\mathrm{Non}(A)$ *ou* $\mathrm{Non}(B))$ » ;
- « A *ou* B » *et* « $\mathrm{Non}(\mathrm{Non}(A)$ *et* $\mathrm{Non}(B))$ » ;
- « *Il existe* x *tel que* P » *et* « $\mathrm{Non}($*Pour tout* x, $\mathrm{Non}(P))$ » ;
- « *Pour tout* x, P » *et* « $\mathrm{Non}($*Il existe* x *tel que* $\mathrm{Non}(P))$ ».

Raisonnement par l'absurde 2/3

Preuve

On se contente de montrer la première, qui donne l'état d'esprit général.
Sens direct (preuve intuitionniste) :

$$\dfrac{\text{Non}(A) \text{ ou } \text{Non}(B) \qquad \dfrac{\dfrac{A \text{ et } B}{A}}{\text{Non}(A) \Rightarrow \bot} \qquad \dfrac{\dfrac{A \text{ et } B}{B}}{\text{Non}(B) \Rightarrow \bot}}{\bot}$$

et donc de A et B on déduit $\text{Non}(\text{Non}(A) \text{ ou } \text{Non}(B))$.
Réciproque :

$$\dfrac{\dfrac{\text{Non}(A)}{\text{Non}(A) \text{ ou } \text{Non}(B)} \qquad \text{Non}(\text{Non}(A) \text{ ou } \text{Non}(B))}{\bot}$$

donc $\text{Non}(\text{Non}(A) \text{ ou } \text{Non}(B))$ entraîne $\text{Non}(\text{Non}(A))$, et de même $\text{Non}(\text{Non}(B))$, et il entraîne donc (classiquement) « A et B ».

Raisonnement par l'absurde 3/3

Il pourrait paraître surprenant que le tiers exclu permette d'introduire des « Il existe » sans témoin alors que, quand on regarde les règles, on a l'impression que (I$\exists$) est la seule règle qui en fasse apparaître. Cependant, les lois de De Morgan rendent évident le fait que (LEM) permet d'introduire « en cachette » des « Il existe » : pour montrer qu'il existe une valeur de x telle que $P(x)$, il suffit de montrer qu'il est impossible qu'aucune valeur de x ne satisfasse $P(x)$, ce qui ne requiert aucunement d'être capable de construire un contre-exemple.

Remarque

Ne pas confondre le raisonnement par l'absurde avec une preuve de $\mathrm{Non}(A)$, qui se fait constructivement en montrant $\bot$ à partir de A.

Intérêt de la logique intuitionniste

Pourquoi s'intéresse-t-on à la logique intuitionniste ?

- Tout à l'heure, j'ai parlé d'algorithme : les preuves intuitionnistes sont beaucoup plus adaptées pour l'informatique (on en reparlera avec Curry-Howard).
  Sujets actuels : formalisation de preuves par ordinateur !.

Intérêt de la logique intuitionniste

Pourquoi s'intéresse-t-on à la logique intuitionniste ?

- Tout à l'heure, j'ai parlé d'algorithme : les preuves intuitionnistes sont beaucoup plus adaptées pour l'informatique (on en reparlera avec Curry-Howard).
  Sujets actuels : formalisation de preuves par ordinateur !.
- Les résultats sont plus durs à démontrer, mais on apprend toujours plus quand on a un résultat intuitionniste.

Intérêt de la logique intuitionniste

Pourquoi s'intéresse-t-on à la logique intuitionniste ?

- Tout à l'heure, j'ai parlé d'algorithme : les preuves intuitionnistes sont beaucoup plus adaptées pour l'informatique (on en reparlera avec Curry-Howard).
  Sujets actuels : formalisation de preuves par ordinateur !.
- Les résultats sont plus durs à démontrer, mais on apprend toujours plus quand on a un résultat intuitionniste.
- On ne perd pas grand chose, quitte à rajouter des $\mathrm{Non}(\mathrm{Non}(...))$ partout !

Intérêt de la logique intuitionniste

Pourquoi s'intéresse-t-on à la logique intuitionniste ?

- Tout à l'heure, j'ai parlé d'algorithme : les preuves intuitionnistes sont beaucoup plus adaptées pour l'informatique (on en reparlera avec Curry-Howard).
  Sujets actuels : formalisation de preuves par ordinateur !.
- Les résultats sont plus durs à démontrer, mais on apprend toujours plus quand on a un résultat intuitionniste.
- On ne perd pas grand chose, quitte à rajouter des $\mathrm{Non}(\mathrm{Non}(...))$ partout !
- Contrairement à ce qu'on pourrait croire, un énoncé d'existence prouvé en logique intuitionniste n'est pas inintéressant (« Pourquoi ne pas directement donner le témoin ? ») : a/ Les $\forall\exists \Rightarrow$ des fonctions calculables ; b/ La normalisation est un processus coûteux !

