UPMC, 2I005
Béatrice Bérard

Année 2015–2016
Aide mémoire

**Structures discrètes : logique**

# Table des matières

**1 Fonctions booléennes** **2**
1.1 Algèbre de Boole . . . . . 2
1.2 Fonctions booléennes . . . . . 2
1.3 Formes normales . . . . . 3

**2 Calcul propositionnel** **4**
2.1 Syntaxe . . . . . 4
2.2 Sémantique . . . . . 4
2.3 Equivalence sémantique . . . . . 6
2.4 Conséquence sémantique . . . . . 6
2.5 Conséquence logique (ou déduction) . . . . . 8

**3 Logique du premier ordre** **9**
3.1 Syntaxe . . . . . 9
3.2 Variables libres et liées . . . . . 10
3.3 Sémantique . . . . . 11
3.4 Propriétés sémantiques . . . . . 13

# 1 Fonctions booléennes

## 1.1 Algèbre de Boole

**Définition 1** (Algèbre de Boole)**.** *Une algèbre de Boole est un tuple*

*Le projet* ***"Interface graphique pour la Logique en L3"*** *consiste à développer un outil dynamique et robuste pour améliorer l'enseignement de la logique en Licence 3. Ce projet nous a été soumis dans le cadre de L'UE PSAR du master 1 Informatique spécialité SAR. Il est sous la responsabilité de Mr Fabrice Kordon suivit par Mme Béatrice Berard,Mr Mathieu Jaume et Mme Bénédicte Legastelois.* $\mathcal{B} = (E, \perp, \top, \vee, \wedge, ^{-})$ *où* $E$ *est un ensemble,* $\perp$ *et* $\top$ *sont deux éléments distincts de* $E$*,* $\vee$ *et* $\wedge$ *sont deux opérations binaires,* $^{-}$ *est une opération unaire, satisfaisant les propriétés suivantes :*

— Associativité *: pour tous* $a, b, c \in E$*,* $(a \vee b) \vee c = a \vee (b \vee c)$ *et* $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
— Commutativité *: pour tous* $a, b \in E$*,* $a \vee b = b \vee a$ *et* $a \wedge b = b \wedge a$
— Distributivité *d'une loi par rapport à l'autre : pour tous* $a, b, c \in E$*,*
$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$ *et* $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$
— Absorption *: pour tous* $a, b \in E$*,* $a \wedge (a \vee b) = a$ *et* $a \vee (a \wedge b) = a$
— Idempotence *: pour tout* $a \in E$*,* $a \vee a = a$ *et* $a \wedge a = a$
— Bornes *: pour tout* $a \in E$*,* $a \wedge \perp = \perp$*,* $a \vee \perp = a$ *et* $a \wedge \top = a$*,* $a \vee \top = \top$
— Complémentarité *: pour tout* $a \in E$*,* $a \wedge \bar{a} = \perp$ *et* $a \vee \bar{a} = \top$

**Exemples.**

1. Soit $E = \mathcal{P}(A)$ pour un ensemble $A$ non vide. On définit alors une algèbre de Boole avec :

| $\perp$ | $\top$ | $\vee$ | $\wedge$ | $^{-}$ |
|---|---|---|---|---|
| $\emptyset$ | A | $\cup$ | $\cap$ | complémentaire |

2. Soit $\mathbb{B} = \{0, 1\}$. On définit alors une algèbre de Boole avec :

| $\perp$ | $\top$ | $\vee$ | $\wedge$ | $^{-}$ |
|---|---|---|---|---|
| 0 (faux) | 1 (vrai) | ou (disjonction) | et (conjonction) | négation |

Pour les calculs dans $\mathbb{B}$, on note généralement $+$ pour $\vee$ et . ou rien pour $\wedge$.

## 1.2 Fonctions booléennes

**Définition 2** (Fonction booléenne)**.** *Soit* $n \in \mathbb{N}$*. Une fonction booléenne à* $n$ *arguments est une application* $f\colon \mathbb{B}^n \longrightarrow \mathbb{B}$*.*

**Remarque.** Si $n = 0$, il y a deux fonctions constantes : 0, 1.
Si $n = 1$, il y a quatre fonctions : $x \to 0$, $x \to 1$, $x \to x$ et $x \to \bar{x}$.
Il y a $2^{2^n}$ fonctions booléennes à $n$ arguments.

**Exemple.** Table de vérité de la fonction $NAND$ (à deux arguments), définie par : $NAND(x, y) = \overline{x.y}$.

| $x$ | $y$ | $NAND(x, y)$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

**Théorème 3.** *Toute fonction booléenne $f$ à $n$ arguments, ($n \geqslant 1$), s'écrit comme combinaison de ses arguments ou de leurs complémentaires avec somme et produit.*

**Exemple.** $NAND(x,\, y) = \bar{x} \cdot \bar{y} + \bar{x} \cdot y + x \cdot \bar{y}$

Ce théorème se démontre par récurrence sur $n$, en utilisant le lemme suivant :

**Lemme 4.** *Soit $f$ une fonction booléenne à $n$ arguments.*
*Alors $f(x_1,\, \ldots,\, x_n) = x_1 f(1,\, x_2,\, \ldots,\, x_n) + \overline{x_1} f(0,\, x_2,\, \ldots,\, x_n)$*

*Démonstration.* Posons $g(x_1,\, \ldots,\, x_n) = x_1 f(1,\, x_2,\, \ldots,\, x_n) + \overline{x_1} f(0,\, x_2,\, \ldots,\, x_n)$ et montrons que $f = g$, c'est-à-dire que pour tout $n$-uplet $(x_1,\, \ldots,\, x_n)$, $g(x_1,\, \ldots,\, x_n) = f(x_1,\, \ldots,\, x_n)$.

