Algèbres de Boole et Fonctions Booléennes

Robert Rolland

R. Rolland C.N.R.S. Laboratoire de Mathématiques Discrètes
Luminy Case 930, F13288 Marseille CEDEX 9
e-mail: rolland@lmd.univ-mrs.fr

1 - La stucture d'algèbre de Boole

La structure **d'algèbre de Boole** est une structure complexe qui contient au moins les stucture suivantes

- Une structure d'**anneau de Boole**
- Une structure de **treillis de Boole**
- Une structure d'**espace vectoriel** sur le corps $\mathbb{F}_2$

Nous allons étudier ces structures et voir leurs liens.

1-1 - La structure d'anneau de Boole

Définition : Un **Anneau de Boole** est un anneau (unitaire) $\mathcal{B}$ vérifiant

AB-1) Pour tout $x \in \mathcal{B}$, $x^2 = x$.

Remarque : Cette définition n'exclut pas le cas où $\mathcal{B} = \{0\}$.

Proposition : Un anneau de Boole $\mathcal{B}$ vérifie

AB-2) $\mathcal{B}$ est commutatif.

AB-3) Pour tout $x \in \mathcal{B}$, $x \oplus x = 0$.

Remarque : L'addition de l'anneau sera notée $\oplus$ pour éviter les confusions avec le "ou" logique parfois noté $+$ par certains auteurs (et que nous noterons ici $\vee$).

1-2 - La structure de treillis de Boole

Définition : Un **treillis de Boole** $\mathcal{B}$ est un ensemble non vide ordonné qui

TB-1) pour tout couple d'éléments x et y admet une borne supérieure $x \vee y$ et une borne inférieure $x \wedge y$

TB-2) est doublement distributif (chacune des deux lois $\vee, \wedge$ est distributive par rapport à l'autre)

TB-3) admet un plus grand élément noté 1 et un plus petit élément noté 0

TB-4) est complémenté, c'est-à-dire que pour tout x il existe un unique élément $\bar{x}$ tel que $x \vee \bar{x} = 1$ et $x \wedge \bar{x} = 0$.

Remarque : On voit tout de suite sur la définition que

$$x \wedge x = x$$

$$x \vee x = x$$

$$(x \leq y) \Longleftrightarrow (x \wedge y = x)$$

$$(x \leq y) \Longleftrightarrow (x \vee y = y)$$

$$x \leq x \vee y \quad et \quad x \wedge y \leq x$$

Proposition : On a les relations suivantes

$$\overline{x \wedge y} = \overline{x} \vee \overline{y}$$

$$\overline{x \vee y} = \overline{x} \wedge \overline{y}$$

$$(y \leq z) \Longrightarrow (x \wedge y \leq x \wedge z)$$

$$(y \leq z) \Longrightarrow (x \vee y \leq x \vee z)$$

$$(x \leq y) \Longleftrightarrow (\overline{y} \leq \overline{x})$$

1-3 - Correspondance entre anneau et treillis de Boole

Théorème : Dans tout anneau de Boole $\mathcal{B}$, la relation $\leq$ définie par

$$(x \leq y) \Longleftrightarrow (xy = x)$$

est une relation d'ordre qui confère à $\mathcal{B}$ une structure de treillis de Boole dite **associée** à l'anneau de Boole.

Proposition : Le *sup*, l'inf, le *complément* du treillis de Boole associé à un anneau de Boole s'expriment en fonction des opérations de l'anneau

$$x \vee y = x \oplus y \oplus xy$$

$$x \wedge y = xy$$

$$\overline{x} = 1 \oplus x$$

Théorème : Dans tout treillis de Boole $\mathcal{B}$, les opérations définies par

$$x \oplus y = (x \wedge \overline{y}) \vee (\overline{x} \wedge y)$$

$$xy = x \wedge y$$

confèrent à $\mathcal{B}$ une structure d'anneau de Boole dite **associée** au treillis de Boole. Le 0 et le 1 du treillis sont respectivement le 0 et le 1 de l'anneau.

Ainsi dès que l'on dispose d'une des deux structures **anneau de Boole** ou **treillis de Boole** on a automatiquement l'autre.

1-4 - Structure d'espace vectoriel

Théorème : Soit $\mathcal{B}$ un anneau, treillis de Boole. En prenant comme addition l'addition de la structure d'anneau, comme corps des scalaires, le corps à deux éléments $\mathbb{F}_2$ et comme multiplication externe

$$0.x = 0 \quad et \quad 1.x = x$$

on obtient un espace vectoriel.

