Algèbre de Boole

1 Introduction

Au moment de l'étude des ensembles nous avons vu plusieurs opérations entre sous-ensembles d'un même ensemble E. L'intersection et la réunion sont des opérations (lois) binaires. À deux ensembles A et B, l'intersection associe l'ensemble $A \cap B$ et la réunion associe $A \cup B$.
Une autre loi binaire est la différence symétrique notée Δ, $A\Delta B = (A \cup B) \setminus (A \cap B)$.
Par contre l'opération qui à une partie A de l'ensemble E associe son complémentaire $C_E A = \overline{A}$ est une loi unaire.
En logique nous avons vu les opérateurs binaires $\wedge$, $\vee$, ou exclusif, $\Rightarrow$, $\Leftrightarrow$ et l'opérateur unaire $\neg$.

Les lois ensemblistes et les opérateurs logiques sont directement liés :

Opérateur / loi	prédicats logiquement équivalents utilisant l'opérateur logique	puis la loi ensembliste
$\vee, \cup$	$(x \in A) \vee (x \in B)$	$x \in A \cup B$
$\wedge, \cap$	$(x \in A) \wedge (x \in B)$	$x \in A \cap B$
ou$_e$, Δ	$(x \in A)$ ou$_e$$(x \in B)$	$x \in A\Delta B$
$\neg$, C_E	$\neg(x \in A)$	$x \in C_E A$, $x \in \overline{A}$
$\Leftrightarrow$	$(x \in A) \iff (x \in B)$	$x \in \overline{A\Delta B}$
$\Rightarrow$	$(x \in A) \Rightarrow (x \in B)$	$x \in \overline{A} \cup B$

Par ailleurs $\forall x, (x \in A) \Leftrightarrow (x \in B)$ est vrai si et seulement si $A = B$. $\forall x, (x \in A) \Rightarrow (x \in B)$ correspond de même à la relation d'inclusion $A \subset B$.

À tout prédicat, c'est-à-dire à toute propriété $P(x)$ des éléments x d'un ensemble E, on associe la partie $A \subset E$ des éléments de E pour lesquels la propriété est vérifiée :
$x \in A$ est logiquement équivalent à $P(x)$.
Évidemment, $x \in \mathrm{C}_E A$ que l'on écrit $x \in \bar{A}$ est logiquement équivalent à $\neg P(x)$.

Ainsi $(x \in A) \Rightarrow (x \in B)$ est logiquement équivalent à $\neg(x \in A) \vee (x \in B)$, $(x \in \bar{A}) \vee (x \in B)$, $x \in \bar{A} \cup B$.
Cet ensemble $\bar{A} \cup B$ est égal à E si et seulement si $A \subset B$. On en déduit que $\forall x, (x \in A) \Rightarrow (x \in B)$ équivaut logiquement à $A \subset B$.

$(x \in A) \iff (x \in B)$ est logiquement équivalent à $(x \in \bar{A} \vee x \in B) \wedge (x \in A \vee x \in \bar{B})$, $(x \in \bar{A} \cup B) \wedge (x \in A \cup \bar{B})$, $x \in (\bar{A} \cup B) \cap (A \cup \bar{B})$, $x \in (\bar{A} \cap \bar{B}) \cup (A \cap B)$, $x \in \overline{(A \cup B)} \cup (A \cap B)$.
L'ensemble $(\bar{A} \cap \bar{B}) \cup (A \cap B)$ est égal à E si et seulement si $A = B$, c'est ce qui justifie que $\forall x, (x \in A) \Leftrightarrow (x \in B)$ est logiquement équivalent à $A = B$.

La relation d'appartenance à un ensemble permet de mettre en correspondance les opérateurs logiques et les lois ensemblistes, et aussi les propriétés des opérateurs logiques à celles des lois ensemblistes.

