Mathématiques Discrètes

Chapitre 5
Calcul propositionnel et Algèbre de Boole

Leo Donati   Noëlle Stolfi

Université de Nice Sophia Antipolis
IUT Nice Côte d'Azur
DUT Informatique

2015-2016

Chapitre 5 : Calcul propositionnel et Algèbre de Boole

Algèbre de Boole

Une algèbre de Boole est un ensemble $\mathbb{B}$ possédant

- au moins deux éléments distincts notés 0 et 1
- deux opérations de composition interne $+$ et $\times$
- une loi qui à tout élément $x \in \mathbb{B}$ associe $\overline{x} \in \mathbb{B}$

Ces lois doivent vérifier 5 groupes de 2 axiomes :

1. **Règle de la barre** : $x + \overline{x} = 1 \qquad x \times \overline{x} = 0$
2. **O et 1 sont des éléments neutres** :
   $x + 0 = 0 + x = x \qquad x \times 1 = x \times 1 = x$
3. **Commutativité** : $x + y = y + x \qquad x \times y = y \times x$
4. **Associativité** :
   $x + (y + z) = (x + y) + z \qquad x \times (y \times z) = (x \times y) \times z$
5. **Distributivité** : $x \times (y + z) = (x \times y) + (x \times z)$
   $x + (y \times z) = (x + y) \times (x + z)$

$\mathbb{B}_2$

Algèbre de Boole $\mathbb{B}_2$

L'algèbre de Boole la plus simple de toutes n'a que deux éléments :

$$\mathbb{B}_2 = \{0, 1\}$$

$+$	0	1
0	0	1
1	1	1

$\times$	0	1
0	0	0
1	0	1

Remarque

Cette algèbre de Boole est celle de la logique mathématique où

- 0 c'est Faux et 1 c'est Vrai
- $+$ c'est OU et $\times$ c'est ET
- $\overline{x}$ c'est NON(x)

Propriétés fondamentales

Théorème 1

$$\overline{0} = 1 \text{ et } \overline{1} = 0$$

Démonstration

Comme le 0 est l'élément neutre de $+$ on a

$$\overline{0} + 0 = \overline{0}$$

d'autre part, d'après l'axiome de la barre

$$\overline{0} + 0 = 1$$

donc

$$\overline{0} = 1$$

Propriétés fondamentales - 2

Théorème 2

$$\forall x \in \mathbb{B} \; x + x = x$$

Démonstration

$\forall x \in \mathbb{B}$ on a

$$\begin{aligned} x &= x + 0 \\ &= x + (x \times \overline{x}) \\ &= (x + x) \times (x + \overline{x}) \\ &= (x + x) \times 1 \\ &= x + x \end{aligned}$$

Propriétés fondamentales - 3

Théorèmes 3

- $\forall x \in \mathbb{B} \; x \times x = x$
- $\forall x \in \mathbb{B} \; x + 1 = 1$
- $\forall x \in \mathbb{B} \; x \times 0 = 0$

Démonstration

En TD

Lemme

Si dans une algèbre de Boole $\mathbb{B}$ il existe deux élémente x et y tels que $x+y=1$ et $x \times y = 0$ alors on a

$$y = \overline{x}$$

Démonstration

Preuve :

$$\begin{array}{rccc} & x+y & = & 1 \\ \Rightarrow & \overline{x}(x+y) & = & \overline{x} \\ \Rightarrow & (\overline{x}x)+(\overline{x}y) & = & \overline{x} \\ \Rightarrow & 0+(\overline{x}y) & = & \overline{x} \\ \Rightarrow & (xy)+(\overline{x}y) & = & \overline{x} \\ \Rightarrow & (x+\overline{x})y & = & \overline{x} \\ \Rightarrow & (1y) & = & \overline{x} \\ \Rightarrow & y & = & \overline{x} \end{array}$$

Loi de De Morgan

Lois de De Morgan : $\forall x \in \mathbb{B},\ \forall y \in \mathbb{B}$

- $\overline{x \times y} = \overline{x} + \overline{y}$
- $\overline{x + y} = \overline{x} \times \overline{y}$

