Informatique *Cours*

Logique Ipesup

Objectifs

À l'issue de cette section, l'étudiant devra être capable de :
- comprendre le principe de la déduction naturelle et la notion de séquent ;
- identifier et appliquer correctement les règles d'introduction et d'élimination ;
- construire des arbres de dérivation en logique propositionnelle et du premier ordre ;
- raisonner avec des hypothèses locales, des quantificateurs et le raisonnement par l'absurde.

1 Logique du premier ordre

La logique du premier ordre étend la logique propositionnelle en introduisant des objets (*termes*) décrits par des *prédicats*, et des *quantificateurs* permettant d'exprimer des propriétés valables pour tout ou partie de ces objets.

1.1 Domaine, termes et prédicats

Considérons un tableau a de 4 entiers $a[0], a[1], a[2], a[3]$. Le tableau lui-même, les valeurs qu'il contient et les indices de ses cases constituent le *domaine* sur lequel portent nos formules. La notation $a[i]$ peut être vue comme l'application d'un *symbole de fonction* `pos`, d'arité 2, tel que $\texttt{pos}(a, i) = a[i]$.

Introduisons ensuite des *symboles de prédicats*. Le prédicat unaire `even` exprime la parité d'un entier, tandis que le prédicat binaire `leq` représente la relation « inférieur ou égal à ». Ces symboles sont définis indépendamment de toute valeur de vérité et peuvent être combinés pour former des *formules atomiques*, par exemple

$$\texttt{even}(\texttt{pos}(a, 0)) \qquad \texttt{leq}(\texttt{pos}(a, 2), \texttt{pos}(a, 0)).$$

À l'aide des connecteurs logiques usuels, on peut construire des formules plus complexes, telles que

$$\texttt{even}(\texttt{pos}(a, 0)) \wedge \texttt{even}(\texttt{pos}(a, 1)) \wedge \texttt{even}(\texttt{pos}(a, 2)) \wedge \texttt{even}(\texttt{pos}(a, 3)),$$

qui affirme que tous les éléments du tableau sont pairs. Cette conjonction peut être abrégée sous la forme

$$\bigwedge_{i=0}^{3} \texttt{even}(\texttt{pos}(a, i)),$$

sans changer la structure logique de la formule.

Pour exprimer plus directement le caractère universel de cette propriété, on introduit le *quantificateur universel* $\forall$ et on écrit

$$\forall i \in [0, 3].\ \texttt{even}(\texttt{pos}(a, i)),$$

ou, de manière équivalente,

$$\forall i.\ \Big((\texttt{leq}(0,i) \wedge \texttt{leq}(i,3)) \rightarrow \texttt{even}(\texttt{pos}(a,i))\Big).$$

Une telle formule est vraie dès lors que l'énoncé qu'elle contient est satisfait pour tout élément du domaine.

On y distingue alors :

— les *symboles de constantes* 0, 3 et a ;
— le *symbole de fonction* `pos` ;
— les *symboles de prédicats* `leq` et `even` ;
— le *symbole de variable* i ;
— les *connecteurs* $\wedge$ et $\rightarrow$;
— le *quantificateur* $\forall$.

De manière générale, un domaine logique est spécifié en fixant :

— un ensemble infini dénombrable X de *symboles de variables* ;
— un ensemble S_f de *symboles de fonctions*, chaque symbole étant muni d'une arité ;
— un ensemble non vide S_p de *symboles de prédicats*.

Ces ensembles sont supposés disjoints. Les symboles de fonctions d'arité k forment l'ensemble S_f^k, les constantes correspondant au cas $k = 0$. De même, S_p^k désigne l'ensemble des prédicats d'arité k ; les éléments de S_p^0, appelés *propositions*, jouent le rôle des variables propositionnelles de la logique des propositions.

Exemple

La formule

$$\forall i.\ \Big((\texttt{leq}(0,i) \wedge \texttt{leq}(i,3)) \rightarrow \texttt{even}(\texttt{pos}(a,i))\Big)$$

fait intervenir les ensembles suivants :
— $X = \{i\}$;
— $S_f = S_f^0 \cup S_f^2$ avec $S_f^0 = \{0, 3, a\}$ et $S_f^2 = \{\texttt{pos}\}$;
— $S_p = S_p^1 \cup S_p^2$ avec $S_p^1 = \{\texttt{even}\}$ et $S_p^2 = \{\texttt{leq}\}$.

Terme

Une *signature* sur X et S_f définit l'ensemble des termes par induction :
— tout symbole de variable de X est un terme ;
— tout symbole de constante de S_f^0 est un terme ;
— si $t_1, \ldots, t_k$ sont des termes et si $f \in S_f^k$, alors $f(t_1, \ldots, t_k)$ est un terme.

Exemple

Soit le symbole de constante Z (arité 0), le symbole de fonction `suc` (arité 1) qui représente la fonction successeur, les symboles de fonction `add` et `mul` d'arité 2 qui représentent les fonctions d'addition et de multiplication.
Ainsi,

$$S_f = \{Z^{(0)}, \texttt{suc}^{(1)}, \texttt{add}^{(2)}, \texttt{mul}^{(2)}\}.$$

Alors (X, S_f) définit une signature sur les entiers naturels.
Si $x, y \in X$, l'expression suivante est un terme sur (X, S_f) :

$$\texttt{add}(\texttt{mul}(\texttt{suc}(\texttt{suc}(\texttt{suc}(Z))), x), \texttt{suc}(\texttt{mul}(\texttt{suc}(\texttt{suc}(Z)), y)))$$

qui représente l'expression mathématique $(3x + (2y + 1))$. On peut lui associer l'arbre suivant.

1.2 Formules du premier ordre

Les prédicats appliqués à des éléments du domaine constituent les briques de base de la logique du premier ordre : ce sont les *formules atomiques*.

Formule atomique

Une *formule atomique* sur (X, S_f, S_p) est une expression de la forme

$$p(t_1, \dots, t_k),$$

où $p \in S_p^k$ est un symbole de prédicat et $t_1, \dots, t_k$ sont des termes.

Outre les connecteurs logiques usuels, la logique du premier ordre introduit des *quantificateurs*, qui précisent la portée des variables sur le domaine.

