LC – Logique classique

Sylvain Brandel
2024 – 2025
sylvain.brandel@univ-lyon1.fr

Partie 2

LOGIQUE PROPOSITIONNELLE

Pourquoi ?

- Niveau matériel = modèle logique
- Niveau programme : preuve de propriété = logique
- Niveau applicatif, BD : vérification de propriétés = logique
- …

- Plus généralement
  - Criticité : sécurité, sureté …
  - Financier
  - Pas d’ambiguïté

Syntaxe

- $\mathcal{V} = \{x_1, x_2, \dots, x_n, \ \dots\}$ un ensemble infini de variables propositionnelles

- Ensemble $\mathcal{F}$ des formules du calcul propositionnel : ensemble inductif
  - x variable propositionnelle alors $x \in \mathcal{F}$
  - $\perp \in \mathcal{F}$
  - Si $A \in \mathcal{F}$ alors $\neg A \in \mathcal{F}$
  - Si $A \in \mathcal{F}$ et $B \in \mathcal{F}$ alors $A \vee B \in \mathcal{F}$, $A \wedge B \in \mathcal{F}$, $A \Rightarrow B \in \mathcal{F}$

- Formule atomique : soit une variable propositionnelle, soit $\perp$

- Notation : $A \Leftrightarrow B$: $(A \Rightarrow B) \wedge (B \Rightarrow A)$

- Priorités : $\neg \ > \ \wedge \ > \ \vee \ > \ \Rightarrow$

- Associativité : à gauche pour $\wedge$ et $\vee$, à droite pour $\Rightarrow$

Sémantique

- Sens des formules → interprétation dans l'algèbre de Boole

- Interprétation du calcul propositionnel : fonction $I : \mathcal{V} \rightarrow \mathbb{B}$
  - $\mathcal{V} = \{x_1, x_2, \dots, x_n, \ \dots\}$: variables
  - $\mathbb{B} = \{0,1\}$

- I étendue à $\mathcal{F}$
  - Cas des variables déjà traité
  - $I(\perp) = 0$
  - $A \in \mathcal{F}$ alors $I(\neg A) = \overline{I(A)}$
  - $A \in \mathcal{F}$ et $B \in \mathcal{F}$ alors $I(A \vee B) = I(A) + I(B)$
  - $A \in \mathcal{F}$ et $B \in \mathcal{F}$ alors $I(A \wedge B) = I(A) \,.\, I(B)$
  - $A \in \mathcal{F}$ et $B \in \mathcal{F}$ alors $I(A \Rightarrow B) = I(A) \ \dot{\Rightarrow}\ I(B)$

  Seule vérité autorisée, valeur de vérité de$A \in \mathcal{F}$ notée $I(A)$

Algèbre de Boole

- George Boole 1815 – 1864 (Royaume-Uni)

- Booléens : oui, non ; 0, 1 ; haut, bas ; rouge, noir ; etc.

- Relation d'ordre : 0 < 1

- Soit $\mathbb{B} = \{0,1\}$. Opérations :
  - $\overline{} : \mathbb{B} \to \mathbb{B}$ complément
  - $+ : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ ∪, ou, disjonction, max
  - $. : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ ∩, et, conjonction, min
  - $\dot{\Rightarrow} : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ si … alors, implication

Algèbre de Boole

x	y	$\mathrm{x}\,.\,y$
0	0	0
0	1	0
1	0	0
1	1	1

x	y	$\mathrm{x}+y$
0	0	0
0	1	1
1	0	1
1	1	1

x	y	$\mathrm{x}\dot{\Rightarrow} y$
0	0	1
0	1	1
1	0	0
1	1	1

x	$\bar{x}$
0	1
1	0

Algèbre de Boole

- 0 : minimum, 1 maximum

- $x\,.\,1 = x \qquad x\,.\,0 = 0$
- $x + 0 = x \qquad x + 1 = 1$

- Complément : $x\,.\,\bar{x} = 0 \qquad x + \bar{x} = 1$

- Commutativité
- Associativité
- Distributivité

- De Morgan :
  - $\bar{x}\,.\,\bar{y} = \overline{x + y}$
  - $\bar{x} + \bar{y} = \overline{x\,.\,y}$

Tables de vérité

- Idée : notation par extension

- Une ligne par valeurs possible des variables
- Présentation des sous-fonctions en colonnes

- Fonctions booléennes : par extension, une fonction par table de vérité
  → combien ?

Interprétations

- Interprétation : fonction $I : \mathcal{V} \to \mathbb{B}$

- Soit A une formule.

