Déduction naturelle

$\langle \vee \wedge \rangle$

Montaigne 2023-2024

– mpi23@arrtes.net –

Introduction

La **logique** constitue un moyen de clarifier le discours et le raisonnement. Cependant, la sémantique à base de tables de vérité ne reflète guère la manière dont on construit une preuve mathématique, ni un argumentaire de quelque nature que ce soit.

Ce chapitre s'intéresse à la **déduction**, c'est-à-dire à la manière dont il est possible d'utiliser des faits logiques supposés vrais pour justifier d'autres faits.

Plus précisément, c'est davantage la manière dont les formules se combinent, pour justifier une conclusion en partant d'hypothèses, que la valeur de chaque formule qui est mise en avant.

Introduction

En première approche, le cadre du raisonnement déductif peut se résumer par la phrase suivante.

En supposant certains faits de départ vrais (hypothèses), établir que certains autres faits s'ensuivent nécessairement, et ce jusqu'à obtenir le fait terminal (conclusion).

Cette phrase exprime l'existence d'une relation entre des hypothèses et une conclusion. Elle ne dit rien du bien fondé des hypothèses ou de la véracité de la conclusion.

Ce qu'on obtient n'est qu'un lien de conséquence :

- si les hypothèses sont valides alors la conclusion l'est aussi ;
- si les hypothèses sont infondées, on n'apprend rien sur la validité ou sur la fausseté de la conclusion.

Introduction

Ainsi, **établir la validité d'un fait par déduction** nécessite de répondre aux deux questions suivantes.

- Comment établir la validité d'un fait de départ pouvant servir d'hypothèse ?
  Cette question est de nature philosophique.
- Quel critères garantissent qu'un fait est nécessairement la conséquence d'un autre fait ou d'un ensemble d'autres faits ?
  Cette question est l'objet de cet exposé.

Brève histoire de la logique

Racines antiques

Les premières formalisations connues d'un raisonnement correct remontent à l'antiquité et comprennent notamment :

- une *caractérisation des énoncés* sur lesquels il est possible de raisonner, jouant le même rôle que les formules logiques ;
- des *règles* appelées syllogismes, qui, à partir de faits acquis, permettent de déduire d'autres faits qui nécessairement en découlent.

Racines antiques

En la matière, les travaux d'*Aristote* (quatrième siècle av. J.-C.) ont très fortement imprégné la science européenne jusqu'au dix-neuxième siècle.

Les syllogismes aristotéliciens ont une forme codifiée très distinctive, illustrée par l'exemple célèbre :

- *Tous les hommes sont mortels.*
- *Or Socrate est un homme.*
- *Donc Socrate est mortel.*

Le format est rigide, centré sur des termes et des catégories (*homme*, *mortel*, *Socrate*) mais les quantifications universelle et existentielle y apparaissent.

Racines antiques

Moins connu, *Chrysippe de Soles* (troisième siècle av. J.-C.) introduit la première forme de logique propositionnelle, avec en particulier des formes d'implication, de conjonction, de disjonction.

Les syllogismes associés concernent cette fois les propriétés de ces connecteurs, y compris leurs interactions avec la négation.

On lui doit notamment ce qu'on appelle aujourd'hui le syllogisme disjonctif : partant d'une alternative entre deux propositions, rejeter l'une des deux propositions impose d'accepter l'autre.

Raisonnement syllogistique

Partons des énoncés suivants, qu'un élève est en train d'essayer de résoudre mentalement pendant une séance de cours.

1. *Si je participe, je vais dire des bêtises.*
2. *Si je dis des bêtises, je vais avoir la honte.*
3. *Si participer me donne la honte, je ne vais pas participer.*
4. *Pour réussir, il faut participer.*
5. *Si j'échoue, je vais avoir la honte.*

Raisonnement syllogistique

Ce raisonnement peut être détourné, parfois de manière fallacieuse.

Tout ce qui est rare est cher.
Un cheval bon marché est rare.
Donc un cheval bon marché est cher.

On le rencontre aussi au cinéma, comme dans le film de *Sergio Leone* intitulé *Le Bon, la Brute, le Truant (1966)*. Un dialogue, légèrement modifié, est le suviant.

Tu vois, le monde se divise en deux catégories :
ceux qui ont un pistolet chargé et ceux qui creusent.
Toi, tu creuses.

Raisonnement syllogistique

En notant P le fait de participer, B celui de dire des bêtises, H avoir la honte et R réussir, on peut traduire ces énoncés en formules propositionnelles comme suit.

1. $P \to B$
2. $B \to H$
3. $(P \to H) \to \neg P$
4. $R \to P$
5. $\neg R \to H$

Quelques exemples de syllogismes classiques, venant des écoles aristotélicienne et stoïcienne, permettent d'en tirer des conclusions.

Raisonnement syllogistique

Le syllogisme *barbara* indique que des faits $\varphi_1 \to \varphi_2$ et $\varphi_2 \to \varphi_3$ on peut déduire le fait $\varphi_1 \to \varphi_3$. Ce n'est autre que le syllogisme aristotélicien rencontré plus haut, traduit pour faire apparaître le connecteur d'implication.

En combinant les faits 1 et 2, on peut déduire :

6. $P \to H$: *si je participe, je vais avoir la honte*.

On désigne aussi ce principe comme la *transitivité de l'implication*.