Interprétation catégorique de la logique intuitionniste

Soit $\mathrm{Dem}(P)$ l'ensemble des preuves de P (avec des axiomes fixés).

- $\mathrm{Dem}(\bot) = \emptyset$ (idéalement) ; si A est un axiome, $\mathrm{Dem}(A) \neq \emptyset$;
- On a vu en utilisant (MP) et (I$\Rightarrow$) que les éléments de $\mathrm{Dem}(A \Rightarrow B)$ étaient essentiellement les fonctions de $\mathrm{Dem}(A)$ dans $\mathrm{Dem}(B)$.
- De même, en utilisant (Iet) et (Eet), les éléments de $\mathrm{Dem}(A \text{ et } B)$ sont essentiellement les couples de $\mathrm{Dem}(A) \times \mathrm{Dem}(B)$.
- Pour compléter le tableau, il ne manque que $\mathrm{Dem}(A \text{ ou } B) \sim \mathrm{Dem}(A) \cup \mathrm{Dem}(B)$...

Interprétation catégorique de la logique intuitionniste

Soit $\mathrm{Dem}(P)$ l'ensemble des preuves de P (avec des axiomes fixés).

- $\mathrm{Dem}(\bot) = \emptyset$ (idéalement) ; si A est un axiome, $\mathrm{Dem}(A) \neq \emptyset$;
- On a vu en utilisant (MP) et (I⇒) que les éléments de $\mathrm{Dem}(A \Rightarrow B)$ étaient essentiellement les fonctions de $\mathrm{Dem}(A)$ dans $\mathrm{Dem}(B)$.
- De même, en utilisant (Iet) et (Eet), les éléments de $\mathrm{Dem}(A \text{ et } B)$ sont essentiellement les couples de $\mathrm{Dem}(A) \times \mathrm{Dem}(B)$.
- Pour compléter le tableau, il ne manque que $\mathrm{Dem}(A \text{ ou } B) \sim \mathrm{Dem}(A) \cup \mathrm{Dem}(B)$...
  Cependant, bien que la fonction $\leftarrow$ existe (c'est la règle (Iou)), la fonction $\rightarrow$ n'existe qu'en logique intuitionniste !

Cela montre qu'en logique intuitionniste, l'espace des propositions est (à application de Dem près) très structuré. Il ressemble aux ensembles : on peut y prendre des espaces de fonctions, des produits, des unions (on parle de catégorie [co]complète). Ceci est au cœur d'une idée puissante : les propositions sont des « types » dont les habitants sont les preuves.

Récapitulatif de toutes les règles de déduction

- Règles d'introduction :

$$\frac{A \quad B}{A \text{ et } B} \qquad \frac{A}{A \text{ ou } B} \quad \frac{B}{A \text{ ou } B} \qquad \frac{A(x)}{\text{Pour tout } x, A(x)} \qquad \frac{A(t)}{\text{Il existe } x, A(x)}$$

$$\frac{\begin{array}{|c|}\hline \mathcal{A} \quad B \\ \hline \vdots \\ C \\ \hline \end{array}}{B \Rightarrow C}\ \mathcal{A}$$

- Règles d'élimination :

$$\frac{A \text{ et } B}{A} \qquad \frac{A \text{ et } B}{B} \qquad \frac{A \text{ ou } B \quad A \Rightarrow C \quad B \Rightarrow C}{C}$$

$$\frac{\text{Pour tout } x, A(x)}{A(t)} \qquad \frac{\text{Il existe } x, A(x) \quad A(x) \Rightarrow B}{B} \qquad \frac{\bot}{A}$$

- Tiers exclu :

$$\frac{}{A \text{ ou } \mathrm{Non}(A)}$$

Syntaxe et sémantique

- **Preuves :** symboles, syntaxe, règles de déduction (réécriture), mécanique : « juste du texte »
- **Propositions mathématiques :** notion intuitive de *vérité* (sémantique !) : semble exister « en dehors des preuves ». Mal formalisable.

Syntaxe et sémantique

- **Preuves :** symboles, syntaxe, règles de déduction (réécriture), mécanique : « juste du texte »
- **Propositions mathématiques :** notion intuitive de *vérité* (sémantique !) : semble exister « en dehors des preuves ». Mal formalisable.
- Qu'on puisse construire un arbre de preuve menant à l'énoncé « $2 + 2 = 4$ » est intéressant, mais il est encore plus intéressant que la somme de deux et de deux soit effectivement quatre !

Syntaxe et sémantique

- **Preuves :** symboles, syntaxe, règles de déduction (réécriture), mécanique : « juste du texte »
- **Propositions mathématiques :** notion intuitive de *vérité* (sémantique !) : semble exister « en dehors des preuves ». Mal formalisable.
- Qu'on puisse construire un arbre de preuve menant à l'énoncé « $2 + 2 = 4$ » est intéressant, mais il est encore plus intéressant que la somme de deux et de deux soit effectivement quatre !
- Certaines branches de la logique donnent un sens à cette dichotomie : exemple de la *théorie des modèles*.

