ALGEBRES DE BOOLES - FONCTIONS BOOLEENNES

R.Rolland

30 Septembre 1996

1 Introduction

Les notes qui suivent constituent une première approche des algèbres de Boole et des fonctions booléennes. Le sujet est très vaste et pourrait donner lieu à bien des développements algébriques avec des incursions dans divers domaines des mathématiques comme par exemple la théorie de la mesure, les filtres, les espaces compacts, la logique etc... Aussi s'est on limité pour ce cours à un exposé restreint à l'usage des applications les plus directes que sont les circuits électroniques, les codes correcteurs d'erreurs, les signaux digitaux. L'accent est mis sur le cas des algèbres de Boole finies et notamment sur les espaces de fonctions booléennes de plusieurs variables booléennes.

2 Exemples

2.1 Le corps à 2 éléments $\{0, 1\}$

L'ensemble à deux éléments $\{0, 1\}$ est d'une grande importance puisqu'il est à la base des signaux digitaux, de la logique binaire et de beaucoups d'applications dans divers domaines des mathématiques. Il joue un rôle particulier parmi les algèbres de Boole, d'une part car c'est évidemment la plus simple et d'autre part car c'est le seul anneau booléen qui est un corps. Il dispose de diverses structures que nous allons voir ici et qui se généralisent, avec des applications intéressantes, à des ensembles plus compliqués.

2.1.1 La structure de corps

Dans un premier temps on considère $\{0,1\}$ comme $\mathbf{Z}/2\mathbf{Z}$, c'est-à-dire l'ensemble des classes d'entiers modulo 2. On dispose alors de deux opérations "+" et "." qui donnent à cet ensemble une structure de corps (anneau dans lequel tout élément non nul a un inverse).

Voici la table d'addition

+	0	1
0	0	1
1	1	0

et la table de multiplication

.	0	1
0	0	0
1	0	1

Ce corps, comme tous les corps finis, est commutatif. Les identités suivantes ont lieu

$$a + a = 0$$
$$a^2 = a.$$

2.1.2 La structure de treillis

On définit sur $\{0,1\}$ une relation d'ordre $\leq$ en posant $0 \leq 1$. Il est facile de vérifier alors que

$$(a \leq b) \Longleftrightarrow (ab = a).$$

Pour cette relation d'ordre on dispose pour tout couple d'éléments (x, y) d'une borne supérieure notée $x \vee y$ et d'une borne inférieure notée $x \wedge y$. On a alors une structure de treillis dont les opérations $\vee$ et $\wedge$ sont liées à la multiplication et à l'addition par les identités suivantes

$$x \wedge y = x.y$$
$$x \vee y = x + y + x.y \ .$$

Il existe un plus grand élément (un maximum) qui est 1, et un plus petit élément (un minimum) qui est 0. Pour tout élément x il existe un unique complément de x noté $\bar{x}$ qui vérifie

$$x \vee \bar{x} = 1$$

$$x \wedge \bar{x} = 0.$$

On peut alors exprimer entièrement les opérations de la structure de corps en fonctions de celles de la structure de treillis

$$x.y = x \wedge y$$

$$x + y = (x \wedge \bar{y}) \vee (\bar{x} \wedge y) = (x \vee y) \wedge (\overline{x \wedge y}).$$

On vérifie aussi que

$$\bar{x} = 1 + x.$$

L'opération "$\vee$" est distributive par rapport à l'opération "$\wedge$" et l'opération "$\wedge$" est distributive par rapport à l'opération "$\vee$", ce qui veut dire que

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

De plus le passage au complément se comporte de la fçon suivante

$$\overline{a \vee c} = \bar{a} \wedge \bar{c}$$

$$\overline{a \wedge c} = \bar{a} \vee \bar{c}.$$

La table de l'opération "$\wedge$" est la même que la table de multiplication, la table de l'opération "$\vee$' est

