Un peu de théorie de la démonstration

Lionel Vaux Auclair

I2M, université d'Aix-Marseille

Logique et calculabilité
M1 Mathématiques et applications, 2020–2021

Trois niveaux d'implication

- Dans les formules : $A \Rightarrow B$ (*si* A *alors* B) est une formule comme les autres.
- Dans les séquents : $\Gamma \vdash A$ représente un état courant dans une démonstration (A se déduit des hypothèses de Γ).
- Dans les règles :

$$\frac{\Gamma_1 \vdash A_1 \quad \cdots \quad \Gamma_n \vdash A_n}{\Gamma \vdash A}\ (R)$$

  dit qu'on peut déduire $\Gamma \vdash A$ des $\Gamma_i \vdash A_i$.

Trois niveaux d'implication

- Dans les formules : $A \Rightarrow B$ (*si A alors B*) est une formule comme les autres.
- Dans les séquents : $\Gamma \vdash A$ représente un état courant dans une démonstration (A se déduit des hypothèses de Γ).
- Dans les règles :

$$\frac{\Gamma_1 \vdash A_1 \quad \cdots \quad \Gamma_n \vdash A_n}{\Gamma \vdash A}\ (R)$$

dit qu'on peut déduire $\Gamma \vdash A$ des $\Gamma_i \vdash A_i$.

$A \Rightarrow B$ est une tautologie ssi le séquent $A \vdash B$ est valide

ssi la règle $\dfrac{\Gamma \vdash A}{\Gamma \vdash B}$ est correcte

ssi la règle $\dfrac{\Gamma, B \vdash C}{\Gamma, A \vdash C}$ est correcte

Arbres de démonstration

Un système logique $\mathcal{L}$ est un ensemble fini (ou au moins *calculable*) de règles.

Un argument (ou une démonstration ouverte) dans $\mathcal{L}$ est un arbre dont les nœuds sont des séquents, muni d'un étiquetage partiel des nœuds par des règles de sorte que :

- si un nœud n'est pas étiqueté alors c'est une feuille (c'est une prémisse de l'argument) ;
- pour chaque nœud étiqueté par la règle (R), il y a une instance de (R) dont ce nœud est la conclusion, et ses fils sont les hypothèses.

Une démonstration est un argument sans prémisse.

On dit que $\Gamma \vdash A$ est dérivable (ou démontrable) dans $\mathcal{L}$ s'il existe une démonstration dont la racine est de conclusion $\Gamma \vdash A$.
On écrit alors $\Gamma \vdash_{\mathcal{L}} A$.

Correction

Soit $\mathcal{L}$ un système logique correct (c'est-à-dire que toutes les règles sont correctes).

Théorème

Si $\vdash_{\mathcal{L}} A$ alors A est une tautologie.

Démonstration: On montre par induction sur un arbre de démonstration quelconque que son séquent conclusion est valide. Soit π un arbre de démonstration de conclusion $\Gamma \vdash A$, et

$$\frac{\Gamma_1 \vdash A_1 \quad \cdots \quad \Gamma_n \vdash A_n}{\Gamma \vdash A}\ (R)$$

la règle dont la racine de π est une instance. Par hypothèse d'induction appliquée aux sous-arbres de π, on obtient que chaque séquent $\Gamma_i \vdash A_i$ est valide. Comme (R) est correcte, on en déduit que $\Gamma \vdash A$ est valide. □

Correction

Soit $\mathcal{L}$ un système logique correct (c'est-à-dire que toutes les règles sont correctes).

Théorème

Si $\vdash_{\mathcal{L}} A$ alors A est une tautologie.

Démonstration: On montre par induction sur un arbre de démonstration quelconque que son séquent conclusion est valide. Soit π un arbre de démonstration de conclusion $\Gamma \vdash A$, et

$$\frac{\Gamma_1 \vdash A_1 \quad \cdots \quad \Gamma_n \vdash A_n}{\Gamma \vdash A}\ (R)$$

la règle dont la racine de π est une instance. Par hypothèse d'induction appliquée aux sous-arbres de π, on obtient que chaque séquent $\Gamma_i \vdash A_i$ est valide. Comme (R) est correcte, on en déduit que $\Gamma \vdash A$ est valide. □

Encore heureux !

