

ARCHI – Architecture des ordinateurs

*Sylvain Brandel*

2023 – 2024

[sylvain.brandel@univ-lyon1.fr](mailto:sylvain.brandel@univ-lyon1.fr)



CM 2

# LOGIQUE PROPOSITIONNELLE

# Logique propositionnelle

## *Pourquoi ?*

- Niveau matériel = modèle logique
- Niveau programme : preuve de propriété = logique
- Niveau applicatif, BD : vérification de propriétés = logique
- ...
  
- Plus généralement
  - Criticité : sécurité, sûreté ...
  - Financier
  - Pas d'ambiguïté

# Logique propositionnelle

## Syntaxe

- $V = \{x_1, x_2, \dots, x_n, \dots\}$  un ensemble infini de variables propositionnelles
- Ensemble  $\mathcal{F}$  des formules du calcul propositionnel : ensemble inductif
  - $x$  variable propositionnelle alors  $x \in \mathcal{F}$
  - $\perp \in \mathcal{F}$
  - Si  $A \in \mathcal{F}$  alors  $\neg A \in \mathcal{F}$
  - Si  $A \in \mathcal{F}$  et  $B \in \mathcal{F}$  alors  $A \vee B \in \mathcal{F}$ ,  $A \wedge B \in \mathcal{F}$ ,  $A \Rightarrow B \in \mathcal{F}$
- Notation :  $A \Leftrightarrow B : (A \Rightarrow B) \wedge (B \Rightarrow A)$
- Priorités :  $\neg > \wedge > \vee > \Rightarrow$
- Associativité : à gauche pour  $\wedge$  et  $\vee$ , à droite pour  $\Rightarrow$
- Ex :  $p \vee q \Rightarrow r$

# Logique propositionnelle

## Sémantique

- Sens des formules → interprétation dans l'algèbre de Boole
- Interprétation du calcul propositionnel : fonction  $I : V \rightarrow \mathbb{B}$ 
  - $V = \{x_1, x_2, \dots, x_n, \dots\}$  : variables
  - $\mathbb{B} = \{0,1\}$
- $I$  étendue à  $\mathcal{F}$ 
  - Cas des variables déjà traité
  - $I(\perp) = 0$
  - $A \in \mathcal{F}$  alors  $I(\neg A) = \overline{I(A)}$
  - $A \in \mathcal{F}$  et  $B \in \mathcal{F}$  alors  $I(A \vee B) = I(A) + I(B)$
  - $A \in \mathcal{F}$  et  $B \in \mathcal{F}$  alors  $I(A \wedge B) = I(A) \cdot I(B)$
  - $A \in \mathcal{F}$  et  $B \in \mathcal{F}$  alors  $I(A \Rightarrow B) = I(A) \dot{\Rightarrow} I(B)$

Seule vérité autorisée

# Algèbre de Boole



- George Boole 1815 – 1864 (Royaume-Uni)
- Booléens : oui, non ; 0, 1 ; haut, bas ; rouge, noir ; etc.
- Relation d'ordre :  $0 < 1$
- Soit  $\mathbb{B} = \{0,1\}$ . Opérations :
  - $\bar{\phantom{x}} : \mathbb{B} \rightarrow \mathbb{B}$  complément
  - $+$  :  $\mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$   $\cup$ , ou, disjonction, max
  - $\cdot$  :  $\mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$   $\cap$ , et, conjonction, min
  - $\Rightarrow$  :  $\mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$  si ... alors, implication

# Algèbre de Boole

$x$	$y$	$x \cdot y$
0	0	0
0	1	0
1	0	0
1	1	1

$x$	$y$	$x + y$
0	0	0
0	1	1
1	0	1
1	1	1

$x$	$y$	$x \Rightarrow y$
0	0	1
0	1	1
1	0	0
1	1	1

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

# Algèbre de Boole

- 0 : minimum, 1 maximum
- $x \cdot 1 = x$        $x \cdot 0 = 0$
- $x + 0 = x$        $x + 1 = 1$
- Complément :  $x \cdot \bar{x} = 0$        $x + \bar{x} = 1$
- Commutativité
- Associativité
- Distributivité
- De Morgan :
  - $\bar{x} \cdot \bar{y} = \overline{x + y}$
  - $\bar{x} + \bar{y} = \overline{x \cdot y}$

# Algèbre de Boole

## *Tables de vérité*

- Idée : notation par extension
- Une **ligne** par valeurs possible des variables
- Présentation des sous-fonctions en **colonnes**
- **Fonctions booléennes** : par extension, une fonction par table de vérité  
→ combien ?



