
Logique des propositions

Auteur : Marc LORENZI
Mis à jour le 4 août 2025

Table des matières

1	Lettres et mots	5
1	Alphabet, mot, langage	6
2	Produit de deux mots	6
3	Annexe	9
2	Syntaxe	11
1	Notion de formule	12
2	Induction structurelle	14
3	Le théorème de lecture unique	16
3	Sémantique	21
1	Environnements	22
2	Substitution	25
3	Équivalence	27
4	Preuves	31
1	Notion de théorie formelle	32
2	Une théorie formelle de la logique des propositions	33
3	Une liste de théorèmes	37
4	La complétude de $\mathcal{L}$	44
5	Indépendance	48
	Index	51

Chapitre 1

Lettres et mots

1 Alphabet, mot, langage

Ce chapitre est une courte introduction à la théorie des langages. Nous allons y définir le vocabulaire nécessaire à la compréhension des chapitres suivants.

Un *alphabet* est un ensemble non vide $\mathcal{A}$. Les éléments de l'alphabet sont appelés des *lettres*. Un *mot* sur l'alphabet $\mathcal{A}$ est un n -uplet $u = (x_0, \dots, x_{n-1}) \in \mathcal{A}^n$ de lettres, où $n \in \mathbb{N}$. L'entier $n = |u|$ est la *longueur* du mot u . Notons que deux mots $u = (u_0, \dots, u_{m-1})$ et $v = (v_0, \dots, v_{n-1})$ sont égaux si et seulement si $m = n$ et pour tout $i \in \llbracket 0, n-1 \rrbracket$, $u_i = v_i$.

Le seul mot de longueur 0 est le mot vide, noté ε . L'ensemble des mots sur l'alphabet $\mathcal{A}$ est noté $\mathcal{A}^*$. On a donc

$$\mathcal{A}^* = \bigcup_{n=0}^{\infty} \mathcal{A}^n$$

Si $u = (u_0, \dots, u_{n-1}) \in \mathcal{A}^*$, on note le mot u par la simple juxtaposition de ses lettres : $u = u_0 u_1 \dots u_{n-1}$. Pour tout $i \in \llbracket 0, n-1 \rrbracket$, u_i est la i^e lettre du mot u . Un mot de longueur 1 est identifié avec son unique lettre. Via cette identification, on a donc $\mathcal{A}^1 = \mathcal{A}$.

Un *langage* sur l'alphabet $\mathcal{A}$ est une partie $\mathcal{L}$ de $\mathcal{A}^*$. Le plus grand langage, au sens de l'inclusion, est $\mathcal{L} = \mathcal{A}^*$. Le plus petit langage est $\mathcal{L} = \emptyset$.

2 Produit de deux mots

2.1 Structure de monoïde

On définit une loi de composition interne sur $\mathcal{A}^*$. Si $u = u_0 \dots u_{m-1}$ et $v = v_0 \dots v_{n-1}$, on pose

$$u \times v = u_0 \dots u_{m-1} v_0 \dots v_{n-1}$$

Comme il est d'usage pour les produits, on note la plupart du temps uv au lieu de $u \times v$. On dispose aussi des puissances du mot u : $u^0 = \varepsilon$ et pour tout $n \in \mathbb{N}$, $u^{n+1} = u^n \times u$.

Pour être précis, si $u, v \in \mathcal{A}^*$ sont deux mots de longueurs respectives m et n , $u \times v$ est le mot w de longueur $m+n$ défini par

- Pour tout $i \in \llbracket 0, m-1 \rrbracket$, $w_i = u_i$.
- Pour tout $i \in \llbracket m, m+n-1 \rrbracket$, $w_i = v_{i-m}$.

Proposition 1.1. *$(\mathcal{A}^*, \times)$ est un monoïde de neutre ε . Ce monoïde est non commutatif dès que l'alphabet $\mathcal{A}$ a au moins deux lettres.*

Démonstration. Le mot vide ε est clairement neutre pour le produit. Soient $u, v, w \in \mathcal{A}^*$ de longueurs respectives m, n, p . Soient $x = (uv)w$ et $y = u(vw)$. On a

$$|x| = |uv| + |w| = (|u| + |v|) + |w| = m + n + p$$

et, de même, $|y| = m + n + p$. Ainsi, $|x| = |y|$. Soit $i \in \llbracket 0, m+n+p-1 \rrbracket$. Trois cas se présentent

- Si $i \in \llbracket 0, m-1 \rrbracket$, on a $y_i = u_i$. Comme $i \in \llbracket 0, m+n-1 \rrbracket$, on a $x_i = (uv)_i = u_i$.
- Si $i \in \llbracket m, m+n-1 \rrbracket$, on a $y_i = (vw)_{i-m}$. Comme $i-m \in \llbracket 0, n-1 \rrbracket$, on a $y_i = v_{i-m}$. Par ailleurs, $x_i = (uv)_i = v_{i-m}$.

- Si $i \in \llbracket m+n, m+n+p-1 \rrbracket$, on a $y_i = (vw)_{i-m}$. Mais $i-m \in \llbracket n, n+p-1 \rrbracket$, donc $y_i = w_{i-m-n}$. Par ailleurs, $x_i = w_{i-m-n}$.

Finalement, x et y ont la même longueur ($m+n+p$) et pour tout $i \in \llbracket 0, m+n+p-1 \rrbracket$, $x_i = y_i$. Ainsi, $x = y$. L'opération de produit est donc associative.

Supposons que l'alphabet $\mathcal{A}$ contient au moins deux lettres distinctes a et b . On a $ab \neq ba$, donc le produit n'est pas commutatif. $\square$

Proposition 1.2. *Soit $\mathcal{A}$ un alphabet. La fonction de longueur des mots, $|\cdot| : \mathcal{A}^* \longrightarrow \mathbb{N}$ est un morphisme de monoïdes : pour tous $u, v \in \mathcal{A}^*$, $|uv| = |u| + |v|$.*

Remarque. Si $\mathcal{A} = \{a\}$ possède une unique lettre, alors

$$\mathcal{A}^* = \{a^n : n \in \mathbb{N}\}$$

La fonction de longueur des mots est alors un isomorphisme du monoïde $(\mathcal{A}^*, \times)$ sur le monoïde $(\mathbb{N}, +)$. L'isomorphisme réciproque est la fonction $n \longmapsto a^n$.

Proposition 1.3. *Tout mot s'écrit de façon unique comme un produit de lettres.*

Démonstration. C'est une conséquence immédiate de la définition des mots. $\square$

De façon plus générale, soit $\mathcal{L}$ un langage sur l'alphabet $\mathcal{A}$. Soit $\mathcal{C}$ une partie de $\mathcal{L}$. L'ensemble $\mathcal{C}$ est un *code* pour $\mathcal{L}$ si tout mot de $\mathcal{L}$ s'écrit de façon unique comme produit de mots de $\mathcal{C}$. Ainsi, $\mathcal{A}$ est un code pour $\mathcal{A}^*$. En fait, c'est le seul. En effet, soit $\mathcal{C}$ un code pour $\mathcal{A}^*$. Pour tout $a \in \mathcal{A}$, a est un produit de mots de $\mathcal{C}$. Mais a est de longueur 1, ce qui impose facilement $a \in \mathcal{C}$. Ainsi, $\mathcal{A} \subseteq \mathcal{C}$. Inversement, soit $u \in \mathcal{C}$. Le mot u s'écrit *de façon unique* comme produit de mots de $\mathcal{C}$. Or, u est le produit de ses lettres, qui appartiennent à $\mathcal{C}$, mais aussi $u = u \in \mathcal{C}$. Donc, par unicité du produit, $u \in \mathcal{A}$. Ainsi, $\mathcal{C} = \mathcal{A}$.

2.2 Régularité

Proposition 1.4. *Tous les mots sont réguliers à gauche et à droite pour l'opération de produit : pour tous $u, v, w \in \mathcal{A}^*$,*

$$uv = uw \implies v = w \quad \text{et} \quad vu = wu \implies v = w$$

Démonstration. Montrons la première implication. Soient $u, v, w \in \mathcal{A}^*$. Supposons $uv = uw$. On a

$$|v| = |uv| - |u| = |uw| - |u| = |w|$$

Posons $|u| = m$ et $|v| = |w| = n$. Pour tout $i \in \llbracket 0, n-1 \rrbracket$,

$$v_i = (uv)_{i+m} = (uw)_{i+m} = w_i$$

Ainsi, $v = w$. La preuve de la seconde implication est analogue. $\square$

2.3 Préfixes

La « divisibilité à gauche » dans le monoïde $\mathcal{A}^*$ est introduite par la notion de préfixe.

Définition 1.1. Si $u, v \in \mathcal{A}^*$, u est un *préfixe* de v s'il existe $w \in \mathcal{A}^*$ tel que $v = uw$.

Notons que par la régularité de u , un tel w est unique. Nous noterons $u \sqsubseteq v$ lorsque u est préfixe de v .

Proposition 1.5. La relation $\sqsubseteq$ est une relation d'ordre sur $\mathcal{A}^*$.

Démonstration. Soit $u \in \mathcal{A}^*$. On a $u = u\varepsilon$, donc $u \sqsubseteq u$. La relation $\sqsubseteq$ est réflexive.

Soient $u, v, w \in \mathcal{A}^*$. Supposons $u \sqsubseteq v$ et $v \sqsubseteq w$. Il existe donc $x, y \in \mathcal{A}^*$ tels que $v = ux$ et $w = vy$. De là,

$$w = vy = (ux)y = u(xy)$$

et donc $u \sqsubseteq w$. La relation $\sqsubseteq$ est transitive.

Soient $u, v \in \mathcal{A}^*$. Supposons $u \sqsubseteq v$ et $v \sqsubseteq u$. Il existe donc $x, y \in \mathcal{A}^*$ tels que $v = ux$ et $u = vy$. On a ainsi

$$u = vy = uxy$$

Comme u est régulier, $xy = \varepsilon$. En passant aux longueurs,

$$|x| + |y| = |\varepsilon| = 0$$

et donc $|x| = |y| = 0$, d'où $x = y = \varepsilon$. Ainsi, $u = v$. La relation est antisymétrique. $\square$

Notons que si l'alphabet $\mathcal{A}$ contient au moins deux lettres a et b , alors $a \not\sqsubseteq b$ et $b \not\sqsubseteq a$. La relation $\sqsubseteq$ est donc un ordre partiel. En revanche, si $\mathcal{A} = \{a\}$ est un singleton, l'ordre est total. Pour tous $m, n \in \mathbb{N}$,

$$a^m \sqsubseteq a^n \iff m \leq n$$

Le plus petit élément de $\mathcal{A}^*$ est le mot vide. En revanche, $\mathcal{A}^*$ ne possède pas de plus grand élément.

Une propriété importante de l'opération de produit concerne l'égalité de deux produits.

Proposition 1.6. Soient $u, v, u', v' \in \mathcal{A}^*$ tels que $uv = u'v'$. Si $|u| \leq |u'|$, alors $u \sqsubseteq u'$. Si $|u'| \leq |u|$, alors $u' \sqsubseteq u$. Enfin, si $|u| = |u'|$, alors $u = u'$.

Démonstration. Supposons $m = |u| \leq |u'| = n$. Pour tout $i \in \llbracket 0, m-1 \rrbracket$,

$$(uv)_i = u_i = (u'v')_i = u'_i$$

Posons $x = u'_m \dots u'_{n-1}$. On a alors $u' = ux$, donc $u \sqsubseteq u'$.

Si $|u'| \leq |u|$, il suffit de renverser les rôles de u et u' dans ce qui précède pour obtenir $u' \sqsubseteq u$.

Enfin, si $|u| = |u'|$ on a à la fois $u \sqsubseteq u'$ et $u' \sqsubseteq u$ donc, par antisymétrie, $u = u'$. $\square$

3 Annexe

Terminons cette courte introduction par une condition nécessaire et suffisante pour que deux mots commutent.

Proposition 1.7. *Soit $\mathcal{A}$ un alphabet. Soient $u, v \in \mathcal{A}^*$. On a $uv = vu$ si et seulement si u et v sont deux puissances d'un même mot.*

Démonstration. Si $u = w^m$ et $v = w^n$ où $w \in \mathcal{A}^*$ et $m, n \in \mathbb{N}$, alors

$$uv = w^m w^n = w^{m+n} = w^{n+m} = w^n w^m = vu$$

Montrons la réciproque par récurrence forte sur $n = |u| + |v|$. Si $n = 0$, alors $u = v = \varepsilon$ et donc $u = \varepsilon^1 = v$. Les mots u et v sont deux puissances d'un même mot. Soit $n \geq 1$. Supposons que pour tous mots u et v tels que $|u| + |v| < n$, si $uv = vu$ alors u et v sont des puissances d'un même mot. Soient $u, v \in \mathcal{A}^*$ tels que $|u| + |v| = n$. Supposons $uv = vu$. Pour fixer les idées, prenons $|u| \leq |v|$. Si $u = \varepsilon$, la conclusion est immédiate puisque $v = v^1$ et $u = v^0$. Supposons donc $|u| \geq 1$. Par la proposition 6, $u \sqsubseteq v$. Il existe donc $x \in \mathcal{A}^*$ tel que $v = ux$. L'égalité $uv = vu$ devient

$$uux = uxu$$

d'où, en simplifiant

$$ux = xu$$

Remarquons que $|v| = |u| + |x| \geq 1 + |x|$, et donc $|x| < |v|$. De là,

$$|u| + |x| < |u| + |v| = n$$

L'hypothèse de récurrence appliquée à u et x montre qu'il existe $w \in \mathcal{A}^*$ et $p, q \in \mathbb{N}$ tels que $u = w^p$ et $x = w^q$. De là,

$$v = ux = w^{p+q}$$

Ainsi, u et v sont des puissances de w . $\square$

Chapitre 2

Syntaxe

1 Notion de formule

1.1 Introduction

On se donne un ensemble dénombrable $\mathcal{V}$. Les éléments de $\mathcal{V}$ sont les *variables propositionnelles*. On se donne également 5 objets $\neg$, $\Leftrightarrow$, $\Rightarrow$, $\vee$ et $\wedge$. On suppose que ces objets sont distincts, et qu'ils n'appartiennent pas à $\mathcal{V}$.

- L'objet $\neg$ est le *connecteur de négation*.
- L'objet $\Leftrightarrow$ est le *connecteur d'équivalence*.
- L'objet $\Rightarrow$ est le *connecteur d'implication*.
- L'objet $\vee$ est le *connecteur de disjonction*.
- L'objet $\wedge$ est le *connecteur de conjonction*.