Cette structure comportant la structure d'anneau de Boole, la structure de treillis de Boole et la structure vectorielle est une **algèbre de Boole**.

1-5 - Exemples

Voici Quelques exemples :

- L'algèbre de Boole à deux éléments $\{0, 1\}$. c'est la seule algèbre de Boole qui soit un corps.
- L'algèbre de Boole des parties $\mathcal{P}(E)$ des parties d'un ensemble E (L'addition est la différence symétrique)
- L'algèbre de Boole des fonctions définies sur un ensemble E, à valeurs dans une algèbre de Boole. En particulier $\{0, 1\}^E$.

1-6 - Représentation des algèbres de Boole

Théorème : Toute algèbre de Boole $\mathcal{B}$ est isomorphe à l'algèbre de Boole des sous ensembles ouverts et fermés d'un espace compact totalement discontinu.

Sans faire le détail de la démonstration on peut donner une idée pour la réalisation de cet isomorphisme.

Soit $H \subset \{0,1\}^{\mathcal{B}}$ l'ensemble de tous les homomorphismes non nuls de B dans $\{0,1\}$. H est un compact totalement discontinu, et l'application qui à tout $x \in \mathcal{B}$ fait correspondre
$H(x) = \{h \in H \mid h(x) = 1\}$ est un isomorphisme de $\mathcal{B}$ sur l'algèbre de Boole des ouverts fermés de H.

Remarque : Si de plus l'algèbre $\mathcal{B}$ est complète, alors le compact dont il est question dans le théorème est un compact **extrèmement discontinu** (compact de Stone).

Dans le cas des **algèbres de Boole finies** on peut énoncer

Théorème : Toute algèbre de Boole finie a un nombre d'éléments de la forme 2^n, et elle est isomorphe à $\{0,1\}^n$.

La structure d'espace vectoriel sur $\mathbb{F}_2$ impose un nombre d'éléments de la forme 2^n. Pour avoir un isomorphisme avec $\{0,1\}^n$ il suffit de construire une base ayant des éléments deux à deux disjoints pour conclure. Ceci se fait à partir d'une base initiale $(e_i)_i$ en considérant une base extraite du système générateur $(F_J)_J$ formé par les atomes de la base initiale

$$F_j = \prod_{i \in J} e_i \prod_{i \notin J} \overline{e_i}$$

Remarque : On peut aussi dire que toute algèbre de boole finie est isomorphe à l'ensemble des parties d'un ensemble E à n éléments ou encore à l'espace des fonctions caractéristiques des parties de E, c'est à dire à l'espace des fonctions de E dans $\{0, 1\}$.

2 - Compléments sur la structure d'anneau

Soit $\mathcal{B}$ une algèbre de Boole $\neq \{0\}$. Les idéaux de l'anneau de Boole $\mathcal{B}$ peuvent aussi être définis avec les opérations du treillis grâce aux équivalences suivantes

Théorème : Soit $\mathcal{I}$ une partie de $\mathcal{B}$. Les conditions a), b), c), d) suivantes sont équivalentes (et définissent la notion d'idéal)

a) $\mathcal{I}$ possède les propriétés

a-1) $\forall x\ \forall y,\ (x \in \mathcal{I}\ et\ y \in \mathcal{I}) \Longrightarrow (x \oplus y \in \mathcal{I})$

a-2) $\forall x\ \forall y,\ (x \in \mathcal{B}\ et\ y \in \mathcal{I}) \Longrightarrow (xy \in \mathcal{I})$

b) $\mathcal{I}$ est le noyau d'un homomorphisme d'algèbres de Boole.

c) $\mathcal{I}$ possède les propriétés

c-1) $\forall x\ \forall y,\ (x \in \mathcal{I}\ et\ y \in \mathcal{I}) \Longrightarrow (x \vee y \in \mathcal{I})$

c-2) $\forall x\ \forall y,\ (x \in \mathcal{B}\ et\ y \in \mathcal{I}) \Longrightarrow (x \wedge y \in \mathcal{I})$

d) $\mathcal{I}$ possède les propriétés

d-1) $\forall x\ \forall y,\ (x \in \mathcal{I}\ et\ y \in \mathcal{I}) \Longrightarrow (x \vee y \in \mathcal{I})$

d-2) $\forall x\ \forall y,\ (x \in \mathcal{B}\ et\ y \in \mathcal{I}\ et\ x \leq y) \Longrightarrow (x \in \mathcal{I})$

De manière duale on définit la notion de **filtre** :

Définition : Une partie $\mathcal{F}$ de $\mathcal{B}$ est un **filtre** s'il existe un idéal $\mathcal{I}$ tel que

$$F = \{x \in \mathcal{B} \mid \overline{x} \in \mathcal{I}\}.$$

A partir des conditions équivalentes définissant les idéaux on obtient de manière duale des conditions équivalentes définissant les filtres.