  $I(A) = 1 : I$ satisfait A noté $I \vDash A$

- Ex :
  - Si $I(p) = 0$ et $I(q) = 0$ et $I(r) = 0$ alors $I \vDash p \vee q \Rightarrow r$
  - Si $I(p) = 1$ et $I(q) = 1$ et $I(r) = 0$ alors I ne satisfait pas $p \vee q \Rightarrow r$

- Soit E un ensemble de formules.

  Si $I \vDash A$ pour tout $\mathrm{A} \in E$: I satisfait E noté $I \vDash E$

- Ex :
  - Si $I(p) = 1$ alors $I \vDash \{p \vee q, \neg p \Rightarrow r\}$
  - Si $I(p) = 1$ alors I ne satisfait pas $\{p \vee q, \neg p\}$

Interprétations

A : formule, E : ensemble de formules, I : interprétation

- A tautologie, ou A valide — noté $\vDash A$
  si pour toute interprétation I, $I \vDash A$

- E contradictoire, ou E non satisfiable
  s'il n'existe aucune interprétation I telle que $I \vDash E$

- E satisfiable
  s'il existe une (au moins) interprétation I telle que $I \vDash E$

- E déduit sémantiquement A — noté $E \vDash A$
  si toute interprétation satisfaisant E satisfait aussi A

- A et B sémantiquement équivalentes — noté $A \equiv B$
  si $\{ A \} \vDash B$ et $\{ B \} \vDash A$

Modélisation

- Un logicien écoute un étudiant énumérer ses ressentis à propos des cours qu'il suit :
  - « J'aime l'informatique ou j'aime la logique »,
  - « Si j'aime l'informatique alors j'aime la logique ».
- Le logicien en déduit que l'étudiant aime la logique. Pourquoi ?

- Soient p et q deux variables propositionnelles :
  - p représente « j'aime l'informatique »
  - q représente « j'aime la logique »
- Les deux phrases de l'étudiant représentées par :
  1. $p \vee q$
  2. $p \Rightarrow q$
- Déduction du logicien représentée par q
- Démontrer $p \vee q,\ p \Rightarrow q\ \vDash q$

Remplacements

- Ne pas confondre avec les substitutions (de variables)
- Remplacement d'une variable propositionnelle p par une formule R dans une formule A, noté $A[p \coloneqq R]$, défini par induction sur A :
  - $p[p \coloneqq R] = R$
  - $q[p \coloneqq R] = q$ si $q \neq p$
  - $\bot\ [p \coloneqq R] = \bot$

  - $\neg A[p \coloneqq R] = \neg(A[p \coloneqq R])$

  - $(A \vee B)[p \coloneqq R] = (A[p \coloneqq R]) \vee (B[p \coloneqq R])$
  - $(A \wedge B)[p \coloneqq R] = (A[p \coloneqq R]) \wedge (B[p \coloneqq R])$
  - $(A \Rightarrow B)[p \coloneqq R] = (A[p \coloneqq R]) \Rightarrow (B[p \coloneqq R])$

- Ex : $(p \wedge q \Rightarrow q)[q \coloneqq r \vee s] = ?$

Quelques résultats

- Proposition 1

  $A \in \mathcal{F}$ et $B \in \mathcal{F}$, E ensemble de formules

  - $E \vDash A \Rightarrow B$ ssi $E \cup \{A\} \vDash B$
  - $E \vDash A$ ssi $E \cup \{\neg A\}$ contradictoire

- Proposition 2

  $A \in \mathcal{F}$ et $R \in \mathcal{F}$, $p \in \mathcal{V}, I$ une interprétation

  I' définie par $I'(p) = I(C)$ et $I'(q) = I(q)\ si\ q \neq p$

  On a $I(A[p \coloneqq R]) = I'(A)$

- Proposition 3

  $A \in \mathcal{F},\ B \in \mathcal{F},\ R \in \mathcal{F},\ R' \in \mathcal{F}, p \in \mathcal{V}$

  - Si $\vDash A$ alors $\vDash A[p \coloneqq R]$
  - Si $A\ \equiv B$ alors $A[p \coloneqq R] \equiv B[p \coloneqq R]$
  - Si $R \equiv R'$ alors $A[p \coloneqq R] \equiv A\ [p \coloneqq R']$