Les connecteurs $\Leftrightarrow$, $\Rightarrow$, $\wedge$ et $\vee$ sont dit *binaires*. Le connecteur $\neg$ est dit *unaire*. Nous noterons

$$\mathcal{U} = \{\neg\} \quad \text{et} \quad \mathcal{B} = \{\Leftrightarrow, \Rightarrow, \wedge, \vee\}$$

On se donne enfin 2 objets différents des variables propositionnelles et des connecteurs, que nous noterons « (» et «) ». Nous les appellerons la *parenthèse ouvrante* et la *parenthèse fermante*. Notons

$$\mathcal{A} = \mathcal{V} \cup \mathcal{U} \cup \mathcal{B} \cup \{(,)\}$$

Définition 2.1. Une *expression* est un mot sur l'alphabet $\mathcal{A}$.

Certaines expressions, que nous appellerons les formules, sont plus intéressantes que d'autres. Nous allons maintenant décrire le langage des formules.

Pour toute partie $\mathcal{F}$ de $\mathcal{A}^*$, notons (V), (U) et (B) les trois propriétés suivantes.

- (V) Pour tout $A \in \mathcal{V}$, $A \in \mathcal{F}$.
- (U) Pour tout $F \in \mathcal{F}$, $(\neg F) \in \mathcal{F}$.
- (B) Pour tous $F, G \in \mathcal{F}$ et tout $\oplus \in \mathcal{B}$, $(F \oplus G) \in \mathcal{F}$.

Proposition 2.1. L'intersection $\mathcal{F}$ de toutes les parties de $\mathcal{A}^*$ qui vérifient (V), (U) et (B) est la plus petite partie de $\mathcal{A}^*$ qui vérifie ces trois propriétés.

Démonstration. Notons E l'ensemble des parties de $\mathcal{A}^*$ qui vérifient (V), (U) et (B). Remarquons que $E \neq \emptyset$, puisque $\mathcal{A}^* \in E$. L'intersection qui nous intéresse est donc bien définie. On a

$$\mathcal{F} = \bigcap_{\mathcal{G} \in E} \mathcal{G}$$

Il est évident que pour tout $\mathcal{G} \in E$, $\mathcal{F} \subseteq \mathcal{G}$. Montrons que $\mathcal{F} \in E$. Soient $F, G \in \mathcal{F}$ et $\oplus \in \mathcal{B}$. Soit $\mathcal{G} \in E$. On a $F, G \in \mathcal{G}$ donc, puisque $\mathcal{G}$ vérifie (I), $(F \oplus G) \in \mathcal{G}$. Ceci étant vrai pour tout $\mathcal{G} \in E$, on a donc $(F \oplus G) \in \mathcal{F}$. Ainsi, $\mathcal{F}$ vérifie (B). On vérifie de la même manière que $\mathcal{F}$ vérifie (V) et (U). $\square$

Définition 2.2. Une *formule* est un élément de $\mathcal{F}$.

Nous disposons dorénavant de la fonction $\mathcal{N} : \mathcal{F} \rightarrow \mathcal{F}$ définie par

$$\mathcal{N}(F) = (\neg F)$$

et, pour tout $\oplus \in \mathcal{B}$, de la fonction $\Phi_{\oplus} : \mathcal{F}^2 \longrightarrow \mathcal{F}$ définie par

$$\Phi_{\oplus}(F, G) = (F \oplus G)$$

Remarque. Le lecteur attentif s'apercevra que d'ici la fin du chapitre *nous n'utilisons plus jamais explicitement les connecteurs $\Leftrightarrow, \Rightarrow, \vee$ et $\wedge$* . Nous aurions tout aussi bien pu supposer qu'il y a 3 connecteurs binaires, ou qu'il y en a 10. De même, nous avons un unique connecteur unaire ($\neg$) mais nous pourrions sans difficulté supposer qu'il y en a d'autres.

1.2 Construction des formules

Le défaut de la proposition 2.1 est qu'elle ne dit pas comment créer des formules. Nous allons maintenant donner une construction « par le bas » de l'ensemble des formules. Cette construction montre que toute formule peut être construite en un nombre fini d'étapes à partir des variables propositionnelles, à l'aide des 5 fonctions $\mathcal{N}$ et $\Phi_{\oplus}$, où $\oplus \in \mathcal{B}$.

Posons $\mathcal{F}_0 = \mathcal{V}$ et, pour tout $n \in \mathbb{N}^*$,

$$\mathcal{F}_n = \mathcal{F}_{n-1} \cup \{\mathcal{N}(F) : F \in \mathcal{F}_{n-1}\} \cup \{\Phi_{\oplus}(F, G) : F, G \in \mathcal{F}_{n-1}, \oplus \in \mathcal{B}\}$$

On définit ainsi par récurrence sur n une suite $(\mathcal{F}_n)_{n \in \mathbb{N}}$ d'ensembles d'expressions. Remarquons que cette suite est croissante au sens de l'inclusion.

Proposition 2.2.

$$\mathcal{F} = \bigcup_{n \in \mathbb{N}} \mathcal{F}_n$$

Démonstration. Notons $\mathcal{F}'$ la réunion ci-dessus.

($\subseteq$) Pour montrer que $\mathcal{F} \subseteq \mathcal{F}'$, il nous suffit (minimalité) de prouver que $\mathcal{F}'$ vérifie (V), (N) et (I). Soient $F, G \in \mathcal{F}'$ et $\oplus \in \mathcal{B}$. Il existe $m, n \in \mathbb{N}$ tels que $F \in \mathcal{F}_m$ et $G \in \mathcal{F}_n$. Soit $p = \max(m, n)$. Par croissance, $F, G \in \mathcal{F}_p$ et donc $(F \oplus G) \in \mathcal{F}_{p+1} \subseteq \mathcal{F}'$. Ainsi, $\mathcal{F}'$ vérifie (B). On montre de même que cet ensemble vérifie (V) et (U).

($\supseteq$) Montrons maintenant que $\mathcal{F}' \subseteq \mathcal{F}$. Pour cela, montrons par récurrence sur n que pour tout $n \in \mathbb{N}$, $\mathcal{F}_n \subseteq \mathcal{F}$.

Comme $\mathcal{F}$ vérifie (V), on a $\mathcal{F}_0 \subseteq \mathcal{F}$.

Soit $n \in \mathbb{N}^*$. Supposons $\mathcal{F}_{n-1} \subseteq \mathcal{F}$. Soit $F \in \mathcal{F}_n$. Trois cas se présentent.

- Cas 1, $F \in \mathcal{F}_{n-1}$. Par l'hypothèse de récurrence, $F \in \mathcal{F}$.
- Cas 2, $F = (\neg G)$ où $G \in \mathcal{F}_{n-1}$. Par l'hypothèse de récurrence, $G \in \mathcal{F}$. Comme $\mathcal{F}$ vérifie (N), on a aussi $F \in \mathcal{F}$.
- Cas 3, $F = (F_1 \oplus F_2)$ où $F_1, F_2 \in \mathcal{F}_{n-1}$ et $\oplus \in \mathcal{B}$. Ce cas se traite comme le cas 2.

□

Définition 2.3. Soit $F \in \mathcal{F}$. La *hauteur* de F est le plus petit entier naturel n tel que $F \in \mathcal{F}_n$.

Nous noterons $h(F)$ la hauteur de la formule F .

Cela va sans dire, mais disons le quand même. La première lettre d'une formule ne peut pas être n'importe quoi.

Proposition 2.3. *La première lettre d'une formule est une variable propositionnelle ou une parenthèse ouvrante.*

Démonstration. Soit $F \in \mathcal{F}$. Soit $n = h(F)$. Si $n = 0$, alors F est une variable propositionnelle, sa première lettre est donc une variable propositionnelle. Si $n \geq 1$ alors, par minimalité de n , $F \notin \mathcal{F}_{n-1}$, donc

$$F \in \{\mathcal{N}(F) : F \in \mathcal{F}_{n-1}\} \cup \{\Phi_{\oplus}(F, G) : F, G \in \mathcal{F}_{n-1}, \oplus \in \mathcal{B}\}$$

La première lettre de F est donc une parenthèse ouvrante. $\square$

2 Induction structurelle

Pour montrer des propriétés relatives aux formules, il existe plusieurs possibilités. On peut effectuer des récurrences sur la longueur des formules, ou encore des récurrences sur leur hauteur. Il existe un troisième type de « récurrence », souvent plus élégant : *l'induction structurelle*.

2.1 Preuves par induction structurelle

Une *propriété des expressions* est un ensemble $P \subseteq \mathcal{A}^*$. Pour toute expression E , nous noterons $P(E)$ lorsque $E \in P$. Nous dirons alors que E *vérifie* la propriété P .

Proposition 2.4. *Soit P une propriété des expressions. On suppose que P vérifie les trois propriétés ci-dessous.*

- (1) *Les variables propositionnelles vérifient P .*
- (2) *Pour toute formule G , si G vérifie P , alors $(\neg G)$ vérifie P .*
- (3) *Pour toutes formules G et H et tout connecteur binaire $\oplus$, si G et H vérifient P , alors $(G \oplus H)$ vérifie P .*

Alors, toutes les formules vérifient P .

Démonstration. Montrons par récurrence sur n que pour tout $n \in \mathbb{N}$, pour toute formule F de hauteur n , on a $P(F)$.

Par (1), la propriété est vérifiée pour $n = 0$. Soit $n \geq 1$. Supposons la propriété vérifiée pour $n - 1$. Soit F une formule de hauteur n . Deux cas se présentent.

- Cas 1, il existe $G \in \mathcal{F}_{n-1}$ telle que $F = (\neg G)$. Par l'hypothèse de récurrence, on a $P(G)$. Par (2), on a donc $P(F)$.
- Cas 2, il existe $G, H \in \mathcal{F}_{n-1}$ et $\oplus \in \mathcal{B}$ tels que $F = (G \oplus H)$. Par l'hypothèse de récurrence, on a $P(G)$ et $P(H)$. Par (3), on a donc $P(F)$.

$\square$

2.2 Compter les parenthèses

Nous allons utiliser le théorème d'induction structurelle pour montrer une propriété importante concernant le nombre de parenthèses ouvrantes et de parenthèses fermantes d'une formule.

Pour toute expression E , notons $o(E)$ le nombre de parenthèses ouvrantes de E et $f(E)$ le nombre de parenthèses fermantes de E . Les fonctions $o, f : \mathbb{E} \rightarrow \mathbb{N}$ sont des morphismes de monoïdes. On a $o(\varepsilon) = f(\varepsilon) = 0$ et pour toutes expressions E, E' , $o(E E') = o(E) + o(E')$ et $f(E E') = f(E) + f(E')$.

Proposition 2.5. *Pour toute formule F et tout préfixe E de F , on a $o(E) \geq f(E)$. On a égalité si et seulement si $E = \varepsilon$ ou $E = F$.*

Démonstration. Montrons le résultat par induction structurelle.

- (1) La propriété est immédiate si F est une variable propositionnelle A . Dans ce cas $E = \varepsilon$ ou $E = A = F$.
- (2) Soit G une formule. Supposons la propriété vérifiée par G . Soit $F = (\neg G)$. Soit E un préfixe de F . Si $E = \varepsilon$, $o(E) = f(E) = 0$. Si $E = ($ ou $E = (\neg$, $o(E) = 1 > f(E) = 0$. Si $E = (\neg E'$ où E' est un préfixe de G alors, par l'hypothèse d'induction,

$$o(E) = 1 + o(E') \geq 1 + f(E') = 1 + f(E) > f(E)$$

Enfin, si $E = F$ alors, toujours par l'hypothèse d'induction,

$$o(E) = 1 + o(G) = 1 + f(G) = f(E)$$

- (3) Soient G et H deux formules et $\oplus$ un connecteur binaire. Supposons la propriété vérifiée par G et H . Soit $F = (G \oplus H)$. Soit E un préfixe de F . Si $E = \varepsilon$, $o(E) = f(E)$. Si $E = ($, $o(E) = 1 > f(E) = 0$. Si $E = (E'$ où E' est un préfixe de G alors, par l'hypothèse d'induction sur G ,

$$o(E) = 1 + o(E') \geq 1 + f(E') = 1 + f(E) > f(E)$$

Si $E = (G \oplus E'$ où E' est un préfixe de H alors, par l'hypothèse d'induction sur G et sur H ,

$$\begin{aligned} o(E) &= 1 + o(G) + o(E') \\ &= 1 + f(G) + f(E') \\ &\geq 1 + f(G) + f(E') \\ &= 1 + f(E) \\ &> f(E) \end{aligned}$$

Enfin, si $E = (G \oplus H) = F$, alors, toujours par l'hypothèse d'induction,

$$o(E) = 1 + o(G) + o(H) = 1 + f(G) + f(H) = f(E)$$

□

Cette proposition montre deux choses intéressantes. Si F est une formule alors

- $o(F) = f(F)$.

- Si E est un préfixe de F différent de ε et de F , alors $o(E) > f(E)$

D'où le corollaire ci-dessous.

Corollaire 2.6. *Soit F une formule. Si E est un préfixe de F différent de ε et de F , alors E n'est pas une formule.*

Ce corollaire sera la clé de la preuve du théorème de lecture unique dont nous allons parler maintenant.

3 Le théorème de lecture unique

3.1 Le résultat

La construction par le bas de l'ensemble $\mathcal{F}$ nous a montré que toute formule peut être construite en un nombre fini d'étapes à partir des variables propositionnelles à l'aide des fonctions $\mathcal{N}$ et $\mathcal{I}$. Nous allons maintenant montrer l'*unicité* de cette construction.

Proposition 2.7. *Soit F une formule. On est dans un et un seul des trois cas suivants.*

- Cas 1, F est une variable propositionnelle.
- Cas 2, il existe une unique formule G telle que $F = (\neg G)$.
- Cas 3, il existe une unique formule G , une unique formule H et un unique connecteur binaire $\oplus$ tels que $F = (G \oplus H)$.

Démonstration. Soit n la hauteur de F . Si $n = 0$, alors F est une variable propositionnelle. On est donc dans le cas 1 et il est clair que l'on n'est ni dans le cas 2, ni dans le cas 3. Supposons que $n \geq 1$. Par minimalité de n , $F = (\neg G)$ ou $F = (H \oplus K)$, où G, H, K appartiennent à $\mathcal{F}_{n-1}$ et $\oplus \in \mathcal{B}$.

Supposons un instant que $(\neg G) = (H \oplus K)$. La première lettre de H est alors la lettre $\neg$, ce qui est impossible. On est donc dans le cas 2 *ou bien* dans le cas 3. Il reste à montrer l'unicité.

Supposons $(\neg G) = (\neg G')$, où G et G' sont deux formules. En simplifiant par $(\neg$ à gauche et par $)$ à droite, on en déduit $G = G'$.