Raisonnement syllogistique

Le *modus ponens*, ou règle du détachement, concrétise la notion d'implication : si on a l'implication $\varphi_1 \to \varphi_2$ et que φ_1 est vraie alors cette règle permet de déduire que la conclusion φ_2 est nécessairement vraie également.

Ici, on peut ainsi combiner les faits 3 et 6 pour déduire :

7. $\neg P$: *je ne participe pas.*

Raisonnement syllogistique

Le *modus tollens* est une utilisation inversée de l'implication : si on a une implication $\varphi_1 \rightarrow \varphi_2$ mais que φ_2 est connue pour être fausse, alors nécessairement φ_1 doit être fausse également. Cette règle est liée à la notion de *contraposition*.

On combine donc les faits 4 et 7 pour déduire :

8. $\neg R$: *je ne vais pas réussir.*

Raisonnement syllogistique

Une dernière utilisation du *modus ponens* appliqué aux faits 5 et 8 permet enfin de déduire :

9. H : *je vais avoir la honte.*

Raisonnement syllogistique

Notre élève a donc établi qu'échouer et avoir la honte étaient des conséquences nécessaires des cinq énoncés de départ.

Attention cependant à la nature du raisonnement syllogistique : la conclusion n'est nécessairement vraie que si tous les faits de départ sont effectivement vrais. Il ne tient donc qu'à l'élève de briser lui-même les énoncés de départ qu'il est en mesure de réfuter, pour ne pas se condamner à une issue funeste !

Notations alternative des syllogismes

Le **syllogisme** qui des prémisses φ_1 et φ_2 déduit une conclusion ψ est couramment résumé par la notation $\varphi_1, \varphi_2 \vdash \psi$, où le symbole $\vdash$ dénote une forme de **conséquence logique**.

- Syllogisme *barbara* : $\varphi_1 \to \varphi_2, \varphi_2 \to \varphi_3 \vdash \varphi_1 \to \varphi_3$
- *Modus ponens* : $\varphi_1 \to \varphi_2, \varphi_1 \vdash \varphi_2$
- *Modus tollens* : $\varphi_1 \to \varphi_2, \neg\varphi_2 \vdash \neg\varphi_1$
- Syllogisme disjonctif : $\varphi_1 \vee \varphi_2, \neg\varphi_1 \vdash \varphi_2$

Logique moderne

La *logique* a fortement évolué à partir de la fin du XIXe siècle cherchant notamment à *formaliser le raisonnement mathématique*.

Cette renaissance s'est faite grâce à des scientifiques venant de la philosophie comme du monde scientifique dont *Gottlob Frege* ou *Bertrand Russel* sont d'illustres représentants.

La logique s'est fortement rapprochée de la pratique mathématique moderne et a réintégré des contributions de la logique stoïcienne, mises de côté par la scholastique du Moyen Âge.

La suite de cet exposé se concentre sur la présentation moderne des mécanismes de raisonnement.

Logique moderne

Traditionnellement, une **preuve mathématique** a une **structure arborescente** avec un contexte d'hypothèses différent d'un point à l'autre de l'arbre.

Un formalisme logique apte à parler de ces preuves doit incorporer ces notions de branches et de contexte local. C'est précisément l'objet de la **déduction naturelle**.

Règles d’inférence

Syntaxe des formules propositionnelles (rappels)

Soit $\mathcal{V}$ un ensemble dénombrable de **variables propositionnelles**.

Les **formules atomiques** sont constituées des variables propositionnelles $\mathcal{V}$ ains que de la formule atomique $\perp$ (absurde).

On se donne un **connecteur unaire** $\neg$ (non) et trois **connecteurs binaires** $\wedge$ (et), $\vee$ (ou) et $\rightarrow$ (implique).

Syntaxe des formules propositionnelles (rappels)

Les **formules propositionnelles** sont construites à partir de formules atomiques en utilisant ces **connecteurs**.

L'ensemble $\mathcal{F}$ des formules propositionnelles est inductivement défini par les règles suivantes.

- $\bot \in \mathcal{F}$
- $\mathcal{V} \subseteq \mathcal{F}$
- Si $A \in \mathcal{F}$ alors $\neg A \in \mathcal{F}$
- Si $A, B \in \mathcal{F}$ alors $(A \wedge B) \in \mathcal{F}, (A \vee B) \in \mathcal{F}$ et $(A \rightarrow B) \in \mathcal{F}$

Syntaxe des formules propositionnelles (rappels)

On peut ajouter une **formule atomique tautologique** $\top$ à la syntaxe.

Le **connecteur** $\leftrightarrow$ n'est pas ajouté à la syntaxe ; on convient que $A \leftrightarrow B$ est une notation pour $(A \to B) \land (B \to A)$.

On convient des **priorités usuelles** : $\neg$ prioritaire sur $\land$ prioritaire sur $\lor$ prioritaire sur $\to$.

$\land$ et $\lor$ sont **syntaxiquement associatifs**. $\to$ est **syntaxiquement associatif à droite**.

Ceci évite l'écriture systématique de parenthèses. Par exemple :

$$(A \land (B \land C)) \to ((\neg D \lor E) \to F)$$

peut être remplacé par :

$$A \land B \land C \to \neg D \lor E \to F$$

Système déductif

Un **système déductif** est constitué d'**axiomes** (*vérités premières*) et de **règles d'inférence** qui permettent de déduire de nouveaux faits préalablement connus ou supposés vrais.