Quelques équivalences remarquables

$A \wedge A \equiv A$

$A \vee A \equiv A$

$A \wedge B \equiv B \wedge A$

$A \vee B \equiv B \vee A$

$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$

$A \vee (B \vee C) \equiv (A \vee B) \vee C$

$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

$\neg(A \wedge B) \equiv \neg A \vee \neg B$

$\neg(A \vee B) \equiv \neg A \wedge \neg B$

$A \Rightarrow B \equiv \neg A \vee B$

$\neg(A \Rightarrow B) \equiv A \wedge \neg B$

$\perp \wedge A \equiv \perp$

$\perp \vee A \equiv A$

$\neg\neg A \equiv A$

Systèmes de preuve

- Systèmes de preuve par séquents
  - Gerhard Gentzen (1909 – 1945)
  - Déduction naturelle
  - Calcul des séquents : LK, G …

- Systèmes de preuve par résolution
  - À partir de formes clausales
  - SAT solving …

Séquents

- Séquent : paire (Γ, Δ) noté $\Gamma \vdash \Delta$
  - $\Gamma = \{A_1, \dots, A_n\}$ et $\Delta = \{B_1, \dots, B_m\}$: ensembles de formules
  - I satisfait (Γ, Δ) ssi $I \models (A_1 \wedge \cdots \wedge A_n) \Rightarrow (B_1 \vee \cdots \vee B_n)$

- Rappel ensembles inductifs
  - E : ensemble, R : ensemble de règles sur E
  - Schéma d'induction : (E, R)
  - Ensemble inductif : la plus petite partie close pour (E, R)

- On définit un schéma d'induction (E, R) avec E : ensemble de séquents

- $R = \{ \quad \dots$

- On obtient un ensemble inductif nommé séquents prouvables

Calcul des séquents
Règles du système G

$$
\begin{array}{llll}
R = \{ & & \rightarrow \quad \Gamma, A \vdash \Delta, A & (1) \\
& \Gamma \vdash \Delta, A, \quad \Gamma, A \vdash \Delta & \rightarrow \quad \Gamma \vdash \Delta & (2) \\
& \Gamma \vdash \Delta, A, \quad \Gamma, B \vdash \Delta & \rightarrow \quad \Gamma, A \Rightarrow B \vdash \Delta & (3) \\
& \Gamma, A \vdash \Delta, \quad \Gamma, B \vdash \Delta & \rightarrow \quad \Gamma, A \vee B \vdash \Delta & (4) \\
& \Gamma, A, B \vdash \Delta & \rightarrow \quad \Gamma, A \wedge B \vdash \Delta & (5) \\
& \Gamma \vdash \Delta, A & \rightarrow \quad \Gamma, \neg A \vdash \Delta & (6) \\
& \Gamma, A \vdash \Delta, B & \rightarrow \quad \Gamma \vdash \Delta, A \Rightarrow B & (7) \\
& \Gamma \vdash \Delta, A, B & \rightarrow \quad \Gamma \vdash \Delta, A \vee B & (8) \\
& \Gamma \vdash \Delta, A, \quad \Gamma \vdash \Delta, B & \rightarrow \quad \Gamma \vdash \Delta, A \wedge B & (9) \\
& \Gamma, A \vdash \Delta & \rightarrow \quad \Gamma \vdash \Delta, \neg A \quad \} & (10)
\end{array}
$$

$\Gamma \cup \{A\}$ est noté Γ, A

Calcul des séquents

Règles du système G – exemple 1

$X = \{ \quad p \vdash p, q$	(1)	(s1)
$p, q \vdash q$	(1)	(s2)
$p, p \Rightarrow q \vdash q$	(3) à partir de (s1) et (s2)	(s3)
$q, p \Rightarrow q \vdash q$	(1) à partir de (s3)	(s4)
$p \vee q, p \Rightarrow q \vdash q \quad \}$	(4) à partir de (s4)	(s5)

$R = \{$	$\rightarrow$	$\Gamma, A \vdash \Delta, A$	(1)
$\Gamma \vdash \Delta, A, \quad \Gamma, A \vdash \Delta$	$\rightarrow$	$\Gamma \vdash \Delta$	(2)
$\Gamma \vdash \Delta, A, \quad \Gamma, B \vdash \Delta$	$\rightarrow$	$\Gamma, A \Rightarrow B \vdash \Delta$	(3)
$\Gamma, A \vdash \Delta, \quad \Gamma, B \vdash \Delta$	$\rightarrow$	$\Gamma, A \vee B \vdash \Delta$	(4)
$\Gamma, A, B \vdash \Delta$	$\rightarrow$	$\Gamma, A \wedge B \vdash \Delta$	(5)
$\Gamma \vdash \Delta, A$	$\rightarrow$	$\Gamma, \neg A \vdash \Delta$	(6)
$\Gamma, A \vdash \Delta, B$	$\rightarrow$	$\Gamma \vdash \Delta, A \Rightarrow B$	(7)
$\Gamma \vdash \Delta, A, B$	$\rightarrow$	$\Gamma \vdash \Delta, A \vee B$	(8)
$\Gamma \vdash \Delta, A, \quad \Gamma \vdash \Delta, B$	$\rightarrow$	$\Gamma \vdash \Delta, A \wedge B$	(9)
$\Gamma, A \vdash \Delta$	$\rightarrow$	$\Gamma \vdash \Delta, \neg A \; \}$	(10)