Quantificateurs

La logique du premier ordre utilise deux quantificateurs :
- le quantificateur universel $\forall$, qui exprime qu'une propriété est vérifiée par tous les éléments du domaine ;
- le quantificateur existentiel $\exists$, qui affirme l'existence d'au moins un élément satisfaisant une propriété.

Dans les formules, les quantificateurs sont prioritaires sur les connecteurs logiques.

Formule du premier ordre

Les formules du premier ordre sur (X, S_f, S_p) sont définies inductivement :
- toute formule atomique est une formule ;
- si φ est une formule, alors $\neg\varphi$ en est une ;
- si φ et ψ sont des formules, alors $\varphi \wedge \psi$, $\varphi \vee \psi$ et $\varphi \to \psi$ sont des formules ;
- si $x \in X$ et φ est une formule, alors $\forall x.\varphi$ et $\exists x.\varphi$ sont des formules.

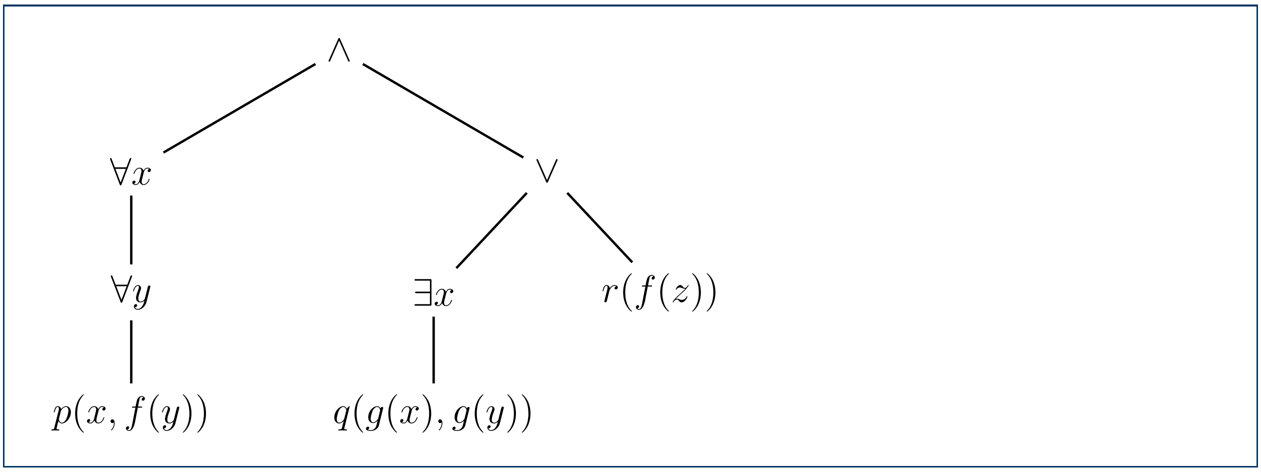
Toute formule peut être représentée par un arbre syntaxique, dont les feuilles correspondent aux formules atomiques.

Exemple

La formule :

$$\varphi = (\forall x.\forall y.p(x, f(y))) \wedge ((\exists x.q(g(x), g(y))) \vee r(f(z)))$$

peut être représentée par l'arbre suivant.



Dans une formule, les variables de X peuvent apparaître sous un quantificateur ou de manière isolée.

Variables libres et liées

Une variable $x \in X$ est dite *liée* lorsqu'elle apparaît dans la portée d'un quantificateur. Sinon, elle est dite *libre*.

Dans l'exemple precedente, la formule atomique $p(x, f(y))$ contient deux variables liées x et y, introduites respectivement par les quantificateurs $\forall x$ et $\forall y$, dont la portée se limite à cette formule. La formule $q(g(x), g(y))$ contient une variable liée x et une variable libre y, tandis que la formule $r(f(z))$ ne contient qu'une variable libre z.

Portée

Dans une formule $\forall x.\varphi$ ou $\exists x.\varphi$, la *portée* du quantificateur est la formule φ.

1.3 Substitution d'une variable

Pour exploiter une formule de portée générale dans des cas particuliers, on peut procéder à une *substitution*, consistant à remplacer une variable *libre* par un terme.

Par exemple, si $f \in S_f^1$ et $p \in S_p^2$, la substitution de x par $f(z)$ dans la formule

$$\exists y.p(x, y)$$

donne

$$\exists y.p(f(z), y),$$

ce que l'on note

$$(\exists y.p(x, y))^{\{x \leftarrow f(z)\}} = \exists y.p(f(z), y).$$

La substitution n'a de sens que pour des variables libres : substituer une variable liée est interdit. Lorsqu'une variable liée interfère avec la substitution, il faut d'abord *renommer* cette variable, puis effectuer la substitution. Ainsi,

$$(\exists y.p(x, y))^{\{x \leftarrow f(y)\}} = (\exists z.p(x, z))^{\{x \leftarrow f(y)\}} = (\exists z.p(f(y), z)).$$

Substitution d'une variable libre

Soit φ et ψ deux formules logiques, t un terme et x une variable libre susceptible d'être présente dans les deux formules.

$$\begin{aligned}
p(t_1,\dots,t_k)^{\{x\leftarrow t\}} &= p(t_1^{\{x\leftarrow t\}},\dots,t_k^{\{x\leftarrow t\}})\\
(\neg\varphi)^{\{x\leftarrow t\}} &= \neg(\varphi^{\{x\leftarrow t\}})\\
(\varphi\diamond\psi)^{\{x\leftarrow t\}} &= \varphi^{\{x\leftarrow t\}}\diamond\psi^{\{x\leftarrow t\}} \qquad (\diamond \text{ connecteur binaire})\\
(\forall y.\varphi)^{\{x\leftarrow t\}} &= \forall y.(\varphi^{\{x\leftarrow t\}})\\
(\exists y.\varphi)^{\{x\leftarrow t\}} &= \exists y.(\varphi^{\{x\leftarrow t\}})
\end{aligned}$$

Variables propositionnelles et variables du premier ordre

Selon le contexte, la lettre x peut désigner soit une variable propositionnelle, représentant un fait logique indéterminé en logique propositionnelle, soit une variable du premier ordre, représentant un objet indéterminé du domaine. Ces deux usages n'apparaissent toutefois jamais dans une même formule, ce qui exclut toute ambiguïté.