— Si $x_1 = 1$, $g(x_1,\, \ldots,\, x_n) = f(1,\, x_2,\, \ldots,\, x_n) = f(x_1,\, \ldots,\, x_n)$
— Si $x_1 = 0$, $g(x_1,\, \ldots,\, x_n) = f(0,\, x_2,\, \ldots,\, x_n) = f(x_1,\, \ldots,\, x_n)$

Donc $f = g$. □

## 1.3 Formes normales

Pour une fonction booléenne $f$ à $n$ arguments, on note $b = (b_1,\, \ldots,\, b_n)$ un élément de $\mathbb{B}^n$ et $\mathcal{D}_f = \{b \in \mathbb{B}^n / f(b) = 1\}$.

**Définition 5** (Formes disjonctives et conjonctives)**.**

— *Une fonction est sous forme normale disjonctive (FND) si elle s'écrit comme une somme de produits de $x_i$ ou $\overline{x_i}$.*
— *Une fonction est sous forme normale conjonctive (FNC) si elle s'écrit comme produit de sommes de $x_i$ ou $\overline{x_i}$.*

Pour une fonction booléenne $f$ à $n$ arguments, une forme normale disjonctive pour $f$ est obtenue par :

$$f(x_1,\, \ldots,\, x_n) = \sum_{b \in \mathcal{D}_f} M_b(x_1,\, \ldots,\, x_n) \text{ où } \begin{array}{r} M_b(x_1,\, \ldots,\, x_n) = x'_1 \cdot \cdots \cdot x'_n \\ \text{avec } x'_i = \begin{cases} x_i & \text{si } b_i = 1 \\ \overline{x_i} & \text{si } b_i = 0 \end{cases} \end{array}$$

**Exemple.** Pour la fonction $NAND$, on a : $NAND(x,\, y) = \underbrace{\bar{x} \cdot \bar{y}}_{M_{(0,\,0)}(x,y)} + \underbrace{\bar{x} \cdot y}_{M_{(0,\,1)}(x,y)} + \underbrace{x \cdot \bar{y}}_{M_{(1,\,0)}(x,y)}$

Soit $f$ une fonction booléenne à $n$ arguments, une forme normale conjonctive pour $f$ est obtenue par :

$$f(x_1,\,\ldots,\,x_n) = \prod_{b \notin \mathcal{D}_f} S_b(x_1,\,\ldots,\,x_n) \text{ où } \quad S_b(x_1,\,\ldots,\,x_n) = x'_1 + \cdots + x'_n$$
$$\text{avec } x'_i = \begin{cases} x_i & \text{si } b_i = 0 \\ \overline{x_i} & \text{si } b_i = 1 \end{cases}$$

**Exemple.** Pour la fonction $NAND$, on a : $NAND(x,\,y) = \underbrace{\bar{x} + \bar{y}}_{S_{(1,\,1)}(x,y)}$

# 2 Calcul propositionnel

## 2.1 Syntaxe

**Définition 6.** *Soit $\mathcal{P}$ un ensemble de symboles propositionnels (ou variables propositionnelles). Les formules du calcul propositionnel sont définies inductivement par :*

*(B) Si $p \in \mathcal{P}$, alors $p$ est une formule.*

*(I) Si $F$ est une formule, alors $\neg F$ est une formule,*
*si $F_1$ et $F_2$ sont deux formules, alors $(F_1 \vee F_2)$ et $(F_1 \wedge F_2)$ sont aussi des formules.*

**Exemple 1.** $F = ((q \wedge r) \vee \neg p))$ est une formule utilisant les symboles $p$, $q$ et $r$.

**Définition 7.** *On définit deux nouvelles opérations $\rightarrow$ et $\leftrightarrow$ par :*

— $F_1 \rightarrow F_2 = F_2 \vee \neg F_1$

— $F_1 \leftrightarrow F_2 = (F_1 \rightarrow F_2) \wedge (F_2 \rightarrow F_1)$

**Exemple 2.** $G = (p \rightarrow (p \rightarrow q))$ est une formule utilisant les deux symboles $p$ et $q$.

**Remarque 1.** Le symbole $\supset$ est parfois utilisé au lieu de $\rightarrow$ pour l'implication et parfois aussi $\equiv$ au lieu de $\leftrightarrow$.

**Remarque 2.** Les formules du calcul propositionnel peuvent être vues comme les termes construits avec $F_0 = \mathcal{P}$, $F_1 = \{\neg\}$ et $F_2 = \{\vee, \wedge, \rightarrow, \leftrightarrow\}$, avec une notation infixe pour les opérateurs binaires, c'est-à-dire par exemple $p \vee q$ au lieu de $\vee(p, q)$.

**Exemple 3.** $F = \neg p \wedge ((q \vee r) \rightarrow s)$ est une formule sur le sous-ensemble $\{p,\,q,\,r,\,s\}$ de $\mathcal{P}$, qui peut être représentée (comme un terme) par un arbre.

## 2.2 Sémantique : interprétation des formules

**Exemple.** On reprend l'exemple ci-dessus. En associant des valeurs dans $\mathbb{B} = \{0,\,1\}$ aux propositions $p$, $q$, $r$ et $s$, on peut obtenir une valeur (également dans $\mathbb{B}$) pour la formule $F$, et plus généralement pour toute formule portant sur des propositions de $\{p,\,q,\,r,\,s\}$. Par exemple, l'interprétation $p \mapsto 0,\ q \mapsto 0,\ r \mapsto 1,\ s \mapsto 1$ produit la valeur 1 pour $F$.

Dans le cas général, une interprétation est une application $I\colon \mathcal{P} \longrightarrow \mathbb{B}$. A partir d'une telle application, qui associe à chaque proposition de $\mathcal{P}$ une valeur dans $\mathbb{B} = \{0,\,1\}$, il est possible de déduire une interprétation de toutes les formules de CP.