Calcul des séquents

Règles du système G – exemple 2

$X = \{ \quad p \vdash p, q$	(1)	(s1)
$p, q \vdash q$	(1)	(s2)
$p, p \Rightarrow q \vdash q$	(3) à partir de (s1) et (s2)	(s3)
$p \vdash (p \Rightarrow q) \Rightarrow q$	(7) à partir de (s3)	(s4)
$\vdash p \Rightarrow (p \Rightarrow q) \Rightarrow q \quad \}$	(7) à partir de (s4)	(s5)

$R = \{$	$\rightarrow$	$\Gamma, A \vdash \Delta, A$	(1)
$\Gamma \vdash \Delta, A, \quad \Gamma, A \vdash \Delta$	$\rightarrow$	$\Gamma \vdash \Delta$	(2)
$\Gamma \vdash \Delta, A, \quad \Gamma, B \vdash \Delta$	$\rightarrow$	$\Gamma, A \Rightarrow B \vdash \Delta$	(3)
$\Gamma, A \vdash \Delta, \quad \Gamma, B \vdash \Delta$	$\rightarrow$	$\Gamma, A \vee B \vdash \Delta$	(4)
$\Gamma, A, B \vdash \Delta$	$\rightarrow$	$\Gamma, A \wedge B \vdash \Delta$	(5)
$\Gamma \vdash \Delta, A$	$\rightarrow$	$\Gamma, \neg A \vdash \Delta$	(6)
$\Gamma, A \vdash \Delta, B$	$\rightarrow$	$\Gamma \vdash \Delta, A \Rightarrow B$	(7)
$\Gamma \vdash \Delta, A, B$	$\rightarrow$	$\Gamma \vdash \Delta, A \vee B$	(8)
$\Gamma \vdash \Delta, A, \quad \Gamma \vdash \Delta, B$	$\rightarrow$	$\Gamma \vdash \Delta, A \wedge B$	(9)
$\Gamma, A \vdash \Delta$	$\rightarrow$	$\Gamma \vdash \Delta, \neg A \}$	(10)

Calcul des séquents
Règles du système G

$$
R = \left\{
\begin{array}{llll}
 & \rightarrow & \Gamma, A \vdash \Delta, B & \text{(axiome)} \\
 & & & \\
\Gamma \vdash \Delta, A, \quad \Gamma, A \vdash \Delta & \rightarrow & \Gamma \vdash \Delta & \text{(coupure)} \\
 & & & \\
\Gamma \vdash \Delta, A, \quad \Gamma, B \vdash \Delta & \rightarrow & \Gamma, A \Rightarrow B \vdash \Delta & (\Rightarrow_G) \\
\Gamma, A \vdash \Delta, \quad \Gamma, B \vdash \Delta & \rightarrow & \Gamma, A \vee B \vdash \Delta & (\vee_G) \\
\Gamma, A, B \vdash \Delta & \rightarrow & \Gamma, A \wedge B \vdash \Delta & (\wedge_G) \\
\Gamma \vdash \Delta, A & \rightarrow & \Gamma, \neg A \vdash \Delta & (\neg_G) \\
 & & & \\
\Gamma, A \vdash \Delta, B & \rightarrow & \Gamma \vdash \Delta, A \Rightarrow B & (\Rightarrow_D) \\
\Gamma \vdash \Delta, A, B & \rightarrow & \Gamma \vdash \Delta, A \vee B & (\vee_D) \\
\Gamma \vdash \Delta, A, \quad \Gamma \vdash \Delta, B & \rightarrow & \Gamma \vdash \Delta, A \wedge B & (\wedge_D) \\
\Gamma, A \vdash \Delta & \rightarrow & \Gamma \vdash \Delta, \neg A \quad \} & (\neg_D)
\end{array}
\right.
$$

Calcul des séquents
Règles du système G

$$\frac{}{\Gamma, A \vdash \Delta, A}\,(ax)$$

$$\frac{\Gamma \vdash \Delta, A \qquad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}\,(coupure)$$

$$\frac{\Gamma \vdash \Delta, A \qquad \Gamma, B \vdash \Delta}{\Gamma, A \Rightarrow B \vdash \Delta}\,(\Rightarrow_G)$$

$$\frac{\Gamma, A \vdash \Delta, B}{\Gamma \vdash \Delta, A \Rightarrow B}\,(\Rightarrow_D)$$