Il nous reste à traiter le cas intéressant. Supposons $(H \oplus K) = (H' \otimes K')$, où H, K, H', K' sont des formules et $\oplus, \otimes$ sont deux connecteurs binaires. En simplifiant à gauche par $($, on a donc

$$(1) H \oplus K = H' \otimes K'$$

Pour fixer les idées, la longueur de H est inférieure ou égale à celle de H' . La formule H est alors un préfixe de la formule H' . Par le corollaire 2.6, aucun préfixe de H' autre que H' et le mot vide n'est une formule. Or, H n'est pas le mot vide, donc $H = H'$. En simplifiant (1) à gauche par H , il vient

$$\oplus K = \otimes K')$$

Les deux mots ci-dessus ont la même première lettre, donc $\oplus = \otimes$. En simplifiant par $\oplus$ et par la parenthèse fermante, on obtient $K = K'$. $\square$

3.2 Définitions par induction structurelle

Nous avons vu la possibilité de *prouver des propriétés* par induction structurelle. Nous allons maintenant voir qu'il est possible de *définir des fonctions* par induction structurelle.

Proposition 2.8. *Soit E un ensemble. Soient $\varphi_0 : \mathcal{V} \rightarrow E$, $\varphi_{\neg} : E \rightarrow E$ et pour tout connecteur binaire $\oplus$, $\varphi_{\oplus} : E \times E \rightarrow E$. Il existe une unique fonction $f : \mathcal{F} \rightarrow E$ telle que*

- Pour toute variable propositionnelle A , $f(A) = \varphi_0(A)$.
- Pour toute formule G , $f(\neg G) = \varphi_{\neg}(f(G))$.
- Pour toutes formules G et H et tout connecteur binaire $\oplus$, $f((G \oplus H)) = \varphi_{\oplus}(f(G), f(H))$.

Démonstration. Soient f, f' deux fonctions qui conviennent. On montre facilement par induction structurelle que pour toute formule F , $f(F) = f'(F)$. Soit dit en passant, le théorème de lecture unique intervient de façon cruciale dans la preuve. Ainsi, $f = f'$, d'où l'unicité.

Pour montrer l'existence, considérons la fonction f définie par récurrence forte sur la hauteur des formules comme suit.

- Pour toute formule F de hauteur 0 (c'est à dire une variable propositionnelle), $f(F) = \varphi_0(F)$.
- Pour tout $n \in \mathbb{N}^*$ et toute formule F de hauteur n , en supposant $f(G)$ définie pour toute formule G de hauteur inférieure ou égale à $n - 1$,
 - Si $F = (\neg G)$ où G est de hauteur $n - 1$, $f(F) = \varphi_{\neg}(f(G))$.
 - Si $F = (G \oplus H)$ où G et H sont de hauteur inférieure ou égale à $n - 1$ et $\oplus$ est un connecteur binaire, $f(F) = \varphi_{\oplus}(f(G), f(H))$.

Ici encore, le théorème de lecture unique est indispensable. On est dans un et un seul des cas ci-dessus, et dans chacun des cas, il y a une seule façon d'écrire la formule F . Clairement, la fonction f que nous venons de définir convient. $\square$

Exemple 1. Remarquons que pour toutes formules G et H et tout connecteur binaire $\oplus$,

$$|(\neg G)| = 3 + |G|$$

$$|(G \oplus H)| = 3 + |G| + |H|$$

La fonction longueur $|\cdot| : \mathcal{F} \rightarrow \mathbb{N}$ peut donc être définie par induction structurelle en posant

- Pour toute variable propositionnelle A , $\varphi_0(A) = 1$.
- Pour tout $n \in \mathbb{N}$, $\varphi_{\neg}(n) = n + 3$.
- Pour tout $\oplus \in \mathcal{B}$ et tous $m, n \in \mathbb{N}$, $\varphi_{\oplus}(m, n) = m + n + 3$.

Exemple 2. La fonction « nombre de parenthèses ouvrantes » $o : \mathcal{F} \rightarrow \mathbb{N}$ est définie par induction structurelle en posant

- Pour toute variable propositionnelle A , $\varphi_0(A) = 0$.
- Pour tout $n \in \mathbb{N}$, $\varphi_{\neg}(n) = n + 1$.
- Pour tout $\oplus \in \mathcal{B}$ et tous $m, n \in \mathbb{N}$, $\varphi_{\oplus}(m, n) = m + n + 1$.

Qu'en est-il de la fonction hauteur ?

3.3 Retour sur la hauteur

Proposition 2.9.

- Pour toute formule F , $h(F) = 0$ si et seulement si F est une variable propositionnelle.
- Pour toute formule F , $h(\neg F) = h(F) + 1$.
- Pour toutes formules F et G et tout connecteur binaire $\oplus$, $h((F \oplus G)) = 1 + \max(h(F), h(G))$.

Démonstration. Le premier point est immédiat. Montrons le troisième point et laissons le second point au lecteur. Soient $G, H \in \mathcal{F}$ et $\oplus \in \mathcal{B}$. Soit $F = (G \oplus H)$. Par la croissance des $\mathcal{F}_n$, on a $G \in \mathcal{F}_{\max(h(G), h(H))}$ et $H \in \mathcal{F}_{\max(h(G), h(H))}$. De là, $F \in \mathcal{F}_{\max(h(G), h(H)) + 1}$, donc $h(F) \leq \max(h(G), h(H)) + 1$.

Comme $F \in \mathcal{F}_{h(F)}$, il existe $G', H' \in \mathcal{F}_{h(F)-1}$ et $\otimes \in \mathcal{B}$ tels que $F = (G' \otimes H')$. Par le théorème de lecture unique, $G = G'$, $H = H'$ et $\oplus = \otimes$. Puisque $G \in \mathcal{F}_{h(F)-1}$, on a $h(G) \leq h(F) - 1$. De même, $h(H) \leq h(F) - 1$. Ainsi, $h(F) \geq 1 + h(G)$ et $h(F) \geq 1 + h(H)$, donc $h(F) \geq 1 + \max(h(G), h(H))$. $\square$

Remarque. Reprenons les notations du paragraphe précédent. La fonction hauteur $h : \mathcal{F} \rightarrow \mathbb{N}$ peut donc être définie par induction structurelle en posant

- Pour toute variable propositionnelle A , $\varphi_0(A) = 0$.
- Pour tout $n \in \mathbb{N}$, $\varphi_{-}(n) = n + 1$.
- Pour tout connecteur binaire $\oplus$ et tous $m, n \in \mathbb{N}$, $\varphi_{\oplus}(m, n) = 1 + \max(m, n)$.

Existe-t-il un lien entre la hauteur d'une expression et sa longueur? Nous allons voir que c'est la cas. Assez intuitivement, les expressions de hauteur n et de longueur minimale sont constituées uniquement de négations. Celles de longueur maximale sont constituées uniquement d'implications.

Proposition 2.10. Pour toute formule F ,

$$3h(F) + 1 \leq |F| \leq 2^{h(F)+2} - 3$$

Démonstration. Montrons le résultat par récurrence forte sur la hauteur n de la formule F . Soit F une formule de hauteur 0. La formule F est une variable propositionnelle, les deux inégalités sont ici des égalités. Soit $n \geq 1$. Supposons la propriété vérifiée pour tous les entiers strictement inférieurs à n . Soit F une formule de hauteur n . Deux cas se présentent.

- Cas 1, $F = (\neg G)$ où $h(G) = n - 1$. Par l'hypothèse d'induction,

$$3n - 2 \leq |G| \leq 2^{n+1} - 3$$

Comme $|F| = |G| + 3$, il vient

$$3n + 1 \leq |F| \leq 2^{n+1}$$

Il reste à remarquer que

$$2^{n+1} \leq 2^{n+2} - 3$$

En effet, $n \geq 1$ donc

$$2^{n+2} - 3 - 2^{n+1} = 2^{n+1} - 3 \geq 1 \geq 0$$

- Cas 2, $F = (G \oplus H)$ où $\max(h(G), h(H)) = n - 1$ et $\oplus \in \mathcal{B}$. Posons $p = h(G)$ et $q = h(H)$. Pour fixer les idées, $p \leq q = n - 1$. Par l'hypothèse d'induction,

$$3p + 1 \leq |G| \leq 2^{p+2} - 3$$

$$3n - 2 \leq |H| \leq 2^{n+1} - 3$$

Comme $|F| = |G| + |H| + 3$, il vient

$$3p + 3n + 2 \leq |F| \leq 2^{p+2} + 2^{n+1} - 3$$

Comme $p \geq 0$, on a

$$3p + 3n + 2 \geq 3n + 2 \geq 3n + 1$$

Comme $p \leq n - 1$, on a aussi

$$2^{p+2} + 2^{n+1} - 3 \leq 2^{n+1} + 2^{n+1} - 3 = 2^{n+2} - 3$$

La formule F vérifie donc la propriété voulue.

□

Nous allons maintenant voir que ces inégalités sont optimales, et donner des conditions nécessaires et suffisantes d'égalité.

Proposition 2.11. *Soit $n \in \mathbb{N}$. Pour toute formule F , $|F| = 3h(F) + 1$ si et seulement si aucun des connecteurs binaires n'apparaît dans F .*

Démonstration. Montrons ce résultat par récurrence forte sur la hauteur n de la formule F . C'est immédiat pour $n = 0$. Soit $n \geq 1$. Supposons la propriété vérifiée pour tous les entiers strictement inférieurs à n . Soit F une formule de hauteur n . Deux cas se présentent.

- Cas 1, $F = (\neg G)$ où G est de hauteur $n - 1$. On a $|F| = 3n + 1$ si et seulement si $|G| = 3n - 2 = 3(n - 1) + 1$. Par l'hypothèse de récurrence, cette condition équivaut à dire qu'aucun connecteur binaire n'apparaît dans G , c'est à dire qu'aucun connecteur binaire n'apparaît dans F .
- Cas 2, $F = (G \oplus H)$ où $\max(h(G), h(H)) = n - 1$ et $\oplus \in \mathcal{B}$. En reprenant la preuve de la proposition précédente, on voit que

$$|F| \geq 3n + 2 > 3n + 1$$

Dans le cas 2, on n'a donc jamais égalité.

□

Définissons maintenant par induction structurelle la notion de formule équilibrée.

Définition 2.4. La formule F est *équilibrée* lorsque F est une variable propositionnelle, ou alors $F = (\neg G)$ où G est équilibrée, ou alors $F = (G \oplus H)$ où G et H sont équilibrées et de même hauteur et $\oplus \in \mathcal{B}$.

Proposition 2.12. *Soit $n \in \mathbb{N}$. Pour toute formule F , $|F| = 2^{h(F)+2} - 3$ si et seulement si F est équilibrée et ne contient pas le connecteur $\neg$.*

Démonstration. Montrons ce résultat par récurrence forte sur la hauteur n de la formule F . C'est immédiat si $n = 0$. Soit $n \geq 1$. Supposons la propriété vérifiée pour tous les entiers strictement inférieurs à n . Soit F une formule de hauteur n . Deux cas se présentent.

- Cas 1, $F = (\neg G)$ où G est de hauteur $n - 1$. En reprenant la preuve de la proposition ??, on voit que

$$|F| = |G| + 3 \leq 2^{n+1} \leq 2^{n+2} - 4 < 2^{n+2} - 3$$

Dans le cas 1 on n'a donc jamais égalité.

- Cas 2, $F = (G \oplus H)$ où $\max(h(G), h(H)) = n - 1$ et $\oplus \in \mathcal{B}$. On a

$$|F| = |G| + |H| + 3 \leq (2^{n+1} - 3) + (2^{n+1} - 3) + 3$$

On a l'égalité voulue si et seulement si

$$(1) \quad |G| = 2^{n+1} - 3 \quad \text{et} \quad |H| = 2^{n+1} - 3$$

Remarquons que

$$|G| \leq 2^{h(G)+2} - 3$$

L'égalité ci-dessus impose donc $h(G) = n - 1$. De même, $h(H) = n - 1$. Par l'hypothèse de récurrence, on a (1) si et seulement si G et H sont équilibrées et ne contiennent pas le connecteur $\neg$. Ceci équivaut à dire que F est équilibrée et ne contient pas le connecteur $\neg$.

□

Chapitre 3

Sémantique

1 Environnements

1.1 Notion d'environnement

Dans tout le chapitre, on note $\mathbb{B} = \{0, 1\}$. Nous appellerons 0 et 1 les *valeurs de vérité*. Un *environnement* est une fonction $\gamma : \mathcal{V} \longrightarrow \mathbb{B}$, c'est à dire une fonction qui assigne à chaque variable propositionnelle une valeur de vérité. Nous noterons Γ l'ensemble des environnements.

1.2 Fonctions booléennes

Nous allons définir 5 fonctions associées aux 5 connecteurs, que nous appellerons les *fonctions booléennes*. On a $\varphi_{\neg} : \mathbb{B} \longrightarrow \mathbb{B}$. Pour tout connecteur binaire $\oplus$, on a $\varphi_{\oplus} : \mathbb{B}^2 \longrightarrow \mathbb{B}$. Pour tous $x, y \in \mathbb{B}$,

- $\varphi_{\neg}(x) = \bar{x}$ où $\bar{x} = 1 - x$.
- $\varphi_{\vee}(x, y) = \max(x, y)$.
- $\varphi_{\wedge}(x, y) = \min(x, y)$.
- $\varphi_{\Rightarrow}(x, y) = \max(\bar{x}, y)$.
- $\varphi_{\Leftrightarrow}(x, y) = \min(\max(\bar{x}, y), \max(x, \bar{y}))$.

Remarquons qu'il existe un lien entre ces fonctions. Par exemple,

$$\varphi_{\Rightarrow}(x, y) = \varphi_{\vee}(\varphi_{\neg}(x), y)$$

ou encore

$$\varphi_{\Leftrightarrow}(x, y) = \varphi_{\wedge}(\varphi_{\Rightarrow}(x, y), \varphi_{\Rightarrow}(y, x))$$

Les fonctions associées aux connecteurs $\neg$, $\wedge$ et $\vee$ suffisent donc pour exprimer toutes les fonctions booléennes. On pourrait même se passer, par exemple, de $\varphi_{\vee}$: on laisse en exercice montrer que

$$\varphi_{\vee}(x, y) = \varphi_{\neg}(\varphi_{\wedge}(\varphi_{\neg}(x), \varphi_{\neg}(y)))$$

Les deux tableaux ci-dessous résument les valeurs des fonctions booléennes.

		x		0	1
		$\varphi_{\neg}(x)$		1	0
x	y	$\varphi_{\Leftrightarrow}(x, y)$	$\varphi_{\Rightarrow}(x, y)$	$\varphi_{\vee}(x, y)$	$\varphi_{\wedge}(x, y)$
0	0	1	1	0	0
0	1	0	1	1	0
1	0	0	0	1	0
1	1	1	1	1	1

FIGURE 3.1 – Les fonctions booléennes

Exercice. Soit $\varphi_0 : \mathbb{B}^2 \longrightarrow \mathbb{B}$ définie par $\varphi_0(x, y) = \min(\bar{x}, \bar{y})$. Exprimer les 5 fonctions booléennes à l'aide de φ_0 .