Démonstration

Posons $A = xy$ et $B = \overline{x} + \overline{y}$. On cherche à montrer que $\overline{A} = B$.
Utilisons le lemme : il nous faut prouver que $A + B = 1$ et $AB = 0$.

$$\begin{array}{rcc}
A + B & = & \overline{x} + \overline{y} + (xy) \\
 & = & (\overline{x} + \overline{y} + x)(\overline{x} + \overline{y} + y) \\
 & = & (1 + \overline{y})(1 + \overline{x}) \\
 & = & 1 \times 1 \\
 & = & 1
\end{array}
\qquad
\begin{array}{rcc}
A \times B & = & (\overline{x} + \overline{y}) \times (xy) \\
 & = & (\overline{x}.y.x)(\overline{y}.x.y) \\
 & = & (0.y) + (0.x) \\
 & = & 0 + 0 \\
 & = & 0
\end{array}$$

De même pour l'autre loi de Morgan.

Involution

Théorème d'Involution

$$\forall a \in \mathbb{B}, \overline{\overline{a}} = a$$

Démonstration

On utilise le lemme avec $x = \overline{a}$ et $y = a$.
On a $x + y = \overline{a} + a = 1$ et $x \times y = a \times \overline{a} = 0$.
Donc par le lemme on a bien $y = \overline{x}$
c'est à dire $\overline{\overline{a}} = a$.

$\mathbb{B}_2^2$

Algèbre de Boole $\mathbb{B}_2^n$

On applique sur des mots de n bits, le ou et le et bit–à–bit (bitwise or/and) et le complément à 1.
C'est une algèbre de Boole avec 2^n éléments.

Cas de $\mathbb{B}_2^2$

$\mathbb{B}_2^2 = \{00, 01, 10, 11\}$ et on a les tables suivantes :

$+$	00	01	10	11
00	00	01	10	11
01	01	01	11	11
10	10	11	10	11
11	11	11	11	11

$\times$	00	01	10	11
00	00	00	00	00
01	00	01	00	01
10	00	10	00	10
11	00	01	10	11

Parties d'un ensemble

Parties de E

On obtient une algèbre de Boole en prenant l'intersection ($\times$), l'union ($+$) et le complémentaire (barre).

Si $E = \{a, b\}$

On obtient une algèbre de Boole à 4 éléments $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ avec les opérations suivantes :

$\cup$	$\emptyset$	{a}	{b}	E
$\emptyset$	$\emptyset$	{a}	{b}	E
{a}	{a}	{a}	E	E
{b}	{b}	E	{b}	E
E	E	E	E	E

$\cap$	$\emptyset$	{a}	{b}	E
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
{a}	$\emptyset$	{a}	$\emptyset$	{a}
{b}	$\emptyset$	$\emptyset$	{b}	{b}
E	$\emptyset$	{a}	{b}	E

Chapitre 5 : Calcul propositionnel et Algèbre de Boole

Fonction Booléenne

Définition

Une fonction booléenne (ou fonction logique) est une application de $\mathbb{B}_2^n \to \mathbb{B}_2$.

Exemple

$$\begin{aligned} f : \quad \mathbb{B}_2^3 &\to \mathbb{B}_2 \\ (x,y,z) &\mapsto x \cdot (y + \overline{x \cdot z}) \end{aligned}$$

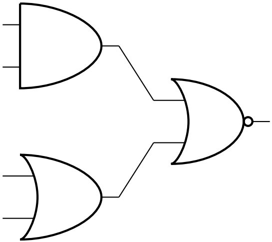
Remarque

Une table de vérité permet de préciser l'état de la sortie en fonction de l'état de l'entrée.

Composant électronique

Circuits logiques

Une fonction booléenne modélise le comportement de n'importe quel composant électronique qui, en fonction de l'état de l'entrée (des 0 et des 1 selon le niveau du courant électrique) donne un résultat en sortie (toujours sous la forme de 0 et de 1).
Ainsi un circuit logique est modélisé par la composition de plusieurs fonctions logiques.



Combien de fonctions booléennes différentes ?