**Définition 8.** *Soit* $I\colon \mathcal{P} \longrightarrow \{0,\, 1\}$ *une interprétation des symboles de* $\mathcal{P}$*. Le prolongement de* $I$ *aux formules du calcul propositionnel est l'application encore notée* $I$ *(au lieu de* $I^*$*) de* $CP \longrightarrow \{0,\, 1\}$ *définie inductivement par :*

*(B) Si* $F = p$*, alors* $I(F) = I(p)$*.*

*(I) Si* $F = \neg G$*, alors* $I(F) = \overline{I(G)}$*,*

*si* $F = F_1 \vee F_2$ *alors* $I(F) = I(F_1) + I(F_2)$

*et si* $F = F_1 \wedge F_2$ *alors* $I(F) = I(F_1)I(F_2)$*.*

Ceci correspond bien à interpréter les symboles d'opérations de la façon usuelle : $\neg$ comme la négation, $\wedge$ comme la conjonction et $\vee$ comme la disjonction.

**Proposition 9.** *Soit* $I$ *une interprétation. Alors :*

1. $I(F_1 \to F_2) = I(F_2) + \overline{I(F_1)}$
2. $I(F_1 \leftrightarrow F_2) = I(F_1).I(F_2) + \overline{I(F_1)}.\overline{I(F_2)}$

*Démonstration.* Montrons le premier point de la proposition précédente, le point 2. est laissé en exercice.

$$\begin{array}{rcl} I(F_1 \to F_2) & = & I(F_2 \vee \neg F_1) \text{ par définition de } F_1 \to F_2 \\ & = & I(F_2) + I(\neg F_1) \text{ par définition de } I(X \vee Y) \\ & = & I(F_2) + \overline{I(F_1)} \text{ par définition de } I(\neg X) \\ \text{donc } I(F_1 \vee F_2) & = & I(F_2) + \overline{I(F_1)} \end{array}$$

□

**Exemple.** Soit $F = \neg p \wedge ((q \vee r) \to s)$

$$\begin{array}{rcl} I(F) & = & \overline{I(p)}.I((q \vee r) \to s) \\ & = & \overline{I(p)}.(\overline{I(q \vee r)} + I(s)) \\ & = & \overline{I(p)}.(\overline{I(q) + I(r)} + I(s)) \\ I(F) & = & \overline{I(p)}.(\overline{I(q)}.\overline{I(r)} + I(s)) \text{ d'après les lois de De Morgan} \end{array}$$

On retrouve le fait que si $I(p) = 0,\ I(r) = 1,\ I(q) = 0$ et $I(s) = 1$, alors $I(F) = 1$.

**Définition 10.** *Soit* $F$ *une formule.*

— $F$ *est valide (ou une tautologie) si pour toute interprétation* $I$*,* $I(F) = 1$*.*
— $F$ *est satisfaisable s'il existe une interprétation* $I$ *telle que* $I(F) = 1$*.*
— $F$ *est non satisfaisable si pour toute interprétation* $I$*,* $I(F) = 0$*.*

**Remarque 1.** Lorsqu'une interprétation $I$ est telle que $I(F) = 1$, on note parfois $I \vDash F$ qui se lit : « $I$ satisfait $F$ » ou « $F$ est vraie pour $I$ ».
**Remarque 2.** Une formule $F$ est non satisfaisable si et seulement si $\neg F$ est valide.
**Exemple.** Pour le problème de Kerstin, Pollet et Anne, on considère la formule : $F = A \wedge B \wedge C$ (en omettant les parenthèses puisque l'interprétation de $\wedge$ est associative), avec

$A = p \to (q \wedge r)$, $B = \neg p \to q$ et $C = \neg p \to r$. Donc pour toute interprétation $I$, on a : $I(A) = I(q)I(r) + \overline{I(p)}$, $I(B) = I(q) + I(p)$ et $I(C) = I(r) + I(p)$. Le problème posé revient à chercher les interprétations $I$ pour lesquelles $F$ est vraie, c'est-à-dire $I(F) = 1$.
En posant $x = I(p)$, $y = I(q)$, $z = I(r)$, on obtient $I(F) = (yz + \overline{x})(x + y)(x + z)$, on retrouve donc la fonction booléenne : $f(x, y, z) = (yz + \overline{x})(x + y)(x + z)$, pour laquelle on avait vu que $f(x, y, z) = yz$. Donc $I(F) = 1$ si et seulement si l'interprétation $I$ est telle que $y = I(q) = 1$ et $z = I(r) = 1$. Ainsi, on en déduit que Anne et Pollet iront à la conférence mais qu'on ne sait pas pour Kerstin.

## 2.3 Equivalence sémantique

**Définition 11.** *Deux formules $F$ et $G$ sont équivalentes, noté $F \sim G$, si pour toute interprétation $I$, on a : $I(F) = I(G)$.*

**Remarque 1.** La relation $\sim$ sur l'ensemble $CP$ des formules du calcul propositionnel est une relation d'équivalence.
**Exemples.** Les formules $p$ et $\neg(\neg p)$ sont équivalentes, et en général :
- $F \sim \neg(\neg F)$
- $F \vee G \sim G \vee F$ (car + est commutatif dans $\mathbb{B}$)
- $\neg(F \vee G) \sim (\neg F \wedge \neg G)$

**Remarque 2.** On obtient des propriétés similaires à l'associativité, l'idempotence, l'absorption, la distributivité, etc. mais avec $\sim$ au lieu de l'égalité. Ainsi, l'ensemble quotient $CP/\sim$ est une algèbre de Boole.

**Remarque 3.** Sur $\mathcal{P} = \{p_1, \ldots, p_n\}$, une interprétation $I \colon \mathcal{P} \longrightarrow \mathbb{B}$ peut être identifiée au $n$-uplet de ses valeurs $I = (I(p_1), \ldots, I(p_n)) \in \mathbb{B}^n$. On peut donc associer à toute formule $F$ sur $\mathcal{P}$ une fonction booléenne $g_F \colon \mathbb{B}^n \longrightarrow \mathbb{B}$ définie par $g_F(I) = I(F)$. Ainsi :

**Proposition 12.** *L'ensemble des fonctions booléennes est en bijection avec l'ensemble $CP/\sim$ (qui contient les formules du calcul propositionnel à équivalence près).*

**Exemple.** Soit $f \colon \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x, y) & \longrightarrow & \overline{x + y} \end{array}$
La formule $F$ de $CP$ qui lui est associée est $\neg(p \vee q)$ sur $\{p, q\}$.
Cette correspondance permet d'associer à toute formule $F$ une formule $F'$ sous forme normale conjonctive (FNC) et une formule $F''$ sous forme normale disjonctive (FND), qui sont équivalentes à $F$.