Beaucoup mais pas trop

- Si on cherche à produire une démonstration, on a intérêt à avoir un *maximum* de règles (surtout si on veut une démonstration lisible).
  Mais on s'en tient à des règles correctes.

$\rightsquigarrow$ Correction

Beaucoup mais pas trop

- Si on cherche à produire une démonstration, on a intérêt à avoir un *maximum* de règles (surtout si on veut une démonstration lisible).
  Mais on s'en tient à des règles correctes.

$\rightsquigarrow$ Correction

- Si on veut démontrer une propriété *du système de démonstration* on a intérêt à avoir un *minimum* de règles (et même de connecteurs) pour avoir moins de cas à traiter.
  Mais on aimerait pouvoir prouver tout ce qui est vrai.

$\rightsquigarrow$ Complétude

D'autres règles de raisonnement correctes

$$\frac{\Gamma, A \vdash B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (coup) \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ (\wedge_{gg}) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (r.a.)$$

D'autres règles de raisonnement correctes

$$\frac{\Gamma, A \vdash B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (coup) \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ (\wedge_{gg}) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (r.a.)$$

Faut-il les ajouter ?

D'autres règles de raisonnement correctes

$$\frac{\Gamma, A \vdash B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (coup) \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ (\wedge_{gg}) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (r.a.)$$

Faut-il les ajouter ? Inutile :

$$\Gamma, A \vdash B$$

$$\Gamma \vdash A$$

$$\Gamma \vdash B$$

D'autres règles de raisonnement correctes

$$\frac{\Gamma, A \vdash B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (coup) \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ (\wedge_{gg}) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (r.a.)$$

Faut-il les ajouter ? Inutile :

$$\frac{\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ (\Rightarrow_i) \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (\Rightarrow_e)$$

D'autres règles de raisonnement correctes

$$\frac{\Gamma, A \vdash B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (coup) \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ (\wedge_{gg}) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (r.a.)$$

Faut-il les ajouter ? Inutile :

$$\dfrac{\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ (\Rightarrow_i) \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (\Rightarrow_e)$$

$\Gamma, A \vdash C$

$\Gamma, A \wedge B \vdash C$

D'autres règles de raisonnement correctes

$$\frac{\Gamma, A \vdash B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (coup) \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ (\wedge_{gg}) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (r.a.)$$

Faut-il les ajouter ? Inutile :

$$\frac{\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ (\Rightarrow_i) \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (\Rightarrow_e)$$

$$\frac{\dfrac{\Gamma, A \vdash C}{\Gamma, A \wedge B, A \vdash C}\ (aff) \qquad \dfrac{\dfrac{}{\Gamma, A \wedge B \vdash A \wedge B}\ (ax)}{\Gamma, A \wedge B \vdash A}\ (\wedge_{eg})}{\Gamma, A \wedge B \vdash C}\ (coup)$$

D'autres règles de raisonnement correctes

$$\frac{\Gamma, A \vdash B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (coup) \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ (\wedge_{gg}) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (r.a.)$$

Faut-il les ajouter ? Inutile :

$$\frac{\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ (\Rightarrow_i) \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (\Rightarrow_e)$$

$$\frac{\dfrac{\Gamma, A \vdash C}{\Gamma, A \wedge B, A \vdash C}\ (aff) \qquad \dfrac{\dfrac{}{\Gamma, A \wedge B \vdash A \wedge B}\ (ax)}{\Gamma, A \wedge B \vdash A}\ (\wedge_{eg}) \qquad \Gamma, \neg A \vdash \bot}{\Gamma, A \wedge B \vdash C}\ (coup) \qquad \Gamma \vdash A$$