1.3 Évaluation

Définissons maintenant par induction structurelle un fonction $\text{ev} : \mathcal{F} \times \Gamma \longrightarrow \mathbb{B}$. Plus précisément, pour tout environnement γ nous définissons par induction structurelle la fonction $F \longmapsto \text{ev}(F, \gamma)$. Soit $\gamma \in \Gamma$.

- Pour toute variable propositionnelle A , $\text{ev}(A, \gamma) = \gamma(A)$.
- Pour toute formule F ,

$$\text{ev}((\neg F), \gamma) = \varphi_{\neg}(\text{ev}(F, \gamma))$$

- Pour toutes formules G, H et tout connecteur binaire $\oplus$,

$$\text{ev}((G \oplus H), \gamma) = \varphi_{\oplus}(\text{ev}(G, \gamma), \text{ev}(H, \gamma))$$

Définition 3.1. Soient $F \in \mathcal{F}$ une formule et $\gamma \in \Gamma$. L'environnement γ *satisfait* la formule F si $\text{ev}(F, \gamma) = 1$.

Définition 3.2. Soit $F \in \mathcal{F}$.

- La formule F est *satisfiable* si elle est satisfaite par au moins un environnement.
- La formule F est une *contradiction* si elle n'est pas satisfiable.
- La formule F est une *tautologie* si elle est satisfaite par tous les environnements.

Notation. Nous noterons $\models F$ lorsque F est une tautologie.

Proposition 3.1. La formule F est une tautologie (resp : contradiction) si et seulement si $(\neg F)$ est une contradiction (resp : tautologie).

Démonstration. Pour tout environnement γ ,

$$\text{ev}((\neg F), \gamma) = 1 - \text{ev}(F, \gamma)$$

d'où facilement, le résultat. $\square$

1.4 Les variables d'une formule

Définissons par induction structurelle l'ensemble $V(F)$ des variables propositionnelles qui apparaissent dans une formule F .

- Si A est une variable propositionnelle, $V(A) = \{A\}$.
- Si F est une formule, $V((\neg F)) = V(F)$.
- Si F et G sont deux formules et $\oplus$ est un connecteur binaire, $V((F \oplus G)) = V(F) \cup V(G)$.

Lorsqu'on évalue une formule dans un environnement, la valeur obtenue ne dépend que de la valeur de l'environnement pour les variables propositionnelles qui interviennent dans F . Soyons plus précis.

Proposition 3.2. Soit F une formule. Soient $\gamma, \gamma' \in \Gamma$. On suppose que pour tout $A \in V(F)$, $\gamma(A) = \gamma'(A)$. Alors, $\text{ev}(F, \gamma) = \text{ev}(F, \gamma')$.

Démonstration. Montrons par induction structurelle que pour toute formule F , pour tous environnements γ, γ' , si γ et γ' coïncident sur $V(F)$ alors $\text{ev}(F, \gamma) = \text{ev}(F, \gamma')$.

Soit $F = A$ est une variable propositionnelle. Soient $\gamma, \gamma' \in \Gamma$. Supposons $\gamma(A) = \gamma'(A)$. Alors,

$$\text{ev}(F, \gamma) = \gamma(A) = \gamma'(A) = \text{ev}(F, \gamma')$$

Soit G une formule. Soient $\gamma, \gamma' \in \Gamma$. Supposons pour tous environnements γ et γ' qui coïncident sur $V(G)$, on a $\text{ev}(G, \gamma) = \text{ev}(G, \gamma')$. Soit $F = (\neg G)$. Soient γ et γ' deux environnements qui coïncident sur $V(F)$. Comme $V(F) = V(G)$, γ et γ' coïncident sur $V(G)$. De là, par l'hypothèse d'induction,

$$\text{ev}(F, \gamma) = \varphi_{\neg}(\text{ev}(G, \gamma)) = \varphi_{\neg}(\text{ev}(G, \gamma')) = \text{ev}(F, \gamma')$$

Soient G et H deux formules et $\oplus$ un connecteur binaire. Soient $\gamma, \gamma' \in \Gamma$. Supposons pour tous environnements γ et γ' qui coïncident sur $V(G)$, on a $\text{ev}(G, \gamma) = \text{ev}(G, \gamma')$, et de même pour H . Soit $F = (G \oplus H)$. Soient γ et γ' deux environnements qui coïncident sur $V(F)$. Comme $V(F) = V(G) \cup V(H)$, γ et γ' coïncident sur $V(G)$ et aussi sur $V(H)$. De là, par l'hypothèse d'induction,

$$\text{ev}(F, \gamma) = \varphi_{\oplus}(\text{ev}(G, \gamma), \text{ev}(H, \gamma)) = \varphi_{\oplus}(\text{ev}(G, \gamma'), \text{ev}(H, \gamma')) = \text{ev}(F, \gamma')$$

□

1.5 Tables de vérité

Ce résultat montre que pour déterminer $\text{ev}(F, \gamma)$, il suffit de s'intéresser aux valeurs de γ sur les variables propositionnelles qui interviennent dans F . Clairement, l'ensemble $V(F)$ est un ensemble fini (très grossièrement, le cardinal de cet ensemble est inférieur ou égal à la longueur de la formule). Il est donc possible de déterminer la valeur de $\text{ev}(F, \gamma)$ sur la totalité des environnements (qui sont en nombre infini) en un nombre fini d'étapes. C'est le principe des *tables de vérité*. Soit F une formule dont les variables sont $A_1, \dots, A_n$. On construit une table possédant 2^n lignes. Chaque ligne de la table est étiquetée par un n -uplet $(x_1, \dots, x_n) \in \mathbb{B}^n$. On indique ensuite dans cette ligne la valeur de $\text{ev}(F, \gamma)$ pour tous les environnements γ tels que $\gamma(A_i) = x_i$, $i \in \llbracket 1, n \rrbracket$.

Il est évidemment possible de rajouter dans la table des colonnes donnant la valeur de $\text{ev}(G, \gamma)$ pour des « sous-formules » G de la formule F . Prenons un exemple. Soit

$$F = (A \Rightarrow (B \vee C))$$

où A , B et C sont trois variables propositionnelles. « La » table de vérité de F est

A	B	C	$(B \vee C)$	F
0	0	0	0	1
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Les étiquettes des colonnes devraient être plus rigoureusement $\text{ev}(A, \gamma)$, $\text{ev}(B, \gamma)$, etc. Par exemple, la première ligne de la table nous dit que pour tout $\gamma \in \Gamma$ tel que $\text{ev}(A, \gamma) = \text{ev}(B, \gamma) = \text{ev}(C, \gamma) = 0$, on a $\text{ev}((B \vee C), \gamma) = 0$ et $\text{ev}(F, \gamma) = 1$.

1.6 Une première liste de tautologies

Dans les formules ci-dessous, A , B et C sont des variables propositionnelles. Des tables de vérité permettent de montrer les tautologies ci-dessous.

- | | |
|---|-------------------------------|
| 1. $\models (A \vee (\neg A))$ | tiers exclu |
| 2. $\models (\neg(A \wedge (\neg A)))$ | non contradiction |
| 3. $\models ((A \wedge B) \Rightarrow A)$ | élimination du $\wedge$ (1) |
| 4. $\models (A \Rightarrow (A \vee B))$ | élimination du $\wedge$ (2) |
| 5. $\models ((A \wedge (A \Rightarrow B)) \Rightarrow B)$ | modus ponens |
| 6. $\models (((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C))$ | transitivité de l'implication |
| 7. $\models (((A \Leftrightarrow B) \wedge (B \Leftrightarrow C)) \Rightarrow (A \Leftrightarrow C))$ | transitivité de l'équivalence |

Voici une dernière tautologie, le *principe de démonstration par l'absurde*.

Proposition 3.3. *Soit C une contradiction. Pour toute formule F ,*

$$\models (((\neg F) \Rightarrow C) \Rightarrow F)$$

Démonstration. Soit γ un environnement. Comme C est une contradiction, $\text{ev}(C, \gamma) = 0$. De là,

$$\begin{aligned} \text{ev}(((\neg F) \Rightarrow C), \gamma) &= \varphi_{\Rightarrow}(\text{ev}((\neg F), \gamma), \text{ev}(C, \gamma)) \\ &= \varphi_{\Rightarrow}(\overline{\text{ev}(F, \gamma)}, 0) \\ &= \max(\overline{\text{ev}(F, \gamma)}, 0) \\ &= \max(\text{ev}(F, \gamma), 0) \\ &= \text{ev}(F, \gamma) \end{aligned}$$

De là,

$$\text{ev}((((\neg F) \Rightarrow C) \Rightarrow F), \gamma) = \max(\overline{\text{ev}(F, \gamma)}, \text{ev}(F, \gamma)) = 1$$

d'où le résultat. $\square$

2 Substitution

2.1 Notion de substitution

Une *fonction de substitution* est une fonction $\sigma : \mathcal{V} \longrightarrow \mathcal{F}$. On prolonge σ à l'ensemble des formules par induction structurelle. Pour toute formule F qui n'est pas une variable propositionnelle,

- Si $F = (\neg G)$ où G est une formule, alors $\sigma(F) = (\neg \sigma(G))$.
- Si $F = (G \oplus H)$ où G et H sont deux formules et $\oplus$ est un connecteur binaire, alors $\sigma(F) = (\sigma(G) \oplus \sigma(H))$.

Soient σ une fonction de substitution et γ un environnement. Définissons $\sigma * \gamma : \mathcal{V} \longrightarrow \mathbb{B}$ par

$$\sigma * \gamma(A) = \text{ev}(\sigma(A), \gamma)$$

La fonction $\sigma * \gamma$ est un environnement.

Proposition 3.4. *Soient σ une fonction de substitution et γ un environnement. Pour toute formule F ,*

$$\text{ev}(\sigma(F), \gamma) = \text{ev}(F, \sigma * \gamma(F))$$

Démonstration. Montrons le résultat par induction structurelle sur F .

Si $F = A$ est une variable propositionnelle,

$$\text{ev}(\sigma(A), \gamma) = \sigma * \gamma(A) = \text{ev}(A, \sigma * \gamma)$$

Soit G une formule. Supposons la propriété vraie pour G . Soit $F = (\neg G)$. On a $\sigma(F) = (\neg \sigma(G))$. De là,

$$\text{ev}(\sigma(F), \gamma) = \varphi_{\neg}(\text{ev}(\sigma(G), \gamma)) = \varphi_{\neg}(\text{ev}(G, \sigma * \gamma)) = (\text{ev}((\neg G), \sigma * \gamma)) = (\text{ev}(F, \sigma * \gamma))$$

Soient enfin G et H deux formules. Supposons la propriété vraie pour G et H . Soit $\oplus$ un connecteur binaire. Soit $F = (G \oplus H)$. On a $\sigma(F) = (\sigma(G) \oplus \sigma(H))$. De là,

$$\begin{aligned} \text{ev}(\sigma(F), \gamma) &= \varphi_{\oplus}(\text{ev}(\sigma(G), \gamma), \text{ev}(\sigma(H), \gamma)) \\ &= \varphi_{\oplus}(\text{ev}(G, \sigma * \gamma), \text{ev}(H, \sigma * \gamma)) \\ &= \text{ev}((G \oplus H), \sigma * \gamma) \\ &= \text{ev}(F, \sigma * \gamma) \end{aligned}$$

□

Proposition 3.5. *Soit F une tautologie (resp : une contradiction). Pour toute fonction de substitution σ , la formule $\sigma(F)$ est encore une tautologie (resp : une contradiction).*

Démonstration. Faisons la preuve lorsque F est une tautologie. Soient γ un environnement et σ une fonction de substitution. On a

$$\text{ev}(\sigma(F), \gamma) = \text{ev}(F, \gamma')$$

où $\gamma' = \sigma * \gamma$. Comme γ' est un environnement et F est une tautologie, $\text{ev}(F, \gamma') = 1$. Ainsi, $\sigma(F)$ est une tautologie. □

À partir d'une tautologie, on peut donc créer une infinité de tautologies en substituant des formules quelconques aux variables propositionnelles. Par exemple, si A est une variable propositionnelle, $(A \vee (\neg A))$ est une tautologie. Et donc, pour toute formule F , $(F \vee (\neg F))$ est une tautologie. Les exemples de tautologies que nous avons donné à la fin de la section précédente s'étendent ainsi en une infinité de tautologies.

2.2 Sous-formules

La discussion qui précède permet de substituer des formules aux variables d'une formule. Nous pouvons généraliser en définissant la notion de substitution d'une formule à une des sous-formules d'une formule.

Définissons par induction structurelle l'ensemble $\mathcal{S}(F)$ des sous-formules d'une formule F .

- Si $F = A$ est une variable propositionnelle, $\mathcal{S}(F) = \{A\}$.

- Si $F = (\neg G)$ où G est une formule, $\mathcal{S}(F) = \mathcal{S}(G) \cup \{F\}$.
- Si $F = (G \Rightarrow H)$ où G et H sont deux formules, $\mathcal{S}(F) = \mathcal{S}(G) \cup \mathcal{S}(H) \cup \{F\}$.

Nous pouvons à partir de là définir la notion de substitution d'une formule à une sous-formule.

Soient F, F_0, F_1 trois formules. Définissons la substitution $\sigma(F, F_1, F_0)$ de F_1 à F_0 dans F .

Si F_0 n'est pas une sous-formule de F , alors $\sigma(F, F_1, F_0) = F$.

Supposons que F_0 est une sous-formule de F . Si $F_0 = F$, alors $\sigma(F, F_1, F_0) = F_1$. Sinon, F n'est pas une variable propositionnelle. Deux cas se présentent.

- Si $F = (\neg G)$ où G est une formule, $\sigma(F, F_1, F_0) = (\neg \sigma(G, F_1, F_0))$.
- Si $F = (G \Rightarrow H)$ où G et H sont deux formules, $\sigma(F, F_1, F_0) = (\sigma(G, F_1, F_0) \Rightarrow \sigma(H, F_1, F_0))$.

3 Équivalence

3.1 Notion d'équivalence

Définition 3.3. Les formules F et G sont *équivalentes* si pour tout environnement γ , $\text{ev}(F, \gamma) = \text{ev}(G, \gamma)$. On note $F \equiv G$.

Clairement, la relation $\equiv$ est une relation d'équivalence sur l'ensemble $\mathcal{F}$ des formules.

