Première partie
Algèbre de Boole

I Fonctions booléennes

I.1 Définitions

Définition : Une fonction booléenne à n variables ($\Leftrightarrow$ d'arité n) est une application

$$f : \mathbb{B}^n \longrightarrow \mathbb{B}$$

qui à un $n-$uplet de booléens associe un booléen.

Remarque : On note $\mathbb{F}_n$ l'ensemble des fonctions d'arité n et

$$\mathbb{F} = \bigcup_{n=0}^{\infty} \mathbb{F}_n$$

Définition : Toute fonction booléenne $f \in \mathbb{F}_n$ possède une fonction duale notée f^* telle que :

$$f^*(x_1, ...x_i, ..., x_n) = \overline{f}(\overline{x_1}, ..., \overline{x_i}, ..., \overline{x_n})$$

I.2 Fonctions usuelles

I.2.1 Fonctions de $\mathbb{F}_0$

Il existe 2 fonctions dans $\mathbb{F}_0$:

$$\mathbf{0} : \begin{array}{l} \longrightarrow \mathbb{B} \\ \longmapsto 0 \end{array} \quad \text{et} \quad \mathbf{1} : \begin{array}{l} \longrightarrow \mathbb{B} \\ \longmapsto 1 \end{array}$$

Ces deux fonctions sont bien évidemment des constantes.

I.2.2 Fonctions de $\mathbb{F}_1$

F_1 contient 4 éléments : les deux fonctions constantes

$$\mathbf{0} : \begin{array}{ccc} \mathbb{B} & \longrightarrow & \mathbb{B} \\ x & \longmapsto & 0 \end{array} \quad \text{et} \quad \mathbf{1} : \begin{array}{ccc} \mathbb{B} & \longrightarrow & \mathbb{B} \\ x & \longmapsto & 1 \end{array}$$

ainsi que deux fonctions de projections (positive et négative) :

$$\textbf{identité} : \begin{array}{ccc} \mathbb{B} & \longrightarrow & \mathbb{B} \\ x & \longmapsto & x \end{array} \quad \text{et} \quad \textbf{négation} : \begin{array}{ccc} \mathbb{B} & \longrightarrow & \mathbb{B} \\ x & \longmapsto & \overline{x} \end{array}$$

I.2.3 Fonctions de $\mathbb{F}_2$

F_2 contient 16 éléments : les deux fonctions constantes

$$\mathbf{0} : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & 0 \end{array} \quad \text{et} \quad \mathbf{1} : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & 1 \end{array}$$

deux fonctions de projections

$$x_1 : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & x_1 \end{array} \quad \text{et} \quad x_2 : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & x_2 \end{array}$$

deux fonctions de négations :

$$\textbf{négation de } x_1 : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & \overline{x_1} \end{array} \quad \text{et} \quad \textbf{négation de } x_2 : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & \overline{x_2} \end{array}$$

les fonctions "somme" (ou) et "produit" (et) :

$$\textbf{ou} : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & x_1 + x_2 \end{array} \quad \text{et} \quad \textbf{et} : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & x_1 \times x_2 \\ \multicolumn{3}{c}{(\textit{également noté } x_1.x_2)} \end{array}$$

les fonctions "implique" et "est impliqué par" :

$$\Rightarrow : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & \overline{x_1} + x_2 \end{array} \quad \text{et} \quad \Leftarrow : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & x_1 + \overline{x_2} \end{array}$$

les fonctions $\downarrow$ (nor) et $\uparrow$ (nand) :

$$\downarrow : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & \overline{x_1 + x_2} \end{array} \quad \text{et} \quad \uparrow : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & \overline{x_1.x_2} \end{array}$$

les fonctions "n'implique pas" et "n'est pas impliqué par" :

$$\not\Rightarrow : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & x_1.\overline{x_2} \end{array} \quad \text{et} \quad \not\Leftarrow : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & \overline{x_1}.x_2 \end{array}$$

enfin, les fonctions "équivalent" et "ou exclusif" :

$$\Leftrightarrow : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & x_1.x_2 + \overline{x_1}.\overline{x_2} \end{array} \quad \text{et} \quad \oplus : \begin{array}{ccc} \mathbb{B}^2 & \longrightarrow & \mathbb{B} \\ (x_1, x_2) & \longmapsto & x_1.\overline{x_2} + \overline{x_1}.x_2 \end{array}$$

I.3 Propriétés

Les fonctions que nous venons de présenter possèdent un certain nombre de propriétés dont les suivantes :

$\overline{0} = 1$	$\overline{1} = 0$	$\overline{\overline{x}} = x$	$0 + x = x + 0 = x$
$1 + x = x + 1 = 1$	$0.x = x.0 = 0$	$1.x = x.1 = x$	$x + x = x$
$x.x = x$	$x + y = y + x$	$x.y = y.x$	$x + x.y = x$
$x + \overline{x} = 1$	$x.\overline{x} = 0$	$x \oplus 0 = 0 \oplus x = x$	$1 \oplus x = x \oplus 1 = \overline{x}$
$x.(y + z) = x.y + x.z$	$x + y.z = (x + y).(x + z)$	$x \oplus x = 0$	$x.(y \oplus z) = x.y \oplus x.z$
lois de De Morgan :	$\overline{x + y} = \overline{x}.\overline{y}$	$\overline{x.y} = \overline{x} + \overline{y}$	