Les **raisonnements** à l'intérieur d'un système déductif sont **purement syntaxiques** : d'hypothèses qui ont une certaine forme on peut déduire tel autre fait.

Il est donc possible de *vérifier algorithmiquement la correction d'une preuve* dans le système, sans aucune référence à une sémantique (c'est-à-dire à une signification donnée aux symboles).

Séquent

Définition 1

Un **séquent** est un couple (Γ, A), noté $\Gamma \vdash A$ où :

- Γ est un ensemble fini de formules et représente l'ensemble des hypothèses ou le contexte du séquent ;
- A est une formule appelée la conclusion du séquent.

Le symbole $\vdash$ se lit *thèse* ou *montre*.

L'interprétation intuitive du séquent $\Gamma \vdash A$ est :

des hypothèses Γ, *on peut montrer* A.

Séquent

Si $\Gamma = \{A_1, A_2, \dots, A_n\}$, on peut noter le séquent $A_1, A_2, \dots A_n \vdash A$.

Si $\Gamma = \varnothing$ on note $\vdash A$.

Si $\Gamma_1, \Gamma_2, \dots, \Gamma_n$ sont des ensembles de formules on note $\Gamma_1, \Gamma_2, \dots$, $\Gamma_n \vdash A$ le séquent d'hypothèses $\bigcup_{1 \leqslant i \leqslant n} \Gamma_i$.

De même, on note $\Gamma, A \vdash B$ le séquent $\Gamma \cup \{A\} \vdash B$.

Remarquons que la formule A peut déjà être dans Γ.

Séquent prouvable

Définition 2

Un **séquent** $\Gamma \vdash A$ est **prouvable** ou **démontrable** ou **dérivable** s'il peut être obtenu par une application finie des règles du système d'inférence.
Une **formule** A est un **théorème** si elle est $\varnothing$-dérivable, c'est-à-dire si $\vdash A$ est prouvable.

Par exemple que le séquent $A, A \rightarrow B \vdash B$ est prouvable.
Le séquent $\vdash A \rightarrow A$ l'est également.

Règles d'inférence

Les **règles d'inférence** permettent de construire les **dérivations**.

Une **dérivation formelle** est un assemblage fini de règles.

Cet assemblage n'est pas linéaire mais prend la forme d'un **arbre**.

Définition 3

Une règle se compose :

- de **prémisses**, ensemble, éventuellement vide, de séquents ;
- d'un séquent appelé **conclusion**.

Une règle sans prémisses est appelée un **axiome**

L'**arité** d'une règle est son nombre de prémisses.

Règles d'inférence

Une **règle** se représente sous la forme suivante :

- une **barre horizontale** ;
- les **prémisses (en haut)** ;
- la **conclusion (en bas)** ;
- le **nom de la règle (à droite)**.

prémisses

nom

$$\frac{\Gamma_1 \vdash A_1 \qquad \Gamma_2 \vdash A_2 \qquad \dots \qquad \Gamma_2 \vdash A_n}{\Gamma \vdash B}\ \textit{nom de la règle}$$

barre horizontale

conclusion

Règles d'inférence

Une **preuve** est un **arbre**.

La **racine** (représentée en bas) est la **conclusion** de la preuve.

Chaque **nœud** correspond à une **règle**.

Les **feuilles** correspondent aux **axiomes**, règles d'arité 0.

Règles d'inférence

À chaque symbole logique correspondent deux types de règles :

- une **règle d'introduction**, dont la conclusion est un séquent dans lequel le connecteur est introduit dans la partie de droite ;
- une **règle d'élimination**, où le connecteur apparaît dans la partie de droite d'un séquent d'une prémisse mais pas dans la conclusion.

Axiome

La règle suivante définit un **axiome** : si la conclusion fait partie des hypothèses alors le séquent est dérivable.

$$\dfrac{}{\Gamma, A \vdash A}\ ax$$

Introduction de l'implication

La règle d'**introduction de l'implication**, désignée par $\rightarrow_i$, est définie par comme suit.

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow_i$$

Cette règle peut se lire de deux façons.

- De haut en bas : si à partir de Γ et de A on peut montrer B, alors à partir de Γ on peut montrer $A \rightarrow B$.
- De bas en haut : pour montrer $A \rightarrow B$, on suppose A (on l'ajoute aux hypothèses) et on montre B.

Exemple

Montrer que pour toute formule $A \in \mathcal{F}, A \to A$ est un théorème, c'est-à-dire que l'on peut dériver le séquent $\vdash A \to A$.

Élimination de l'implication

La **règle d'éliminition de l'implication**, désignée par $\rightarrow_e$ est définie comme suit.

$$\frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \rightarrow_e$$

On reconnaît le *modus ponens*.

- De haut en bas : si à partir de Γ, on sait montrer $A \rightarrow B$ et A, alors à partir de Γ on peut montrer B.
- De bas en haut : pour montrer B, il suffit de montrer un lemme de la forme $A \rightarrow B$ et de montrer A.

Exemple

Montrer que $A, A \to B \vdash B$ (*modus ponens*) est prouvable.