Proposition 3.6. Les formules F et G sont équivalentes si et seulement si la formule $(F \Leftrightarrow G)$ est une tautologie.

Démonstration. Supposons F et G équivalentes. Soit γ un environnement. Soit $x = \text{ev}(F, \gamma) = \text{ev}(G, \gamma)$. On a

$$\text{ev}((F \Leftrightarrow G), \gamma) = \varphi_{\Leftrightarrow}(\text{ev}(F, \gamma), \text{ev}(G, \gamma)) = \varphi_{\Leftrightarrow}(x, x) = 1$$

Ainsi, $(F \Leftrightarrow G)$ est une tautologie.

Inversement, supposons que $(F \Leftrightarrow G)$ est une tautologie. Soit γ un environnement. On a

$$1 = \text{ev}((F \Leftrightarrow G), \gamma) = \varphi_{\Leftrightarrow}(\text{ev}(F, \gamma), \text{ev}(G, \gamma))$$

et donc $\text{ev}(F, \gamma) = \text{ev}(G, \gamma)$. Ainsi, $F \equiv G$. $\square$

Proposition 3.7. Soient F et G deux formules équivalentes. Pour toute fonction de substitution σ , on a $\sigma(F) \equiv \sigma(G)$.

Démonstration. On a

$$\models (F \Leftrightarrow G)$$

Par la proposition 5,

$$\models \sigma(F \Leftrightarrow G)$$

c'est à dire

$$\models (\sigma(F) \Leftrightarrow \sigma(G))$$

d'où $\sigma(F) \equiv \sigma(G)$. $\square$

Proposition 3.8. *Soit F une formule. Soient F_0, F_1 deux formules équivalentes. On a $\mathcal{S}(F, F_1, F_0) \equiv F$.*

Démonstration. Notons $F' = \mathcal{S}(F, F_1, F_0)$.

Si F_0 n'est pas une sous-formule de F , alors $F' = F$.

Si $F_0 = F$, alors $F' = F_1$ d'où le résultat puisque $F_0 \equiv F_1$.

Supposons dorénavant que F_0 est une sous-formule de F différente de F . Montrons le résultat par induction structurelle sur F .

- Cas 1, F est une variable propositionnelle. Le résultat est trivialement vrai, puisqu'une variable propositionnelle n'a pas de sous-formule stricte.
- Cas 2, $F = (\neg G)$ où G vérifie le résultat. La formule F_0 est une sous-formule de G , donc $G' \equiv G$. De plus, $F' = (\neg G')$, d'où le résultat.
- Cas 3, $F = (G \Rightarrow H)$ où G et H vérifient le résultat. On a $F' = (G' \Rightarrow H')$. Par l'hypothèse d'induction, $G' \equiv G$ et $H' \equiv H$. Pour tout environnement γ ,

$$\begin{aligned} \text{ev}(F, \gamma) &= \varphi_{\Rightarrow}(\text{ev}(G, \gamma), \text{ev}(H, \gamma)) \\ &= \varphi_{\Rightarrow}(\text{ev}(G', \gamma), \text{ev}(H', \gamma)) \\ &= \text{ev}(F', \gamma) \end{aligned}$$

Ainsi, $F' \equiv F$.

$\square$

Un corollaire immédiat est le suivant : si on remplace, dans une tautologie, une sous-formule par une formule équivalente, alors on a encore une tautologie.

Corollaire 3.9. *Soit F une formule. Soient F_0, F_1 deux formules équivalentes. Si F est une tautologie, alors $\mathcal{S}(F, F_1, F_0)$ est une tautologie.*

3.2 Une liste d'équivalences

La définition de l'équivalence nous dit que les formules F et G sont équivalentes si et seulement si elles ont la « même » table de vérité. Il est donc facile de prouver des équivalences. En voici quelques unes. Les lettres A, B et C désignent des variables propositionnelles mais, en vertu de la proposition 3.7, elles peuvent être remplacées par des formules quelconques.

- | | |
|--|---|
| 1. $(A \wedge B) \equiv (B \wedge A)$ | commutativité de $\wedge$ |
| 2. $((A \wedge B) \wedge C) \equiv (A \wedge (B \wedge C))$ | associativité de $\wedge$ |
| 3. $(A \wedge A) \equiv A$ | idempotence de $\wedge$ |
| 4. $(A \vee B) \equiv (B \vee A)$ | commutativité de $\vee$ |
| 5. $((A \vee B) \vee C) \equiv (A \vee (B \vee C))$ | associativité de $\vee$ |
| 6. $(A \vee A) \equiv A$ | idempotence de $\vee$ |
| 7. $(A \wedge (B \vee C)) \equiv ((A \wedge B) \vee (A \wedge C))$ | distributivité de $\wedge$ par rapport à $\vee$ |

- | | |
|---|---|
| 8. $(A \vee (B \wedge C)) \equiv ((A \vee B) \wedge (A \vee C))$ | distributivité de $\vee$ par rapport à $\wedge$ |
| 9. $(\neg(\neg A)) \equiv A$ | double négation |
| 10. $(\neg(A \wedge B)) \equiv ((\neg A) \vee (\neg B))$ | lois de Morgan (1) |
| 11. $(\neg(A \vee B)) \equiv ((\neg A) \wedge (\neg B))$ | lois de Morgan (2) |
| 12. $(\neg(A \Rightarrow B)) \equiv (A \wedge (\neg B))$ | négation d'une implication |
| 13. $(A \Rightarrow B) \equiv ((\neg B) \Rightarrow (\neg A))$ | contraposition |
| 14. $(A \Rightarrow B) \equiv ((\neg A) \vee B)$ | disjonction vs implication (1) |
| 15. $(A \vee B) \equiv ((\neg A) \Rightarrow B)$ | disjonction vs implication (2) |
| 16. $(A \Leftrightarrow B) \equiv ((A \Rightarrow B) \wedge (B \Rightarrow A))$ | équivalence logique |

Chapitre 4

Preuves

1 Notion de théorie formelle

1.1 Théories formelles

Une *théorie formelle* est un quadruplet $\mathcal{T} = (\mathcal{A}, \mathcal{F}, \mathcal{X}, \mathcal{I})$ où

- $\mathcal{A}$ est un alphabet.
- $\mathcal{F}$ est un sous-ensemble de l'ensemble $\mathcal{A}^*$ des expressions. Les éléments de $\mathcal{F}$ sont les *formules* de la théorie.
- $\mathcal{X}$ est un sous-ensemble de $\mathcal{F}$. Les éléments de $\mathcal{X}$ sont les *axiomes* de la théorie.
- $\mathcal{I} = \{R_1, \dots, R_n\}$ est un ensemble fini de relations entre les formules. Les éléments de l'ensemble $\mathcal{I}$ sont les *règles d'inférence* de la théorie.

Pour chaque règle d'inférence $R \in \mathcal{I}$, il existe un unique entier naturel $j \geq 1$ tel que $R \subseteq \mathcal{F}^{j+1}$. On fait l'hypothèse que pour toutes formules $F_1, \dots, F_j, F$, il existe une procédure effective permettant de décider si on a $R(F_1, \dots, F_j, F)$. Si c'est le cas, on dit que F est une *conséquence directe* de $F_1, \dots, F_j$ par la règle d'inférence R .

1.2 Théorèmes, preuves

Une *preuve* dans la théorie $\mathcal{T}$ est une suite finie de formules

$$\mathcal{P} = (F_1, \dots, F_n)$$

telle que, pour tout $i \in \llbracket 1, n \rrbracket$,

- F_i est un axiome, ou alors
- F_i est une conséquence directe de certaines formules parmi $F_1, \dots, F_{i-1}$ par une des règles d'induction de $\mathcal{T}$.

Un *théorème* de $\mathcal{T}$ est une formule F pour laquelle il existe une preuve $\mathcal{P} = (F_1, \dots, F_n)$ dans la théorie $\mathcal{T}$ telle que $F_n = F$. La preuve $\mathcal{P}$ est alors appelée une preuve de F .

Remarquons que pour tout $i \in \llbracket 1, n \rrbracket$, $(F_1, \dots, F_i)$ est une preuve de F_i . Chacune des formules F_i est donc un théorème. Remarquons également que pour tout axiome F , F est un théorème puisque le 1-uplet (F) est une preuve de F .

Notation. Lorsque F est un théorème de $\mathcal{T}$, nous noterons $\vdash_{\mathcal{T}} F$, ou plus simplement $\vdash F$ si la théorie mise en jeu est claire.

1.3 Conséquences d'un ensemble de formules

Soit Γ un ensemble de formules de la théorie $\mathcal{T}$. La formule F est une *conséquence* de Γ dans $\mathcal{T}$ lorsqu'il existe une suite finie de formules $(F_1, \dots, F_n)$ vérifiant

- $F_n = F$.
- Pour tout $i \in \llbracket 1, n \rrbracket$, F_i est un axiome, ou alors $F_i \in \Gamma$, ou alors F_i est une conséquence directe de certaines formules parmi $F_1, \dots, F_{i-1}$ par une des règles d'inférence de $\mathcal{S}$.

Une telle suite $(F_1, \dots, F_n)$ est une *preuve* de F à partir de Γ .

S'il existe une preuve de la formule F à partir de Γ , nous noterons

$$\Gamma \vdash_{\mathcal{T}} F$$

Si la théorie $\mathcal{T}$ est évidente par le contexte, nous noterons simplement $\Gamma \vdash F$. Remarquons que $\emptyset \vdash F$ si et seulement si $\vdash F$. Enfin, si $G_1, G_2, \dots$ sont des formules, nous

noterons

$$\Gamma, G_1, G_2, \dots \vdash F$$

au lieu de

$$\Gamma \cup \{G_1, G_2, \dots\} \vdash F$$

Proposition 4.1.

- Soient Γ et Δ deux ensembles de formules. Soit F une formule. Si $\Gamma \subseteq \Delta$ et $\Gamma \vdash F$, alors $\Delta \vdash F$.
- Soient Γ un ensemble de formules. Soit F une formule. $\Gamma \vdash F$ si et seulement si il existe un sous-ensemble fini Δ de Γ tel que $\Delta \vdash F$.
- Soient Γ et Δ deux ensembles de formules. Soit G une formule. Si $\Delta \vdash G$ et pour tout $F \in \Delta$, $\Gamma \vdash F$, alors $\Gamma \vdash G$.

Démonstration. Ce sont des conséquences immédiates de la notion de conséquence (si j'ose dire). $\square$

2 Une théorie formelle de la logique des propositions

2.1 La théorie

Il existe de nombreuses théorie formelles de la logique des propositions. Nous allons en étudier une en particulier. Nous la noterons $\mathcal{L}$.

Nous avons déjà défini dans les chapitres précédents l'alphabet $\mathcal{A}$ et l'ensemble des formules $\mathcal{F}$ de la logique des propositions. Nous allons ici restreindre l'alphabet à

$$\mathcal{A}' = \mathcal{A} \setminus \{\wedge, \vee, \Leftrightarrow\}$$

L'ensemble des formules de $\mathcal{L}$ est donc $\mathcal{F}' = \mathcal{F} \cap \mathcal{A}'^*$. Une formule de $\mathcal{F}'$ est une variable propositionnelle, ou alors $(\neg G)$ où G est une formule, ou alors $(G \Rightarrow H)$ où G et H sont deux formules.

Voici maintenant les axiomes de $\mathcal{L}$. Si F , G et H sont des formules, alors les trois formules ci-dessous sont des axiomes :

$$(A1) (F \Rightarrow (G \Rightarrow F))$$

$$(A2) ((F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H)))$$

$$(A3) (((\neg G) \Rightarrow (\neg F)) \Rightarrow (((\neg G) \Rightarrow F) \Rightarrow G))$$

(A1), (A2) et (A3) ne sont pas des axiomes mais des *schémas d'axiomes*. En prenant trois formules F , G et H arbitraires, on obtient un axiome. La théorie $\mathcal{L}$ possède donc une infinité d'axiomes.

Enfin, la théorie $\mathcal{L}$ ne possède qu'une seule règle d'inférence, le *modus ponens*. En notant MP cette règle, si F et G sont des formules, alors

$$\text{MP}(F, (F \Rightarrow G), G)$$

Dit autrement, G est une conséquence directe de F et $(F \Rightarrow G)$. De façon très abrégée, si Γ est un ensemble de formules, alors

$$\Gamma, F, (F \Rightarrow G) \vdash G$$

La théorie $\mathcal{L}$ est ainsi

$$\mathcal{L} = (\mathcal{A}', \mathcal{F}', \{A1, A2, A3 : F, G, H \in \mathcal{F}'\}, \{(F, (F \Rightarrow G), G) : F, G \in \mathcal{F}'\})$$

2.2 Abréviations

Nous introduisons les connecteurs $\wedge$, $\vee$ et $\Leftrightarrow$ comme des abréviations de formules.

(D1) $(F \wedge G)$ est une abréviation pour $(\neg(F \Rightarrow (\neg G)))$.

(D2) $(F \vee G)$ signifie $((\neg F) \Rightarrow G)$.

(D3) $(F \Leftrightarrow G)$ signifie $((F \Rightarrow G) \wedge (G \Rightarrow F))$.

Plus formellement, on définit par induction structurelle une fonction $F \mapsto F'$ de $\mathcal{F}$ vers $\mathcal{F}'$ en posant

- Pour toute variable propositionnelle A , $A' = A$.
- Pour toute formule $G \in \mathcal{F}$, $(\neg G)' = (\neg G')$.
- Pour toutes formules $G, H \in \mathcal{F}$,
 - $(F \Rightarrow G)' = (F' \Rightarrow G')$.
 - $(F \wedge G)' = (\neg(F' \Rightarrow (\neg G')))$.
 - $(F \vee G)' = ((\neg F') \Rightarrow G')$.
 - $(F \Leftrightarrow G)' = ((F' \Rightarrow G') \wedge (G' \Rightarrow F'))$.

2.3 Un premier théorème

La lettre F désigne une formule quelconque.

Proposition 4.2. $(T1) \vdash (F \Rightarrow F)$.

Démonstration. Comme il s'agit de notre première démonstration, nous allons entrer dans tous les détails.