## 2.4 Conséquence sémantique

**Définition 13.** *Pour deux formules $F$ et $G$, on dit que $G$ est conséquence de $F$, ou que $F$ satisfait $G$, noté $F \models G$ si pour toute interprétation $I$, si $I(F) = 1$, alors $I(G) = 1$.*

**Proposition 14.** *$F$ satisfait $G$ ssi $(F \to G)$ est valide.*

*Démonstration.* Montrons l'équivalence des négations, c'est-à-dire : $F$ ne satisfait pas $G$ ssi $(F \to G)$ n'est pas valide.

• Si $F$ ne satisfait pas $G$, alors, par définition, il existe une interprétation $I$ telle que $I(F) = 1$ et $I(G) = 0$. Pour cette interprétation $I$, on a $I(F \to G) = \overline{I(F)} + I(G) = 0$, donc $(F \to G)$ n'est pas valide.

• Réciproquement, si $(F \to G)$ n'est pas valide, alors il existe une interprétation $I$ telle que $I(F \to G) = 0$, avec $I(F \to G) = \overline{I(F)} + I(G)$. Pour que la somme soit nulle, il faut que $I(F) = 1$ et $I(G) = 0$, donc $F$ ne satisfait pas $G$.
Conclusion : $F$ satisfait $G$ ssi $(F \to G)$ est valide. □

**Proposition 15.** *$F$ est équivalente à $G$ ssi $F \leftrightarrow G$ est valide.*

La démonstration reprend le schéma précédent, elle est laissée en exercice. On peut aussi vérifier que $F \sim G$ ssi $F \models G$ et $G \models F$ et utiliser la proposition précédente.

On étend les définitions de la conséquence sémantique $\models$ à des ensembles de formules.

**Définition 16.** *Soit $\mathcal{F} = \{F_1, \ldots, F_n\}$ un ensemble fini de formules et $G$ une formule.*

— *On dit que $\mathcal{F}$ est satisfaisable s'il existe une interprétation $I$ telle que pour toute formule $F \in \mathcal{F}$, on ait $I(F) = 1$. Donc $\mathcal{F}$ est satisfaisable si la formule $\bigwedge_{i=1}^{n} F_i$ est satisfaisable.*

— *On note $\mathcal{F} \models G$ si $\bigwedge_{i=1}^{n} F_i \models G$, c'est-à-dire : pour toute interprétation $I$, si pour toute formule $F \in \mathcal{F}$, $I(F) = 1$, alors $I(G) = 1$.*

**Exemple.** Montrer que $\mathcal{H} = \{p, p \to q, \neg q\}$ n'est pas satisfaisable.

**Définition 17.** *Un séquent est une paire $(\mathcal{F}, G)$ où $\mathcal{F}$ est un ensemble de formules et $G$ une formule. Le séquent $(\mathcal{F}, G)$ est valide si $\mathcal{F} \models G$.*

**Exemple.** Soient $\mathcal{F} = \{p, p \to q\}$ et $G = q$, on vérifie que $(\mathcal{F}, G)$ est un séquent valide.

Montrons que pour toute interprétation $I$, si pour toute $F \in \mathcal{F}$, $I(F) = 1$, alors $I(G) = 1$. Ceci revient à montrer $(p) \wedge (p \to q) \models q$.

Supposons $I(p) = I(p \to q) = 1$. Or $I(p \to q) = \overline{I(p)} + I(q) = 1$. Mais comme $I(p) = 1$, on a $\overline{I(p)} = 0$ et $I(q) = 1$. Ainsi, $(\mathcal{F}, G)$ est un séquent valide.

**Remarque.** Soit $\mathcal{F}'$ l'ensemble obtenu en remplaçant dans $\mathcal{F}$ un des $F_i$ par $F_i'$ tel que $F_i \sim F_i'$. Alors :
- $\mathcal{F}$ est satisfaisable ssi $\mathcal{F}'$ est satisfaisable et
- $(\mathcal{F}, G)$ est valide ssi $(\mathcal{F}', G)$ est valide.

**Proposition 18.** *Soit $\mathcal{H}$ un ensemble de formules, et $F$, $G$ deux formules. On a les équivalences suivantes :*

1. *$\mathcal{H} \models G$ ssi $\mathcal{H} \cup \{\neg G\}$ est non satisfaisable.*
2. *$\mathcal{H} \cup \{F\} \models G$ ssi $\mathcal{H} \models (F \to G)$*

*Démonstration.* 1. On démontre l'équivalence des négations.

— Supposons $\mathcal{H} \cup \{\neg G\}$ satisfaisable.
Alors il existe une interprétation $I$ telle que $I(F) = 1$ pour toute formule $F$ de $\mathcal{H}$ et $I(\neg G) = 1$, donc $I(G) = 0$.
Donc on n'a pas $\mathcal{H} \models G$.

— Réciproquement, supposons que $\mathcal{H} \models G$ est faux. Alors il existe une interprétation $I$ telle que $I(F) = 1$ pour toute $F$ de $\mathcal{H}$ et $I(G) = 0$.
Alors $I(\neg G) = 1$ donc $I$ satisfait $\mathcal{H} \cup \{\neg G\}$.