Introduction de la conjonction

La **règle d'introduction de la conjonction**, désignée par $\wedge_i$ est définie comme suit.

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge_i$$

- De haut en bas : si on a A et si on a aussi B alors on a $A \wedge B$.
- De bas en haut : pour montrer $A \wedge B$, on montre A et on montre B.

Exemple

Montrer que $A, B \vdash A \wedge B$.

Élimination de la conjonction

Deux **règles d'éliminination de la conjonction**, notées $\wedge_i^g$ et $\wedge_i^d$, sont définies comme suit.

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge_e^g \qquad\qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge_e^d$$

Leurs noms ne sont pas toujours différenciés comme ci-dessus.

- De haut en bas : si on peut montrer $A \wedge B$ alors on peut montrer A (élimination gauche) et on peut montrer B (élimination droite).

Exemple

Montrer que $A \wedge B \vdash B \wedge A$.

Introduction de la disjonction

Deux **règles d'introduction de la disjonction**, notées $\vee_i^g$ et $\vee_i^d$, sont définies comme suit.

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_i^g \qquad\qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee_i^d$$

Leurs noms ne sont pas toujours différenciés comme ci-dessus.

- De haut en bas : si on peut montrer A alors on peut montrer $A \vee B$ (introduction gauche). De même à droite.
- De bas en haut : pour montrer $A \vee B$, il suffit de montrer A. De même pour B.

Élimination de la disjonction

La **règle d'élimination de la conjonction** est plus subtile. Savoir $A \vee B$ ne permet pas d'utiliser directement ni A ni B. Cette règle d'élimination correspond au *raisonnement par cas*.

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \vee_e$$

- De haut en bas : si on a C à la fois dans le cas où l'on a A et dans le cas où l'on a B et que l'on a $A \vee B$ alors on a C.
- De bas en haut : pour montrer C, on peut raisonner par cas en le montrant sous l'hypothèse A et sous l'hypothèse B, si on montre également $A \vee B$.

Exemple

Montrer le séquent $A \vee B \vdash B \vee A$.

Exemple

Montrer que $(A \to C) \vee (B \to C) \vdash (A \wedge B) \to C$.
Poser $D = (A \to C) \vee (B \to C)$ et $\Gamma = \{D, A \wedge B\}$.

Introduction de la négation

La **règle d'introduction de la négation**, désignée par $\neg_i$ est définie comme suit.

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_i$$

- De haut en bas : si en supposant A, on aboutit à une contradiction alors on n'a pas A.
- De bas en haut : pour montrer $\neg A$, on montre que supposer A aboutit à une contradiction.

Élimination de la négation

La **règle d'élimination de la négation**, désignée par $\neg_e$ est définie comme suit.

$$\frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash \bot}\ \neg_e$$

- De haut en bas : si on montre A et son contraire alors on aboutit à une contradiction.
- De bas en haut : pour montrer qu'un ensemble d'hypothèses mène à une contradiction il suffit de montrer que l'on peut en déduire une formule A et son contraire.

Exemple

Montrons que $\vdash A \to \neg\neg A$.

Affaiblissement

La règle suivante n'est pas réellement nécessaire mais elle peut être pratique. On l'appelle **règle d'affaiblissement**.

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

- De haut en bas : si on montre B en utilisant les hypothèses Γ, alors en ajoutant une hypothèse, on peut toujours montrer B.
- De bas en haut : des hypothèses peuvent ne pas servir.

Exemple

On suppose que le séquent $A \vdash B$ est dérivable (hypothèse).
Montrer que le séquent $\Gamma \vdash A \to B$ est dérivable.

Règles dérivées

Logique minimale

Les règles énoncées jusqu'ici sont celles de la **logique minimale**.

Dans cette logique le symbole $\perp$ et, par voie de conséquence, le symbole $\neg$, ne jouent pas de rôle particulier.

Elle n'est **pas complète** car on ne peut pas dériver $\vdash \perp \to A$ par exemple.

Règles dérivées

Si le jeu de règles minimal permet de démonstrer des propriétés logiques, les démonstrations peuvent parfois être longues et répétitives.

Une **règle dérivée** est une nouvelle règle obtenue à partir des règles d'inférence élémentaires. Elle n'apporte aucun pouvoir expressif mais permet de raccourcir les démonstrations.

Exemple

Montrer que la règle suivante est dérivable :

$$\frac{\Gamma \vdash A \rightarrow B}{\Gamma, A \vdash B} \rightarrow_{e'}$$

Introduction de $\top$

Si on ajoute le symbole $\top$ aux formules, il nous faut une règle pour le considérer comme un symbole particulier.

$$\frac{}{\Gamma \vdash \top}\ \top_i$$

Il s'agit d'une règle axiomatique qui indique que l'on peut toujours démontrer la formule tautologique $\top$. On ne peut en revanche rien en déduire de particulier et il n'y a pas de règle d'élimination associée.

Élimination de l'absurde

Une règle, appelée **absurdité intuitionniste**, attribue à $\perp$ un rôle particulier.

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A}\ \perp_e$$

elle correspond à la locution latine *ex falso sequitur quodlibet* : du faux, on peut déduire ce que l'on veut.

Elle peut également être vue comme une règle d'élimination du symbole $\perp$ d'où son nom $\perp_e$.

Exemple

Montrer que $\vdash \bot \to A$.