Théorème

Il y a exactement

$$2^{2^n}$$

fonctions booléennes à n arguments (de arité n).

Démonstration

Définir une fonction booléenne à n arguments revient à remplir un tableau de vérité qui a 2^n lignes (une ligne pour chaque choix de 0 et de 1 de chaque argument).
Pour chacune de ces 2^n lignes, il faut choisir entre deux valeurs : 0 ou 1, ce qui donne bien

$$2^{2^n}$$

choix possibles.

Fonctions booléennes à deux arguments

Proposition

- Il y a 16 fonction booléennes à 2 arguments.
- Il y a 256 fonction booléennes à 3 arguments.
- Il y a 65536 fonction booléennes à 4 arguments.

Liste

Exercice en TD pour trouver toutes celles à 2 arguments.

Théorème

Théorème

Toutes les fonctions booléennes peuvent s'exprimer à l'aide des trois opérations élémentaires de l'algèbre de Boole :

- la somme
- le produit
- la barre

Remarque

En général, il peut y avoir plusieurs façons de l'écrire.
Par exemple pour le ou exclusif :

$$(x \cdot \overline{y}) + (\overline{x} \cdot y) \text{ où } (x + y) \cdot \overline{x \cdot y}$$

Chapitre 5 : Calcul propositionnel et Algèbre de Boole

Formules du calcul propositionnel

Définition

Une formule du calcul des propositions est une phrase construite avec les éléments suivants :

- des symboles propositionnels (atomes) : $P = \{p, p', q, q', \ldots\}$
- des symboles de liaison qui sont : $\neg$ pour la négation, $\Rightarrow$ pour l'implication et les parenthèses $()$,

En suivant les règles suivantes :

1. tout atome est une proposition
2. si F est une proposition alors $\neg F$ est aussi une proposition
3. si F et F' sont des propositions alors $(F \Rightarrow F')$ est aussi une proposition
4. toute formule est obtenue par application répétée un nombre fini de fois des étapes (1), (2), (3).

Le langage $\mathcal{L}$

Définition

On dénote par $\mathcal{L}$ l'ensemble de toutes les formules du calcul des propositions.
Il s'agit d'un langage dont les règles ci–dessus donnent la syntaxe.

Extension

On ajoute à $\mathcal{L}$ deux nouveaux symboles : $\wedge$ (et) et $\vee$ (ou) qui sont des "raccourcis" pour :

- $F \wedge F'$ est $\neg(F \Rightarrow \neg F')$
- $F \vee F'$ est $\neg F \Rightarrow F'$

Exemples de formules

Exemples

- $\neg((p \Rightarrow q) \Rightarrow (p \Rightarrow \neg p'))$ est une proposition ;
- $p \Rightarrow (\Rightarrow p))$ n'est pas une proposition.
- $((p \wedge q) \Rightarrow (p \vee q))$

Trois niveaux de langage

Il ne faut pas confondre

- le méta–langage qui est celui utilisé pour parler de la logique ;
- le langage formel $\mathcal{L}$ qui est le langage sujet ;
- l'algèbre de Boole $\mathbb{B}_2$ qui est un espace où l'on calcule.

Bien qu'il y ait des correspondances :

Notion	métalangage	$\mathcal{L}$	$\mathbb{B}_2$
disjonction	*ou*	$\vee$	$+$
conjonction	*et*	$\wedge$	$\times$
implication	*si…alors*	$\Rightarrow$	$\overline{x}+y$
négation	*non*	$\neg$	$\overline{x}$

Sémantique

Donner du sens

Une formule du calcul propositionnel n'est a priori qu'une phrase, construite en suivant certaines règles syntaxique, faisant partie d'un langage.
Ajouter du sens, c'est faire parler les symboles.
Dans notre cas, on donne un sens en définissant une interprétation de la formule.
La même formule peut avoir plusieurs interprétations : l'analyse sémantique consiste à examiner ces interprétation possibles et ce qui en découle.

Interprétation

Définition

Une interprétation est une application $I : P \to \mathbb{B}_2$ qui donne à chaque variable propositionnelle de $P = \{p, p', q \ldots\}$ une valeur de vérité 0 ou 1 dans $\mathbb{B}_2$.