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\,(\vee_G)$$

$$\frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}\,(\vee_D)$$

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\,(\wedge_G)$$

$$\frac{\Gamma \vdash \Delta, A \qquad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B}\,(\wedge_D)$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma, \neg A \vdash \Delta}\,(\neg_G)$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \Delta, \neg A}\,(\neg_D)$$

Déduction naturelle

- Séquent particulier : paire (Γ, B) noté $\Gamma \vdash B$
  - $\Gamma = \{A_1, \dots, A_n\}$: ensemble de formules — Prémisses
  - B : formule — Conclusion
  - I satisfait (Γ, B) ssi $I \vDash (A_1 \wedge \cdots \wedge A_n) \Rightarrow B$

Déduction naturelle

Règles

$$
\begin{array}{llll}
R = \{ & \rightarrow & \Gamma, A \vdash A & \text{(ax)} \\
\\
\Gamma \vdash A & \rightarrow & \Gamma, B \vdash A & \text{(aff)} \\
\\
\Gamma, A \vdash B & \rightarrow & \Gamma \vdash A \Rightarrow B & (\Rightarrow_i) \\
\Gamma \vdash A & \rightarrow & \Gamma \vdash A \vee B & (\vee_i^g) \\
\Gamma \vdash B & \rightarrow & \Gamma \vdash A \vee B & (\vee_i^d) \\
\Gamma \vdash A, \quad \Gamma \vdash B & \rightarrow & \Gamma \vdash A \wedge B & (\wedge_i) \\
\Gamma, A \vdash \perp & \rightarrow & \Gamma \vdash \neg A & (\neg_i) \\
\\
\Gamma \vdash A \Rightarrow B, \quad \Gamma \vdash A & \rightarrow & \Gamma \vdash B & (\Rightarrow_e) \\
\Gamma \vdash A \vee B, \quad \Gamma, A \vdash C, \quad \Gamma, B \vdash C & \rightarrow & \Gamma \vdash C & (\vee_e) \\
\Gamma \vdash A \wedge B & \rightarrow & \Gamma \vdash A & (\wedge_e^g) \\
\Gamma \vdash A \wedge B & \rightarrow & \Gamma \vdash B & (\wedge_e^d) \\
\Gamma \vdash \neg A, \quad \Gamma \vdash A & \rightarrow & \Gamma \vdash \perp & (\neg_e) \\
\\
\Gamma, \neg A \vdash \perp & \rightarrow & \Gamma \vdash A \quad \} & (\perp_c)
\end{array}
$$

Déduction naturelle

Exemple 1

$X = \{$	$p \vee q, p \Rightarrow q, p \vdash p \Rightarrow q$	(ax)	(s1)
	$p \vee q, p \Rightarrow q, p \vdash p$	(ax)	(s2)
	$p \vee q, p \Rightarrow q, p \vdash q$	($\Rightarrow_e$) à partir de (s1) et (s2)	(s3)
	$p \vee q, p \Rightarrow q, q \vdash q$	(ax)	(s4)
	$p \vee q, p \Rightarrow q \vdash p \vee q$	(ax)	(s5)
	$p \vee q, p \Rightarrow q \vdash q \ \}$	($\vee_e$) à partir de (s3), (s4) et (s5)	(s6)

$R = \{$		$\rightarrow$	$\Gamma, A \vdash A$	(ax)
	$\Gamma \vdash A$	$\rightarrow$	$\Gamma, B \vdash A$	(aff)
	$\Gamma, A \vdash B$	$\rightarrow$	$\Gamma \vdash A \Rightarrow B$	($\Rightarrow_i$)
	$\Gamma \vdash A$	$\rightarrow$	$\Gamma \vdash A \vee B$	($\vee_i^g$)
	$\Gamma \vdash B$	$\rightarrow$	$\Gamma \vdash A \vee B$	($\vee_i^d$)
	$\Gamma \vdash A, \quad \Gamma \vdash B$	$\rightarrow$	$\Gamma \vdash A \wedge B$	($\wedge_i$)
	$\Gamma, A \vdash \perp$	$\rightarrow$	$\Gamma \vdash \neg A$	($\neg_i$)
	$\Gamma \vdash A \Rightarrow B, \quad \Gamma \vdash A$	$\rightarrow$	$\Gamma \vdash B$	($\Rightarrow_e$)
	$\Gamma \vdash A \vee B, \quad \Gamma, A \vdash C, \quad \Gamma, B \vdash C$	$\rightarrow$	$\Gamma \vdash C$	($\vee_e$)
	$\Gamma \vdash A \wedge B$	$\rightarrow$	$\Gamma \vdash A$	($\wedge_e^g$)
	$\Gamma \vdash A \wedge B$	$\rightarrow$	$\Gamma \vdash B$	($\wedge_e^d$)
	$\Gamma \vdash \neg A, \quad \Gamma \vdash A$	$\rightarrow$	$\Gamma \vdash \perp$	($\neg_e$)
	$\Gamma, \neg A \vdash \perp$	$\rightarrow$	$\Gamma \vdash A \quad \}$	($\perp_c$)