Logique intuitionniste

Logique intuitionniste

Les règles de la logique minimale complétées par l'absurdité intuitionniste sont celle de la **logique intuitionniste**.

Il s'agit d'une **logique constructive** dans laquelle le **raisonnement par l'absurde** ou **le tiers exclus** ne sont **pas admis**.

Par exemple, $\vdash A \vee \neg A$ n'est pas dérivable dans cette logique.

Exemple

Comment montrer l'existence d'un couple d'irrationnels (x, y) tel que x^y soit rationnel ?

Considérons le nombre $r = \sqrt{2}^{\sqrt{2}}$.

- Si r est rationnel, il suffit de choisir $x = \sqrt{2}$ et $y = \sqrt{2}$.
- Sinon, on choisit $x = r$ et $y = \sqrt{2}$. Alors $x^y = 2$, rationnel.

L'existence du couple est ainsi établie mais la démonstration n'est pas constructive. Elle ne donne pas explicitement le couple sauf à savoir si r est rationnel ou non [1].

1. On sait montrer que r n'est pas rationnel mais la démonstration est difficile.

Logique intuitionniste

La **logique intuitionniste** rejette donc la démonstration ci-dessus. Elle n'accepte que des preuves constructives.

Dans cette logique, avec les règles introduites jusqu'ici, pour dériver un séquent de la forme $\vdash A \vee B$, il faut être capable de dériver explicitement soit le séquent $\vdash A$ soit le séquent $\vdash B$, les seules règles à notre disposition étant les règles d'introduction de $\vee$.

On comprend pourquoi on ne peut pas dériver $\vdash A \vee \neg A$.

Raisonnement par l'absurde

Pour obtenir un **système de règles complet** et obtenir les mathématiques *classiques*, il convient d'ajouter une règle [2].

Le **raisonnement par l'absurde** (*reductio ad absurdum*) est l'une des ces règles.

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ raa$$

- De haut en bas : si supposer $\neg A$ aboutit à une contradiction alors on peut démonter A.
- De bas en haut : pour montrer A, on peut supposer que $\neg A$ et aboutir à une contradiction.

2. Plusieurs règles possibles qui donnent un système équivalent.

Raisonnement par l'absurde

Cette règle peut être appliquée à tout moment. Elle rend la recherche de preuve (un peu) plus difficile.

Elle n'est cependant nécessaire que pour des preuves non constructives, typiquement pour un séquent $\vdash A \vee B$ sans que l'on sache prouver directement $\vdash A$ ou bien $\vdash B$.

Raisonnement par l'absurde (exemple)

Montrer que l'on a $\vdash A \lor \neg A$. On note $\Gamma = \{\neg(A \lor \neg A)\}$.

Tiers exclus

Le principe du tiers exclus (*tertium non datur*) affirme que la proposition $A \vee \neg A$ est un théorème.

Le séquent $\vdash A \vee \neg A$ n'est pas dérivable en logique intuitionniste mais l'est en logique classique.

De manière intéressante la réciproque est vraie en un certain sens : ajouter à la logique intuitionniste la *règle axiomatique* suivante permet d'obtenir la logique classique !

$$\frac{}{\vdash A \vee \neg A}\ te$$

On peut également utiliser la règle suivante qui se ramène à la précédente par une séquence d'affaiblissements.

$$\frac{}{\Gamma \vdash A \vee \neg A}\ te$$

Tiers exclus

Vérifions que le raisonnement par l'absurde est dérivable dans le système formé de la logique intuitionniste auquel on adjoint l'axiome du tiers exclus.

$$\dfrac{\dfrac{}{\Gamma \vdash A \vee \neg A}\,te \qquad \dfrac{}{\Gamma, A \vdash A}\,ax \qquad \dfrac{\dfrac{}{\Gamma, \neg A \vdash \bot}\,hyp}{\Gamma, \neg A \vdash A}\,\bot_e}{\Gamma \vdash A}\,\vee_e$$

Tiers exclus

Plutôt que d'utiliser une *règle axiomatique*, on peut également utiliser la règle suivante qui indique que pour montrer B, il suffit de la montrer sous l'hypothèse A et sous l'hypothèse $\neg A$ (puisque l'on doit avoir soit l'une, soit l'autre) :

$$\frac{\Gamma, A \vdash B \quad \Gamma, \neg A \vdash B}{\Gamma \vdash B} \text{ t.e.}$$

- On dérive immédiatement cette règle à partir de la règle axiomatique du tiers exclus par une simple application de l'élimination de $\vee$.
- Inversement la règle axiomatique est immédiatement dérivable de celle-ci avec $\Gamma = \varnothing$ et $B = A \vee \neg A$.

Arbre de preuve

Arbre de preuve

Définition 4

Étant donné un système déductif, à savoir un ensemble de règles, un **arbre de preuve** ou une **dérivation** est défini par induction.