D'autres règles de raisonnement correctes

$$\frac{\Gamma, A \vdash B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (coup) \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ (\wedge_{gg}) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (r.a.)$$

Faut-il les ajouter ? Inutile :

$$\frac{\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ (\Rightarrow_i) \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (\Rightarrow_e)$$

$$\frac{\dfrac{\Gamma, A \vdash C}{\Gamma, A \wedge B, A \vdash C}\ (aff) \qquad \dfrac{\dfrac{}{\Gamma, A \wedge B \vdash A \wedge B}\ (ax)}{\Gamma, A \wedge B \vdash A}\ (\wedge_{eg})}{\Gamma, A \wedge B \vdash C}\ (coup) \qquad \frac{\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma, \neg A \vdash A}\ (\bot_e) \qquad \dfrac{}{\Gamma, A \vdash A}\ (ax)}{\Gamma \vdash A}\ (t.e.)$$

Règles dérivables

Rappel : un argument = une démonstration ouverte = un arbre de déduction dont les feuilles ne sont pas nécessairement étiquetées par des règles 0-aires.

Définition

La règle

$$\frac{\Gamma_1 \vdash A_1 \quad \cdots \quad \Gamma_n \vdash A_n}{\Gamma \vdash A}\ (R)$$

est dérivable dans $\mathcal{L}$, s'il existe un argument dans $\mathcal{L}$ permettant de dériver $\Gamma \vdash A$, à partir de prémisses parmi $\Gamma_1 \vdash A_1, \ldots, \Gamma_n \vdash A_n$.

Règles dérivables

Rappel : un argument = une démonstration ouverte = un arbre de déduction dont les feuilles ne sont pas nécessairement étiquetées par des règles 0-aires.

Définition

La règle

$$\frac{\Gamma_1 \vdash A_1 \quad \cdots \quad \Gamma_n \vdash A_n}{\Gamma \vdash A}\ (R)$$

est dérivable dans $\mathcal{L}$, s'il existe un argument dans $\mathcal{L}$ permettant de dériver $\Gamma \vdash A$, à partir de prémisses parmi $\Gamma_1 \vdash A_1, \ldots, \Gamma_n \vdash A_n$.

Exemple

Les règles (*coup*), ($\wedge_g$) et (*r.a.*) sont dérivables dans *DN*
(= les règles d'introduction et d'élimination + (*ax*) + (*t.e.*) + les règles structurelles)

Règles admissibles

Définition

Une règle (R) est admissible dans $\mathcal{L}$, si $\mathcal{L}$ et $\mathcal{L} \cup \{R\}$ démontrent les mêmes séquents.
Une règle de $\mathcal{L}$ est superflue si elle est admissible dans $\mathcal{L} \setminus \{R\}$.

Une règle dérivable est évidemment admissible.

Exemple

Les règles d'affaiblissement et contraction sont superflues dans DN.

Démonstration: Il suffit de démontrer, par induction sur les arbres de $DN \setminus \{aff, cont\}$, que pour tout arbre de conclusion $\Gamma \vdash B$ (respectivement $\Gamma, A, A \vdash B$) il existe un arbre de conclusion $\Gamma, A \vdash B$. □

Attention : ces règles ne sont pas pour autant dérivables dans $DN \setminus \{aff, cont\}$.

Règles réversibles

Définition

La règle

$$\frac{\Gamma_1 \vdash A_1 \quad \cdots \quad \Gamma_n \vdash A_n}{\Gamma \vdash A}\ (R)$$

est réversible si chacune des règles $\dfrac{\Gamma \vdash A}{\Gamma_i \vdash A_i}$ est admissible.

Autrement dit, appliquer (R) ne « coûte »rien : la conclusion est équivalente aux hypothèses.