1.4 Sémantique intuitive des quantificateurs

Donner formellement une sémantique aux formules du premier ordre est assez technique, et hors programme en MP2I/MPI. On se basera sur les interprétations intuitives suivantes.

Quantification universelle

Une formule $\forall x.\varphi$ est valide lorsque la formule φ est vraie pour toute valeur v du domaine, c'est-à-dire lorsque $\varphi^{\{x\leftarrow v\}}$ est vraie pour tout v.

Quantification existentielle

Une formule $\exists x.\varphi$ est valide lorsqu'il existe au moins une valeur v du domaine telle que $\varphi^{\{x\leftarrow v\}}$ soit vraie.
On peut interpréter $\forall x.\varphi$ comme une conjonction (éventuellement infinie) de toutes les instanciations de φ, et $\exists x.\varphi$ comme la disjonction correspondante. Cette lecture conduit aux équivalents quantifiés des lois de De Morgan :

$$\neg(\forall x.\varphi) \equiv \exists x.\neg\varphi \qquad \neg(\exists x.\varphi) \equiv \forall x.\neg\varphi.$$

Quantification bornée

On a couramment l'utilité de restreindre le domaine sur lequel porte une quantification. On en vient alors à écrire des formules quantifiées ressemblant à

$$\forall x\in[0,n[.\varphi \qquad \text{ou} \qquad \exists x\in[a,b[.\varphi.$$

Cette forme n'appartient pas à notre syntaxe des formules du premier ordre, mais peut être utilisée comme une notation, autrement dit du sucre syntaxique, pour les formules suivantes :

$$\begin{aligned}
\forall x\in E.\varphi &\equiv \forall x.(x\in E\to\varphi)\\
\exists x\in E.\varphi &\equiv \exists x.(x\in E\wedge\varphi)
\end{aligned}$$

Exemple

Considérons un tableau a de longueur n. Un objet x est le plus petit élément du tableau a si, d'une part il appartient bien au tableau, et d'autre part il est inférieur ou égal à tous les éléments du tableau. Ces deux parties de la spécification s'écrivent par deux quantifications bornées :

$$\exists i.\Big(i \in [0, n[\wedge x = a[i]\Big) \qquad \forall i.\Big(i \in [0, n[\to x \leq a[i]\Big)$$

ou, sous forme abrégée :

$$\exists i \in [0, n[.\ x = a[i] \qquad \forall i \in [0, n[.\ x \leq a[i].$$

2 Déduction naturelle

Après avoir motivé l'étude de la logique par la clarification du raisonnement, on constate que la sémantique par tables de vérité ne rend pas compte de la construction des preuves. On s'intéresse donc désormais à la *déduction*, qui étudie comment des faits supposés vrais permettent de justifier une *conclusion* à partir d'*hypothèses*.

2.1 Déduire

Le raisonnement déductif consiste à établir une *conclusion* à partir d'*hypothèses* supposées vraies, en montrant que certains faits s'ensuivent nécessairement d'autres. Il ne garantit ni la validité des hypothèses, ni celle de la conclusion en elle-même, mais seulement un lien de conséquence : si les hypothèses sont vraies, alors la conclusion l'est aussi.

La déduction soulève ainsi deux questions distinctes : déterminer ce qui peut servir d'hypothèse valide, et caractériser les règles garantissant qu'un fait est une conséquence nécessaire d'autres faits. La première relève de considérations philosophiques, tandis que la seconde constitue le cœur de la logique, auquel nous allons désormais nous consacrer.

Racines antiques.

Les premières formalisation du raisonnement correct apparaissent dans l'Antiquité. Elles reposent sur l'identification des énoncés pertinents et sur des règles de déduction, appelées *syllogismes*, permettant d'inférer de nouveaux faits à partir de faits établis.
La tradition aristotélicienne (IV^{e} siècle av. J.-C.) domine longtemps la pensée logique européenne. Elle propose une forme rigide de raisonnement fondée sur des catégories et des quantifications, illustrée par le syllogisme classique « Tous les hommes sont mortels, Socrate est un homme, donc Socrate est mortel ».
Parallèlement, Chrysippe de Soles (III^{e} siècle av. J.-C.) développe une logique propositionnelle primitive, centrée sur les connecteurs logiques et leurs interactions, dont le *syllogisme disjonctif* constitue un exemple fondamental.

Raisonnement syllogistique

Considérons les énoncés suivants, qu'un élève tente de traiter mentalement pendant un 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.

En notant P le fait de participer, B celui de dire des bêtises, H avoir la honte et R réussir, ces énoncés se traduisent en logique propositionnelle par :

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

À partir de ces formules, on peut déduire certaines conséquences en appliquant des syllogismes classiques, issus aussi bien de la tradition aristotélicienne que de la logique stoïcienne.

Le syllogisme *barbara*, ou transitivité de l'implication, affirme que de $\varphi_1 \to \varphi_2$ et $\varphi_2 \to \varphi_3$, on peut déduire $\varphi_1 \to \varphi_3$. En combinant les faits 1 et 2, on obtient ainsi :

$$6.\ P \to H \quad \text{« si je participe, je vais avoir la honte ».}$$

Le *modus ponens* permet ensuite d'exploiter une implication : si $\varphi_1 \to \varphi_2$ est vraie et que φ_1 l'est aussi, alors φ_2 est nécessairement vraie. En combinant les faits 3 et 6, on en déduit :

$$7.\ \neg P \quad \text{« je ne participe pas ».}$$

Le *modus tollens*, lié à la contraposition, permet quant à lui de raisonner à partir de la négation de la conclusion : si $\varphi_1 \to \varphi_2$ est vraie et que φ_2 est fausse, alors φ_1 est nécessairement fausse. En combinant les faits 4 et 7, on obtient :

$$8.\ \neg R \quad \text{« je ne vais pas réussir ».}$$

Enfin, une dernière application du *modus ponens* aux faits 5 et 8 conduit à :

$$9.\ H \quad \text{« je vais avoir la honte ».}$$

L'élève conclut ainsi que l'échec et la honte sont des conséquences nécessaires des cinq énoncés initiaux. Il faut toutefois rappeler que ce raisonnement n'est valide que si toutes les hypothèses de départ sont effectivement vraies. Libre à l'élève de remettre en question celles qu'il juge infondées afin d'éviter une conclusion aussi peu réjouissante.