Déduction naturelle

Exemple 2

$X = \{ \; p, p \Rightarrow q \vdash p \Rightarrow q$	(ax)	(s1)
$p, p \Rightarrow q \vdash p$	(ax)	(s2)
$p, p \Rightarrow q \vdash q$	($\Rightarrow_e$) à partir de (s1) et (s2)	(s3)
$p \vdash (p \Rightarrow q) \Rightarrow q$	($\Rightarrow_i$) à partir de (s3)	(s4)
$\vdash p \Rightarrow (p \Rightarrow q) \Rightarrow q \; \}$	($\Rightarrow_i$) à partir de (s4)	(s5)

$R = \{$

	$\rightarrow$	$\Gamma, A \vdash A$	(ax)
$\Gamma \vdash A$	$\rightarrow$	$\Gamma, B \vdash A$	(aff)
$\Gamma, A \vdash B$	$\rightarrow$	$\Gamma \vdash A \Rightarrow B$	($\Rightarrow_i$)
$\Gamma \vdash A$	$\rightarrow$	$\Gamma \vdash A \vee B$	($\vee_i^g$)
$\Gamma \vdash B$	$\rightarrow$	$\Gamma \vdash A \vee B$	($\vee_i^d$)
$\Gamma \vdash A, \quad \Gamma \vdash B$	$\rightarrow$	$\Gamma \vdash A \wedge B$	($\wedge_i$)
$\Gamma, A \vdash \perp$	$\rightarrow$	$\Gamma \vdash \neg A$	($\neg_i$)
$\Gamma \vdash A \Rightarrow B, \quad \Gamma \vdash A$	$\rightarrow$	$\Gamma \vdash B$	($\Rightarrow_e$)
$\Gamma \vdash A \vee B, \quad \Gamma, A \vdash C, \quad \Gamma, B \vdash C$	$\rightarrow$	$\Gamma \vdash C$	($\vee_e$)
$\Gamma \vdash A \wedge B$	$\rightarrow$	$\Gamma \vdash A$	($\wedge_e^g$)
$\Gamma \vdash A \wedge B$	$\rightarrow$	$\Gamma \vdash B$	($\wedge_e^d$)
$\Gamma \vdash \neg A, \quad \Gamma \vdash A$	$\rightarrow$	$\Gamma \vdash \perp$	($\neg_e$)
$\Gamma, \neg A \vdash \perp$	$\rightarrow$	$\Gamma \vdash A \; \}$	($\perp_c$)

Déduction naturelle

Règles de la déduction naturelle

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

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

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}(\vee_i^g) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}(\vee_i^d) \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}(\vee_e)$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}(\wedge_i) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}(\wedge_e^g) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}(\wedge_e^d)$$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}(\neg_i) \qquad \frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \bot}(\neg_e) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}(\bot_c)$$

Déduction naturelle
Exemple 1

$p \vee q, p \Rightarrow q \vdash q$ prouvable ?

Prouver $\Gamma \vdash q$, avec $\Gamma = \{p \vee q, p \Rightarrow q\}$

$$
\dfrac{\dfrac{}{p \vee q, p \Rightarrow q \vdash p \vee q}\,ax \qquad \dfrac{}{p \vee q, p \Rightarrow q, p \vdash p}\,ax \qquad \dfrac{?}{p \vee q, p \Rightarrow q, q \vdash p}}{\vdots}\,\vee_e
$$

$$
\dfrac{\dfrac{}{p \vee q, p \Rightarrow q \vdash p \Rightarrow q}\,ax \qquad p \vee q, p \Rightarrow q \vdash p}{p \vee q, p \Rightarrow q \vdash q}\Rightarrow_e
$$

$$
\dfrac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}(\vee_e) \qquad \dfrac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}(\Rightarrow_e)
$$

Déduction naturelle

Exemple 1

$p \vee q, p \Rightarrow q \vdash q$ prouvable ?