- Tout axiome $\dfrac{}{\Gamma \vdash A}\,ax$ du système de règles est un arbre de preuve réduit à une feuille racine dont la conclusion est $\Gamma \vdash A$.
- Si :

  $$\frac{\Gamma_1 \vdash A_1 \quad \Gamma_2 \vdash A_2 \quad \cdots \quad \Gamma_n \vdash A_n}{\Gamma \vdash B}\,nom$$

  est une règle d'arité $n > 0$ et si $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ sont des arbres de preuves de conclusions respectives $\Gamma_1 \vdash A_1, \Gamma \vdash A_2, \ldots, \Gamma \vdash A_n$ alors :

  $$\frac{\mathcal{A}_1 \quad \mathcal{A}_2 \quad \cdots \quad \mathcal{A}_n}{\Gamma \vdash B}\,nom$$

  est un arbre de preuve dont la racine est la règle (nom) et dont la conclusion est le séquent $\Gamma \vdash B$.

Démonstration

Définition 5

Un **séquent** $\Gamma \vdash A$ est **prouvable** ou **dérivable** s'il est la conclusion d'un arbre de preuve du système déductif. On dit que cet arbre de preuve est une preuve ou la démonstration du séquent $\Gamma \vdash A$.

Il n'y a pas unicité de la preuve, c'est-à-dire de l'arbre de preuve.

Les preuves sont des objets mathématiques, ou dit autrement simplement des arbres. La théorie de la démonstration s'intéresse aux propriétés de ces arbres,à savoir démontrer des choses à propros des démonstrations !

Taille d’une démonstration

Définition 6

La **taille** $|\mathcal{A}|$ d’une démonstration $\mathcal{A}$ est le nombre de règles utilisées dans cette démonstration. C’est le nombre de nœuds de son arbre de preuve.

On peut être amené à raisonner par induction sur la structure de la preuve ou par récurrence sur la taille de la preuve.

Proposition

Soit un système déductif de règles $\mathcal{R}$ et $r \notin \mathcal{R}$ une nouvelle règle dérivée de $\mathcal{R}$, c'est-à-dire dont la conclusion de la règle est établie en utilisant uniquement les règles de $\mathcal{R}$, en supposant ses prémisses comme hypothèses.
Alors un séquent $\Gamma \vdash A$ est dérivable dans le système $\mathcal{R} \cup \{r\}$ si et seulement si il est dérivable dans le système $\mathcal{R}$.

Démonstration

Le sens réciproque est immédiat puisque qu'un arbre de preuve sur $\mathcal{R}$ est *a fortiori* un arbre de preuve sur $\mathcal{R} \cup \{r\}$.
Pour le sens direct, il suffit de remarquer que tout nœud correspondant à la règle r peut être remplacé dans l'arbre de preuve par le sous-arbre correspondant à la dérivation de la règle r dans le système $\mathcal{R}$. Pour être parfaitement rigoureux, il faudrait mener à bien l'induction, soin que l'on laisse au lecteur.

Correction et complétude d'un système déductif

Sémantique de la logique propositionnelle (rappels)

Une **valuation** est une application $v : \mathcal{V} \to \mathbb{B}$ où $\mathbb{B} = \{0, 1\}$ est un ensemble binaire représentant le faux et le vrai. $\mathbb{V}$ est l'ensemble des valuations possibles.

Par induction, la valuation v se prolonge en $v^* : \mathcal{F} \to \mathbb{B}$, appelée fonction **évaluation**, définie sur les formules. A et B étant deux formules, on a :

- $v^*(\bot) = 0$
- $v^*(\top) = 1$
- $\forall x \in \mathcal{V},\ v^*(x) = v(x)$
- $v^*(\neg A) = 1 - v^*(A)$
- $v^*(A \wedge B) = \min\{v^*(A), v^*(B)\}$
- $v^*(A \vee B) = \max\{v^*(A), v^*(B)\}$
- $v^*(A \to B) = \max\{1 - v^*(A), v^*(B)\}$

Sémantique de la logique propositionnelle (rappels)

Une valuation v est un **modèle d'une formule** $A \in \mathcal{F}$ si $v^*(A) = 1$, ce qu'on note $v \vDash A$. On dit alors que **v satisfait A**.

On note $\mathbb{M}(A) = \{v \mid v \vDash A\}$ l'**ensemble des modèles** de A.

Satisfiabilité

Une formule A est **satisfiable** si elle admet au moins un modèle : $\mathbb{M}(A) \neq \varnothing$. Il existe donc une valuation v telle que $v \models A$.

Une formule A insatisfiable est appelée une **contradiction** ou une **antilogie** : $\mathbb{M}(A) = \varnothing$.

Une formule A est une **tautologie** ou est dite **valide** si toute valuation est un modèle de A : $\mathbb{M}(A) = \mathbb{V}$. On note $\models A$.

Équivalence sémantique et équisatisfiabilité

Deux formules A et B sont **sémantiquement équivalentes** si elles ont les mêmes modèles : $\mathbb{M}(A) = \mathbb{M}(B)$. Dit autrement, elle sont satisfaites par exactement les mêmes valuations. On note $A \equiv B$.

Deux formules A et B sont **équisatisfiables** si $\mathbb{M}(A) \neq \varnothing$ est équivalent à $\mathbb{M}(B) \neq \varnothing$: l'une est satisfiable si et seulement si l'autre l'est, sans que ce soit nécessairement exactement pour les mêmes valuations.

Équivalence sémantique et équisatisfiabilité

Proposition

Soient $A, B \in \mathcal{F}$. $A \equiv B$ si et seulement si $\vDash A \leftrightarrow B$.

Attention aux trois sens différents de l'équivalence.