$\vee$	0	1
0	0	1
1	1	1

2.2 L'algèbre $\mathcal{P}(E)$ des parties d'un ensemble E

Soit E un ensemble non vide et $\mathcal{P}(E)$ l'ensemble des parties de E. On a de façon très naturelle une structure de treillis sur $\mathcal{P}(E)$ en prenant comme relation d'ordre l'inclusion. La borne supérieure de deux éléments est alors leur réunion et la borne inférieure leur intersection. Le complément d'un élément A est son complémentaire dans E. On définit alors une multiplication en prenant l'intersection, et une addition en prenant la différence symétrique

$$AB = A \cap B$$
$$A \oplus B = (A \cup B) \cap (\overline{A \cap B}).$$

On obtient ainsi un anneau commutatif qui vérifie pour tout élément A

$$A^2 = A$$
$$A + A = 0.$$

Remarquons que $\mathcal{P}(E)$ peut être représenté comme l'ensemble des applications de E dans $\{0, 1\}$. En effet il suffit de faire correspondre à toute partie A de E la fonction de E dans $\{0, 1\}$ qui vaut 1 sur A et 0 sur le complémentaire de A (fonction caractéristique de A). Si on muni l'ensemble des fonctions caractéristiques de l'addition des fonctions (à valeurs dans le corps $\{0, 1\}$) et de la multiplication des fonctions on obtient un anneau isomorphe à l'anneau $\mathcal{P}(E)$. On constate en effet que

$$f_A + f_b = f_{A \oplus B}$$

et que

$$f_A f_B = f_{A \cap B}.$$

De plus on peut aussi remarquer que cet isomorphisme respecte la structure d'ordre

$$(f_A \leq f_B) \Longleftrightarrow (A \subset B).$$

3 La structure d'algèbre de Boole

Munis des deux exemples fondamentaux précédents nous pouvons maintenant dégager un certain nombre de structures dont on pourra voir qu'elles sont intimement liées.

3.1 La structure d'anneau de Boole

Un **anneau de Boole** est un anneau (unitaire) $\mathcal{B}$ qui vérifie pour tout élément $x \in \mathcal{B}$ l'identité $x^2 = x$.

Un anneau de Boole $\mathcal{B}$ vérifie les propriétés suivantes

- Pour tout x de $\mathcal{B}$ on a $x + x = 0$.
- L'anneau $\mathcal{B}$ est commutatif.

3.2 La structure de treillis de Boole

Un **treillis de Boole** $\mathcal{B}$ est un ensemble, ayant au moins deux éléments, ordonné qui

- pour tout couple d'éléments x et y admet une borne supérieure $x \vee y$ et une borne inférieure $x \wedge y$
- est doublement distributif (chacune des deux lois $\vee, \wedge$ est distributive par rapport à l'autre)
- admet un plus grand élément noté 1 et un plus petit élément noté 0
- 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 $x \wedge \bar{x} = 0$.

3.3 Liens entre treillis et anneaux de Boole

Nous allons voir qu'un anneau de Boole a naturellement une stucture de treillis de Boole et réciproquement.

3.3.1 Un anneau de Boole est un treillis de Boole

Soit donc $\mathcal{B}$ un anneau de Boole. Définissons alors une relation d'ordre $\leq$ sur $\mathcal{B}$ de la manière suivante

$$(a \leq b) \Longleftrightarrow (ab = a).$$

Il est alors facile de voir qu'on a pour tout couple d'éléments une borne supérieure et une borne inférieure en posant

$$x \vee y = x + y + xy$$

$$x \wedge y = xy$$

que la double distributivité est réalisée.

On voit que l'élément neutre de l'addition 0 est le plus petit élément et que l'élément neutre de la multiplication 1 est le plus grand élément.

Enfin tout élément a un unique complémentaire obtenu en posant

$$\bar{x} = 1 + x.$$

3.3.2 Un treillis de Boole est un anneau de Boole

Soit maintenant $\mathcal{B}$ un treillis de Boole. Définissons alors

$$x + y = (x \wedge \bar{y}) \vee (\bar{x} \wedge y)$$

et

$$xy = x \wedge y.$$

On montre facilement qu'on obtient ainsi un anneau de Boole. L'élément neutre de l'addition est le 0 du treillis de Boole et l'élément neutre pour la multiplication est le 1 du treillis de Boole. Il est clair aussi que le treillis associé à cet anneau est le treillis dont on est parti.