# Interprétations

- **Interprétation** : fonction  $I : V \rightarrow \mathbb{B}$

- Soit  $A$  une formule.

$$I(A) = 1 : I \text{ satisfait } A \qquad \text{noté } I \models A$$

- Ex :

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

- Soit  $F$  un ensemble de formules.

$$\text{Si } I \models A \text{ pour tout } A \in F : I \text{ satisfait } F \qquad \text{noté } I \models F$$

- Ex :

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

# Interprétations

- $A$  **tautologie**, ou  $A$  **valide** noté  $\models A$   
si **pour toute** interprétation  $I$ ,  $I \models A$
- $F$  **contradictoire**, ou  $F$  **non satisfiable**  
s'il n'existe **aucune** interprétation  $I$  telle que  $I \models F$
- $F$  **satisfiable**  
s'il existe **une** (au moins) interprétation  $I$  telle que  $I \models F$
- $F$  **déduit sémantiquement**  $A$  noté  $F \models A$   
si **toute** interprétation satisfaisant  $F$  satisfait aussi  $A$
- $A$  et  $B$  **sémantiquement équivalentes** noté  $A \equiv B$   
si  $\{A\} \models B$  et  $\{B\} \models A$

# Logique propositionnelle

## Modélisation

- Un logicien écoute un étudiant énumérer ses ressentis à propos des cours qu'il suit :
  - « J'aime la logique ou j'aime l'informatique, »
  - « Si j'aime l'informatique alors j'aime la logique. »
- Le logicien en déduit que l'étudiant aime la logique. Pourquoi ?
- Soient  $a$  et  $b$  deux variables propositionnelles :
  - $a$  représente « j'aime la logique »
  - $b$  représente « j'aime l'informatique »
- Les deux phrases de l'étudiant représentées par :
  1.  $a \vee b$
  2.  $b \Rightarrow a$
- Dédution du logicien représentée par  $a$
- Démontrer  $a \vee b, b \Rightarrow a \vDash a$

# Logique propositionnelle

## *Substitution*

- Remplacement d'une variable  $p$  par une formule  $B$  dans une formule  $A$ , noté  $A[p := B]$ , défini par **induction** sur  $A$  :

- $p[p := B] = B$

- $q[p := B] = q$  si  $q \neq p$

- $\perp [p := B] = \perp$

- $\neg A[p := B] = \neg(A[p := B])$

- $(A_1 \vee A_2)[p := B] = (A_1[p := B]) \vee (A_2[p := B])$

- $(A_1 \wedge A_2)[p := B] = (A_1[p := B]) \wedge (A_2[p := B])$

- $(A_1 \Rightarrow A_2)[p := B] = (A_1[p := B]) \Rightarrow (A_2[p := B])$

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

# Logique propositionnelle

## Propositions

- Proposition 1.  $A \in \mathcal{F}$  et  $B \in \mathcal{F}$ ,  $F$  ensemble de formules.
  - $F \models A \Rightarrow B$  si et seulement si  $F, A \models B$ ,
  - $F \models A$  si et seulement si  $F, \neg A$  contradictoire.
- Proposition 2.  $A \in \mathcal{F}$  et  $B \in \mathcal{F}$ ,  $p$  une variable,  $I$  une interprétation.  
 $I'$  définie par  $I'(p) = I(B)$  et  $I'(q) = I(q)$  si  $q \neq p$   
On a  $I(A[p := B]) = I'(A)$
- Proposition 3.  $A, A', B, B'$  des formules,  $p$  une variable.
  - Si  $F \models A$  alors  $F \models A[p := B]$
  - Si  $A \equiv A'$  alors  $A[p := B] \equiv A'[p := B]$
  - Si  $B \equiv B'$  alors  $A[p := B] \equiv A[p := B']$

