LOG : Algèbre de Boole - Fonctions booléennes

Soient :

- $\mathbb{B} = 0, 1$ l'ensemble des booléens
- $\mathbb{B}^n$ l'ensemble des n-uplets de booléens
- $card(\mathbb{B}^n) = 2^n$

Définition : Fonction booléenne
Une fonction booléenne f à n variables est une application de $\mathbb{B}^n$ vers $\mathbb{B}$

- $\mathbb{F}_n$ est l'ensemble des fonctions booléennes à n variables. $card(\mathbb{F}_n) = 2^{2^n}$
- $\mathbb{F}$ est l'ensemble des fonctions booléennes, $\mathbb{F} = \bigcup_{i \in \mathbb{N}} \mathbb{F}_i$

Définitions/Remarques :

- 0 et 1 sont les fonctions constantes
- $+$ est l'addition booléenne ou le **OU (OR)** logique (Aussi appelé disjonction)
- $*$ est la multiplication booléenne ou le **ET (AND)** logique (Aussi appelé conjonction)
- **NOR** et **NAND** sont respectivement les négations de $+$ et $*$
- $x_1 \Rightarrow x_2$ équivaut à $\overline{x_1} + x_2$
- $\Leftrightarrow$ équivaut à $x_1 x_2 + \overline{x_1 x_2}$
- $\not\Leftrightarrow$ est la négation de l'équivalence logique, notée aussi $\oplus$ (**XOR**) équivalent à $\overline{x_1} x_2 + x_1 \overline{x_2}$
- $x_1 \not\Rightarrow x_2$ équivaut à $x_1 \overline{x_2}$

Propriétés des fonctions usuelles

- $\overline{0} = 1$; $\overline{1} = 0$; $\overline{\overline{x}} = x$
- $0 + x = x + 0 = x$ (0 élément neutre de $+$)
- $1x = x1 = x$ (1 élément neutre de .)
- $1 + x = x + 1 = 1$ (1 élément absorbant de $+$
- $0x = x0 = 0$ (0 élément absorbant de .)
- $x + x = x$; $xx = x$ (Idempotence de $+$ et .)
- $x + y = y + x$; $xy = yx$ (Commutativité de $+$ et .)
- $x + (y + z) = (x + y) + z$; $x(yz) = (xy)z$ (Associativité de $+$ et .
- $x + \overline{x} = 1$; $x\overline{x} = 0$
- $\overline{x + y} = \overline{x}.\overline{y}$; $\overline{x.y} = \overline{x} + \overline{y}$ (Lois de De Morgan)
- $x(y + z) = xy + yz$;$x + yz = (x + y)(x + z)$ (Distributivité à gauche de . par rapport à $+$ et de $+$ par rapport à .)
- $(x + y)z = xz + yz$;$xy + z = (x + z)(y + z)$ (Distributivité à droite de . par rapport à $+$ et de $+$ par rapport à .)
- $\mathbb{Z}/2\mathbb{Z} = \mathbb{B}$; $(\mathbb{Z}/2\mathbb{Z}, \oplus, x)$ est un corps.

Définition : Fonctions monômes

- Un monôme conjonctif est une fonction booléenne obtenue par **PRODUIT** de fonctions projections ou négations. Une projection et sa négation ne peuvent pas être présentes simultanément dans un monôme. Ainsi 0 n'est pas un monôme conjonctif.
- Un monôme disjonctif est une fonction booléenne obtenue par **SOMME** de projections ou négations. Une projection et sa négation ne peuvent pas être présentes simultanément dans un monôme. Ainsi 1 n'est pas un monôme disjonctif.
- Un monôme à n variables est dit canonique si toutes les variables de 1 à n interviennent dans son écriture.

Définition : Support d'une fonction booléenne
Soit f une fonction booléenne à n variables. Le support de f est $S_n(f) = \{\epsilon | \epsilon \in \mathbb{B}^n \;\; et \;\; f(\epsilon) = 1\}$

Proposition :
Soient f et g deux fonctions de $\mathbb{F}_n$, on a :

- $S_n(f+g) = S_n(f) \cup S_n(g)$
- $S_n(f.g) = S_n(f) \cap S_n(g)$
- $S_n(\overline{f} = \overline{S_n(f)}$

Théorème de Lagrange (Première forme)
Soit $f \in \mathbb{F}_n$, f s'écrit de manière unique comme somme de monômes conjonctifs canoniques sous la forme suivante :

$$f(x_1, ..., x_n) = \sum_{(\epsilon_1, ..., \epsilon_n) \in S_n(f)} x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n} = \sum_{\epsilon \in S_n(f)} = x^{\epsilon} = \sum_{\epsilon \in \mathbb{B}^n} f(\epsilon) x^{\epsilon}$$

Avec $x_i^{\epsilon_i} = \begin{cases} x_i & si \;\; \epsilon_i = 1 \\ \overline{x_i} & sinon \end{cases}$ ***Théorème de Lagrange (Seconde forme)***