1. On utilise le schéma d'axiomes (A2) avec F , $G = (F \Rightarrow F)$ et $H = F$. Ceci nous donne l'axiome

$$F_1 = ((F \Rightarrow ((F \Rightarrow F) \Rightarrow F)) \Rightarrow ((F \Rightarrow (F \Rightarrow F)) \Rightarrow (F \Rightarrow F)))$$

Remarquons que

$$F_1 = (U \Rightarrow V)$$

où

$$U = (F \Rightarrow ((F \Rightarrow F) \Rightarrow F))$$

et

$$V = ((F \Rightarrow (F \Rightarrow F)) \Rightarrow (F \Rightarrow F))$$

2. On utilise le schéma d'axiomes (A1) avec F et $G = (F \Rightarrow F)$. On obtient l'axiome

$$F_2 = (F \Rightarrow ((F \Rightarrow F) \Rightarrow F)) = U$$

3. On utilise la règle d'inférence MP sur F_1 et F_2 (avec les formules U et V) pour obtenir

$$F_3 = ((F \Rightarrow (F \Rightarrow F)) \Rightarrow (F \Rightarrow F))$$

Remarquons que

$$F_3 = (U' \Rightarrow V')$$

où

$$U' = (F \Rightarrow (F \Rightarrow F))$$

et

$$V' = (F \Rightarrow F)$$

4. Le schéma d'axiomes (A1) utilisé avec F et $G = F$ donne

$$F_4 = (F \Rightarrow (F \Rightarrow F)) = U'$$

5. On utilise la règle d'inférence MP sur F_3 et F_4 (avec les formules U' et V') pour obtenir

$$F_5 = (F \Rightarrow F)$$

Pour conclure, la suite $(F_1, F_2, F_3, F_4, F_5)$ est une démonstration de F_5 . $\square$

Remarque. Voici la même preuve, en abrégé. Dorénavant, nous présenterons les preuves comme ci-dessous.

- | | | |
|----|---|----------|
| 1. | $((F \Rightarrow ((F \Rightarrow F) \Rightarrow F)) \Rightarrow ((F \Rightarrow (F \Rightarrow F)) \Rightarrow (F \Rightarrow F)))$ | (A2) |
| 2. | $(F \Rightarrow ((F \Rightarrow F) \Rightarrow F))$ | (A1) |
| 3. | $((F \Rightarrow (F \Rightarrow F)) \Rightarrow (F \Rightarrow F))$ | 1, 2, MP |
| 4. | $(F \Rightarrow (F \Rightarrow F))$ | (A1) |
| 5. | $(F \Rightarrow F)$ | 3, 4, MP |

La preuve d'un théorème aussi « évident » nous a donné du mal. Il existe heureusement un (méta)théorème qui peut nous faire gagner beaucoup de temps : il s'agit du *théorème de déduction*.

2.4 Le théorème de déduction

Dans la pratique courante des mathématiques, pour montrer $(F \Rightarrow G)$ on suppose F et on déduit G . Le théorème de déduction nous dit que cette démarche est licite.

Proposition 4.3. *Soit Γ un ensemble de formules. Soient F et G deux formules. Si $\Gamma, F \vdash G$ alors $\Gamma \vdash (F \Rightarrow G)$.*

Démonstration. Soit $(G_1, \dots, G_n)$ une preuve de G à partir de Γ et F . Montrons par récurrence forte sur k que pour tout $k \in \llbracket 1, n \rrbracket$, $\Gamma \vdash (F \Rightarrow G_k)$. Ceci nous donnera le résultat, puisque $G_n = G$.

Remarquons que G_1 est un axiome, ou alors $G_1 \in \Gamma$, ou alors $G_1 = F$. Par le schéma d'axiomes (A1), $(G_1 \Rightarrow (F \Rightarrow G_1))$ est un axiome. Dans les deux premiers cas, on a donc, par MP, $\Gamma \vdash (F \Rightarrow G_1)$. Si $G_1 = F$ alors, par le théorème T1, $\vdash (F \Rightarrow G_1)$ d'où, a fortiori, $\Gamma \vdash (F \Rightarrow G_1)$.

Soit $k \in \llbracket 2, n \rrbracket$. Supposons que pour tout $j \in \llbracket 1, k-1 \rrbracket$, $\Gamma \vdash (F \Rightarrow G_j)$.

- Cas 1, G_k est un axiome ou $G_k \in \Gamma$ ou $G_k = F$. On procède comme dans le cas $k = 1$.

- Cas 2, G_k est une conséquence directe par MP de G_i et $G_j = (G_i \Rightarrow G_k)$, où $i, j \in \llbracket 1, k-1 \rrbracket$. Par l'hypothèse de récurrence,

$$1. \Gamma \vdash (F \Rightarrow G_i)$$

$$2. \Gamma \vdash (F \Rightarrow (G_i \Rightarrow G_k))$$

Par le schéma d'axiomes (A2),

$$3. \vdash ((F \Rightarrow (G_i \Rightarrow G_k)) \Rightarrow ((F \Rightarrow G_i) \Rightarrow (F \Rightarrow G_k)))$$

Par 2, 3 et MP,

$$4. \Gamma \vdash ((F \Rightarrow G_i) \Rightarrow (F \Rightarrow G_k))$$

Enfin, par 1, 4 et MP,

$$5. \Gamma \vdash (F \Rightarrow G_k)$$

□

Remarque. La réciproque du théorème de déduction est immédiate. En effet, supposons que $\Gamma \vdash (F \Rightarrow G)$. On a l'évidence $\Gamma, F \vdash F$ et aussi, par la proposition 4.1, $\Gamma, F \vdash (F \Rightarrow G)$. Par MP, $\Gamma, F \vdash G$. Dit de façon un peu rapide, le théorème de déduction est la réciproque du modus ponens.

Exemple. Soit F une formule. On a $F \vdash F$ donc, par le théorème de déduction, $\vdash (F \Rightarrow F)$. Plus formellement, en notant « Hyp » une hypothèse à gauche du symbole $\vdash$ et « Déd » l'utilisation du théorème de déduction,

- | | | |
|----|----------------------------|--------|
| 1. | F | Hyp |
| 2. | F | 1 |
| 3. | $F \vdash F$ | 1,2 |
| 4. | $\vdash (F \Rightarrow F)$ | 3, Déd |

Le seul problème est qu'en écrivant cette « preuve », nous avons triché. En effet, notre démonstration du théorème de déduction utilise T1. En fait T1 est le seul théorème du système formel $\mathcal{L}$ que nous ayons utilisé pour montrer le théorème de déduction. En d'autres termes, nous pouvons montrer tous les théorèmes de $\mathcal{L}$ à l'aide du théorème de déduction, *sauf* T1.

Voici deux exemples simples d'utilisation du théorème de déduction. Les lettres F , G et H désignent des formules.

Proposition 4.4. $(T2) (F \Rightarrow G), (G \Rightarrow H) \vdash (F \Rightarrow H)$

Démonstration.

- | | | |
|----|---|----------|
| 1. | $(F \Rightarrow G)$ | Hyp |
| 2. | $(G \Rightarrow H)$ | Hyp |
| 3. | F | Hyp |
| 4. | G | 1, 3, MP |
| 5. | H | 2, 4, MP |
| 6. | $(F \Rightarrow G), (G \Rightarrow H), F \vdash H$ | 1-5 |
| 7. | $(F \Rightarrow G), (G \Rightarrow H) \vdash (F \Rightarrow H)$ | 6, Déd |

□

Proposition 4.5. $(T3) (F \Rightarrow (G \Rightarrow H)), G \vdash (F \Rightarrow H)$

Démonstration.

- | | | |
|----|---|----------|
| 1. | $(F \Rightarrow (G \Rightarrow H))$ | Hyp |
| 2. | G | Hyp |
| 3. | F | Hyp |
| 4. | $(G \Rightarrow H)$ | 1, 3, MP |
| 5. | H | 2, 4, MP |
| 6. | $(F \Rightarrow (G \Rightarrow H)), G, F \vdash H$ | 1-5 |
| 7. | $(F \Rightarrow (G \Rightarrow H)), G \vdash (F \Rightarrow H)$ | 6, Déd |

□

3 Une liste de théorèmes

3.1 Quelques théorèmes de $\mathcal{L}$

En plus des théorèmes T1, T2 et T3, nous allons démontrer 7 autres théorèmes de la théorie $\mathcal{L}$, numérotés T4 à T10. Ces théorèmes nous seront utiles pour prouver le théorème central de ce chapitre, à savoir que toutes les théorèmes de $\mathcal{L}$ sont les tautologies. Le graphe de la page suivante montre les dépendances entre les théorèmes. Une flèche du théorème (ou de l'axiome) T vers le théorème T' indique que T est utilisé de façon *explicite* dans la preuve de T' . Il faut rajouter à ces dépendances le fait que certaines preuves utilisent le (méta)théorème de déduction D . En toute rigueur, ce n'est pas D qui est utilisé : ce sont les axiomes et théorèmes de $\mathcal{L}$ qui permettent de montrer D , à savoir (A1), (A2) et T1. La règle d'inférence MP sera utilisée explicitement dans toutes les démonstrations, sauf dans celle de T4.

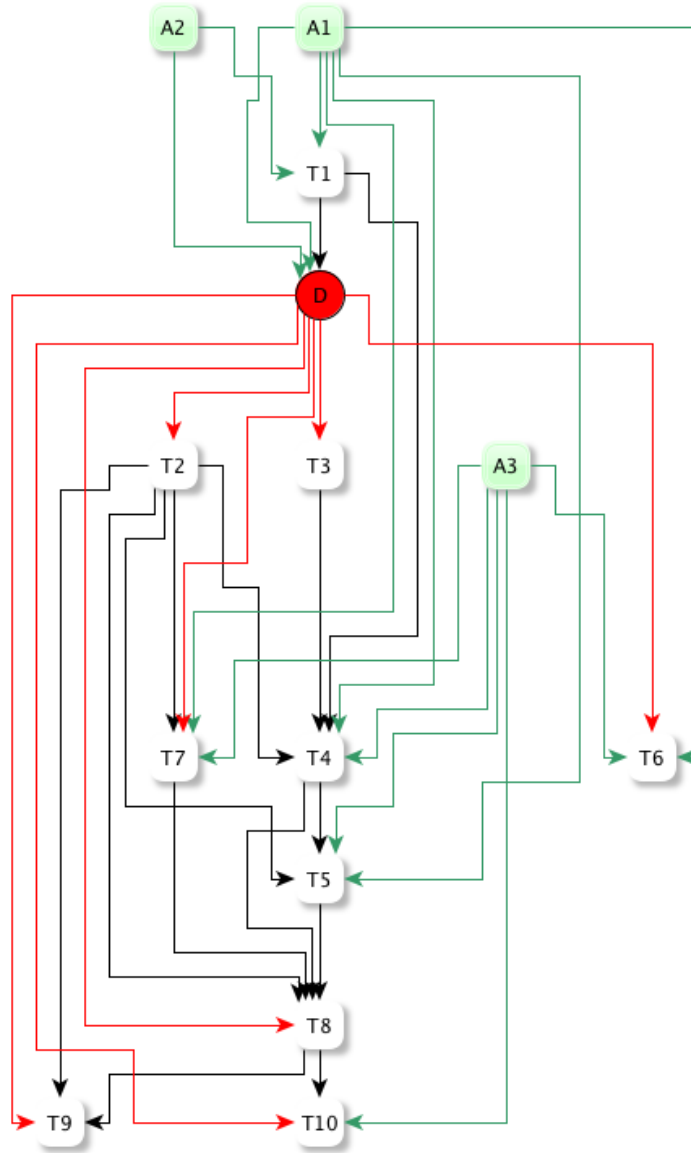


FIGURE 4.1 – Les relations entre les théorèmes T1 - T10

À partir de maintenant, pour alléger l'écriture des formules, nous allons faire un certain nombre de conventions. Nous n'écrivons pas les parenthèses les plus extérieures. Nous supposons également que le connecteur $\neg$ est prioritaire devant $\Rightarrow$, ce qui permet d'écrire toute formule du type $(\neg G)$ sous la forme $\neg G$. Avec ces conventions, les théorèmes T1, T2 et T3 s'écrivent

$$(T1) \vdash F \Rightarrow F$$

$$(T2) F \Rightarrow G, G \Rightarrow H \vdash F \Rightarrow H$$

$$(T3) F \Rightarrow (G \Rightarrow H), G \vdash F \Rightarrow H$$

Dans les résultats qui suivent, les lettres F et G désignent des formules quelconques.

Proposition 4.6. $(T4) \vdash \neg\neg F \Rightarrow F$

L'écriture complètement parenthésée de T4 est $\vdash ((\neg(\neg F)) \Rightarrow F)$.

Démonstration.

1. $(\neg F \Rightarrow \neg\neg F) \Rightarrow ((\neg F \Rightarrow \neg F) \Rightarrow F)$ (A3)
2. $\neg F \Rightarrow \neg F$ T1
3. $(\neg F \Rightarrow \neg\neg F) \Rightarrow F$ 1, 2, T3
4. $\neg\neg F \Rightarrow (\neg F \Rightarrow \neg\neg F)$ (A1)
5. $\neg\neg F \Rightarrow F$ 3, 4, T2

□

Faisons une remarque concernant cette preuve. La ligne 2 de la preuve *utilise* le théorème T1. De même, la ligne 3 utilise le théorème T3 et la ligne 5 utilise le théorème T2. Si nous voulions écrire une preuve complète de T4, il nous suffirait de recopier à la place les preuves de T1, T2 et T3. Nous ne ferons bien sûr jamais une chose pareille. Le principe même de l'écriture des démonstrations en mathématiques consiste à invoquer des théorèmes précédemment montrés.

Proposition 4.7. $(T5) \vdash F \Rightarrow \neg\neg F$

Démonstration.

1. $(\neg\neg\neg F \Rightarrow \neg F) \Rightarrow ((\neg\neg\neg F \Rightarrow F) \Rightarrow \neg\neg F)$ (A3)
2. $\neg\neg\neg F \Rightarrow \neg F$ T4
3. $(\neg\neg\neg F \Rightarrow F) \Rightarrow \neg\neg F$ 1, 2, MP
4. $F \Rightarrow (\neg\neg\neg F \Rightarrow F)$ (A1)
5. $F \Rightarrow \neg\neg F$ 3, 4, T2

□

Proposition 4.8. $(T6) \vdash \neg F \Rightarrow (F \Rightarrow G)$

Démonstration.

1. $\neg F$ Hyp
2. F Hyp
3. $F \Rightarrow (\neg G \Rightarrow F)$ (A1)
4. $\neg F \Rightarrow (\neg G \Rightarrow \neg F)$ (A1)
5. $\neg G \Rightarrow F$ 2, 3, MP
6. $\neg G \Rightarrow \neg F$ 1, 4, MP
7. $(\neg G \Rightarrow \neg F) \Rightarrow ((\neg G \Rightarrow F) \Rightarrow F)$ (A3)
8. $(\neg G \Rightarrow F) \Rightarrow G$ 6, 7, MP
9. G 5, 8, MP
10. $\neg F, F \vdash G$ 1-9
11. $\neg F \vdash F \Rightarrow G$ 10, Déd
12. $\vdash \neg F \Rightarrow (F \Rightarrow G)$ 11, Déd

□

Proposition 4.9. $(T7) \vdash (\neg G \Rightarrow \neg F) \Rightarrow (F \Rightarrow G)$

Démonstration.