- $\leftrightarrow$ est un symbole logique reliant deux formules et donnant une formule. Ce n'est qu'une notation pour $(A \to B) \land (B \to A)$ mais on pourrait parfaitement le rajouter à la syntaxe.
- $\equiv$ est l'équivalence sémantique entre deux formules.
- *Si et seulement si* est l'équivalence du discours mathématique dans lequel on se place.

Conséquence sémantique

Une formule A a pour **conséquence logique** ou pour **conséquence sémantique** une formule B si $\mathbb{M}(A) \subseteq \mathbb{M}(B)$: tout modèle de A est un modèle de B. On note $A \models B$.

C'est la même notation que pour $v \models B$ qui veut dire que la valuation v satisfait B alors que $A \models B$ veut dire que toute valuation qui satisfait A satisfait aussi B. Comme ce ne ce sont pas les mêmes objets, cela ne prête normalement pas à confusion.

Généralisation aux ensembles de formules

Proposition

Soient $A, B \in \mathcal{F}$. $A \models B$ si et seulement si $\models A \rightarrow B$.

Définition 7

Un **modèle d'un ensemble de formules** $\Gamma \subseteq \mathcal{F}$ est une valuation v qui satisfait toutes les formules de Γ. On note $\mathbb{M}(\Gamma)$ l'ensemble des modèles de Γ.

Γ est **satisfiable** si $\mathbb{M}(\Gamma) \neq \varnothing$; **insatisfiable** sinon.

Une formule A est **conséquence logique** d'un ensemble de formules Γ, ce qu'on note $\Gamma \models A$, si $\mathbb{M}(\Gamma) \subseteq \mathbb{M}(A)$: toute valuation qui satisfait toutes les formules de Γ satisfait aussi A.

Syntaxe et sémantique

Soient un système déductif (ensemble de règles), $\Gamma \subseteq \mathcal{F}$ un ensemble de formules et $A \in \mathcal{F}$ une formule.

- $\Gamma \vdash A$ signifie qu'**il existe une démonstration**, c'est-à-dire un arbre de preuve de conclusion $\Gamma \vdash A$.
  Intuitivement : *sous les hypothèses des formules de* Γ *on peut montrer la formule* A. C'est le **domaine syntaxique**.

- $\Gamma \vDash A$ signifie que A est **conséquence sémantique des formules** de Γ.
  Intuitivement : *si toutes les formules de* Γ *sont « vraies », alors* A *aussi*. C'est le **domaine sémantique**.

Correction et complétude

Il reste à relier ces deux domaines, c'est-à-dire vérifier que l'on ne démontre que des choses « vraies », c'est ce que l'on appelle la **correction** et inversement que si quelque chose est « vraie », alors on sait le **démontrer**.

- Un **système déductif** est **correct** si $\Gamma \vdash A$ implique $\Gamma \vDash A$. Autrement dit, si on peut montrer le séquent $\Gamma \vdash A$ alors c'est que A est conséquence logique de Γ.
- Un **système déductif** est **complet** si $\Gamma \vDash A$ implique $\Gamma \vdash A$. Autrement dit, si A est conséquence sémantique de Γ, alors on peut prouver A sous les hypothèses Γ.

Correction et complétude

Proposition

La logique classique est correcte.

Démonstration

La démonstration, longue et pénible en toute rigueur, montre que toutes les règles sont correctes et puis conclut par induction. Montrons-le pour quelques règles.

Règle axiomatique. Il faut vérifier que l'on a bien $\Gamma, A \vDash A$. D'après le deuxième point de l'exercice précédent on a $\mathbb{M}(\Gamma \cup \{A\}) \subseteq \mathbb{M}(A)$ car $\{A\} \subseteq \Gamma \cup \{A\}$, ce qui est précisément ce qu'il fallait montrer.

Règle d'introduction de la conjonction. Il faut montrer que sous les hypothèses $\Gamma \vDash A$ et $\Gamma \vDash B$ on a $\Gamma \vDash A \wedge B$. On suppose que l'on a $\Gamma \vDash A$, donc $\mathbb{M}(\Gamma) \subseteq \mathbb{M}(A)$, et $\Gamma \vDash B$, donc $\mathbb{M}(\Gamma) \subseteq \mathbb{M}(B)$. On a donc $\mathbb{M}(\Gamma) \subseteq \mathbb{M}(A) \cap \mathbb{M}(B) = \mathbb{M}(A \wedge B)$ et donc $\Gamma \vDash A \wedge B$, ce qu'il fallait montrer.

Règle d'élimination de la disjonction. On suppose que l'on $a\Gamma \vDash A \vee B$ et donc $\mathbb{M}(\Gamma) \subseteq \mathbb{M}(A) \cup \mathbb{M}(B)$. On suppose également que $\Gamma, A \vDash C$ donc que $\mathbb{M}(\Gamma) \cap \mathbb{M}(A) \subseteq \mathbb{M}(C)$ et de même que $\mathbb{M}(\Gamma) \cap \mathbb{M}(B) \subseteq \mathbb{M}(C)$. Soit $v \in \mathbb{M}(\Gamma)$. Si $v \in \mathbb{M}(A)$, on a donc $v \in \mathbb{M}(\Gamma) \cap \mathbb{M}(A)$ donc $v \in \mathbb{M}(C)$. Sinon comme $\mathbb{M}(\Gamma) \subseteq \mathbb{M}(A) \cup \mathbb{M}(B)$ on a $v \in \mathbb{M}(B)$, donc $v \in \mathbb{M}(\Gamma) \cap \mathbb{M}(C)$ et donc $v \in \mathbb{M}(C)$. Dans les deux cas $v \in \mathbb{M}(C)$. On a donc $\mathbb{M}(\Gamma) \in \mathbb{M}(C)$ c'est-à-dire $\Gamma \vDash C$, ce qu'il fallait montrer.