Cette interprétation est étendue à toute formule F de $\mathcal{L}$ de la façon suivante :

- si $F = p \in P$ alors $I(F) = I(p)$
- si $F = \neg F'$ alors $I(F) = \overline{I(F')}$
- si $F = (F_1 \Rightarrow F_2)$ alors $I(F) = \overline{I(F_1)} + I(F_2)$

Il en découle les interprétations suivantes

- si $F = (F_1 \wedge F_2)$ alors $I(F) = I(F_1) \times I(F_2)$
- si $F = (F_1 \vee F_2)$ alors $I(F) = I(F_1) + I(F_2)$

Interprétation et Vérité

Vérité

On dit qu'une formule du calcul des propositions F est vraie pour l'interprétation I si $I(F) = 1$ et fausse si $I(F) = 0$.

Exemple

La formule

$$\neg(p \Rightarrow (q \Rightarrow \neg p'))$$

est

- vraie pour l'interprétation $I(p) = 1,\ I(q) = 1,\ I(p') = 1$
- fausse pour l'interprétation $I(p) = 0,\ I(q) = 1,\ I(p') = 1$

Tautologie

Définitions

Soit F une formule du calcul des propositions.

On dit que :

- F est une tautologie si et seulement si $\forall I : P \to \mathbb{B}_2,\ I(F) = 1$
- F est satisfaisable si et seulement si il existe une interprétation I telle que $I(F) = 1$
- F est insatisfaisable si et seulement si $\forall I : P \to \mathbb{B}_2,\ I(F) = 0$

Proposition

Si F est une tautologie, alors $\neg F$ est insatisfaisable.

Exemples

Exemples

Pour montrer que $p \vee \neg p$ est une tautologie, il y a deux méthodes possibles :

- table de vérité : chaque ligne est une interprétation possible. Pour avoir une tautologie, toutes doivent donner 1.

$I(p)$	$I(\neg p)$	$I(p \vee \neg p)$
0	1	1
1	0	1

- on utilise les propriétés de I et les connaissances de $\mathbb{B}_2$: soit I une interprétation quelconque, alors $I(p \vee \neg p) = I(p) + \overline{I(p)} = 1$

Séquents

Définition

Un séquent est un couple $(\mathcal{A}, F)$ où $\mathcal{A}$ est un ensemble fini de formules du calcul des propositions formant les hypothèses, et F une formule du calcul des propositions formant la conclusion.

Exemples

- $(\{p, q, p \Rightarrow r\}, q \Rightarrow r)$
- $(\{p \Rightarrow q, q \Rightarrow r\}, p \Rightarrow r)$

Conséquences

Définition

Soit $\mathcal{A}$ un ensemble de formules du calcul des propositions et F une formule. On dit que de $\mathcal{A}$ on déduit F lorsque

$$\forall I : P \rightarrow \mathbb{B}_2, [\text{ si } \forall \beta \in \mathcal{A} \text{ t.q. } I(\beta) = 1, \text{ alors } I(F) = 1]$$

on note

$$\mathcal{A} \models F$$

Vocabulaire

On dit que F est une conséquence de $\mathcal{A}$.
Ou encore que le séquent $(\mathcal{A}, F)$ est valide.

Exemple

Pour prouver que

$$p \Rightarrow q, q \Rightarrow r \models p \Rightarrow r$$

- on applique toutes les interprétations possibles (il y en a 8) ;
- on sélectionne celles qui rendent vraies toutes les hypothèses ;
- on vérifie que pour ces interprétations là, la conclusion est aussi vraie.

Remarque

Tautologies

Si F est une tautologie, alors le séquent $(\emptyset, F)$ est valide.

$$\models F$$

Prolongements possibles

$$\mathcal{A} \models F$$

correspond à une vérité sémantique du séquent puisqu'elle se base sur les interprétations des propositions.
Il existe une théorie de la preuve qui permet de définir quand on peut construire une preuve de F à partie des hypothèses $\mathcal{A}$. Dans ce cas on notera :

$$\mathcal{A} \vdash F$$