Notations alternatives des syllogismes

Un syllogisme permettant de déduire une conclusion ψ à partir de prémisses φ_1 et φ_2 est souvent noté

$$\varphi_1, \varphi_2 \vdash \psi,$$

où $\vdash$ exprime une relation de conséquence logique, par analogie avec la conséquence sémantique notée $\models$. On peut ainsi écrire :

- **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** : $\varphi_1 \lor \varphi_2,\ \neg\varphi_1 \vdash \varphi_2$.

Nous n'utiliserons toutefois pas cette notation afin d'éviter toute confusion avec l'usage ultérieur du symbole $\vdash$.
Les noms traditionnels des syllogismes constituent un mnémotechnique médiéval. Les voyelles qu'ils contiennent codent la nature des prémisses et de la conclusion (affirmatives ou négatives, universelles ou particulières), selon une classification introduite par Aristote. Seuls les schémas effectivement valides ont reçu un nom.

2.2 Vers la logique moderne.

À partir de la fin du XIXᵉ siècle, la logique connaît un profond renouvellement visant la formalisation du raisonnement mathématique, sous l'impulsion de chercheurs issus à la fois de la philosophie et des mathématiques, tels que Frege ou Russell. Cette évolution rapproche la logique de la pratique mathématique moderne et réintègre certaines idées issues de la logique stoïcienne, longtemps délaissées par la scholastique médiévale. Dans la suite du chapitre, nous nous concentrons sur cette approche moderne du raisonnement, que nous illustrons à l'aide d'une démonstration mathématique.

Lors de l'étude de la recherche dichotomique, on est amené à démontrer un énoncé de la forme

$$lo < hi \ \to\ lo \leq lo + \left\lfloor \frac{hi - lo}{2} \right\rfloor < hi.$$

Nous en donnons ici une version détaillée afin d'en mettre en évidence la structure logique.

Démonstration. Soient lo et hi deux entiers positifs, et posons

$$mid = lo + \left\lfloor \frac{hi - lo}{2} \right\rfloor.$$

Supposons $lo < hi$, ce qui implique immédiatement $hi - lo > 0$. Raisonnons par cas sur la parité de $hi - lo$.

Cas $hi - lo$ pair

Il existe alors un entier k tel que $hi - lo = 2k$, d'où

$$\left\lfloor \frac{hi - lo}{2} \right\rfloor = k \qquad \text{et} \qquad mid = lo + k.$$

Borne gauche. Comme $k \geq 0$, on a $mid \geq lo$.

Borne droite. Puisque $hi - lo > 0$, on a $k \neq 0$ et donc

$$mid = lo + k < lo + (hi - lo) = hi.$$

Cas $hi - lo$ impair

Il existe alors un entier k tel que $hi - lo = 2k + 1$, ce qui donne encore

$$\left\lfloor \frac{hi - lo}{2} \right\rfloor = k \qquad \text{et} \qquad mid = lo + k.$$

Borne gauche. Comme précédemment, $k \geq 0$ implique $mid \geq lo$.

Borne droite. On a

$$mid = lo + k < lo + 2k + 1 = hi.$$

Dans les deux cas, l'encadrement recherché est vérifié, ce qui conclut la démonstration. □

Cette preuve illustre plusieurs traits fondamentaux du raisonnement mathématique. Elle est d'abord structurée en branches correspondant à des cas distincts, eux-mêmes subdivisés en objectifs intermédiaires. Chaque branche est traitée indépendamment, et leurs conclusions se combinent pour établir le résultat global.

Par ailleurs, la démonstration fait intervenir des hypothèses introduites de manière locale : l'hypothèse de parité de $hi - lo$ n'est valable que dans la branche correspondante, tandis que l'hypothèse initiale $lo < hi$ est commune à l'ensemble de la preuve. Ainsi, à chaque étape, seules les hypothèses introduites le long de la branche courante sont accessibles.

Une preuve mathématique ordinaire possède donc une structure arborescente et repose sur des contextes d'hypothèses variables. Un formalisme logique destiné à décrire de telles preuves doit rendre compte de ces notions de branches et de contextes locaux : c'est précisément l'objectif de la *déduction naturelle*, que nous allons maintenant étudier.

2.3 Déduction naturelle propositionnelle

La *déduction naturelle*, introduite par Gerhard Gentzen en 1934, est un système de règles de déduction visant à formaliser au plus près les raisonnements utilisés dans les preuves mathématiques usuelles.

L'idée centrale est la suivante : à chaque étape d'une démonstration, on dispose d'un ensemble de faits — hypothèses supposées vraies ou résultats déjà établis — et l'on cherche à justifier une conclusion donnée. La démonstration consiste alors à réduire progressivement l'écart entre ces faits disponibles et la conclusion visée.

On note

$$hyp_1, \ldots, hyp_n \vdash concl$$

lorsqu'une conclusion *concl* peut être déduite des hypothèses $hyp_1, \ldots, hyp_n$. La déduction naturelle étudie précisément quelles conclusions sont démontrables à partir d'un ensemble donné d'hypothèses.

Certaines situations sont immédiates : une preuve est terminée dès que la conclusion recherchée appartient déjà à l'ensemble des hypothèses. Dans les autres cas, la démonstration progresse à l'aide de *règles d'inférence*, qui relient différentes configurations « hypothèses–conclusion » correspondant aux étapes successives du raisonnement.

Cadre de la déduction naturelle. La déduction naturelle manipule essentiellement des relations entre un ensemble d'hypothèses et une conclusion.

Séquents

Soit $\mathcal{F}$ l'ensemble des formules logiques. Le symbole $\vdash$ désigne une relation binaire sur $\mathcal{P}(\mathcal{F}) \times \mathcal{F}$: un *séquent* $\Gamma \vdash \varphi$ exprime que la formule φ peut être justifiée en ne supposant que les hypothèses $\Gamma \subseteq \mathcal{F}$. On parle également de *jugement*.

Un séquent $\Gamma \vdash \varphi$ peut être interprété comme une forme de conséquence logique : si toutes les formules de Γ sont vraies, alors φ l'est nécessairement. Cette conséquence n'est toutefois pas définie sémantiquement, mais par l'existence d'une déduction fondée sur des règles de raisonnement.