- | | | |
|----|--|----------|
| 1. | $\neg G \Rightarrow \neg F$ | Hyp |
| 2. | $(\neg G \Rightarrow \neg F) \Rightarrow ((\neg G \Rightarrow F) \Rightarrow G)$ | (A3) |
| 3. | $F \Rightarrow (\neg G \Rightarrow F)$ | (A1) |
| 4. | $(\neg G \Rightarrow F) \Rightarrow G$ | 1, 2, MP |
| 5. | $F \Rightarrow G$ | 3, 4, T2 |
| 6. | $\neg G \Rightarrow \neg F \vdash F \Rightarrow G$ | 1-5 |
| 7. | $\vdash (\neg G \Rightarrow \neg F) \Rightarrow (F \Rightarrow G)$ | 6, Déd |

□

Proposition 4.10. $(T8) \vdash (F \Rightarrow G) \Rightarrow (\neg G \Rightarrow \neg F)$

Démonstration.

- | | | |
|----|---|----------|
| 1. | $F \Rightarrow G$ | Hyp |
| 2. | $\neg\neg F \Rightarrow F$ | T4 |
| 3. | $\neg\neg F \Rightarrow G$ | 1, 2, T2 |
| 4. | $G \Rightarrow \neg\neg G$ | T5 |
| 5. | $\neg\neg F \Rightarrow \neg\neg G$ | 3, 4, T2 |
| 6. | $(\neg\neg F \Rightarrow \neg\neg G) \Rightarrow (\neg G \Rightarrow \neg F)$ | T7 |
| 7. | $\neg G \Rightarrow \neg F$ | 5, 6, MP |
| 8. | $F \Rightarrow G \vdash \neg G \Rightarrow \neg F$ | 1-7 |
| 9. | $\vdash (F \Rightarrow G) \Rightarrow (\neg G \Rightarrow \neg F)$ | 8, Déd |

□

Proposition 4.11. $(T9) \vdash F \Rightarrow (\neg G \Rightarrow \neg(F \Rightarrow G))$

Démonstration.

- | | | |
|----|---|----------|
| 1. | $F, F \Rightarrow G \vdash G$ | MP |
| 2. | $F \vdash (F \Rightarrow G) \Rightarrow G$ | 1, Déd |
| 3. | $\vdash F \Rightarrow ((F \Rightarrow G) \Rightarrow G)$ | 2, Déd |
| 4. | $\vdash ((F \Rightarrow G) \Rightarrow G) \Rightarrow (\neg G \Rightarrow \neg(F \Rightarrow G))$ | 3, T8 |
| 5. | $\vdash F \Rightarrow (\neg G \Rightarrow \neg(F \Rightarrow G))$ | 2, 4, T2 |

□

Proposition 4.12. $(T10) \vdash (F \Rightarrow G) \Rightarrow ((\neg F \Rightarrow G) \Rightarrow G)$

Démonstration.

1.	$F \Rightarrow G$	Hyp
2.	$\neg F \Rightarrow G$	Hyp
3.	$(F \Rightarrow G) \Rightarrow (\neg G \Rightarrow \neg F)$	T8
4.	$\neg G \Rightarrow \neg F$	1, 3, MP
5.	$(\neg F \Rightarrow G) \Rightarrow (\neg G \Rightarrow \neg\neg F)$	T8
6.	$\neg G \Rightarrow \neg\neg F$	2, 5, MP
7.	$(\neg G \Rightarrow \neg\neg F) \Rightarrow ((\neg G \Rightarrow \neg F) \Rightarrow G)$	(A3)
8.	$(\neg G \Rightarrow \neg F) \Rightarrow G$	6, 7, MP
9.	G	4, 8, MP
10.	$F \Rightarrow G, \neg F \Rightarrow G \vdash G$	1-9
11.	$F \Rightarrow G \vdash (\neg F \Rightarrow G) \Rightarrow G$	10, Déd
12.	$\vdash (F \Rightarrow G) \Rightarrow ((\neg F \Rightarrow G) \Rightarrow G)$	11, Déd

□

3.2 Bilan

Voici les abréviations, les trois schémas d'axiomes et les théorèmes T1 à T10. Les lettres F , G et H désignent des formules quelconques.

(D1)	$(F \wedge G) = (\neg(F \Rightarrow (\neg G)))$
(D2)	$(F \vee G) = ((\neg F) \Rightarrow G)$
(D3)	$(F \Leftrightarrow G) = ((F \Rightarrow G) \wedge (G \Rightarrow F))$
(A1)	$\vdash (F \Rightarrow (G \Rightarrow F))$
(A2)	$\vdash ((F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H)))$
(A3)	$\vdash (((\neg G) \Rightarrow (\neg F)) \Rightarrow (((\neg G) \Rightarrow F) \Rightarrow G))$
(T1)	$\vdash F \Rightarrow F$
(T2)	$F \Rightarrow G, G \Rightarrow H \vdash F \Rightarrow H$
(T3)	$F \Rightarrow (G \Rightarrow H), G \vdash F \Rightarrow H$
(T4)	$\vdash \neg\neg F \Rightarrow F$
(T5)	$\vdash F \Rightarrow \neg\neg F$
(T6)	$\vdash \neg F \Rightarrow (F \Rightarrow G)$
(T7)	$\vdash (\neg G \Rightarrow \neg F) \Rightarrow (F \Rightarrow G)$
(T8)	$\vdash (F \Rightarrow G) \Rightarrow (\neg G \Rightarrow \neg F)$
(T9)	$\vdash F \Rightarrow (\neg G \Rightarrow \neg(F \Rightarrow G))$
(T10)	$\vdash (F \Rightarrow G) \Rightarrow ((\neg F \Rightarrow G) \Rightarrow G)$

3.3 Quelques théorèmes

Dans ce qui suit, F et G sont des formules. Nous allons montrer quelques théorèmes faisant intervenir les raccourcis $\vee$ et $\wedge$.

Proposition 4.13. $(T11) \vdash F \Rightarrow (F \vee G)$

Démonstration. Il s'agit de montrer que $\vdash F \Rightarrow (\neg F \Rightarrow G)$.

1. F Hyp
2. $\neg F$ Hyp
3. $\neg F \Rightarrow (F \Rightarrow G)$ T6
4. $F \Rightarrow G$ 2, 3, MP
5. G 1, 5, MP
6. $\neg F \Rightarrow G$ 2, 5, Déd
7. $F \Rightarrow (\neg F \Rightarrow G)$ 1, 6, Déd

□

Proposition 4.14. $(T12) \vdash F \Rightarrow (G \vee F)$

Démonstration. Il s'agit de montrer que $\vdash F \Rightarrow (\neg G \Rightarrow F)$. Mais ceci est une instance du schéma (A1). □

Proposition 4.15. $(T13) \vdash (F \vee G) \Rightarrow (G \vee F)$

Démonstration. Il s'agit de prouver $(\neg F \Rightarrow G) \Rightarrow (\neg G \Rightarrow F)$. □

Démonstration.

1. $\neg F \Rightarrow G$ Hyp
2. $(\neg F \Rightarrow G) \Rightarrow (\neg G \Rightarrow \neg\neg F)$ T8
3. $\neg G \Rightarrow \neg\neg F$ 1, 2, MP
4. $\neg\neg F \Rightarrow F$ T4
5. $\neg G \Rightarrow F$ 3, 4, T2
6. $(\neg F \Rightarrow G) \Rightarrow (\neg G \Rightarrow F)$ 1-5, Déd

□

Proposition 4.16. $(T14) \vdash (F \wedge G) \Rightarrow F$

Démonstration. Il s'agit de montrer $\vdash \neg(F \Rightarrow \neg G) \Rightarrow F$.

1. $\neg(F \Rightarrow \neg G)$ Hyp
2. $\neg F \Rightarrow (\neg\neg F \Rightarrow \neg G)$ T11
3. $\neg\neg F \Rightarrow \neg G$ Hyp
4. $F \Rightarrow \neg\neg F$ T5
5. $F \Rightarrow \neg G$ 3, 4, T2
6. $(\neg\neg F \Rightarrow \neg G) \Rightarrow (F \Rightarrow \neg G)$ 3-5, Déd
7. $\neg F \Rightarrow (F \Rightarrow \neg G)$ 2, 6, T2
8. $\neg(F \Rightarrow \neg G) \Rightarrow \neg\neg F$ 7, T8
9. $\neg\neg F \Rightarrow F$ T4
10. $\neg(F \Rightarrow \neg G) \Rightarrow F$ 8, 9, T2

□

Proposition 4.17. $(T15) \vdash (F \wedge G) \Rightarrow G$

Démonstration. Il s'agit de montrer $\vdash \neg(F \Rightarrow \neg G) \Rightarrow G$.

1. $\neg G \Rightarrow (F \Rightarrow \neg G)$ (A1)
2. $\neg(F \Rightarrow \neg G) \Rightarrow \neg\neg G$ 1, T8
3. $\neg\neg G \Rightarrow G$ T4
4. $\neg(F \Rightarrow \neg G) \Rightarrow G$ 2, 3, T2

□

Proposition 4.18. $(T16) \vdash (F \Rightarrow H) \Rightarrow ((G \Rightarrow H) \Rightarrow ((F \vee G) \Rightarrow H))$

Démonstration.

Rappelons, ligne 3 ci-dessous, que $(F \vee G) = (\neg F \Rightarrow G)$.

1. $F \Rightarrow H$ Hyp
2. $G \Rightarrow H$ Hyp
3. $\neg F \Rightarrow G$ Hyp
4. $\neg F \Rightarrow H$ T2
5. $(F \Rightarrow H) \Rightarrow ((\neg F \Rightarrow H) \Rightarrow H)$ T10
6. $(\neg F \Rightarrow H) \Rightarrow H$ 1, 5, MP
7. H 4, 6, MP
8. $F \Rightarrow H, G \Rightarrow H, F \vee G \vdash H$ 1-7
9. $F \Rightarrow H, G \Rightarrow H \vdash (F \vee G) \Rightarrow H$ 8, Déd
10. $F \Rightarrow H \vdash (G \Rightarrow H) \Rightarrow ((F \vee G) \Rightarrow H)$ 9, Déd
11. $\vdash (F \Rightarrow H) \Rightarrow ((G \Rightarrow H) \Rightarrow ((F \vee G) \Rightarrow H))$ 10, Déd

□

Proposition 4.19. $(T17) F \Rightarrow (G \Rightarrow (F \wedge G))$

Démonstration. Il s'agit de montrer $F \Rightarrow (G \Rightarrow \neg(F \Rightarrow \neg G))$. □

Démonstration.

1. F Hyp
2. G Hyp
3. $F \Rightarrow \neg G$ Hyp
4. $\neg G$ 1, 3, MP
5. $(F \Rightarrow \neg G) \Rightarrow \neg G$ 3, 4, Déd
6. $G \Rightarrow \neg(F \Rightarrow \neg G)$ 5, T8, T4, T2
7. $F \Rightarrow (G \Rightarrow \neg(F \Rightarrow \neg G))$ 1, 6, Déd

À la ligne 6, nous avons abrégé plusieurs étapes de la preuve. □

Pour résumer,

(T11)	$\vdash F \Rightarrow (F \vee G)$
(T12)	$\vdash F \Rightarrow (G \vee F)$
(T13)	$\vdash (F \vee G) \Rightarrow (G \vee F)$
(T14)	$\vdash (F \wedge G) \Rightarrow F$
(T15)	$\vdash (F \wedge G) \Rightarrow G$
(T16)	$\vdash (F \Rightarrow H) \Rightarrow ((G \Rightarrow H) \Rightarrow ((F \vee G) \Rightarrow H))$
(T17)	$F \Rightarrow (G \Rightarrow (F \wedge G))$

Tous les théorèmes de $\mathcal{L}$ que nous avons démontré nous sont familiers : il s'agit de tautologies. Nous allons voir dans la section suivante que les théorèmes de $\mathcal{L}$ sont *les* tautologies. Une fois cette caractérisation établie, nous aurons une méthode « mécanique » pour décider si une formule est un théorème, ou n'en est pas un.

4 La complétude de $\mathcal{L}$

4.1 Consistance

Commençons par une propriété facile.

Proposition 4.20. *Tous les théorèmes de $\mathcal{L}$ sont des tautologies.*

Dit autrement, pour toute formule F , si $\vdash F$ alors $\models F$.

Démonstration. Soit $(F_1, \dots, F_n)$ une preuve de F . Montrons par récurrence forte sur k que pour tout $k \in \llbracket 1, n \rrbracket$, $\models F_k$.

Remarquons que F_1 est un axiome. On vérifie facilement (table de vérité, par exemple) que les axiomes sont des tautologies.

Soit $k \in \llbracket 2, n \rrbracket$. Supposons que pour tout $j \in \llbracket 1, k-1 \rrbracket$, $\models F_j$.

- Cas 1, F_k est un axiome. On procède comme pour $k = 1$.
- Cas 2, F_k est une conséquence directe par MP de F_i et $F_j = (F_i \Rightarrow F_k)$, où $i, j \in \llbracket 1, k-1 \rrbracket$. Par l'hypothèse de récurrence, $\models F_i$ et $\models (F_i \Rightarrow F_k)$. Pour tout environnement γ ,

$$1 = \text{ev}(F_i, \gamma) \leq \text{ev}(F_k, \gamma)$$

et donc

$$\text{ev}(F_k, \gamma) = 1$$

Ainsi, $\models F_k$.

□

Corollaire 4.21. *Le système formel $\mathcal{L}$ est consistant : il n'existe pas de formule F telle que $\vdash F$ et $\vdash \neg F$.*

Démonstration. Soit F une formule. Supposons $\vdash F$ et $\vdash \neg F$. Alors, F et $\neg F$ sont des tautologies, contradiction. □

Nous allons consacrer le reste de cette section à la preuve de la réciproque : toutes les tautologies sont des théorèmes de $\mathcal{L}$. Le système formel $\mathcal{L}$ est *complet*.

4.2 Complétude

Les preuves des propositions qui vont suivre utilisent les théorèmes T5, T6, T9 et T10. Comme la preuve de ces théorèmes utilise T1, T2, T3, T4, T7 et T8, nos 10 théorèmes seront nécessaires.

Pour toute formule F , notons $V(F)$ l'ensemble des variables propositionnelles qui interviennent dans F .