Et ainsi de suite pour toutes les autres règles. On conclut par induction sur la formule A pour montrer que si $\Gamma \vdash A$ alors $\Gamma \vDash A$.

Complétude de la logique classique (HP)

Théorème 8

La logique classique est complète.

En corollaire, le séquent $\Gamma \vdash A$ est dérivable si et seulement si $\Gamma \vDash A$. En corollaire également, les théorèmes sont exactement les tautologies.

Le **thèorème de complétude** et sa démonstration (difficile) sont HP. Il ne peut donc pas être utilisé. Pour montrer qu'un séquent $\vdash A$ est dérivable, il faut **dériver un arbre de preuve** et non établir sémantiquement que A est une tautologie puis conclure avec le théorème.

Pour finir, la logique minimale et la logique intuitionniste ne sont pas complètes.

Logique du premier ordre

Règles pour les quantificateurs

Les **quantifications** font partie intégrante des énoncés et du raisonnement mathématique ordinaires. Elles s'intègrent donc dans la déduction naturelle.

Comme pour les connecteurs de la logique propositionnelle, chaque **quantificateur** est associé à

- une **règle d'introduction** indiquant comment démontrer une formule quantifiée ;
- une **règle d'élimination** indiquant comment utiliser une formule quantifiée préalablement démontrée.

Quantification universelle

Une **formule** $\forall x.\varphi$ est **valide** lorsque la formule φ, qui dépend potentiellement d'un élément x, est vraie indépendamment de la valeur de x. Un critère garantissant cette indépendance est l'absence dans une preuve de toute hypothèse mentionnant x.

La **règle d'introduction de la quantification universelle**, aussi appelée *règle de généralisation*, autorise donc à introduire une quantification universelle dans une formule préalablement démontrée, sous condition que cette démonstration ait été faite dans un contexte ne supposant rien sur la variable concernée.

$$\frac{\Gamma \vdash \varphi \qquad x \text{ n'apparaît pas libre dans } \Gamma}{\Gamma \vdash \forall x.\varphi}\ \forall_i$$

Quantification universelle

Supposons maintenant une formule $\forall x.\varphi$ vraie.

La validité de φ indépendamment de la valeur de x signifie que l'on peut remplacer x dans φ par n'importe quel objet concret, et la formule obtenue sera encore vraie.

La **règle d'élimination de la quantification universelle**, appelée *règle d'instanciation*, énonce précisément ce mode d'utilisation, à l'aide d'une substitution.

$$\frac{\Gamma \vdash \forall x.\varphi}{\Gamma \vdash \varphi^{\{x \leftarrow t\}}} \ \forall_e$$

Quantification existentielle

Une **formule** $\exists x.\varphi$ est **valide** dès lors qu'au moins une des valeurs possibles de x rend la formule φ vraie.

Ainsi, on peut justifier une telle formule en fournissant une telle valeur, appelée **témoin**, et en justifiant la formule obtenue en donnant cette valeur témoin à x.

La **règle d'introduction de la quantification existentielle** réalise ce critère en demandant de justifier une formule obtenue par substitution à partir de φ. La valeur t substituée est précisément le témoin.

$$\frac{\Gamma \vdash \varphi^{\{x \leftarrow t\}}}{\Gamma \vdash \exists x.\varphi}\ \exists_i$$

Quantification existentielle

Dans un raisonnement mathématique usuel, on utilise un résultat existentiel en introduisant un élément témoin.

Lors de cette introduction, on n'a aucun contrôle sur ce qu'est exactement ce témoin : la seule connaissance que nous en avons est qu'il satisfait la formule.

Aussi, on continue à désigner le témoin par un nom de variable x, qu'on suppose indépendant de toutes les autres variables présentes, et on poursuit la démonstration en prenant pour seule hypothèse sur x la validité de la formule φ.

Quantification existentielle

Dans la **règle d'élimination de la quantification existentielle**, ceci se manifeste par un critère secondaire demandant que la variable x ne soit mentionnée dans aucune autre formule : ni les hypothèses, ni même la conclusion.

$$\frac{\Gamma \vdash \exists x.\varphi \qquad \Gamma, \varphi \vdash \psi \qquad x \text{ n'apparaît libre ni dans } \Gamma \text{ ni dans } \psi}{\Gamma \vdash \psi}\ \exists_e$$

Comme pour la disjonction, dont la quantification existentielle est par nature assez proche, on utilise volontiers une variante de règle dans laquelle on élimine une quantification universelle présente en hypothèse. Avec abus de notation, $x \notin \Gamma, \psi$ rappelle l'indépendance de x par rapport aux différentes formules.

$$\frac{\Gamma, \varphi \vdash \psi \qquad x \notin \Gamma, \psi}{\Gamma, \exists x.\varphi \vdash \psi}\ \exists_e$$