Prouver $\Gamma \vdash q$, avec $\Gamma = \{p \vee q, p \Rightarrow q\}$

$$\dfrac{\dfrac{}{p \vee q, p \Rightarrow q \vdash p \vee q}\,ax \qquad \dfrac{\dfrac{\dfrac{}{p \vee q, p \Rightarrow q, p \vdash p \Rightarrow q}\,ax \quad \dfrac{}{p \vee q, p \Rightarrow q, p \vdash p}\,ax}{\vdots}\,\Rightarrow_e}{p \vee q, p \Rightarrow q, p \vdash q} \qquad \dfrac{}{p \vee q, p \Rightarrow q, q \vdash q}\,ax}{p \vee q, p \Rightarrow q \vdash q}\,\vee_e$$

$$\dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\,(\vee_e) \qquad \dfrac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}\,(\Rightarrow_e)$$

Déduction naturelle
Exemple 2

$\vdash p \Rightarrow (p \Rightarrow q) \Rightarrow q$ prouvable ?

$$\dfrac{\dfrac{}{p, p \Rightarrow q \vdash p \Rightarrow q}\,ax \qquad \dfrac{}{p, p \Rightarrow q \vdash p}\,ax}{\dfrac{p, p \Rightarrow q \vdash q}{\dfrac{p \vdash (p \Rightarrow q) \Rightarrow q}{\vdash p \Rightarrow (p \Rightarrow q) \Rightarrow q}\Rightarrow_i}\Rightarrow_i}\Rightarrow_e$$

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

Déduction naturelle
Règles dérivées

- Système précédent : ensemble minimal
  - Démonstrations parfois longues
  - Introduction de règles utilitaires : règles dérivables

- Exemple

$$\frac{\Gamma, A \vdash B \qquad \Gamma \vdash A}{\Gamma \vdash B}(coupure)$$

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

On a une nouvelle règle (coupure)

On n'a pas ajouté de nouveaux séquents prouvables

Déduction naturelle

- Proposition
  Les règles de déduction naturelle sont correctes

- Théorème

$\boxed{\Gamma \vdash F \text{ prouvable par déduction naturelle ssi } \Gamma \vDash F}$

- Preuve
  - Sens $\Rightarrow$ (seulement si) : induction sur $\Gamma \vdash F$

Forme clausale

- Littéral

  Formule atomique ou négation d'une formule atomique

- Clause, ou disjonction élémentaire

  Disjonction de littéraux $l_1 \vee \cdots \vee l_m,\ m > 0$, chaque l_i : littéral

- FNC (Forme Normale Conjonctive)

  Conjonction de clauses $D_1 \wedge \cdots \wedge D_k,\ k > 0$, chaque D_i : clause

  $\bigwedge_{i=1}^{m} \bigvee_{j=1}^{n} l_i^j$, chaque l_i^j : littéral

- Conjonction élémentaire

  Conjonction de littéraux $l_1 \wedge \cdots \wedge n,\ n > 0$, chaque l_i : littéral

- FND (Forme Normale Disjonctive)

  Disjonction de conjonctions élémentaires

  $C_1 \vee \cdots \vee C_l,\ l > 0$, chaque C_i : conj. élém.

  $\bigvee_{i=1}^{m} \bigwedge_{j=1}^{n} l_i^j$, chaque l_i^j : littéral

Forme clausale

- Proposition 4

  Pour toute formule $A \in \mathcal{F}$, il existe $A' \in \mathcal{F}$ et $A'' \in \mathcal{F}$ tq
  - A' est en FNC
  - A'' est en FND
  - $A \equiv A' \equiv A''$

- Preuve
  - On élimine $\perp$ avec l'équivalence $\perp \equiv p \wedge \neg p$
  - On élimine le symbole $\Rightarrow$ avec l'équivalence $A \Rightarrow B \equiv \neg A \vee B$
  - On « fait rentrer » les symboles $\neg$ avec les lois de De Morgan
  - On utilise les lois de distributivité et d'élimination de la double négation

- Exemple
  - $p \Rightarrow (p \Rightarrow q) \Rightarrow q \qquad \equiv \neg p \vee \neg q \vee q$

- Problème, nombre exponentiel de clauses

  → utiliser l'équisatisfiabilité plutôt que l'équivalence

Forme clausale

- Equisatisfiabilité

  Soient $A \in \mathcal{F}$ et $B \in \mathcal{F}$.