2. Montrons cette proposition à l'aide d'équivalences.

$$\begin{array}{rll} \mathcal{H} \cup \{F\} \models G & \text{ssi} & \mathcal{H} \cup \{F, \neg G\} \text{ non satisfaisable d'après (1.)} \\ & \text{ssi} & \mathcal{H} \cup \{\neg(F \to G)\} \text{ non satisfaisable} \\ & \text{ssi} & \mathcal{H} \models (F \to G) \text{ encore par (1.)} \end{array}$$

□

## 2.5 Conséquence logique (ou déduction)

**Définition 19.** *Un séquent $(\mathcal{F}, G)$ est dit prouvable, noté $\mathcal{F} \vdash G$, s'il est obtenu après un nombre fini d'applications des six règles suivantes, où $\mathcal{H}$ est un ensemble de formules, $F$ et $G$ des formules :*

*(a) Utilisation d'une hypothèse : si $F \in \mathcal{H}$, alors $\mathcal{H} \vdash F$*

*(b) Augmentation d'hypothèse : si $G \notin \mathcal{H}$ et $\mathcal{H} \vdash F$, alors $\mathcal{H} \cup \{G\} \vdash F$*

*(c) Modus ponens : si $\mathcal{H} \vdash (F \to G)$ et $\mathcal{H} \vdash F$, alors $\mathcal{H} \vdash G$*

*(d) Retrait d'hypothèse (synthèse) : si $\mathcal{H} \cup \{F\} \vdash G$, alors $\mathcal{H} \vdash (F \to G)$*

*(e) Double négation : $\mathcal{H} \vdash F$ ssi $\mathcal{H} \vdash \neg\neg F$*

*(f) Absurde : si $\mathcal{H} \cup \{F\} \vdash G$ et $\mathcal{H} \cup \{F\} \vdash \neg G$, alors $\mathcal{H} \vdash \neg F$*

**Exemple.** Preuve de la démonstration par contraposée :
On veut prouver : $p \to q \vdash (\neg q \to \neg p)$

1. $\{p \to q, \neg q, p\} \vdash p$ d'après a)
2. $\{p \to q, \neg q, p\} \vdash \neg q$ d'après a)
3. $\{p \to q, \neg q, p\} \vdash p \to q$ d'après a)
4. $\{p \to q, \neg q, p\} \vdash q$ d'après c) appliquée à 1 et 3
5. $\{p \to q, \neg q\} \vdash \neg p$ d'après f) sur 2 et 4
6. $\{p \to q\} \vdash (\neg q \to \neg p)$ d'après d)

**Théorème 20.** *Un séquent $(\mathcal{F}, G)$ est valide ssi il est prouvable.*

**Remarque.** Signification des deux sens de l'équivalence :
— Sens $\Rightarrow$ : Complétude - *Ce qui est vrai peut être prouvé.*

— Sens $\Leftarrow$ : Correction/adéquation : *Ce qui peut être prouvé est vrai.*

*Principe de la démonstration de correction.* Par induction sur la longueur de la preuve. A partir d'un séquent valide, en appliquant une des six règles a), ..., f) on obtient un nouveau séquent valide.

Par exemple avec la règle a) :
On suppose que $\mathcal{F} \vdash G$ a été obtenu par la règle a), donc : $G \in \mathcal{F}$. Si $I$ est une interprétation telle que $I(F) = 1$ pour toute formule $F$ de $\mathcal{F}$, alors $I(G) = 1$ puisque $G \in \mathcal{F}$, donc $\mathcal{F} \models G$ et le séquent est valide. $\square$

# 3 Logique du premier ordre

La logique du premier ordre enrichit le calcul propositionnel en utilisant :
- des termes construits avec des variables et des fonctions,
- des formules construites à partir de relations sur les termes, avec des opérateurs booléens et des quantifications sur les variables.

Par exemple $F : \forall x \exists y R(x, y)$ est une formule de la logique du 1er ordre. Dans cette formule, $x$ et $y$ sont des variables et $R(x, y)$ est une formule atomique construite en utilisant une relation binaire $R$.
- Si $F$ est interprétée sur les entiers naturels, avec pour $R$ la relation $<$, on obtient : *Pour tout entier $x$, il existe un entier $y$ strictement plus grand que $x$*, ce qui exprime que l'ensemble des entiers naturels n'a pas d'élément maximal.
- Si $F$ est interprétée sur l'ensemble des personnes avec pour $R$ la relation défnie par $R(x, y)$ si $y$ est la mère de $x$, la formule exprime que *toute personne a une mère.*
- Si $F$ est interprétée dans les mondes de Tarski, avec pour $R$ la relation $LeftOf$, elle exprime que tout objet est à gauche d'un autre objet.

## 3.1 Syntaxe

On considère un ensemble $\mathcal{G}$ de symboles de fonctions et un ensemble $\mathcal{R}$ de symboles de relations. En particulier, on notera :
- $\mathcal{C} = \mathcal{G}_0$ l'ensemble des symboles de fonctions sans argument, c'est-à-dire les constantes,
- $\mathcal{P} = \mathcal{R}_0$ l'ensemble des symboles de relations d'arité nulle, c'est-à-dire les propositions (du calcul propositionnel), qui seront interprétées dans $\mathbb{B} = \{0, 1\}$.

On considère aussi un ensemble $X$ de variables et on définit les termes et les formules de la logique du premier ordre associés à $\mathcal{G} \cup \mathcal{R} \cup X$.

**Définition 21** (Termes avec variables). *L'ensemble $T(\mathcal{G}, X)$ des termes est défini inductivement par :*

*(B) toute constante de $\mathcal{C}$ est un terme et toute variable de $X$ est un terme,*

*(I) si $f \in \mathcal{G}$ a $n$ arguments et si $t_1, \ldots, t_n$ sont des termes, alors $f(t_1, \ldots, t_n)$ est un terme.*

**Définition 22** (Formules)**.** *Les formules de la logique du premier ordre sur $\mathcal{G}$ et $\mathcal{R}$ sont définies inductivement par :*

*(B) si $R \in \mathcal{R}$ a $n$ arguments et si $t_1, \ldots, t_n$ sont des termes, alors $R(t_1, \ldots, t_n)$ est une formule dite* atomique*,*

*(I) si $F$ et $G$ sont des formules alors $\neg F$, $(F \wedge G)$, $(F \vee G)$, $(F \to G)$ sont des formules, Si $x$ une variable alors $\forall x F$ et $\exists x F$ sont des formules.*

Par exemple, dans la formule $\forall x \forall y (R(f(x,y), a) \to (R(x,a) \wedge R(y,a)))$, on trouve les termes $a$ (constante), $x$, $y$ (variables) et $f(x,y)$, pour une fonction $f$ à deux arguments, ainsi qu'une relation binaire $R$. On pourra par la suite interpréter cette formule dans $\mathbb{N}$, avec l'addition pour $f$, l'égalité pour $R$, et la valeur 0 pour $a$.