Théorème : Soit $\mathcal{F}$ une partie de $\mathcal{B}$. Les conditions suivantes sont équivalentes (et définissent la notion de filtre)

a) Il existe un homomorphisme d'algèbres de Boole f tel que $\mathcal{F} = f^{-1}(1)$.

b) $\mathcal{F}$ possède les propriétés

b-1) $\forall x\ \forall y,\ (x \in \mathcal{F}\ et\ y \in \mathcal{F}) \Longrightarrow (x \wedge y \in \mathcal{F})$

b-2) $\forall x\ \forall y,\ (x \in \mathcal{B}\ et\ y \in \mathcal{F}) \Longrightarrow (x \vee y \in \mathcal{F})$

c) $\mathcal{F}$ possède les propriétés

c-1) $\forall x\ \forall y,\ (x \in \mathcal{F}\ et\ y \in \mathcal{F}) \Longrightarrow (x \wedge y \in \mathcal{F})$

c-2) $\forall x\ \forall y,\ (x \in \mathcal{B}\ et\ y \in \mathcal{F}\ et\ x \geq y) \Longrightarrow (x \in \mathcal{F})$

Théorème : Tout idéal premier $\mathcal{P}$ de l'anneau $\mathcal{B}$ est maximal et le quotient $\mathcal{P}/\mathcal{B}$ est le corps à deux éléments.

Théorème : Tout idéal finiment engendré $\mathcal{P}$ de l'anneau $\mathcal{B}$ est principal. En particulier si $\mathcal{B}$ est finie, tout idéal est principal.

Remarque : L'idéal principal engendré par b est $\{a \in \mathcal{B} \mid a \leq b\}$.

Théorème : Un idéal $\mathcal{I}$ est maximal si et seulement si il vérifie

$$\forall x, (x \in \mathcal{B}) \Longrightarrow \Big((x \in \mathcal{I}) \ XOR \ (\overline{x} \in \mathcal{I}) \Big).$$

Par dualité on obtient la notion de **filtre maximal** ou **ultrafiltre**.

Théorème : Un filtre $\mathcal{F}$ est maximal si et seulement si il vérifie

$$\forall x, (x \in \mathcal{B}) \Longrightarrow \Big((x \in \mathcal{F}) \ XOR \ (\overline{x} \in \mathcal{F}) \Big).$$

Dans le cas des algèbres de Boole finies, la descriptions des idéaux maximaux et des ultrafiltres est aisée. Si $\mathcal{B}$ est une algèbre de Boole finie elle est isomorphe à l'algèbre de Boole des parties d'un ensemble E ayant n élément.

Les idéaux maximaux sont les idéaux ayant pour générateur un sous ensemble de E à $n-1$ éléments (donc constitués des parties de ce sous ensemble)

les ultrafiltres sont les filtres constitués de toutes les parties qui contiennent un élément donné $a \in E$.

Remarque : Sous l'aspect fonctionnel, un idéal maximal est constitué des fonctions qui s'annulent en un point donné.

3 - Compléments sur la structure de treillis

3-1 - Rappels sur la fonction de Möbius

Soit **L** un ensemble **fini ordonné** par une relation notée $\leq$.

Définition : Pour tout entier $p \geq 0$ et tout couple (x, y) d'éléments de **L** tels que $x \leq y$ on appelle chaîne de longueur p joignant x à y toute suite finie $(x_0, x_1, \cdots, x_p)$ d'éléments de **L** tels que

$$x = x_0 < x_1 < \cdots < x_p = y.$$

On note $c_p(x, y)$ le nombre de ces chaînes.

