L1MD – Feuille[1] de référence sur les preuves (déduction naturelle) 2014-15

0. Prérequis : Notion de variables libres, variables liées, constantes et leurs types.

Notations : Dans ce qui suit les variables en majuscule $A, B, P, \ldots$ désignent des énoncés ; les variables en minuscule $x, y, t, \ldots$ désignent des objets d'un certain type $\mathcal{T}$.

On écrit $P(x)$ pour désigner un énoncé où x est une variable libre d'un certain type $\mathcal{T}$ et on dit alors que P est une propriété sur les objets de type $\mathcal{T}$. Par exemple $P(x)$ est l'énoncé $\sin(x) > 0$, où x est une variable de type $\mathbb{R}$.

Une expression de type énoncé est une formule faisant intervenir éventuellement les constantes V, F, des variables de type énoncés, des connecteurs logiques (et , $\neg$, ...), éventuellement des propriétés sur les objets d'un certain type et des quantificateurs $\forall, \exists, \exists!$.

Une expression de type $\mathcal{T}$ est une formule faisant intervenir des constantes, éventuellement des variables, des constructions, dont le résultat est de type $\mathcal{T}$. Par exemple π est une expression de type $\mathbb{R}$ de même que $\int_0^x \frac{dt}{1+t}$ pour x variable de type $\mathbb{R}$.

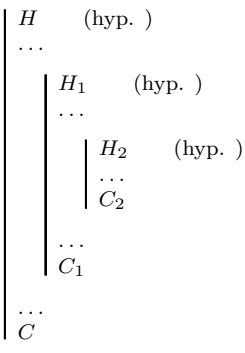
Si t est une expression de type $\mathcal{T}$ et $P(x)$ est une propriété sur les objets de type $\mathcal{T}$, on écrit $P(t)$ pour désigner l'énoncé obtenu en substituant t à x. De même si $f(x)$ est une formule (ou expression) dépendant de la variable libre x de type $\mathcal{T}$ et dont le résultat est un objet de type $\mathcal{T}'$, on écrit $f(t)$ pour désigner l'expression obtenue en substituant t à x.

1. Un théorème se présente sous la forme d'un énoncé sans variable libre (ex. "Toute suite croissante majorée de nombres réels converge") ou par l'introduction d'une ou plusieurs variables libres, la donnée d'hypothèses sur ces variables et d'une conclusion ("Soit (u_n) une suite de nombres réels croissante et majorée, alors (u_n) converge").

La preuve formelle d'un théorème est une suite d'énoncés commençant par les hypothèses (la déclaration des variables libres avec leur type et les énoncés les concernant) déclarées comme telles (Hyp:..., décalage du texte à droite), se terminant par la conclusion, et telle que chaque énoncé de la suite est soit une hypothèse intermédiaire additionnelle déclarée comme telle, soit un axiome ou théorème admis, soit un énoncé se déduisant des précédents (y compris éventuellement des hypothèses intermédiaires) par application des règles de raisonnement, la conclusion du théorème ne devant pas dépendre des hypothèses intermédiaires.

Organisation de la preuve formelle : On écrit les énoncés les uns en dessous des autres. On commente chaque énoncé par le nom de la règle dont il résulte.

On décale vers la droite toute partie de preuve commençant par l'introduction d'une hypothèse additionnelle. On revient à gauche pour ce qui ne dépend plus de l'hypothèse additionnelle. Cf la notation de Fitch sur Wikipedia.



[1]Version du 29 février 2016 — F-X. Dehon, Université de Nice — dehon@unice.fr

Rq. La suite des règles utilisées correspond à un programme informatique (algorithme) ; la preuve écrite correspond au résultat de l'exécution du programme sur les hypothèses initiales.

Une esquisse de preuve formelle est une preuve formelle incomplète (certains énoncés ne sont pas prouvés, les règles appliquées ne sont pas toutes explicitées). Une preuve informelle est un scénario de preuve en langage naturel. Voir les exemples plus loin.

2. Les règles primaires de raisonnement. Dans ce qui suit, les variables $A, B, \ldots$ désignent des énoncés.

$\Rightarrow$: $A \Rightarrow B$ se déduit de B sous l'hypothèse A. Inversement B se déduit de l'énoncé A et de l'énoncé $A \Rightarrow B$: c'est la règle du *modus ponens*.

$\vert\ \vert\ A$ (hyp.) $\vert\ B$ $A \Rightarrow B$ $(\vdash\Rightarrow)$	$\vert\ A$ $\vert\ A \Rightarrow B$ $\vert\ B$ (mp)

Répétition : A se déduit de A (la règle permet de répéter un énoncé, ce qui permet par exemple de prouver $A \Rightarrow A$).

et : Chacun des énoncés A, B se déduisent de l'énoncé A et B. Inversement A et B se déduit de la présence des deux énoncés A, B.