**Remarque 1.** Les formules du calcul propositionnel sont des cas particuliers de cet ensemble.

**Remarque 2.** Les formules peuvent être représentées par des arbres.

## 3.2 Variables libres et liées

**Définition 23** (Variables d'un terme ou d'une formule)**.**

1. *Les variables d'un terme sont définies inductivement par :*
   - $Var(x) = \{x\}$ *si* $x \in X$ *et* $Var(c) = \emptyset$ *si* $c \in \mathcal{C}$,
   - $Var(f(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} Var(t_i)$ *pour un terme* $f(t_1, \ldots, t_n)$.
2. *Les variables d'une formule sont définies inductivement par :*
   - $Var(R(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} Var(t_i)$ *pour une formule atomique,*
   - *si $F$ et $G$ sont des formules, $x$ est une variable et $* \in \{\wedge, \vee, \to\}$, alors :* $Var(\neg F) = Var(F)$, $Var(F * G) = Var(F) \cup Var(G)$, $Var(\exists x F) = Var(\forall x F) = Var(F) \cup \{x\}$.

**Remarque.** Les variables et les constantes n'ayant pas d'argument, elles n'ont pas de descendant et sont toujours en position de feuilles dans l'arbre associé à une formule.

**Définition 24** (Variables libres et liées)**.**

- *Dans l'arbre d'une formule $F$, une feuille d'étiquette $x \in X$ est une occurrence* libre *de $x$ s'il n'y a aucun quantificateur $\forall x$ ou $\exists x$ dans les ascendants de cette feuille. Sinon, l'occurrence est dite* liée.
- *Une variable est* libre *dans une formule $F$ si elle a* ***au moins*** *une occurrence libre dans cette formule. Elle est* liée *dans une formule si elle n'est pas libre dans cette formule.*

On note $L(F)$ l'ensemble des variables libres dans $F$ et $B(F) = Var(F) \setminus L(F)$ l'ensemble des variables liées dans $F$ ($B$ pour *bound* en anglais).

Par exemple, dans la formule $F$ ci-dessus, en considérant les feuilles de gauche à droite, l'occurrence de $x$ est libre, l'occurrence de $z$ est liée, puis les deux occurrences de $y$ sont liées tandis que les deux occurrences de $z$ sont libres.
Par conséquent, $L(F) = \{x, z\}$ et $B(F) = \{y\}$

**Définition 25** (Formule close)**.** *Une formule est dite* close *si elle n'a aucune variable libre.*

**Proposition 26.** *Les variables libres d'une formule sont définies inductivement par :*
*(B)* $L(R(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} Var(t_i)$
*(I) Pour $F$ et $G$ deux formules,*
— $L(\neg F) = L(F)$ *et* $L(F \star G) = L(F) \cup L(G)$ *pour* $\star \in \{\wedge, \vee, \rightarrow\}$
— $L(\forall x F) = L(\exists x F) = L(F) \setminus \{x\}$

## 3.3 Sémantique

Pour interpréter les formules, on va considérer une structure $\mathcal{M}$, donnée par :
— un domaine $D$,
— pour toute fonction $f$ de $\mathcal{G}$ à $n$ arguments, une fonction $f_D \colon D^n \longrightarrow D$
— Pour toute relation $R$ de $\mathcal{R}$ à $n$ arguments, une relation $R_D \subseteq D^n$

En particulier, une constante $a$ correspond à un élément $a_D$ de $D$ et une proposition $p$ (relation sans argument) correspond à un élément de $\mathbb{B} = \{0, 1\}$.

On note $\mathcal{M} = (D, (f_D)_{f \in \mathcal{G}}, (R_D)_{R \in \mathcal{R}})$ une telle structure.

**Exemple 1.** Dans la structure $\mathcal{M} = (\mathbb{R}, 0, 1, +, \times, =)$, le domaine est $D = \mathbb{R}$, l'ensemble des nombres réels, les fonctions sont : les constantes 0 et 1, l'addition, la multiplication et il y a un seul prédicat qui est l'égalité.
Le terme $((x \odot x) \oplus x) \oplus a$ peut être interprété sur ce domaine, avec $a_{\mathbb{R}} = 1$, $\oplus_{\mathbb{R}}$ est l'addition, $\odot_{\mathbb{R}}$ est la multiplication. Il représente donc le polynôme $P$ défini par $P(x) = x^2 + x + 1$.
Considérons maintenant la formule atomique $F \colon Q(((x \odot x) \oplus x) \oplus a, b)$. En interprétant le prédicat binaire $Q$ comme l'égalité et avec $b_{\mathbb{R}} = 0$, cette formule s'interpréte comme un prédicat unaire avec $x$ comme variable libre : $P(x) = 0$.
La formule $\exists x F$ correspond alors à l'énoncé : le polynôme $P$ a une racine dans $\mathbb{R}$.