II Différentes écritures d'une fonction booléenne

II.1 Monômes

Définition : Un monôme conjonctif est une fonction booléenne qui s'écrit sous la forme d'un produit de projections et de négations où chaque variable intervient au plus une fois. Autrement dit, si on considère un sous-ensemble I de [1,n] :

$$\prod_{i \in I} x_i^{\epsilon_i}$$

où $x_i^{\epsilon_i} = x_i$ ou $\overline{x_i}$

Définition : Un monôme disjonctif est une fonction booléenne qui s'écrit sous la forme d'une somme de projections et de négations où chaque variable intervient au plus une fois. Autrement dit, si on considère un sous-ensemble I de [1,n] :

$$\sum_{i \in I} x_i^{\epsilon_i}$$

où $x_i^{\epsilon_i} = x_i$ ou $\overline{x_i}$

Définition : Un monôme est canonique si chaque variable intervient exactement une fois.

II.2 Formes de Lagranges

II.2.1 Support d'une fonction booléenne

Définition : Le support $S_n(f)$ d'une fonction $f \in \mathbb{F}_n$ est l'ensemble des $n-$uplets $(x_1, ..., x_n) \in \mathbb{B}^n$ tels que $f(x_1, ..., x_n) = 1$

Remarque : On a les trois résulats suivants :

$$S_n\left(\sum_{i=1}^{p} f_i\right) = \bigcup_{i=1}^{p} S_n(f_i)$$

$$S_n\left(\prod_{i=1}^{p} f_i\right) = \bigcap_{i=1}^{p} S_n(f_i)$$

$$S_n(\overline{f}) = \overline{S_n(f)}$$

II.2.2 Formes normales de Lagrange

Théorème : Toute fonction booléenne peut s'écrire comme somme de monômes conjonctifs canoniques.

Remarque : On utilise pour cela le support de la fonction et on obtient l'écriture :

$$f(x_1, ..., x_n) = \sum_{(\epsilon_1,...,\epsilon_n)\in S_n(f)} \left(\prod_{i=1}^{n} x_i^{\epsilon_i} \right)$$

où $x_i^{\epsilon_i} = \begin{cases} x_i \text{ si } \epsilon_i = 1 \\ \overline{x_i} \text{ si } \epsilon_i = 0 \end{cases}$

Cette écriture s'appelle la forme normale de Lagrange disjonctive conjonctive.

Théorème : Toute fonction booléenne peut s'écrire comme produit de monômes disjonctifs canoniques.

Remarque : La dualité est involutive : $f^{**} = f$

III Simplification de fonctions booléennes

III.1 Définitions

Définition : Soient f et g deux fonctions booléennes, on définit la relation d'ordre partiel "plus petite que" notée $\leq$ par :

$$f \leq g \Leftrightarrow S_n(f) \subset S_n(g)$$

Remarque : Si $f \leq g$ alors $f + g = g$ et $f.g = f$

Définition : Un monôme m est maximal pour une fonction $f \in \mathbb{F}_n$ ssi
- m est un monôme conjonctif
- $m \leq f$
- $\forall m'$ monôme conjonctif, $m \leq m' \leq f \Rightarrow m = m'$

Définition : Un monôme maximal m est central ssi

$$\nexists\, m_1, ..., m_n \in M(f) \backslash \{m\} \text{ tels que } m \leq \sum_{i=1}^{n} m_i$$

IV Composition de fonctions booléennes

IV.1 Fonctions booléennes obtenues par composition

Définition : (principe de composition) Soit f une fonction booléenne à n variables et $g_1, ..., g_n$ n fonctions d'arité m. La fonction h définie par

$$h(x_1, ..., x_m) = f(g_1(x_1, ..., x_m), ..., g_n(x_1, ...x_m))$$

est une fonction booléenne à m variables, on la note $Cp(f, g_1, ..., g_n)$

Définition : Soit E un ensemble de fonctions booléennes. $comp(E)$ est l'ensemble des fonctions booléennes obtenues par composition à partir :
- des projections : $x_1, ..., x_n$
- des fonctions de E

Exemple : Soit $E = \{+, x \mapsto \overline{x}\}$. La fonction "implique" ($\Rightarrow$) appartient à $comp(E)$ car elle peut s'écrire en utilisant uniquement les fonctions de E et les fonctions projections :

$$x_1 \Rightarrow x_2 = \overline{x_1} + x_2$$

IV.2 Parties génératrices

Définition : E est une partie génératrice ssi $comp(E) = \mathbb{F}$

Définition : E est une partie génératrice minimale ssi
- E est une partie génératrice
- il n'existe pas de sous-partie E' et E, $E' \neq E$ telle que E' soit une partie génératrice

Théorème : Soient les 5 propriétés suivantes :
$P_1 : f(0, ..., 0) = 0$
$P_2 : f(1, ..., 1) = 1$
$P_3 : f = f^*$
$P_4 : f$ croissante
$P_5 : f \in comp(\{0, 1, \oplus\})$
Une partie E est génératrice ssi pour chaque propriété P_i, il existe au moins un élément de E qui ne vérifie pas P_i : $comp(E) = \mathbb{F} \quad \Leftrightarrow \quad \forall i \in \{1, 2, 3, 4, 5\}, \exists e \in E, e \notin P_i$