$\vert\ A$ et B $\vert\ A$ $\vert\ B$	$\vert\ A$ $\vert\ B$ $\vert\ A$ et B

ou : l'énoncé A ou B se déduit de l'énoncé A comme de l'énoncé B. Inversement tout énoncé C se déduit des énoncés A ou B, $A \Rightarrow C$ et $B \Rightarrow C$ (preuve en distinguant suivant A ou B).

$\vert\ A$ $\vert\ A$ ou B	$\vert\ B$ $\vert\ A$ ou B	$\vert\ A$ ou B $\vert\ A \Rightarrow C$ $\vert\ B \Rightarrow C$ $\vert\ C$ (ou $\vdash$)

$\bot$, $\neg$: Contradiction et négation. $\bot$ est une constante désignant l'énoncé faux ou la contradiction. $\bot$ se déduit d'un énoncé A et de sa négation $\neg A$ ("l'énoncé A et $\neg A$ conduit à une contradiction"). $\neg A$ se déduit de $A \Rightarrow \bot$ (autrement dit d'une preuve de $\bot$ sous l'hypothèse A).

$\vert\ A$ $\vert\ \neg A$ $\vert\ \bot$ (contradiction)	$\vert\ A \Rightarrow \bot$ $\vert\ \neg A$ $(\vdash \neg)$

$\forall$: Soit $P(x)$ une propriété sur les objets de type $\mathcal{T}$ et t une expression de type $\mathcal{T}$. L'énoncé $\forall x : \mathcal{T}, P(x)$ se déduit de l'énoncé $P(x)$ sous l'hypothèse $x : \mathcal{T}$, où x est une variable introduite par l'hypothèse $x : \mathcal{T}$ (le nom x ne pourrait pas être utilisée comme variable liée dans $\forall x : \mathcal{T}, P(x)$ s'il désigne une variable libre à ce niveau).

Inversement $P(t)$ se déduit de $\forall x : \mathcal{T}, P(x)$ (c'est la spécialisation de l'énoncé à $x = t$).

$\vert\ \vert$ x:T (hyp.) $\vert\ $ P(x) $\forall x : \mathcal{T}, P(x)$ $(\vdash \forall$	$\vert\ \forall x : \mathcal{T}, P(x)$ $\vert\ t : \mathcal{T}$ $\vert\ P(t)$ $(\forall \vdash)[t]$

$\exists$: Soit comme précédemment P une propriété sur les objets de type $\mathcal{T}$ et t une expression de type $\mathcal{T}$.

L'énoncé $\exists x : \mathcal{T}, P(x)$ se déduit de l'énoncé $P(t)$.

Inversement si A est un énoncé où la variable x n'apparaît pas, une preuve de A sous les hypothèses $x : \mathcal{T}$ et $P(x)$ permet de déduire A de l'énoncé $\exists x : \mathcal{T}, P(x)$.

$\vert\ t : \mathcal{T}$ $\vert\ P(t)$ $\vert\ \exists x : \mathcal{T}, P(x)$ $(\vdash \exists)$	$\vert\ \exists x : \mathcal{T}, P(x)$ $\vert\ \vert\ x : \mathcal{T}$ (hyp.) $\vert\ \vert\ P(x)$ (hyp.) $\vert\ \vert\ A$ $\vert\ A$ $(\exists \vdash)$

3. Macrorègles et axiomes logiques. Un théorème logique est une expression $f(A, B, \ldots)$, où $A, B, \ldots$ sont des variables de type énoncé, se déduisant de l'application des règles primaires. Par exemple $\neg \perp$, $A \Rightarrow A$, $A \Rightarrow \neg\neg A$ sont des théorèmes.

Un axiome logique est une expression $f(A, B, \ldots)$ donnée comme valide sans preuve.

$\neg\neg A \Rightarrow A$ est un axiome en logique classique ; il est a la base du tiers exclu (A ou $\neg A$ est un théorème logique se déduisant de cet axiome) ou de la démonstration par l'absurde (au lieu de prouver A, on prouve que $\neg A \Rightarrow \perp$).

$$\left|\begin{array}{l} \neg\neg A \Rightarrow A \qquad (\text{ax.}\neg\neg) \end{array}\right.$$

$x = x$ et $x = y \Rightarrow (P(x) \Leftrightarrow P(y))$ sont les axiomes d'égalité, où x, y sont des variables de type $\mathcal{T}$ et P une propriété sur les objets de type $\mathcal{T}$.

$$\left|\begin{array}{l} x, y : \mathcal{T} \\ x = x \qquad (\text{ax}) \\ x = y \Rightarrow (P(x) \Leftrightarrow P(y)) \qquad (\text{ax.}=) \end{array}\right.$$

Une macro-règle est une suite d'écriture d'axiomes logiques et d'énoncés sans déduisant par application des règles primaires, qu'on résume par un nom. A chaque axiome ou théorème logique correspond une macro-règle qui consiste à écrire cet axiome ou théorème. On fait référence à l'axiome ou au théorème ou au nom de la macro-règle pour justifier l'écriture de l'énoncé.