Règles d'inférence

Une *règle d'inférence* est constituée d'un ensemble fini de séquents, appelés *prémisses*,

$$\Gamma_1 \vdash \varphi_1,\ \ldots,\ \Gamma_n \vdash \varphi_n,$$

et d'un séquent, appelé *conclusion*, noté $\Gamma \vdash \varphi$. Elle est traditionnellement représentée par

$$\frac{\Gamma_1 \vdash \varphi_1 \qquad \cdots \qquad \Gamma_n \vdash \varphi_n}{\Gamma \vdash \varphi},$$

et autorise la déduction immédiate de la conclusion à partir des prémisses. Une règle sans prémisses est appelée un *axiome*.

Les prémisses d'une règle correspondent aux étapes préalables nécessaires à son application. Les règles sont en général annotées par un nom indiquant la nature du raisonnement effectué.

Le cas le plus simple correspond à une preuve terminée : lorsque la conclusion à établir figure déjà parmi les hypothèses. On dispose alors de l'axiome

$$\frac{}{\varphi_1, \ldots, \varphi_n \vdash \varphi_i}\ (\textsc{hyp}), \qquad i \in [1, n].$$

Le système de déduction naturelle est ensuite construit en répondant, pour chaque connecteur logique, aux deux questions suivantes :

1. comment justifier un séquent $\Gamma \vdash \varphi$?
2. comment exploiter un séquent $\Gamma \vdash \varphi$ déjà établi ?

Les règles associées à la première question sont appelées *règles d'introduction*, celles associées à la seconde des *règles d'élimination*. Nous les introduirons progressivement, connecteur par connecteur, avant d'en donner un récapitulatif global.

Conjonction. Une formule $\varphi_1 \wedge \varphi_2$ est vraie lorsque φ_1 et φ_2 sont toutes deux vraies. Pour justifier une telle formule, il suffit donc de justifier séparément chacune de ses composantes :

$$\frac{\Gamma \vdash \varphi_1 \qquad \Gamma \vdash \varphi_2}{\Gamma \vdash \varphi_1 \wedge \varphi_2}\ (\wedge_i)$$

La démonstration d'une conjonction se décompose ainsi en deux démonstrations indépendantes, menées dans le même contexte d'hypothèses Γ. Comme pour la règle HYP, cette règle est valable pour tout contexte Γ et toutes formules φ_1, φ_2.

Réciproquement, si une conjonction est déjà établie, on peut en extraire chacune de ses composantes à l'aide des règles d'élimination :

$$\frac{\Gamma \vdash \varphi_1 \wedge \varphi_2}{\Gamma \vdash \varphi_1}\ (\wedge_e) \qquad \frac{\Gamma \vdash \varphi_1 \wedge \varphi_2}{\Gamma \vdash \varphi_2}\ (\wedge_e)$$

Les règles sont nommées à partir du connecteur concerné, avec l'indice i pour l'introduction et e pour l'élimination. Cette convention sera conservée dans toute la suite.

Implication. Une formule $\varphi_1 \to \varphi_2$ est valide lorsque la vérité de φ_1 entraîne nécessairement celle de φ_2. Pour justifier une telle implication, on suppose φ_1 vraie et l'on montre que cette hypothèse permet de déduire φ_2 :

$$\frac{\Gamma, \varphi_1 \vdash \varphi_2}{\Gamma \vdash \varphi_1 \to \varphi_2}\ (\to_i)$$

La démonstration d'une implication consiste ainsi à ajouter temporairement φ_1 au contexte d'hypothèses afin d'établir φ_2.

L'utilisation d'une implication correspond au *modus ponens* : si $\varphi_1 \to \varphi_2$ est établie et que φ_1 est vraie, on peut alors conclure φ_2 :

$$\frac{\Gamma \vdash \varphi_1 \to \varphi_2 \qquad \Gamma \vdash \varphi_1}{\Gamma \vdash \varphi_2}\ (\to_e)$$

Dérivation. Un séquent $\Gamma \vdash \varphi$ est justifié en construisant une preuve, représentée sous la forme d'un arbre combinant des règles d'inférence.

Dérivation

Une *dérivation* d'un séquent $\Gamma \vdash \varphi$ est un arbre obtenu en appliquant une règle d'inférence dont la conclusion est $\Gamma \vdash \varphi$, et en reliant chacune de ses prémisses à une dérivation correspondante. Un séquent est dit *dérivable* s'il existe une dérivation finie dont il est la conclusion.

Chaque application de règle constitue un nœud de l'arbre, et les dérivations des prémisses en forment les sous-arbres. Les axiomes, c'est-à-dire les règles sans prémisses, correspondent aux feuilles. Une dérivation est finie si toutes ses branches se terminent par un axiome.

Exemple

On considère le séquent

$$\varphi_1 \to (\varphi_2 \to \psi) \ \vdash \ (\varphi_1 \wedge \varphi_2) \to \psi.$$

Les formules $\varphi_1 \to (\varphi_2 \to \psi)$ et $\varphi_1 \wedge \varphi_2$ apparaissant dans la majorité des contextes, on allège la notation en posant

$$\Gamma := \{\varphi_1 \to (\varphi_2 \to \psi),\ \varphi_1 \wedge \varphi_2\}.$$

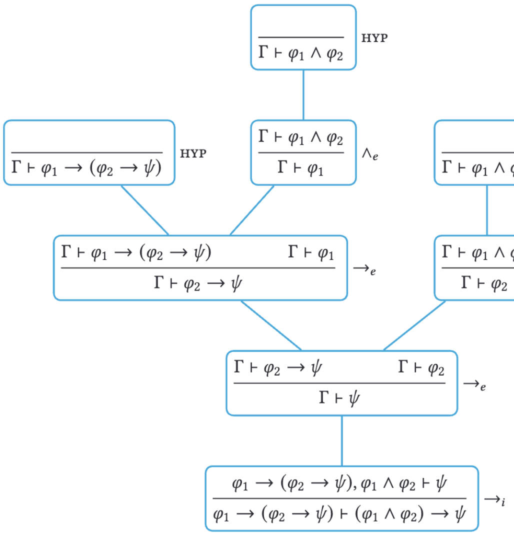
Dans un arbre de dérivation, chaque prémisse d'une règle correspond à la conclusion de la sous-dérivation associée. On notera également que la racine de l'arbre est placée en bas.