La conclusion est que les opérations d'anneau de Boole et de treillis de Boole coexistent dans une même structure appelée **algèbre de Boole**.

En particulier pour manipuler des expressions dans une algèbre de Boole on peut utiliser toutes les possibilités des diveses lois introduites, y compris le passage au complémentaire.

3.3.3 La structure d'espace vectoriel

Toute algèbre de Boole a une structure d'espace vectoriel sur le corps $\{0, 1\}$. Définissons en effet la multiplication par un scalaire (élément du corps de base) en posant

$$0.x = 0$$

$$1.x = x$$

On peut montrer facilement qu'on obtient ainsi en conjonction avec l'addition de l'anneau de Boole un structure d'espace vectoriel et d'algèbre si on prend de plus en compte la multiplication. C'est ceci qui motive en fait le nom d'**algèbre de Boole**.

3.3.4 Algèbre de Boole ayant une structure de corps

Nous avons vu que la structure d'anneau de l'algèbre de Boole $\{0, 1\}$ est en fait une structure de corps. D'autres algèbres de Boole sont elles dans ce cas? La réponse est non.

Pour cela s'il existe un élément x qui n'est ni 0 ni 1 alors $\bar{x} = 1 + x$ n'est ni 0 ni 1. Le produit $x\bar{x}$ est nul. Ce qui montre que l'anneau de boole en question a des diviseurs de zéro, donc n'est pas un corps. Attention, nous avons montré que la structure d'anneau de l'algèbre de Boole n'est pas si cette algèbre a plus de deux éléments une structure de corps, mais ceci ne veut pas dire qu'en définissant d'autres opérations on ne puisse pas avoir une structure de corps. Au contraire on ne se privera pas de munir $\{0, 1\}^m$ par exemple d'une structure de corps en définissant une autre multiplication. Mais ceci entre dans une autre étude.

4 Le cas des algèbres de Boole finies

Si $\mathcal{B}$ est une algèbre de Boole finie, alors c'est nécessairement un espace vectoriel de dimension finie sur $\{0, 1\}$. Donc $\mathcal{B}$ est isomorphe (en tant qu'espace vectoriel) à $\{0, 1\}^m$ où m est la dimension de l'espace vectoriel. Comment se réalise alors la multiplication sur $\{0, 1\}^m$? De la façon suivante

$$(u_1, u_2, ..., u_m).(v_1, v_2, ..., v_m) = (u_1.v_1, u_2.v_2, ..., u_m.v_m).$$

Et par suite la relation d'ordre s'écrit en introduisant le support d'un élément u de $\{0, 1\}^m$

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

où

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

Ceci prouve en particulier qu'une algèbre de Boole finie a toujours une cardinalité qui est une puissance de 2.

On peut aussi considérer qu'un élément de $\{0,1\}^m$ est une fonction de $\{1,2,..,n\}$ dans $\{0,1\}$, et une telle fonction comme décrivant un sous ensemble de $\{1,2,..,n\}$. Si bien qu'on peut dire aussi que toute algèbre de Boole finie est l'algèbre de Boole des parties d'un ensemble fini.

Nous utiliserons ces diverses représentations suivant leur commodité compte tenu des problèmes posés.

5 Les fonctions booléennes

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

$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x)$$
$$(f \leq g) \Longleftrightarrow (\forall x \quad f(x) \leq g(x))$$
$$(sup(f,g))(x) = f(x) \vee g(x)$$
$$(inf(f,g))(x) = f(x) \wedge g(x).$$

Nous allons étudier plus particulièrement le cas des fonctions de $\{0,1\}^m$ dans $\{0,1\}^k$ 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 $\{0,1\}^m$ dans $\{0,1\}$.

5.1 Diverses bases de $\mathcal{F}_m$

5.1.1 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 $\{0,1\}^m$ définissons le **support** de u où $u = (u_1, .., u_m)$

Sur $\{0,1\}^m$ nous noterons

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

5.1.2 La base atomique

Pour tout $u \in \{0,1\}^m$ 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 $(e_u)_{u \in \{0,1\}^m}$ 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

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

5.1.3 La base des monomes

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 $u \in \{0,1\}^m$ 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 $\{0,1\}^m$ 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

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