Exemples de choix de deux lois binaires et d'une loi unaire :

	$\mathcal{P}(E)$ ensemble des parties de E		Propositions, prédicats		Ensemble
1ère loi binaire (additive)	$A \cup B$	$A \Delta B$	$p \vee q$	p ou$_e q$	$x + y$
élément neutre de la 1ère loi	$\emptyset$	$\emptyset$	Faux	Faux	0
2ème loi binaire (multiplicative)	$A \cap B$	$A \cap B$	$p \wedge q$	$p \wedge q$	xy
élément neutre de la 2ème loi	E	E	Vrai	Vrai	1
loi unaire	$C_E A$	$C_E A$	$\neg p$	$\neg p$	$\overline{x}$
cadre :	Ensembles		Logique		Alg. de Boole

Dans ce tableau :
Les lois binaires sont associatives, commutatives, avec élément neutre, et telles que tout élément est idempotent.
Chaque loi binaire est distributive par rapport à l'autre.
D'autres propriétés que l'on verra plus loin font intervenir la loi unaire et les deux lois binaires.
La dernière colonne donne les notations généralement utilisées pour ces lois dans une algèbre de Boole.

2 Définitions et Propriétés des Algèbres de Boole

2.1 Algèbre de Boole

Définition. Un ensemble non vide A contenant deux éléments distincts notés 0 et 1, muni de deux lois de composition interne additive et multiplicative et d'un opérateur unaire, la complémentation, qui à tout élément a fait correspondre son complément (noté $\bar{a}$), a une structure d'algèbre de Boole si :

l'addition	est associative	$\forall a \forall b \forall c, (a+b)+c = a+(b+c)$
	est commutative	$\forall a \forall b, a+b = b+a$
	a pour élément neutre 0	$\forall a, a+0 = a \wedge 0+a = a$
la multiplication	est associative	$\forall a \forall b \forall c, (ab)c = a(bc)$
	est commutative	$\forall a \forall b, ab = ba$
	a pour élément neutre 1	$\forall a, a1 = a \wedge 1a = a$
la loi unaire est telle que		$\forall a, a + \bar{a} = 1$
		$\forall a, a\bar{a} = 0$
L'addition est distributive sur	la multiplication	$\forall a \forall b \forall c, a + bc = (a+b)(a+c)$
La multiplication est distributive sur	l'addition	$\forall a \forall b \forall c, a(b+c) = ab + ac$

0 est appelé l'élément nul, 1 est l'élément unité.

Remarque : Attention, les algèbres de Boole sont aussi parfois définies comme des anneaux de Boole (anneaux unitaires où tout élément est égal à son carré), les deux définitions ne sont pas équivalentes, dans tout anneau de Boole, chaque élément a un opposé : $\forall a\ \exists b,\ a+b=0\ \wedge\ b+a=0$, (et on montre alors que chaque élément est son propre opposé $a+a=0$).
Cet axiome supplémentaire ne sera pas vérifié par la loi $\cup$ dans le cas de l'algèbre $(\mathcal{P}(E), \cup, \cap, \complement_E)$, par contre il l'est par la loi Δ dans l'algèbre $(\mathcal{P}(E), \Delta, \cap, \complement_E)$, en effet pour tout ensemble $A \in \mathcal{P}(E)$ c'est-à-dire pour tout $A \subset E$, on a $A \Delta A = \emptyset$ et A est son propre opposé.

2.2 Propriétés

Idempotence
De l'addition : $\forall a,\ a + a = a$.
De la multiplication : $\forall a,\ aa = a$.

Conséquences :
On n'aura pas à écrire de termes comme $3a$, en effet $3a = a + a + a = a$, ni de puissances comme a^4, en effet $a^4 = aaaa = a$.

Démonstrations :
$a = a1 = a(a + \bar{a}) = aa + a\bar{a} = aa + 0 = aa$
et par dualité, $a = a + 0 = a + a\bar{a} = (a + a)(a + \bar{a}) = (a + a)1 = a + a$.

Éléments absorbants :
De l'addition : $\forall a,\ a + 1 = 1$.
De la multiplication : $\forall a,\ a0 = 0$.
1 est absorbant pour l'addition et 0 est absorbant pour la multiplication.

Démonstrations :
$a + 1 = a + (a + \bar{a}) = (a + a) + \bar{a} = a + \bar{a} = 1$.
et par dualité, $a0 = a(a\bar{a}) = (aa)\bar{a} = a\bar{a} = 0$.