$$
\dfrac{
  \dfrac{
    \dfrac{}{\Gamma \vdash \varphi_1 \to (\varphi_2 \to \psi)}\,\textbf{HYP}
    \qquad
    \dfrac{\dfrac{}{\Gamma \vdash \varphi_1 \wedge \varphi_2}\,\textbf{HYP}}{\Gamma \vdash \varphi_1}\,\wedge_e
  }{\Gamma \vdash \varphi_2 \to \psi}\,\to_e
  \qquad
  \dfrac{\dfrac{}{\Gamma \vdash \varphi_1 \wedge \varphi_2}\,\textbf{HYP}}{\Gamma \vdash \varphi_2}\,\wedge_e
}{
  \dfrac{\varphi_1 \to (\varphi_2 \to \psi), \varphi_1 \wedge \varphi_2 \vdash \psi}{\varphi_1 \to (\varphi_2 \to \psi) \vdash (\varphi_1 \wedge \varphi_2) \to \psi}\,\to_i
}\,\to_e
$$

La démonstration du séquent réciproque $(\varphi_1 \wedge \varphi_2) \to \psi \vdash \varphi_1 \to (\varphi_2 \to \psi)$ est laissée en exercice. Les deux séquents montrent que les formules

$$\varphi_1 \to (\varphi_2 \to \psi) \quad \text{et} \quad (\varphi_1 \wedge \varphi_2) \to \psi$$

sont prouvablement équivalentes.



Disjonction. Une formule $\varphi_1 \vee \varphi_2$ est vraie dès lors qu'au moins l'une des deux formules est vraie. Pour la justifier, il suffit donc d'établir l'une des deux :

$$\dfrac{\Gamma \vdash \varphi_1}{\Gamma \vdash \varphi_1 \vee \varphi_2}\,(\vee_i) \qquad \dfrac{\Gamma \vdash \varphi_2}{\Gamma \vdash \varphi_1 \vee \varphi_2}\,(\vee_i)$$

En revanche, supposer $\varphi_1 \vee \varphi_2$ ne permet pas de conclure directement ni φ_1 ni φ_2. On procède alors par raisonnement par cas : on montre que la conclusion recherchée est valable aussi bien sous l'hypothèse φ_1 que sous l'hypothèse φ_2 :

$$\dfrac{\Gamma \vdash \varphi_1 \vee \varphi_2 \qquad \Gamma, \varphi_1 \vdash \psi \qquad \Gamma, \varphi_2 \vdash \psi}{\Gamma \vdash \psi}\,(\vee_e)$$

Les deux branches correspondent à des contextes distincts, ce qui est essentiel.

Ce principe est celui utilisé dans les raisonnements par cas classiques, par exemple lorsqu'on exploite le fait qu'un entier est soit pair, soit impair.

Pour des raisons de lisibilité, on utilise parfois une variante de la règle d'élimination lorsque la disjonction est directement une hypothèse :

$$\frac{\Gamma, \varphi_1 \vdash \psi \qquad \Gamma, \varphi_2 \vdash \psi}{\Gamma, \varphi_1 \vee \varphi_2 \vdash \psi}\ (\vee_e)$$

Cette variante n'ajoute aucun pouvoir expressif, mais permet des dérivations plus compactes.

Exemple

Montrons $\varphi \vee \psi,\ \varphi \to \psi \vdash \psi$. Le raisonnement repose sur une analyse par cas de la disjonction. On pose

$$\Gamma := \{\varphi \vee \psi,\ \varphi \to \psi\}.$$

Dérivation (version standard) :

$$\dfrac{\dfrac{}{\Gamma \vdash \varphi \vee \psi}\,\text{HYP} \qquad \dfrac{\dfrac{}{\Gamma, \varphi \vdash \varphi \to \psi}\,\text{HYP} \qquad \dfrac{}{\Gamma, \varphi \vdash \varphi}\,\text{HYP}}{\Gamma, \varphi \vdash \psi} \qquad \dfrac{}{\Gamma, \psi \vdash \psi}\,\text{HYP}}{\Gamma \vdash \psi}$$

En utilisant la variante compacte de $\vee_e$, on obtient une preuve de même structure mais plus concise. On pose

$$\Gamma' := \{\varphi \to \psi\}.$$

Dérivation (version compacte) :

$$\dfrac{\dfrac{\dfrac{}{\Gamma', \varphi \vdash \varphi \to \psi}\,\text{HYP} \qquad \dfrac{}{\Gamma', \varphi \vdash \varphi}\,\text{HYP}}{\Gamma', \varphi \vdash \psi} \qquad \dfrac{}{\Gamma', \psi \vdash \psi}\,\text{HYP}}{\Gamma', \varphi \vee \psi \vdash \psi}$$

Négation. Une formule $\neg\varphi$ est vraie lorsque φ conduit à une contradiction. Pour justifier une négation, on montre donc que l'hypothèse φ permet de déduire $\perp$:

$$\frac{\Gamma, \varphi \vdash \perp}{\Gamma \vdash \neg\varphi}\ (\neg_i)$$

Réciproquement, utiliser une négation consiste à produire une contradiction dès lors que φ est également démontrée :

$$\frac{\Gamma \vdash \neg\varphi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \perp}\ (\neg_e)$$

Exemple

Quelle que soit la formule φ, on peut démontrer le séquent $\varphi \vdash \neg\neg\varphi$.

$$\dfrac{\dfrac{\dfrac{}{\varphi, \neg\varphi \vdash \neg\varphi}\,\text{HYP} \qquad \dfrac{}{\varphi, \neg\varphi \vdash \varphi}\,\text{HYP}}{\varphi, \neg\varphi \vdash \perp}}{\varphi \vdash \neg\neg\varphi}\,\neg_e$$

La réciproque n'est pas démontrable avec les règles actuelles ; elle le deviendra après l'introduction du raisonnement par l'absurde.

Tautologie. La constante $\top$ désigne une formule toujours vraie, sans contenu informationnel. Elle se justifie sans hypothèse, mais ne permet aucune déduction particulière, d'où une règle d'introduction triviale et l'absence de règle d'élimination :

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

Se passer de la négation ?