Proposition 4.22. *Soit F une formule. Pour tout environnement γ et toute variable propositionnelle $A \in V(F)$, posons $A' = A$ si $\gamma(A) = 1$ et $A' = \neg A$ si $\gamma(A) = 0$. Soit $F' = F$ si $\text{ev}(F, \gamma) = 1$ et $F' = \neg F$ si $\text{ev}(F, \gamma) = 0$. Alors,*

$$\{A' : A \in V(F)\} \vdash F'$$

Démonstration. Montrons le résultat par récurrence forte sur la hauteur n de la formule F .

Si $n = 0$, alors $F = A$ est une variable propositionnelle. Le résultat nous dit (évidence) que $A \vdash A$ et $\neg A \vdash \neg A$.

Soit $n \geq 1$. Supposons le résultat vérifié pour toutes les formules de hauteur strictement inférieure à n . Soit F une formule de hauteur n . Deux cas se présentent.

- Cas 1, $F = (\neg G)$ où G est une formule de hauteur $n - 1$. Remarquons que $V(F) = V(G)$. Soit γ un environnement.
- Cas 1.1, $\text{ev}(G, \gamma) = 1$. On a alors $\text{ev}(F, \gamma) = 0$. On a donc $G' = G$ et $F' = \neg F$. Par l'hypothèse de récurrence,

$$\{A' : A \in V(G)\} \vdash G$$

Par le théorème T5, $\vdash G \Rightarrow \neg \neg G$. De là, par MP,

$$\{A' : A \in V(G)\} \vdash \neg \neg G$$

Il reste à remarquer que $\neg \neg G = \neg F = F'$.

- Cas 1.2, $\text{ev}(G, \gamma) = 0$. On a alors $\text{ev}(F, \gamma) = 1$. On a donc $G' = \neg G$ et $F' = F$. Par l'hypothèse de récurrence,

$$\{A' : A \in V(G)\} \vdash G'$$

Il reste à remarquer que $G' = F$.

- Cas 2, $F = (G \Rightarrow H)$ où G et H sont des formules de hauteur inférieure ou égale à $n - 1$. On a $V(F) = V(G) \cup V(H)$. Soit γ un environnement. Par l'hypothèse de récurrence,

$$\{A' : A \in V(G)\} \vdash G' \quad \text{et} \quad \{A' : A \in V(H)\} \vdash H'$$

A fortiori,

$$\{A' : A \in V(F)\} \vdash G' \quad \text{et} \quad \{A' : A \in V(F)\} \vdash H'$$

- Cas 2.1, $\text{ev}(G, \gamma) = 0$. On a alors $\text{ev}(F, \gamma) = 1$. De là, $G' = \neg G$ et $F' = F$. Par le théorème T6,

$$\vdash \neg G \Rightarrow (G \Rightarrow H)$$

De là, par MP,

$$\{A' : A \in V(F)\} \vdash G \Rightarrow H$$

Or, $G \Rightarrow H = F$.

- Cas 2.2, $\text{ev}(H, \gamma) = 1$. On a alors $\text{ev}(F, \gamma) = 1$. De là, $H' = H$ et $F' = F$. On a donc

$$\{A' : A \in V(F)\} \vdash H$$

Par l'axiome (A1),

$$\vdash H \Rightarrow (G \Rightarrow H)$$

De là, par MP,

$$\{A' : A \in V(F)\} \vdash G \Rightarrow H$$

Or, $(G \Rightarrow H) = F'$.

- Cas 2.3, $\text{ev}(G, \gamma) = 1$ et $\text{ev}(H, \gamma) = 0$. On a alors $\text{ev}(F, \gamma) = 0$. De là, $G' = G$, $H' = \neg H$ et $F' = \neg F$. On a donc

$$\{A' : A \in V(F)\} \vdash G \quad \text{et} \quad \{A' : A \in V(F)\} \vdash \neg H$$

Par le théorème T9,

$$\vdash G \Rightarrow (\neg H \Rightarrow \neg(G \Rightarrow H))$$

De là, par MP,

$$\{A' : A \in V(F)\} \vdash \neg(G \Rightarrow H)$$

Or, $\neg(G \Rightarrow H) = F'$.

□

Proposition 4.23. *Pour toute formule F , si $\models F$ alors $\vdash F$.*

Démonstration. Soit F une tautologie. Remarquons que pour tout environnement γ , $\text{ev}(F, \gamma) = 1$ et donc, avec les notations de la proposition précédente, $F' = F$.

Soient $A_1, \dots, A_n$ les variables propositionnelles qui apparaissent dans F . Montrons par récurrence descendante sur k que pour tout $k \in \llbracket 0, n \rrbracket$,

$$A'_1, \dots, A'_k \vdash F$$

où $A'_i = A_i$ ou $\neg A_i$.

Par la proposition précédente, le résultat est vrai pour $k = n$. Soit $k \in \llbracket 1, n \rrbracket$. Supposons la propriété vérifiée pour k .

Prenons $A'_k = A_k$ pour obtenir

$$A'_1, \dots, A'_{k-1}, A_k \vdash F$$

Par le théorème de déduction,

$$A'_1, \dots, A'_{k-1} \vdash A_k \Rightarrow F$$

Prenons maintenant $A'_k = \neg A_k$ pour obtenir

$$A'_1, \dots, A'_{k-1}, \neg A_k \vdash F$$

Par le théorème de déduction,

$$A'_1, \dots, A'_{k-1} \vdash \neg A_k \Rightarrow F$$

Par le théorème T10,

$$\vdash (A_k \Rightarrow F) \Rightarrow ((\neg A_k \Rightarrow F) \Rightarrow F)$$

De là, par MP,

$$A'_1, \dots, A'_{k-1} \vdash F$$

La propriété est donc vérifiée pour $k - 1$.

Pour terminer la preuve, en prenant $k = 0$, on obtient $\vdash F$. $\square$

Corollaire 4.24. *Soit G une formule de $\mathcal{F}$ (c'est à dire contenant les symboles $\neg$, $\Rightarrow$ et aussi, éventuellement, $\Leftrightarrow$, $\wedge$ et $\vee$). Soit F la formule correspondante de $\mathcal{F}'$. La formule G est une tautologie si et seulement si la formule F est un théorème.*

Démonstration. Dans les définitions (D1), (D2) et (D3), les abréviations remplacent des formules par des formules équivalentes. De là, G et F sont équivalentes. Ainsi, G est une tautologie si et seulement si F est une tautologie, et donc si et seulement si F est un théorème. $\square$

4.3 Un exemple

Soit F une tautologie. La démonstration du théorème de complétude est suffisamment constructive pour pouvoir nous fournir une preuve de F dans le système formel $\mathcal{L}$. Supposons par exemple que les variables de F sont A et B . La proposition 4.22 nous dit que si $A' = A$ ou $\neg A$ et $B' = B$ ou $\neg B$, alors $A', B' \vdash F$. On a donc

- | | | |
|----|---|-----------|
| 1. | $A', B \vdash F$ | prop 4.22 |
| 2. | $A' \vdash B \Rightarrow F$ | 1, Déd |
| 3. | $A', \neg B \vdash F$ | prop 4.22 |
| 4. | $A' \vdash \neg B \Rightarrow F$ | 3, Déd |
| 5. | $\vdash (B \Rightarrow F) \Rightarrow ((\neg B \Rightarrow F) \Rightarrow F)$ | T10 |
| 6. | $A' \vdash (\neg B \Rightarrow F) \Rightarrow F$ | 2, 5, MP |
| 7. | $A' \vdash F$ | 4, 6, MP |

Les 7 lignes ci-dessus sont en fait deux démonstrations. Une pour $A' = A$, une pour $A' = \neg A$. Notons les numéros de ces deux preuves par des « prime » et des « seconde ». On peut ensuite recommencer pour éliminer A' :

- | | | |
|-----|---|------------|
| 8. | $A \vdash F$ | 7' |
| 9. | $\vdash A \Rightarrow F$ | 8, Déd |
| 10. | $\neg A \vdash F$ | 7'' |
| 11. | $\vdash \neg A \Rightarrow F$ | 10, Déd |
| 12. | $\vdash (A \Rightarrow F) \Rightarrow ((\neg A \Rightarrow F) \Rightarrow F)$ | T10 |
| 13. | $\vdash (\neg A \Rightarrow F) \Rightarrow F$ | 9, 12, MP |
| 14. | $\vdash F$ | 11, 13, MP |

Évidemment, il s'agirait maintenant de développer les preuves de 1', 1'', 3' et 3''. Ces preuves feraient intervenir d'autres preuves portant sur les sous formules de F . On aura compris que bien que nous *puissions* construire une preuve explicite de F en lisant pas à pas la démonstration du théorème de complétude, cette preuve sera de longueur exponentielle en le nombre de variables propositionnelles de F .

5 Indépendance

5.1 Logiques multivaluées

Rappelons qu'un environnement est une application $\gamma : \mathcal{V} \longrightarrow \{0, 1\}$. Généralisons cette notion. Généralisons en définissant un environnement comme une application $\gamma : \mathcal{V} \longrightarrow \mathbb{B}$ où $\mathbb{B}$ est un ensemble quelconque. Si $\mathbb{B} = \{0, 1\}$, on retrouve la notion usuelle. Supposons donnée, pour chaque connecteur α , une fonction « booléenne » φ_α . On a $\varphi_{\neg} : \mathbb{B} \longrightarrow \mathbb{B}$ et, pour tout connecteur binaire α , $\varphi_\alpha : \mathbb{B}^2 \longrightarrow \mathbb{B}$. On prolonge alors sans difficulté la notion d'évaluation d'une formule dans un environnement. Cette fois, pour toute formule F et tout environnement γ , $\text{ev}(F, \gamma) \in \mathbb{B}$.

Soit $D \subseteq \mathbb{B}$. L'ensemble D est l'ensemble des *valeurs désignées*.

Définition 4.1. La formule F est *exceptionnelle* lorsque pour tout environnement γ , $\text{ev}(F, \gamma) \in D$.

Par exemple, en prenant $\mathbb{B} = \{0, 1\}$ et $D = \{1\}$, les formules exceptionnelles sont les tautologies.

5.2 Notion d'indépendance

Nous avons montré que les schémas d'axiomes (A1), (A2) et (A3) *suffisent* pour prouver toutes les tautologies. Une question se pose : sont-ils *nécessaires* ? Par exemple, peut-on prouver une instance du schéma (A1) en utilisant les axiomes de (A2) et (A3) ? Nous allons voir que c'est impossible.

Définition 4.2. Soit X un ensemble d'axiomes de la théorie $\mathcal{L}$. L'ensemble X est *indépendant* s'il existe $F \in X$ qui ne peut pas être prouvée à partir des axiomes qui n'appartiennent pas à X (et du modus ponens).

5.3 L'indépendance des schémas d'axiomes de $\mathcal{L}$

Proposition 4.25. Le schéma (A1) est indépendant.

Démonstration. Soit $\mathbb{B} = \{0, 1, 2\}$. Prenons les fonctions booléennes suivantes.

x	$\varphi_{\neg}(x)$	x	y	$\varphi_{\Rightarrow}(x, y)$
0	1	0	0	0
1	1	1	0	2
2	0	2	0	0
		0	1	2
		1	1	2
		2	1	0
		0	2	2
		1	2	0
		2	0	2

Choisissons $D = \{0\}$ pour l'ensemble des valeurs désignées. On vérifie facilement les propriétés suivantes :

- Si F et $F \Rightarrow G$ sont des formules exceptionnelles, alors G est une formule exceptionnelle. Le modus ponens préserve donc la notion de formule exceptionnelle.
- Toutes les instances du schéma d'axiomes (A2) sont des formules exceptionnelles.
- Toutes les instances du schéma d'axiomes (A3) sont des formules exceptionnelles.

En revanche, si $\text{ev}(F, \gamma) = 1$ et $\text{ev}(G, \gamma) = 2$, alors $\text{ev}(F \Rightarrow (G \Rightarrow F), \gamma) = 2$. Donc il existe des instances de (A1) qui ne sont pas des formules exceptionnelles.

En conséquence, il existe une instance de (A1) qui n'est pas démontrable à l'aide de (A2), (A3) et du modus ponens. $\square$

Proposition 4.26. *Le schéma (A2) est indépendant.*

Démonstration. Soit $\mathbb{B} = \{0, 1, 2\}$. Prenons les fonctions booléennes suivantes.

x	$\varphi_{\neg}(x)$	x	y	$\varphi_{\Rightarrow}(x, y)$
0	1	0	0	0
1	0	1	0	0
2	1	2	0	0
		0	1	2
		1	1	2
		2	1	0
		0	2	1
		1	2	0
		2	0	0

Choisissons $D = \{0\}$ pour l'ensemble des valeurs désignées. On vérifie facilement les propriétés suivantes :

- Le modus ponens préserve la notion de formule exceptionnelle.
- Toutes les instances du schéma d'axiomes (A1) sont des formules exceptionnelles.
- Toutes les instances du schéma d'axiomes (A3) sont des formules exceptionnelles.

En revanche, si $\text{ev}(F, \gamma) = 0$, $\text{ev}(G, \gamma) = 0$ et $\text{ev}(H, \gamma) = 1$, alors

$$\text{ev}((F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H)), \gamma) = 2$$

Donc il existe des instances de (A2) qui ne sont pas des formules exceptionnelles.

En conséquence, il existe une instance de (A2) qui n'est pas démontrable à l'aide de (A1), (A3) et du modus ponens. $\square$

Proposition 4.27. *Le schéma (A3) est indépendant.*

Démonstration. Soit $\mathbb{B} = \{0, 1\}$. Prenons les fonctions booléennes suivantes.

x	$\varphi_{\neg}(x)$	x	y	$\varphi_{\Rightarrow}(x, y)$
0	0	0	0	1
1	0	1	0	0
		0	1	1
		1	1	1

Choisissons $D = \{1\}$ pour l'ensemble des valeurs désignées. La fonction booléenne $\varphi_{\Rightarrow}$ est la fonction usuelle associée au connecteur $\Rightarrow$. La fonction $\varphi_{\neg}$ est en revanche constante, égale à 0. Les schémas d'axiomes (A1) et (A2) ne faisant pas intervenir $\neg$, pour toute formule F qui est une instance de l'un de ces axiomes et pour tout environnement γ , on a $\text{ev}(F, \gamma) = 1$. Également, si $\text{ev}(F, \gamma) = 1$ et $\text{ev}(F \Rightarrow G, \gamma) = 1$, alors $\text{ev}(G, \gamma) = 1$.

En revanche, si $\text{ev}(G, \gamma) = 0$, alors

$$\text{ev}(((\neg G \Rightarrow \neg F) \Rightarrow ((\neg G \Rightarrow F) \Rightarrow G)), \gamma) = 0$$

Donc il existe des instances de (A3) qui ne sont pas des formules exceptionnelles.

En conséquence, il existe une instance de (A3) qui n'est pas démontrable à l'aide de (A1), (A2) et du modus ponens. $\square$