  A et B sont équisatisfiables si A est satisfiable ssi B est satisfiable

- Proposition 5

  Pour toute formule $A \in \mathcal{F}$, il existe $A' \in \mathcal{F}$ tq
  - A' est en FNC
  - A et A' sont équisatisfiables
  - La taille de A' est linéaire en fonction de la taille de A

- Preuve
  - Construire A' en FNC tq taille de A' linéaire en fonction de la taille de A
  - Montrer A et A' équisatisfiables

Forme clausale

- Construction de A'
  - Si $A = \perp$, alors $A' = p \wedge \neg p$, où p est une variable fraiche
  - Si $A = p$, alors $A' = p$
  - Si $A = \neg B$, B de la forme $q \wedge B'$ obtenu par induction sur B, p une variable fraiche
    alors $A' = p \wedge (\neg p \vee \neg q) \wedge (p \vee q) \wedge B'$
  - Si $A = B \vee C$, B de la forme $q \wedge B'$ obtenu par induction sur B, C de la forme $r \wedge C'$ obtenu par induction sur C, p une variable fraiche
    alors $A' = p \wedge (\neg p \vee q \vee r) \wedge (p \vee \neg q) \wedge (p \vee \neg r) \wedge B' \wedge C'$
  - Si $A = B \wedge C$, B de la forme $q \wedge B'$ obtenu par induction sur B, C de la forme $r \wedge C'$ obtenu par induction sur C, p une variable fraiche
    alors $A' = p \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee q) \wedge (\neg p \vee r) \wedge B' \wedge C'$
  - Si $A = B \Rightarrow C$, B de la forme $q \wedge B'$ obtenu par induction sur B, C de la forme $r \wedge C'$ obtenu par induction sur C, p une variable fraiche
    alors $A' = p \wedge (\neg p \vee \neg q \vee r) \wedge (p \vee q) \wedge (p \vee \neg r) \wedge B' \wedge C'$

- Exemples
  - $a \Rightarrow b \quad \rightsquigarrow d \wedge (\neg d \vee \neg a \vee b) \wedge (d \vee a) \wedge (d \vee \neg b)$
  - $a \wedge \neg a \quad \rightsquigarrow d \wedge (d \vee \neg a \vee \neg c) \wedge (\neg d \vee a) \wedge (\neg d \vee c) \wedge (\neg c \vee \neg a) \wedge (c \vee a)$

ATTENTION Avec cette construction, A valide n'implique pas A' valide
En revanche, si A contradictoire alors A' contradictoire

Résolution en logique propositionnelle

- Rappel
  - $E \vDash A$ ssi $E \cup \{\neg A\}$ contradictoire
  - En particulier A valide ssi $\neg A$ contradictoire

- Système de preuve par résolution

  Soient C et C' deux clauses, L un littéral, p une variable propositionnelle

  Règles d'inférence

$$\frac{C \vee p \qquad C' \vee \neg p}{C \vee C'} (résolution) \qquad \qquad \frac{C \vee L \vee L}{C \vee L} (factorisation)$$

Factorisation aussi appelée contraction

Résolution en logique propositionnelle
Déduction

- Déduction par résolution

  Soient E un ensemble de clauses (les hypothèses) et C une clause (le but)

  Une déduction par résolution de C à partir de E est une suite $C_1, \ldots, C_n$ tq

  – $C_n = C$
  – Pour tout $i, 1 \leq i \leq n$
    - Soit $C_i \in E$
    - Soit C_i obtenue à partir de C_j $(j \leq i)$ en appliquant la règle de factorisation
    - Soit C_i obtenue à partir de C_j $et C_{j'}$ $(j \leq i,\ j' \leq i)$ en appliquant la règle de résolution

- Proposition 6

  Soient E un ensemble de clauses (les hypothèses) et C une clause (le but)

  S'il existe une déduction par résolution de C à partir de E, alors $E \vDash C$

- Preuve

Résolution en logique propositionnelle
Réfutation

- Réfutation

  Soit E un ensemble de clauses

  Une réfutation de E est une déduction par résolution de $\emptyset$ à partir de E

- Théorème

  > Soit E un ensemble de clauses
  >
  > E est contradictoire ssi il existe une réfutation de E

- Exemples

  F_1: $p \Rightarrow (p \Rightarrow q) \Rightarrow q$

  $\neg F_1 \rightsquigarrow \{p, \neg p \vee q, \neg q\}$

  $$\cfrac{\cfrac{p \qquad \neg p \vee q}{q} \qquad \neg q}{\emptyset}$$

  F_2: $((a \vee b) \Rightarrow (a \vee c)) \Rightarrow (a \vee (b \Rightarrow c))$

  $\neg F_2 \rightsquigarrow \{\neg b \vee a \vee c, \neg a, b, \neg c\}$

  $$\cfrac{\cfrac{\cfrac{\neg b \vee a \vee c \qquad \neg a}{\neg b \vee c} \qquad b}{c} \qquad \neg c}{\emptyset}$$