En déduction naturelle, le connecteur $\neg$ peut être éliminé au profit de l'équivalence

$$\neg\varphi \equiv \varphi \to \bot.$$

Les règles de la négation se réduisent alors à des instances des règles de l'implication. Il est même possible, au prix de constructions supplémentaires, de se passer également du symbole $\bot$.

Contradiction. La constante $\bot$ représente une contradiction. Elle peut notamment être produite par la combinaison d'une formule et de sa négation, via la règle d'élimination de la négation. Il n'existe pas de règle spécifique d'introduction de $\bot$, mais on dispose en revanche d'une règle d'élimination, fondée sur le *principe d'explosion* (*ex falso quodlibet*) : d'une contradiction, on peut déduire n'importe quelle formule.

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}\ (\bot_e)$$

Ce principe peut sembler contre-intuitif, mais il joue un rôle essentiel dans les raisonnements par cas et sera discuté plus en détail dans l'encadré qui lui est consacré.

Exemple

Le principe d'explosion permet d'éliminer des branches incompatibles lors d'un raisonnement par cas. Considérons le séquent

$$\varphi \vee \psi,\ \neg\psi \vdash \varphi.$$

L'élimination de la disjonction ouvre deux branches. Dans la branche correspondant à l'hypothèse ψ, on obtient une contradiction avec $\neg\psi$, à partir de laquelle on peut conclure φ par explosion. La branche correspondante est ainsi complétée, ce qui permet de conclure globalement.

$$\dfrac{\dfrac{}{\varphi, \neg\psi \vdash \varphi}\ \text{HYP} \qquad \dfrac{\dfrac{\dfrac{}{\psi, \neg\psi \vdash \psi}\ \text{HYP} \quad \dfrac{}{\psi, \neg\psi \vdash \neg\psi}\ \text{HYP}}{\psi, \neg\psi \vdash \bot}\ \neg_e}{\psi, \neg\psi \vdash \varphi}\ \bot_e}{\varphi \vee \psi, \neg\psi \vdash \varphi}$$

Ce principe fournit également, sous certaines hypothèses, un outil pour établir la réciproque de $\varphi \vdash \neg\neg\varphi$.

Raisonnement par l'absurde. Jusqu'ici, les règles de déduction reposaient sur des hypothèses supposées vraies. Le *raisonnement par l'absurde* adopte une approche différente : pour justifier une formule φ, on suppose temporairement son contraire $\neg\varphi$ et l'on montre que cette hypothèse conduit à une contradiction. On en conclut alors que φ est nécessairement vraie :

$$\frac{\Gamma, \neg\varphi \vdash \bot}{\Gamma \vdash \varphi}\ \mathrm{RAA}$$

Fictions

Cette règle met en évidence le caractère hypothétique du raisonnement mathématique : introduire une hypothèse ne revient pas à l'affirmer, mais à explorer, dans un cadre fictif, les conséquences qu'elle aurait si elle était vraie. Ce principe est commun aux autres règles qui enrichissent temporairement le contexte d'hypothèses.

Utilisation de lemmes. Le raisonnement mathématique classique repose sur le fait qu'un résultat démontré peut être réutilisé librement, sans en reproduire la preuve. Cette pratique correspond à l'usage de *lemmes*, établis une fois pour toutes et réemployés dans des démonstrations ultérieures.

Ce principe peut être formalisé en déduction naturelle par la *règle de coupure* (*cut*), qui autorise l'ajout aux hypothèses de tout fait démontrable indépendamment :

$$\frac{\Gamma \vdash \varphi \qquad \Gamma, \varphi \vdash \psi}{\Gamma \vdash \psi}\ \mathrm{CUT}$$

Cette règle clôt la présentation des règles de la déduction naturelle pour la logique propositionnelle. Nous étendrons ensuite ces principes à la logique du premier ordre.

Principe d'explosion

Le *principe d'explosion* exprime le fait que, dès qu'une contradiction est présente, toute formule devient démontrable, ce qui prive la logique de son rôle discriminant. Bien que connu depuis l'Antiquité et longtemps débattu, il est aujourd'hui pleinement intégré à la logique classique.
Ce principe est *admissible* en déduction naturelle : si les séquents $\Gamma \vdash \varphi$ et $\Gamma \vdash \neg\varphi$ sont démontrables, alors $\Gamma \vdash \psi$ l'est pour toute formule ψ.

Élimination des coupures

La règle de coupure n'est pas indispensable : tout séquent démontrable avec coupure l'est également sans y recourir. Intuitivement, l'appel à un lemme peut toujours être remplacé par la reproduction complète de sa preuve.
La démonstration formelle de cette propriété, appelée *élimination des coupures*, constitue un résultat majeur dû à Gentzen, obtenu dans le cadre du calcul des séquents. Elle joue un rôle central dans l'établissement de la *cohérence* de la logique, c'est-à-dire l'impossibilité de dériver une contradiction sans hypothèses.

2.4 Déduction naturelle pour la logique du premier ordre

Les quantificateurs, omniprésents en mathématiques, s'intègrent naturellement à la déduction naturelle. Comme pour les connecteurs propositionnels, chacun est associé à une règle d'introduction et une règle d'élimination.

Quantification universelle

Une formule $\forall x.\varphi$ est considérée comme valide lorsque la formule φ, qui dépend éventuellement de la variable x, est vraie quelle que soit la valeur prise par x. Un critère suffisant pour garantir cette indépendance est que la démonstration de φ ne repose sur aucune hypothèse faisant intervenir x.
La règle d'introduction de la quantification universelle, aussi appelée *règle de généralisation*, autorise donc l'introduction du quantificateur $\forall$ à condition que la variable quantifiée ne soit libre dans aucune des hypothèses :

$$\frac{\Gamma \vdash \varphi \qquad x \notin FV(\Gamma)}{\Gamma \vdash \forall x.\varphi}\ (\forall_i)$$

Inversement, si une formule $\forall x.\varphi$ est supposée vraie, cela signifie que φ est vraie pour toute valeur possible de x. On peut donc remplacer x par n'importe quel terme t, et obtenir une formule encore valide. Cette opération est formalisée par la *règle d'instanciation* :

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

Quantification existentielle

Une formule $\exists x.\varphi$ est valide dès lors qu'il existe au moins une valeur de x pour laquelle la formule φ est vraie. Pour justifier une telle formule, il suffit donc de fournir une valeur particulière, appelée *témoin*, et de démontrer la formule obtenue en substituant cette valeur à x.
La règle d'introduction de la quantification existentielle formalise ce raisonnement :