Il est clair que

- $c_0(x,x) = 1$
- $c_0(x,y) = 0$ pour $x < y$
- $c_p(x,x) = 0$ pour $p > 0$
- $c_1(x,y) = 1$ pour $x < y$

Proposition : On dispose des relations de récurrence suivantes entre les nombres $c_p(x,y)$:

$$c_{p+1}(x,y) = \sum_{x \leq z < y} c_p(x,z)$$

$$c_{p+1}(x,y) = \sum_{x < z \leq y} c_p(z,y)$$

Définition : La fonction de Möbius $\mu_{\mathbf{L}}$ de l'ensemble ordonné $\mathbf{L}$ est la fonction définie sur $\mathbf{L} \times \mathbf{L}$ à valeurs dans $\mathbb{Z}$ par

$$\mu_{\mathbf{L}}(x, y) = \sum_{p \geq 0} (-1)^p c_p(x, y).$$

Proposition : La fonction $\mu_{\mathbf{L}}$ vérifie

$$\mu_{\mathbf{L}}(x, x) = 1$$

et si $x < y$

$$\sum_{x \leq z \leq y} \mu_{\mathbf{L}}(x, z) = 0$$

$$\sum_{x \leq z \leq y} \mu_{\mathbf{L}}(z, y) = 0.$$

Soit f une fonction définie sur $\mathbf{L}$ à valeurs dans un groupe abélien $\mathbf{G}$. Posons

$$g(x) = \sum_{y \leq x} f(y).$$

Théorème d'inversion de Rota: Il est possible de retrouver la fonction f connaissant la fonction g grâce à la formule

$$f(x) = \sum_{y \leq x} \mu_{\mathbf{L}}(y, x) g(y).$$

Exemple : On se place dans l'ensemble $\mathbf{N}$ des nombres naturels. Soit $n \in \mathbf{N}$ et $\mathbf{L}$ l'ensemble des diviseurs de n ordonné par la relation de divisibilité. La fonction de Möbius dans ce cas est

$$\mu_{\mathbf{L}}(r, s) = \mu(s/r)$$

où μ est la fonction de Möbius classique donnée par

$$\mu(1) = 1$$

si $p_1, p_2, \cdots, p_k$ sont des nombres premiers distincts

$$\mu(p_1.p_2 \cdots p_k) = (-1)^k$$

et dans tous les autres cas

$$\mu(r) = 0.$$

3-1 - Cas des algèbres de Boole finies

Soit S un ensemble fini et $\mathbf{L} = \mathcal{P}(S)$ l'ensemble des parties de S ordonné par inclusion. La fonction de Möbius dans ce cas est

$$\mu_{\mathbf{L}}(A, B) = (-1)^{\sharp B - \sharp A}$$

si $A \subset B$ et 0 sinon.

Preuve : La démonstration se fait par récurrence sur $\sharp(B - A)$. Si $\sharp(B - A) = 0$ (cas où A=B) le résultat est vrai (on obtient bien $\mu_{\mathbf{L}}(A, A) = 1$). Supposons le résultat vrai pour toutes les parties $A \subset B$ telles que $\sharp(B - A) = k$ et montrons le résultat pour un couple B, A , où $A \subset B$ et $\sharp(B - A) = k + 1$.

Alors

$$\sum_{A \subset T \subset B} \mu_{\mathbf{L}}(A, T) = 0$$

et par hypothèse de récurrence

$$\sum_{A \subset T \subsetneq B} (-1)^{\sharp T - \sharp A} + \mu_{\mathbf{L}}(A, B) = 0.$$

Or ily a autant de parties entre A et B ayant un nombre pair d'éléments que de parties ayant un nombre impair d'éléments par suite

$$\sum_{A \subset T \subset B} (-1)^{\sharp T - \sharp A} = 0$$

donc

$$\mu_{\mathbf{L}}(A, B) = (-1)^{\sharp B - \sharp A}.$$

4 - Fonctions Booléenes

Si E est un ensemble non vide et $\mathcal{B}$ une algèbre de Boole, nous pouvons définir sur l'espace des fonctions de E dans $\mathcal{B}$ une structure d'algèbre de Boole en prenant pour opérations les opérations habituelles sur les fonctions définies à partir des opérations sur les images, c'est-à-dire

$$(f+g)(x) = f(x) + g(x)$$

$$(fg)(x) = f(x)g(x)$$

$$(f \leq g) \Longleftrightarrow (\forall x \;\; (x) \leq g(x))$$

$$(sup(f,g))(x) = f(x) \vee g(x)$$

$$(inf(f,g))(x) = f(x) \wedge g(x).$$

Nous allons étudier plus particulièrement le cas des fonctions de $\mathbb{F}_2^m$ dans $\mathbb{F}_2^k$ puisque ce cas correspond à un appareil admettant en entrée m signaux digitaux et donnant en sortie k signaux digitaux fonctions des signaux d'entrée.