Exemple

$(\Rightarrow_i)$ est réversible :

$$\frac{\dfrac{\Gamma \vdash A \Rightarrow B}{\Gamma, A \vdash A \Rightarrow B}\ (aff) \qquad \dfrac{}{\Gamma, A \vdash A}\ (ax)}{\Gamma, A \vdash B}\ (\Rightarrow_e)$$

$(\Rightarrow_e)$ ne l'est pas : de B on peut déduire $A \Rightarrow B$ mais pas A en général

Règles gauches

Les règles suivantes sont dérivables dans DN :

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}\ (\wedge_g) \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ (\vee_g)$$

$$\frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \Rightarrow B \vdash C}\ (\Rightarrow_g) \qquad \frac{\Gamma \vdash A}{\Gamma, \neg A \vdash \bot}\ (\neg_g) \qquad \frac{}{\Gamma, \bot \vdash C}\ (\bot_g)$$

Règles gauches

Les règles suivantes sont dérivables dans DN :

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}\ (\wedge_g) \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ (\vee_g)$$

$$\frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \Rightarrow B \vdash C}\ (\Rightarrow_g) \qquad \frac{\Gamma \vdash A}{\Gamma, \neg A \vdash \bot}\ (\neg_g) \qquad \frac{}{\Gamma, \bot \vdash C}\ (\bot_g)$$

Démonstration: On s'en sort facilement avec (*coup*) et les règles d'élimination.

$\rightsquigarrow$ Exercice.

□

Raisonnement sur la vérité

Les règles suivantes sont dérivables dans DN :

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (r.a.) \qquad \frac{\Gamma, \neg A \vdash A}{\Gamma \vdash A}\ (Peirce) \qquad \frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}\ (\neg\neg_e) \qquad \frac{\Gamma \vdash \neg B \Rightarrow \neg A}{\Gamma \vdash A \Rightarrow B}\ (contrap)$$

Raisonnement sur la vérité

Les règles suivantes sont dérivables dans DN :

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (r.a.) \qquad \frac{\Gamma, \neg A \vdash A}{\Gamma \vdash A}\ (Peirce) \qquad \frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}\ (\neg\neg_e) \qquad \frac{\Gamma \vdash \neg B \Rightarrow \neg A}{\Gamma \vdash A \Rightarrow B}\ (contrap)$$

Démonstration: On a déjà vu $(r.a.)$. Pour le reste...

$\rightsquigarrow$ Exercice.

□

Trois niveaux d'implication

Rappel :

$A \Rightarrow B$ est une tautologie ssi le séquent $A \vdash B$ est valide

ssi la règle $\dfrac{\Gamma \vdash A}{\Gamma \vdash B}$ $(A{\downarrow}B)$ est correcte

ssi la règle $\dfrac{\Gamma, B \vdash C}{\Gamma, A \vdash C}$ $(A{\uparrow}B)$ est correcte

Trois niveaux d'implication

Rappel :

$A \Rightarrow B$ est une tautologie ssi le séquent $A \vdash B$ est valide

ssi la règle $\dfrac{\Gamma \vdash A}{\Gamma \vdash B}$ $(A{\downarrow}B)$ est correcte

ssi la règle $\dfrac{\Gamma, B \vdash C}{\Gamma, A \vdash C}$ $(A{\uparrow}B)$ est correcte

Dans *DN* :

$A \Rightarrow B$ est prouvable ssi le séquent $A \vdash B$ est dérivable

ssi la règle $\dfrac{\Gamma \vdash A}{\Gamma \vdash B}$ $(A{\downarrow}B)$ est dérivable

ssi la règle $\dfrac{\Gamma, B \vdash C}{\Gamma, A \vdash C}$ $(A{\uparrow}B)$ est dérivable

$\rightsquigarrow$ Exercice.