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

L'utilisation d'une formule existentielle repose sur un raisonnement différent : on sait qu'un témoin existe, mais on ne connaît rien de sa nature, si ce n'est qu'il satisfait φ. On raisonne donc avec une variable x représentant ce témoin, supposée indépendante de toutes les autres variables du contexte, et en ne prenant pour hypothèse sur x que la validité de φ. Cette contrainte est exprimée dans la règle d'élimination :

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

Comme pour la disjonction, on utilise souvent une variante lorsque la formule existentielle apparaît directement parmi les hypothèses :

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

Exemple

Voici une dérivation du séquent

$$\exists t.\forall x.\ t \leq x \ \vdash \ \forall y.\exists z.\ z \leq y$$

combinant les quatre règles des quantificateurs. Lors de l'application de $(\forall_e)$, on substitue x par y. Lors de l'application de $(\exists_i)$, on substitue z par t.

$$\dfrac{\exists t.\forall x.\, t \leq x \ \vdash \ \exists t.\forall x.\, t \leq x \qquad \dfrac{\dfrac{\dfrac{\forall x.\, t \leq x \ \vdash \ \forall x.\, t \leq x}{\forall x.\, t \leq x \ \vdash \ t \leq y}\,\text{HYP}}{\forall x.\, t \leq x \ \vdash \ \exists z.\, z \leq y}\,(\forall_e)}{\forall x.\, t \leq x \ \vdash \ \forall y.\exists z.\, z \leq y}\,(\exists_i)}{\exists t.\forall x.\, t \leq x \ \vdash \ \forall y.\exists z.\, z \leq y}\,(\forall_i) \quad y \notin FV(\forall x.\, t \leq x)$$

Le séquent $\exists t.\forall x.\, t \leq x \vdash \forall x.\exists t.\, t \leq x$ peut être dérivé avec le même arbre de preuve, seules les substitutions changeant formellement (cas d'un simple *pun*). En revanche, la réciproque est invalide : l'existence d'un témoin dépendant de x n'implique pas l'existence d'un témoin unique valable pour tous les x. Toute tentative de dérivation échoue alors en raison des conditions de liberté des règles $(\forall_i)$ et $(\exists_e)$, ce qui en souligne le rôle essentiel.

2.5 Théories du premier ordre.

La logique du premier ordre ne se limite pas à l'ajout des quantificateurs : elle repose avant tout sur la manipulation d'objets et de prédicats portant sur ces objets. Un raisonnement nécessite donc des connaissances élémentaires sur le domaine considéré, formalisées par des axiomes et des règles propres aux objets manipulés. L'ensemble de ces connaissances constitue une *théorie*.

Exemple

L'égalité de Leibniz juge que deux objets t et u sont égaux, dès lors qu'ils sont indiscernables l'un de l'autre. Conséquence dans une démonstration : tout ce qui a pu être démontré pour l'un vaut encore pour l'autre. On peut intégrer ceci à notre système de déduction avec la règle d'élimination ci-dessous à droite. La règle d'introduction se contente d'énoncer que tout objet est égal à lui-même.

$$\dfrac{}{\Gamma \vdash t = t}\,(=_i) \qquad\qquad \dfrac{\Gamma \vdash t = u \qquad \Gamma \vdash \varphi^{\{x \leftarrow u\}}}{\Gamma \vdash \varphi^{\{x \leftarrow t\}}}\,(=_e)$$

Exemple

L'axiomatisation des nombres entiers de Peano peut s'intégrer à notre déduction naturelle du premier ordre en deux étapes : définir l'ensemble des termes représentant les nombres, puis inclure une règle d'inférence traduisant le principe de raisonnement par récurrence.

$$\dfrac{\Gamma \vdash \varphi^{\{n \leftarrow 0\}} \qquad \Gamma \vdash \forall n. \left(\varphi \to \varphi^{\{n \leftarrow n+1\}}\right)}{\Gamma \vdash \forall n. \varphi}$$

Logique classique et logique intuitionniste

Du point de vue de la sémantique booléenne, toute formule est soit vraie, soit fausse. La formule $\varphi \lor \neg\varphi$ est ainsi une tautologie, appelée *tiers exclu*. Toutefois, cette formule ne se démontre pas directement à l'aide des règles d'introduction de la disjonction, faute de savoir lequel des deux disjoints justifier.
On peut en revanche établir le tiers exclu à l'aide du raisonnement par l'absurde, comme l'illustre la dérivation suivante, où l'on pose $\psi := \neg(\varphi \lor \neg\varphi)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\psi, \varphi \vdash \varphi}{\psi, \varphi \vdash \varphi \lor \neg\varphi}\,\text{HYP} \qquad \psi, \varphi \vdash \psi}{\psi, \varphi \vdash \bot}\,\text{HYP}}{\psi \vdash \neg\varphi}\,\neg_e \qquad \dfrac{\dfrac{\dfrac{\psi, \neg\varphi \vdash \neg\varphi}{\psi, \neg\varphi \vdash \varphi \lor \neg\varphi}\,\text{HYP} \qquad \psi, \neg\varphi \vdash \psi}{\psi, \neg\varphi \vdash \bot}\,\text{HYP}}{\psi \vdash \varphi}\,\neg_e}{\psi \vdash \bot}\,\text{RAA}}{\vdash \varphi \lor \neg\varphi}\,\neg_e$$

Sans le raisonnement par l'absurde, une telle dérivation est impossible. La présence ou l'absence du tiers exclu et du raisonnement par l'absurde marque ainsi la frontière entre la *logique classique*, qui les accepte, et la *logique intuitionniste*, qui les rejette.
Introduite par L. E. J. Brouwer, l'approche intuitionniste fonde les mathématiques sur la notion de preuve constructive plutôt que sur la vérité booléenne. Toute preuve devient alors une construction explicite : démontrer une existence impose de fournir un témoin, et justifier une disjonction requiert de déterminer lequel des deux cas est valide. Cette vision, formalisée par Brouwer, Heyting et Kolmogorov, a profondément influencé l'informatique théorique, notamment à travers les liens entre preuves et programmes.