Remarquons qu'une telle fonction de m variables booléennes (i.e. variables prenant les valeurs 0 et 1) donnant k variables booléennes est connue par la donnée de k fonctions booléennes de m variables booléennes (ce qui revient à considérer séparément chaque signal en sortie).

Si bien qu'en définitive ce que nous allons étudier c'est l'espace $\mathcal{F}_m$ des fonctions de $\mathbb{F}_2^m$ dans $\mathbb{F}_2$.

4-1 - Notations

Pour tout i tel que $1 \leq i \leq m$ notons X_i la fonction de $\mathcal{F}_m$ qui à $x = (x_1, ..., x_m)$ fait correspondre x_i. Notons aussi $\overline{X_i}$ le complément de la fonction X_i, c'est-à-dire la fonction $1 + X_i$.

Si u est un élément de $\mathbb{F}_2^m$ définissons le **support** de u où $u = (u_1, .., u_m)$ par

$$supp(u) = \{i \mid u_i \neq 0\}.$$

4-2 - La base atomique

Pour tout $u \in \mathbb{F}_2^m$ notons e_u la fonction définie par

$$e_u(v) = \begin{cases} 0 & si \quad v \neq u \\ 1 & si \quad v = u. \end{cases}$$

On vérifie que la famille $(e_u)_{u \in \mathbb{F}_2^m}$ est une base de $\mathcal{F}_m$ et que la décomposition d'une fonction f sur cette base se fait sous la forme

$$f = \sum_u f(u) e_u.$$

La composante de f sur e_u est donc la valeur de f au point u.

Cette décomposition très simple fait jouer aux fonctions e_u un rôle très important. On peut voir que ces fonctions s'expriment sous diverses formes commodes qui les relient à des polynômes

$$e_u = \prod_{i \in supp(u)} X_i \prod_{i \notin supp(u)} \overline{X_i}$$

ou encore

$$e_u = \prod_{i=1}^{m} (X_i + \overline{u_i}).$$

Remarquons encore que les fonctions e_u sont disjointes si bien que toute fonction s'écrit aussi

$$f = \bigvee_{\{u|f(u)\neq 0\}} e_u = \bigvee_{\{u|f(u)\neq 0\}} \left((\bigwedge_{i\in supp(u)} X_i) \wedge (\bigwedge_{i\notin supp(u)} \overline{X_i}) \right)$$

Ainsi toute fonction s'écrit comme une disjonction de conjonctions. Par passage au complémentaire il est facile de montrer que f s'écrit aussi comme conjonction de disjonctions

$$f = \bigwedge_{\{u|f(u)=0\}} \overline{e_u} = \bigwedge_{\{u|f(u)=0\}} \left((\bigvee_{i\in supp(u)} X_i) \vee (\bigvee_{i\notin supp(u)} \overline{X_i}) \right)$$

4-3 - La base des monômes

L'écriture des fonctions e_u sous forme polynômiale montre que toute fonction booléenne de m variables booléennes est une fonction polynômiale en m variables, de degré total inférieur ou égal à m et de degré au plus 1 par rapport à chacune des variables (puisque $X^2 = X$).

Pour tout $u \in \mathbb{F}_q^m$ notons ϵ_u la fonction définie par

$$\epsilon_u = X_1^{u_1} X_2^{u_2} ... X_m^{u_m} = \prod_{i \in supp(u)} X_i.$$

Ces fonctions forment aussi une base de l'espace $\mathcal{F}_m$.

Rappelons que la relation d'ordre du treillis de Boole $\mathbb{F}_2^m$ s'écrit

$$(u \leq v) \Longleftrightarrow (supp(u) \subset supp(v)).$$

On vérifie que

$$\epsilon_u(v) = \begin{cases} 1 & si \qquad u \leq v \\ 0 & sinon. \end{cases}$$

Ce qui donne encore

$$\epsilon_u = \sum_{v \geq u} e_v$$

et aussi (formule d'inversion de type Mobius)

$$e_u = \sum_{v \geq u} \epsilon_v.$$

En conséquence si on note $\tilde{f}(v)$ la composante sur ϵ_v de la fonction f on obtient

$$\tilde{f}(v) = \sum_{u \leq v} f(u)$$

et

$$f(u) = \sum_{v \leq u} \tilde{f}(v).$$

La fonction

$$\tilde{f} = \sum_{u} \tilde{f}(u) e_u$$

est appelée **transformée de Reed Muller de** f. On vérifie aisément que

$$\tilde{\tilde{f}}(u) = f(u).$$