Propriétés d'absorption :
$a + ab = a$, en effet $a + ab = a(1 + b) = a1 = a$,
$a(a + b) = a$, en effet $a(a + b) = aa + ab = a + ab = a$.

Exemple :
$abc + ab + bc + a + c = a + c$, il suffit d'utiliser la propriété $a + ab = a$.
Dans cette somme de produits, on repère tous les termes contenant le facteur a, ils seront « absorbés » par le terme a de cette somme ; de même les termes contenant le facteur c le seront par le terme c.

Complément
Si on a à la fois $a + b = 1$ et $ab = 0$, alors $b = \bar{a}$.
$\bar{0} = 1$ et $\bar{1} = 0$.
$\forall a,\ \bar{\bar{a}} = a$.

Démonstrations :
Supposons que $a + b = 1$ et $ab = 0$, alors on peut écrire :
$b = b+0 = b+a\bar{a} = (b+a)(b+\bar{a}) = (a+\bar{a})(b+\bar{a}) = ab+a\bar{a}+\bar{a}b+\bar{a}\bar{a} = ab+a\bar{a}+\bar{a}b+\bar{a} = ab+\bar{a} = a\bar{a}+\bar{a} = \bar{a}$.
On remarque que $a + b = 1$ et $ab = 0$ permet de prouver à la fois que $b = \bar{a}$ et aussi que $a = \bar{b}$.

$0 + 1 = 1$ et $0\ 1 = 0$ donc $0 = \bar{1}$ et aussi $\bar{0} = 1$.

$a + \bar{a} = 1$ et $a\bar{a} = 0$ donc $\bar{\bar{a}} = a$.

Lois de Morgan
$\forall a\, \forall b,\ \overline{a + b} = \bar{a}\bar{b}$.
$\forall a\, \forall b,\ \overline{ab} = \bar{a} + \bar{b}$.

Démonstration :
On montre que $(a + b) + \bar{a}\bar{b} = 1$ et que $(a + b)\bar{a}\bar{b} = 0$ ce qui prouve alors que $\bar{a}\bar{b}$ est le complément de $a + b$ et donc que $\overline{a + b} = \bar{a}\bar{b}$.
En utilisant les propriétés de distributivité, associativité et commutativité :
$(a + b) + \bar{a}\bar{b} = (a + b + \bar{a})(a + b + \bar{b}) = (1 + b)(1 + a) = 1.1 = 1$,
$(a + b)\bar{a}\bar{b} = (a\bar{a}\bar{b}) + (b\bar{a}\bar{b}) = (0\ b) + (0\ \bar{a}) = 0\ 0 = 0$.
D'où la propriété.

2.3 Dualité

Exemple :
Les deux propriétés de commutativité sont dites duales , ce sont
pour les sommes : $\forall a \forall b, a + b = b + a$; les produits : $\forall a \forall b, ab = ba$.
On peut simplement passer de l'une des propriétés à l'autre en échangeant les deux lois, les additions sont remplacées par autant de multiplications, les multiplications sont remplacées par des additions.
En reprenant les propriétés vues plus haut, on remarque qu'il faut également échanger 0 et 1 : $\forall a, a + 0 = a$ et $\forall a; a1 = a$ par exemple.

Propriétés de dualité :
On peut remplacer une égalité quelconque de l'algèbre de Boole par l'égalité obtenue en échangeant
1) $+$ et $\times$ 2) 0 et 1 3) chaque variable x et son complément $\bar{x}$.

On peut remplacer une égalité quelconque de l'algèbre de Boole par l'égalité obtenue en échangeant
1) $+$ et $\times$,
2) 0 et 1, plus généralement chaque constante α et son complément $\bar{\alpha}$,
3) On garde chaque variable x quantifiée existentiellement ($\exists x$) ou universellement ($\forall x$) et son complément tels quels.

Démonstration :
Pour démontrer la première propriété, on rappelle simplement que une égalité $A = B$ est vraie si et seulement si les compléments sont égaux : $\bar{A} = \bar{B}$, que le complément d'une somme (resp. d'un produit) est le produit (resp. la somme) des compléments : $\overline{A+B} = \bar{A}\bar{B}$ et $\overline{AB} = \bar{A} + \bar{B}$, enfin que $\bar{0} = 1$ et $\bar{1} = 0$.