Lois de De Morgan

Les règles suivantes sont dérivables dans DN :

$$\frac{\Gamma \vdash \neg A \vee \neg B}{\Gamma \vdash \neg(A \wedge B)} \qquad \frac{\Gamma, \neg A \vee \neg B \vdash C}{\Gamma, \neg(A \wedge B) \vdash C} \qquad \frac{\Gamma \vdash \neg A \wedge \neg B}{\Gamma \vdash \neg(A \vee B)} \qquad \frac{\Gamma, \neg A \wedge \neg B \vdash C}{\Gamma, \neg(A \vee B) \vdash C}$$

$$\frac{\Gamma \vdash A \wedge \neg B}{\Gamma \vdash \neg(A \Rightarrow B)} \qquad \frac{\Gamma, A \wedge \neg B \vdash C}{\Gamma, \neg(A \Rightarrow B) \vdash C} \qquad \frac{\Gamma \vdash A}{\Gamma \vdash \neg\neg A} \qquad \frac{\Gamma, A \vdash C}{\Gamma, \neg\neg A \vdash C}$$

Lois de De Morgan

Les règles suivantes sont dérivables dans DN :

$$\frac{\Gamma \vdash \neg A \vee \neg B}{\Gamma \vdash \neg(A \wedge B)} \qquad \frac{\Gamma, \neg A \vee \neg B \vdash C}{\Gamma, \neg(A \wedge B) \vdash C} \qquad \frac{\Gamma \vdash \neg A \wedge \neg B}{\Gamma \vdash \neg(A \vee B)} \qquad \frac{\Gamma, \neg A \wedge \neg B \vdash C}{\Gamma, \neg(A \vee B) \vdash C}$$

$$\frac{\Gamma \vdash A \wedge \neg B}{\Gamma \vdash \neg(A \Rightarrow B)} \qquad \frac{\Gamma, A \wedge \neg B \vdash C}{\Gamma, \neg(A \Rightarrow B) \vdash C} \qquad \frac{\Gamma \vdash A}{\Gamma \vdash \neg\neg A} \qquad \frac{\Gamma, A \vdash C}{\Gamma, \neg\neg A \vdash C}$$

Démonstration: Toutes les implications correspondantes étaient en exercice. □

Raisonner modulo l'équivalence

On note $C[X := A]$ la formule obtenue à partir de C en remplaçant toutes les occurrences de la variable propositionnelle X par la formule A.

Théorème

Pour toute formule C, la règle $\dfrac{\Gamma \vdash A \Leftrightarrow B}{\Gamma \vdash C[X := A] \Leftrightarrow C[X := B]}$ *est dérivable dans DN.*

Démonstration: Il suffit de prouver par récurrence sur C qu'on peut dériver $\Gamma, C[X := A] \vdash C[X := B]$ à partir de $\Gamma \vdash A \Rightarrow B$ et $\Gamma \vdash B \Rightarrow A$. Exemples de cas :

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma, D[X := B] \vdash D[X := A]}}{\Gamma, \neg D[X := A], D[X := B] \vdash \bot}\,(\neg_g)}{\Gamma, \neg D[X := A] \vdash \neg D[X := B]}\,(\neg_i) \qquad \dfrac{\dfrac{\vdots}{\Gamma, D[X := A] \vdash D[X := B]}}{\Gamma, D[X := A] \vdash D[X := B] \vee E[X := B]}\,(\vee_{ig}) \qquad \dfrac{\dfrac{\vdots}{\Gamma, E[X := A] \vdash E[X := B]}}{\Gamma, E[X := A] \vdash D[X := B] \vee E[X := B]}\,(\vee_{id})$$

$$\Gamma, D[X := A] \vee E[X := A] \vdash D[X := B] \vee E[X := B]\,(\vee_g) \qquad \square$$

Raisonner modulo l'équivalence

Le théorème précédent nous autorise par exemple à écrire $A \wedge B \wedge C$ plutôt que $A \wedge (B \wedge C)$ ou $(A \wedge B) \wedge C$ n'importe où dans une preuve dès qu'on sait montrer :

$$\vdash A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C.$$

De même, on peut raisonner comme suit

$$\frac{\vdash \neg\neg A \Rightarrow C}{\vdash A \Rightarrow C}$$

dès qu'on sait montrer

$$\vdash A \Leftrightarrow \neg\neg A$$