Voici quelques macro-règles classiques :

Réécritures :

($\equiv$) : l'expression $f(A, B, \ldots)$ se déduit de $g(A, B, \ldots)$ si f et g ont même table de vérité fonction des valeurs de vérités de $A, B, \ldots$. $f(A, B, \ldots)$ est un théorème si c'est une tautologie au sens des tables de vérités (*i.e.* sa table de vérité est constante égale à Vrai).

($=$) : si $P(x)$ est une propriété des objets de type $\mathcal{T}$ et si t, t' sont deux expressions de type $\mathcal{T}$ alors $P(t')$ se déduit de $P(t)$ si t et t' sont égaux comme objets de types $\mathcal{T}$.

Exemples.

$$\left|\begin{array}{l} \neg(A \text{ et } B) \text{ ou } C \\ \neg A \text{ ou } \neg B \text{ ou } C \qquad (\equiv) \end{array}\right.$$

$$\left|\begin{array}{l} \neg B \Rightarrow \neg A \\ A \Rightarrow B \qquad (\equiv) \end{array}\right.$$

Distinguer suivant une hypothèse H, règle notée (H) : l'énoncé A se déduit d'une preuve de A sous l'hypothèse H et d'une preuve de A sous l'hypothèse $\neg H$.

Voici une preuve de cette macro-règle

$$\left|\begin{array}{ll} H \text{ ou } \neg H & (\text{axiome}) \\ \quad \left|\begin{array}{l} H \qquad (\text{hyp. }) \\ A \end{array}\right. & \\ H \Rightarrow A & (\text{règle } \Rightarrow) \\ \quad \left|\begin{array}{l} \neg H \qquad (\text{hyp. }) \\ A \end{array}\right. & \\ \neg H \Rightarrow A & (\text{règle } \Rightarrow) \\ A & (\text{règle ou }) \end{array}\right.$$

4. Définitions et axiomes propres à un type : une définition est une expression, dépendant souvent de variables libres, désignant soit un énoncé soit un objet d'un certain type $\mathcal{T}$. Elle est explicite lorsqu'elle correspond à une règle de réécriture de la forme <expression>$\equiv \ldots$ ou <expression>$= \ldots$.

Elle est implicite lorsque l'objet qu'elle désigne est caractérisé par un énoncé d'existence et d'unicité $\exists!\ x : \mathcal{T},\ P(x)$ auquel cas elle donne lieu à l'axiome $\forall x : \mathcal{T},\ x =$<expression>$\Leftrightarrow P(x)$.

Exemple : **a.** . la fonction ln peut être définie explicitement par l'axiome

$$\ln = \left(x \mapsto \int_1^x \frac{dt}{t}\right)$$

(ou de façon équivalente par l'axiome $\forall x : \mathbb{R},\ \ln(x) = \int_1^x \frac{dt}{t}$) ; la règle de réécriture consiste alors à remplacer ln par son expression.

La fonction ln peut aussi être définie implicitement par l'axiome

$$\forall x, y : \mathbb{R},\ y = \ln(x) \Leftrightarrow \exp(y) = x$$

(pourvu que la fonction exp ait été définie auparavent et qu'on ait prouvé le résultat d'existence et d'unicité).

b. . L'expression a divise b, pour a, b variables de type $\mathbb{N}$, est défini par l'axiome

$$a \text{ divise } b \equiv \exists d : \mathbb{N},\ ad = b$$

donc par la règle de réécriture ($\equiv$) correspondante.

Les types ont leurs axiomes et règles de raisonnement propres. Par exemple :

$$\forall E : \mathcal{E}\text{ns},\ \exists F : \mathcal{E}\text{ns},\ \forall x,\ x \in F \Leftrightarrow x \subset E$$

est un axiome du type ensemble (existence de l'ensemble des parties d'un ensemble) ;

$$\forall x : \mathbb{R},\ \exists n : \mathbb{N},\ n \geq x$$

est un axiome du type $\mathbb{R}$; Le raisonnement par récurrence est une règle de raisonnement propre au type $\mathbb{N}$.

5. Exemples de preuves.