**Exemple 2.** Lorsque $\mathcal{M}$ décrit une base de données, les requêtes sont des formules.

**Définition 27.** *Pour une structure $\mathcal{M}$ avec domaine $D$, une valuation est une application $v \colon X \longrightarrow D$.*

**Proposition 28.** *Etant données une structure $\mathcal{M}$ associée à $\mathcal{G} \cup \mathcal{R}$, avec domaine $D$, et une valuation $v \colon X \longrightarrow D$, la valeur d'un terme $v^*(t) \in D$ est définie inductivement par :*
*(B) $v^*(a) = a_D$ pour une constante $a$ et $v^*(x) = v(x)$ pour une variable $x \in X$,*
*(I) Si $t = f(t_1, \ldots, t_n)$ pour une fonction $f$ à $n$ arguments et des termes $t_1, \ldots, t_n$, alors $v^*(t) = f_D(v^*(t_1), \ldots, v^*(t_n))$.*

**Remarque.** A chaque $v \colon X \longrightarrow \mathcal{D}$, on associe $v^* \colon \begin{array}{ccc} T(\mathcal{G}, X) & \longrightarrow & \mathcal{D} \\ t & \longmapsto & v^*(t) \end{array}$

**Définition 29.** *Soient $\mathcal{M}$ une structure de domaine $D$, $v \colon X \longrightarrow D$ une valuation, $x \in X$ une variable et $a_{\mathcal{D}} \in \mathcal{D}$.*
*La valuation $v' = v[x \mapsto a_D]$ est définie par :* $\begin{cases} v'(y) = v(y) & \textit{si } y \neq x \\ v'(x) = a_D \end{cases}$

**Exemple.** On considère $X = \{x,\, y,\, z,\, w\}$ et $D = \mathbb{N}$.
Déterminer $v_1 = v[z \to 3]$ et $v_2 = v_1[x \to 1]$ pour la valuation $v$ définie par :

$$v\colon \begin{cases} x \mapsto 2 \\ y \mapsto 8 \\ z \mapsto 7 \\ w \mapsto 14 \end{cases}$$

**Définition 30.** *On définit la valuation (ou valeur de vérité, ou interprétation) d'une formule $F$, notée $\hat{v}(F)$, inductivement par :*

*(B) Si $F = R(t_1, \ldots, t_n)$, alors $\hat{v}(F) = 1$ ssi $(v^*(t_1), \ldots, v^*(t_n)) \in R_D$*

*(B) Pour deux formules $F$ et $G$, et une variable $x$,*

- $\hat{v}(\neg F) = \overline{\hat{v}(F)}$
- $\hat{v}(F \wedge G) = \hat{v}(F)\hat{v}(G)$
- $\hat{v}(F \vee G) = \hat{v}(F) + \hat{v}(G)$
- $\hat{v}(F \to G) = \overline{\hat{v}(F)} + \hat{v}(G)$
- $\hat{v}(\forall x F) = 1$ *ssi pour toute* $a_D \in D$, $\widehat{v[x \mapsto a_D]}(F) = 1$
- $\hat{v}(\exists x F) = 1$ *ssi il existe* $a_D \in D$ *tel que* $\widehat{v[x \mapsto a_D]}(F) = 1$

**Exemple 1.** Soit $F$ : $Q(((x \odot x) \oplus x) \oplus a,\, b)$, la formule considérée précédemment, avec le même modèle, et la valuation $v$ telle que $v(x) = 2$. Alors $\hat{v}(F) = 0$. De plus, comme aucune valeur de $x$ ne peut être racine, on a aussi $\hat{v}(\exists x F) = 0$.

**Exemple 2.** Soit $F = R(f(x),\, g(y))$ et la structure $\mathcal{M} = (\mathbb{N},\, f_\mathbb{N},\, g_\mathbb{N},\, \leqslant)$, avec $f_\mathbb{N}(n) = n+1$ et $g_\mathbb{N}(n) = n+3$, et soit $v_0$ la valuation définie par : $v_0 \begin{cases} x \mapsto 4 \\ y \mapsto 3 \end{cases}$

- $v_0^*(f(x)) = f_\mathbb{N}(v_0(x)) = f_\mathbb{N}(4) = 5$
- $v_0^*(g(y)) = g_\mathbb{N}(v_0(y)) = 6$

Ainsi, $\hat{v}_0(F) = 1$ car $5 \leqslant 6$ et, plus généralement, si $v$ est une valuation quelconque, $\hat{v}(F) = 1$ ssi $v(x) + 1 \leq v(y) + 3$.

**Définition 31.**

1. *Etant données une formule $F$ et une structure $\mathcal{M}$,*
   (a) *$F$ est satisfaisable pour $\mathcal{M}$, s'il existe une valuation $v$ telle que $\hat{v}(F) = 1$.*
   (b) *$F$ est valide pour $\mathcal{M}$, si pour toute valuation $v$, $\hat{v}(F) = 1$.*
   *On dit alors que $\mathcal{M}$ est un modèle de $F$ (noté $\mathcal{M} \models F$).*
2. *Etant donnée une formule $F$ :*
   (a) *$F$ est satisfaisable s'il existe une structure $\mathcal{M}$ telle que $F$ est satisfaisable pour $\mathcal{M}$.*
   (b) *$F$ est valide (ou universellement valide), si pour toute structure $\mathcal{M}$, $F$ est valide pour $\mathcal{M}$.*

**Remarque.** Le problème 2.a est indécidable.
Le problème 1.a est décidable pour des structures finies. C'est le cas par exemple pour la satisfaisabilité d'une requête dans une base de données.

**Proposition 32.** *Il existe un algorithme qui prend en entrée une structure* finie $\mathcal{M}$ *et une formule du premier ordre $F$, et qui décide s'il existe une valuation $v$ telle que $\hat{v}(F) = 1$.*

Pour les structures infinies, c'est plus compliqué :

- Pour $\mathcal{M}_1 = (\underbrace{\mathbb{N}}_{D}, \underbrace{0,\ 1,\ +,\ \times,\ \exp}_{\mathcal{G}}, \underbrace{=}_{\mathcal{R}})$, la satisfaisabilité (d'une formule du premier ordre) est indécidable.
  Dommage... : $\exists n \exists x \exists y \exists z (x^n + y^n = z^n) \wedge (n \geqslant 3)$
- Pour $\mathcal{M}_2 = (\mathbb{N},\ 0,\ 1,\ +,\ \times,\ =)$, le problème est également indécidable.
  Dommage... : $\exists x P(x) = 0$ où $P$ est un polynôme.
- Mais pour $\mathcal{M}_3 = (\mathbb{R},\ +,\ \times,\ <)$, le problème est décidable !