Pour expliquer la deuxième propriété, on transforme l'égalité en prenant les compléments, comme ci-dessus, mais dans ce cas a devient $\bar{a}$ ...on remplace alors $\bar{a}$ par a' (et donc a par $\bar{a'}$) ...enfin on obtient l'égalité voulue en remplaçant a' par a ....

Exemple :
$\forall a \forall b \forall c, a(b+c) = ab + ac$
$\forall a \forall b \forall c, \overline{a(b+c)} = \overline{ab+ac}$
$\forall a \forall b \forall c, \bar{a} + (\bar{b}\bar{c}) = (\bar{a} + \bar{b})(\bar{a} + \bar{c})$
$\forall a \forall b \forall c, a' + (b'c') = (a' + b')(a' + c')$
$\forall a \forall b \forall c, a + bc = (a+b)(a+c)$.

Remarque : Ce que l'on vient de faire pour une variable : $\bar{a} \to a' \to a$, on ne peut le faire pour une constante, sauf si on change la définition de cette constante.
par exemple, sachant $c = 1$, on a la propriété $\forall a, a + c = c$ et la propriété duale $\forall a, a\bar{c} = \bar{c}$.
en changeant la définition de c en $c = 0$, on obtient : $\forall a, ac = c$.

2.4 Représentation et simplification des fonctions booléennes

2.4.1 Écriture algébrique

Une fonction booléenne F de trois variables a, b, c, peut être donnée sous la forme d'une expression des trois variables a, b, c, ou de leurs compléments variables $\bar{a}$, $\bar{b}$, $\bar{c}$, comme par exemple : $F = F(a,b,c) = a\bar{b} + \bar{a}(b + \bar{c})$.

2.4.2 Décomposition en une somme de produits

par exemple $F(a,b,c) = a\bar{b} + \bar{a}(b+\bar{c})$ s'écrit successivement $F = a\bar{b} + \bar{a}b + \bar{a}\bar{c}$ ou encore $F = a\bar{b}c + a\bar{b}\bar{c} + \bar{a}bc + \bar{a}b\bar{c} + \bar{a}b\bar{c} + \bar{a}\bar{b}\bar{c}$.
Dans les deux cas on a des sommes de produits.

2.4.3 Tables de vérité

En supposant que les variables booléennes a, b, c ...ne prennent que les deux valeurs 0 ou 1 ; on peut dresser la table de vérité

a	b	c	$F(a,b,c) = a\bar{b} + \bar{a}(b+\bar{c})$
1	1	1	0
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	1
0	0	1	1
0	0	0	1

ou mieux :

a	b	c	$F(a,b,c) = a\bar{b} + \bar{a}(b+\bar{c})$
1	1	1	0
1	1	0	0
1	0	0	1
1	0	1	1
0	0	1	1
0	0	0	1
0	1	0	1
0	1	1	1

Dans la table de droite, d'une ligne à la suivante, seule une variable booléenne change de valeur.

En écrivant F sous la forme $a\bar{b}c + a\bar{b}\bar{c} + \bar{a}bc + \bar{a}b\bar{c} + \bar{a}\bar{b}c + \bar{a}\bar{b}\bar{c}$, à chaque terme de cette somme correspond une ligne unique du tableau, la seule pour laquelle le terme vaut 1, par exemple $a\bar{b}c$ vaut 1 si et seulement si $a = 1$, $b = 0$ et $c = 1$.

Table de KARNAUGH.

a /bc	00	01	11	10
0	1	1	1	1
1	1	1	0	0

On peut voir, à l'aide de cette table, que F se simplifie en $F = \bar{a} + \bar{b}$;

2.4.4 Cube

La face inférieure correspond à $\bar{a}$ la face supérieure à a, celle de gauche à $\bar{b}$, de droite à b, la face avant à $\bar{b}$, arrière à c.
À chaque sommet correspond un terme de $\bar{a}\bar{b}\bar{c}$ à abc.