# Logique propositionnelle

## *Quelques équivalences*

$$A \wedge A \equiv A$$

$$A \vee A \equiv A$$

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

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

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

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

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

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

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

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

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

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

$$\perp \wedge A \equiv \perp$$

$$\perp \vee A \equiv A$$

$$\neg\neg A \equiv A$$

# Logique propositionnelle

## *Forme Clausale*

- Littéral :  
variable ou négation de variable
- Clause :  
disjonction de littéraux (éventuellement un seul)
- FNC (Forme Normale Conjonctive) :  
conjonction de disjonction de littéraux (clauses)  
(éventuellement une seule)
- FND (Forme Normale Disjonctive) :  
disjonction de conjonctions de littéraux  
(éventuellement une seule)

# Logique propositionnelle

## *Forme Clausale*

- Proposition 4 : pour toute formule  $A \in \mathcal{F}$   
on a une formule  $A' \in \mathcal{F}$  et une formule  $A'' \in \mathcal{F}$  telles que
  - $A \equiv A' \equiv A''$
  - $A'$  est en FNC
  - $A''$  est en FND



# Algèbre de Boole

- Tables de vérité

- Ex (binaire) :

	$x$	$y$	$S$
$m_0$	0	0	0
$m_1$	0	1	1
$m_2$	1	0	1
$m_3$	1	1	0

- Termes produits : distinction de lignes
- $m_i$  : ligne  $i$  parmi  $n$

# Algèbre de Boole

- Terme produit : **intersection** des **variables d'entrée**,  
complémentées si valeur 0  
non complémentées si valeur 1
- Expression de  $S$  :  $m_0 \cdot S_0 + m_1 \cdot S_1 + m_2 \cdot S_2 + m_3 \cdot S_3$        $\sum_i (m_i \cdot S_i)$ 
  - Un seul  $m_i$  non 0
  - $1 \cdot S_i = S_i$
  - $m_i \cdot 1 = m_i$
  - $x + 0 = x$

→ Forme canonique : Forme Normale Disjonctive

**Union** des **termes produits** pour lesquels la fonction vaut 1
- Notation  $\sum m$  (*liste des termes produits pertinents*)

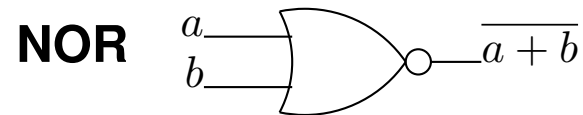
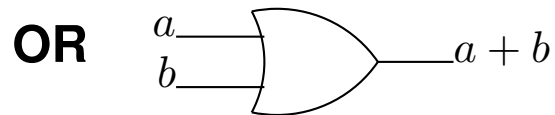
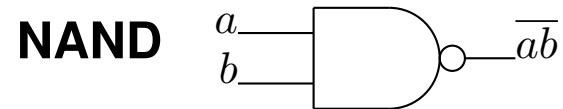
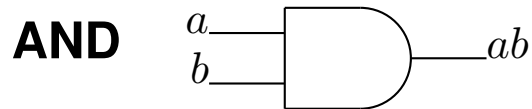
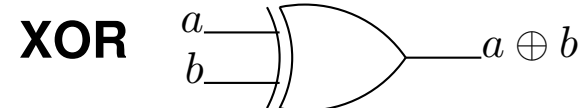
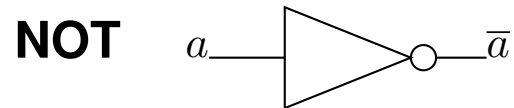
# Algèbre de Boole

- Forme Normale Disjonctive
- Toutes fonctions booléennes exprimables avec et, ou, non
- De plus :
 

- $\overline{x.1} = \bar{x}$	$\bar{x} = \overline{x.x}$
- $\overline{1.\bar{x}.\bar{y}} = x.y$	$x.y = \overline{\overline{x.\bar{y}}} = \overline{\overline{x.y.x.y}}$
- $\overline{\overline{1.x.\overline{1.y}} = x + y$	$x + y = \bar{\bar{x}} + \bar{\bar{y}} = \overline{\bar{x}.\bar{y}} = \overline{\overline{x.x.y.y}}$
- Toutes fonctions booléennes exprimables avec non-et (ou non-ou)
- Ex : DNF  $\rightarrow$  NAND-NAND

# Algèbre de Boole

- Notation :



- Ex : XOR avec 5 portes simples (AND, OR, NOT)
- Ex : XOR avec 4 portes simples