**Exemples de modèles.** Tout ensemble $E$ muni d'une relation binaire $R_E$ réflexive est un modèle de la formule $F_1 :\ \forall x\ R(x, x)$.
Tout ensemble ordonné $\mathcal{M} = (E, \preceq)$ est un modèle de la formule $F_1 \wedge F_2 \wedge F_3$ avec $F_1$ comme ci-dessus et :

$F_2 :\ \forall x\ \forall y\ ((R(x, y) \wedge R(y, x)) \to x = y)$
$F_3 :\ \forall x\ \forall y\ \forall z\ ((R(x, y) \wedge R(y, z)) \to R(x, z))$

## 3.4 Propriétés sémantiques

**Définition 33.** *Soit $\mathcal{M}$ une structure, $F$ et $G$ deux formules.*

- *$F \models G$ si, pour toute valuation $v$ de $\mathcal{M}$, si $\hat{v}(F) = 1$, alors $\hat{v}(G) = 1$.*
- *$F$ et $G$ sont équivalentes, noté $F \sim G$ si pour toute structure $\mathcal{M}$ et pour toute valuation $v$, $\hat{v}(F) = \hat{v}(G)$*

**Remarques.**

- On note parfois $\models_{\mathcal{M}}$ au lieu de $\models$ lorsqu'il y a ambiguïté sur la structure considérée.
- Comme pour le calcul propositionnel, $F \sim G$ ssi pour toute structure $\mathcal{M}$, on a : $F \models G$ et $G \models F$.
- On a toutes les équivalences du calcul propositionnel :
  $\neg(F \vee G) \sim \neg F \wedge \neg G$, $\neg\neg F \sim F$, ...
- On voudrait des équivalences plus « riches », qui impliquent les variables.

**Proposition 34.** *Soit $F$ une formule. On a l'équivalence suivante :*

$$\neg \forall x F \sim \exists x \neg F$$

*Démonstration.* Soit $\mathcal{M}$ une structure et $v$ une valuation. On a :

$$\begin{aligned}\hat{v}(\neg\forall xF) = 1 \quad & \text{ssi} \quad \hat{v}(\forall xF) = 0\\ & \text{ssi} \quad \text{il existe } a \in \mathcal{D} \text{ tq } \widehat{v[x \to a]}(F) = 0\\ & \text{ssi} \quad \text{il existe } a \in \mathcal{D} \text{ tq } \widehat{v[x \to a]}(\neg F) = 1\\ & \text{ssi} \quad \hat{v}(\exists x\neg F) = 1\end{aligned}$$

□

**Lemme 35.** *Soit $\mathcal{M}$ une structure, $v_1$ et $v_2$ deux valuations.*

1. *Si $t$ est un terme tel que $v_1|_{Var(t)} = v_2|_{Var(t)}$ ($v_1$ et $v_2$ coïncident sur $Var(t)$), alors $v_1^*(t) = v_2^*(t)$*
2. *Si $F$ est une formule telle que $v_1|_{L(F)} = v_2|_{L(F)}$ ($v_1$ et $v_2$ coïncident sur les variables libres de $F$),*
   *alors $\hat{v}_1(F) = \hat{v}_2(F)$*

**Exemple pour un terme.** Soit $t = g(x, y)$ et deux valuations $v_1$ et $v_2$ telles que $v_1(x) = v_2(x)$ et $v_1(y) = v_2(y)$.
Alors $v_1^*(t) = g_{\mathcal{D}}(v_1(x), v_1(y)) = g_{\mathcal{D}}(v_2(x), v_2(y)) = v_2^*(t)$.

**Remarque.** Ce lemme exprime que la valeur de vérité d'une formule ne dépend que des valeurs de ses variables libres. Par exemple, la valeur de la formule $F\colon \forall xR(y, x)$ ne dépend que de $y$.

**Corollaire 36** (Conséquences)**.** *Si $F$ est une formule close (c'est-à-dire une formule sans variable libre), alors $\hat{v}(F)$ est constante, indépendante de $v$.*
*Ainsi, $F$ et $\forall xF$ sont équivalentes si $x$ n'est pas libre dans $F$.*
*De même, $F \sim \exists xF$ si $x \notin L(F)$.*

**Exemple.** Soit $F\colon \forall x\exists yR(x, y)$ interprétée avec pour $\mathcal{D}$ l'ensemble des personnes et $R$ la relation définie par $R(x,y)$ si « $y$ est la mère de $x$ ». Alors, pour toute valuation $v$, $\hat{v}(F) = 1$.

**Rappel :** D'après la définition inductive de $L(F)$, on a :
$L(\forall xF) = L(F)\backslash\{x\} = L(F)$ si $x$ n'est pas libre dans $F$.
Démontrons la propriété : si $x \notin L(F)$ alors $F \sim \forall xF$.

On se rappelle tout d'abord que, d'après la définition inductive de $L(F)$, on a : $L(\forall xF) = L(F)\backslash\{x\} = L(F)$ si $x$ n'est pas libre dans $F$.
Soit maintenant $v$ une valuation. On a par définition de $\hat{v}(\forall xF)$ :
$\hat{v}(\forall xF) = 1$ si pour tout $a \in \mathcal{D}$, $\widehat{v[x \to a]}(F) = 1$.
Mais $v$ et $v[x \to a]$ coïncident partout sauf sur $x$, donc elles coïncident sur $L(F) = L(\forall xF)$ d'après ce qui précède.
Donc d'après le lemme : $\hat{v}(F) = \widehat{v[x \to a]}(F) = 1$, et on obtient bien $\hat{v}(F) = \hat{v}(\forall xF)$.