Théorie des modèles

Si on a un langage et un ensemble d'axiomes $\mathcal{A}$, la théorie des modèles définit la notion de *modèle* :

Definition (modèle de $\mathcal{A}$, à la louche)

Les modèles de $\mathcal{A}$ sont tous **les mondes mathématiques possibles** M dans lesquels les axiomes de $\mathcal{A}$ sont vrais.
Pour être un peu plus précis, un modèle est un ensemble muni, pour chaque symbole du langage, d'une "interprétation" de ce symbole, de sorte que les axiomes soient tous vérifiés par ces interprétations.

Definition (vérité d'un énoncé)

Soit un énoncé P (formulé dans le même langage). Alors on dit que P est vrai modulo les axiomes de $\mathcal{A}$ lorsque *tout* modèle de $\mathcal{A}$ vérifie P.

C'est la plus sémantique des définitions de vérité à laquelle on puisse espérer arriver dans ce contexte...

Résultats en théorie des modèles 1/3

Remarque

Attention, même si on raisonne classiquement, un énoncé n'a aucune raison d'être soit vrai soit faux au sens précédent : s'il existe des modèles dans lesquels il est vérifié et d'autres dans lesquels il ne l'est pas, il ne sera ni vrai ni faux.

On a le premier résultat rassurant :

Théorème (théorème de correction)

S'il existe une preuve de P à partir des axiomes de $\mathcal{A}$, alors P est vraie modulo $\mathcal{A}$. Dit plus simplement, ce qu'on peut prouver est toujours vrai.

Preuve (à la louche)

L'idée est simple : soit un modèle M de $\mathcal{A}$. Puisqu'on dispose d'une preuve (syntaxique) de P à partir des axiomes de $\mathcal{A}$, et que M vérifie ces axiomes, il suffit de lire la preuve étape par étape et de recopier le même raisonnement en l'appliquant directement dans M.

Résultats en théorie des modèles 2/3

Un résultat autrement plus fort est le suivant :

Théorème (théorème de complétude en logique du premier ordre)

Si P est vraie modulo $\mathcal{A}$, alors il existe une preuve classique de P à partir des axiomes de $\mathcal{A}$.

Ainsi, si un énoncé est une conséquence inévitable de nos axiomes, il doit en exister une preuve, ce qui est remarquable ! Dans ce contexte, la sémantique et la syntaxe sont liées : tout ce qui est vrai est démontrable, tout ce qui est faux est réfutable, et ce qui n'est ni l'un ni l'autre est indécidable.

Corollaire

Si un ensemble d'axiomes $\mathcal{A}$ est cohérent, alors il admet un modèle.

Preuve

Si $\mathcal{A}$ n'admet pas de modèle, alors $\perp$ est évidemment vrai, et on peut donc le démontrer (vu le théorème), ce qui contredit la cohérence de $\mathcal{A}$. La réciproque résulte du théorème de correction de façon analogue.

Résultats en théorie des modèles 3/3

Théorème (Théorème de compacité)

Soit $\mathcal{A}$ un ensemble infini d'axiomes. Pour montrer qu'il existe un modèle de $\mathcal{A}$, il suffit de montrer que tout choix d'un nombre fini d'axiomes de $\mathcal{A}$ admet un modèle.

Résultats en théorie des modèles 3/3

Théorème (Théorème de compacité)

Soit $\mathcal{A}$ un ensemble infini d'axiomes. Pour montrer qu'il existe un modèle de $\mathcal{A}$, il suffit de montrer que tout choix d'un nombre fini d'axiomes de $\mathcal{A}$ admet un modèle.

Indication : Une preuve est toujours de taille finie !

Résultats en théorie des modèles 3/3

Théorème (Théorème de compacité)

Soit $\mathcal{A}$ un ensemble infini d'axiomes. Pour montrer qu'il existe un modèle de $\mathcal{A}$, il suffit de montrer que tout choix d'un nombre fini d'axiomes de $\mathcal{A}$ admet un modèle.

Indication : Une preuve est toujours de taille finie !

Preuve

L'ensemble d'axiomes $\mathcal{A}$ n'admet pas de modèle si et seulement s'il existe une preuve de $\perp$ à partir des axiomes de $\mathcal{A}$. Une telle preuve étant nécessairement de taille finie, elle ne peut utiliser qu'un nombre fini d'axiomes de $\mathcal{A}$, et on obtiendrait alors une partie finie incohérente de $\mathcal{A}$.

La prochaine fois...

- **Une preuve informatique du théorème d'incomplétude de Gödel :** tout ensemble d'axiomes assez puissant pour multiplier des entiers possède nécessairement des énoncés indécidables (ni démontrables, ni réfutables) ;
- **La correspondance de Curry-Howard :** on peut transformer des preuves mathématiques en programmes informatiques !
- **La normalisation** et le Hauptsatz de Gentzen.