Soit $f \in \mathbb{F}_n$, f s'écrit de manière unique comme produit de monômes disjonctifs canoniques sous la forme suivante :

$$f(x_1, ..., x_n) = \prod_{\epsilon_1, ..., \epsilon_n) \in \overline{S_n(f)}} \left(x_1^{\overline{\epsilon_1}} + x_2^{\overline{\epsilon_2}} + ... + x_n^{\overline{\epsilon_n}} \right)$$

Avec $x_i^{\overline{\epsilon_i}} = \begin{cases} x_i & si \;\; \overline{\epsilon_i} = 1 \\ \overline{x_i} & sinon \end{cases}$

Définition : Fonction duale
Soit $f \in \mathbb{F}_n$, la fonction duale de f, notée f^* est la fonction booléenne à n variables définie par : $f^*(x_1, ..., x_i, ..., x_n) = \overline{f}(\overline{x_1}, ..., \overline{x_i}, ..., \overline{x_n})$
On a $\forall f \in \mathbb{F}, (f^*)^* = f$

Définition : Fonction autoduale
Une fonction f est autoduale si et seulement si $f^* = f*$

Définition : Relation d'ordre sur $\mathbb{B}$
$\leq$ définie sur $\mathbb{B}$ par $0 \leq 0; 0 \leq 1; 1 \leq 1$ est une relation d'ordre définie sur $\mathbb{B}$

Définition : Relation d'ordre sur $\mathbb{B}^n$ $(\epsilon_1, ..., \epsilon_i, ..., \epsilon_n) \leq (\epsilon'_1, ..., \epsilon'_i, ..., \epsilon'_n)$ si et seulement si $\epsilon_1 \leq \epsilon'_1$ et $\epsilon_i \leq \epsilon'_i$ et $\epsilon_n \leq \epsilon'_n$

Définition : Fonction booléenne croissante
$f \in \mathbb{F}_n$ est croissante si et seulement si $\forall \epsilon, \epsilon' \in \mathbb{B}^n, \epsilon \leq \epsilon' \Rightarrow f(\epsilon) \leq f(\epsilon')$

Définition : Principe de composition
Soient $f \in \mathbb{F}_n$ et $g_1, ..., g_n \in \mathbb{F}_m$, on note $f(g_1, ..., g_n)$ la fonction booléenne de $(\mathbb{F}_m)$ définie par : $f(g_1, ..., g_n) : \begin{array}{ccc} \mathbb{B}^m & \to & \mathbb{B} \\ (x_1, ..., x_m) & \mapsto & f(g(x_1), ..., g(\end{array}$

Définition : Partie générée
Soit $E \subseteq \mathbb{F}$ On définit l'ensemble des fonctions obtenues par composition à partir de E, noté $comp(E)$ comme étant l'ensemble défini inductivement par :

- Base : $B = E \cup \{(x_1, ..., x_n) \mapsto x_i, i = 1, ..., n \;\; et \;\; n \geq 1\}$
- Induction : La seule opération est la composition des fonctions booléennes

$comp(E)$ est alors le plus petit ensemble contenant E et les projections et stable par composition.

Définition : Parties génératrices Soit $E \subseteq \mathbb{F}$

- E est une partie génératrice si et seulement si $comp(E) = \mathbb{F}$
- E est une partie génératrice minimale si c'est une partie génératrice et aucune de ses parties propres n'est génératrice.

Définition : Fonction linéaire

Soit $f \in \mathbb{F}_n$ on dit que f est linéaire si $f \in comp(\{0,1,\oplus\})$
Toute fonction linéaire s'exprime donc comme somme exclusive de monômes de degré 0 ou 1.

Théorème

Soient les 5 propriétés suivantes :

$$\begin{cases} P_1(f) \Leftrightarrow f(0,...,0) = 0 \\ P_2(f) \Leftrightarrow f(1,...,1) = 1 \\ P_3(f) \Leftrightarrow f = f^* \ \ (f \ \text{ autoduale}) \\ P_4(f) \Leftrightarrow f \text{croissante} \\ P_5(f) \Leftrightarrow f \in comp(\{0,1,\oplus\}) \ \ (f \ \text{ linéaire}) \end{cases}$$

Ces propriétés sont stables par composition, ainsi :

$$\forall k = 1,...,5, P_k(f_1),...,P_k(f_n) \Rightarrow \forall f \in comp(\{f_1,...,f_n\}), P_k(f)$$

Théorème

On considère les 5 propriétés du théorème précédent. Une partie $E = \{f_1,...,f_n\}$ est génératrice si et seulement si pour chaque propriété P_i, il existe au moins un élément de E qui ne vérifie par P_i :

$$comp(E) = \mathbb{F} \Leftrightarrow \forall k \in \{1,2,3,4,5\}, \exists f \in E, \neg P_k(f)$$

Définition : Ordre partiel sur $\mathbb{F}_n$

La relation $\leq$ est définie sur $\mathbb{F}_n$ par : $f \leq g$ si et seulement si $S_n(f) \subseteq S_n(g)$

Propriétés

- $\mathbb{F}_n$ admet 1 comme plus grand élément et 0 comme plus petit élément
- $+$ et . sont compatibles avec $\leq$ (i.e $f \leq g$ et $f' \leq g' \Rightarrow f + f' \leq g + g'$ et $ff' \leq gg'$)
- $f \leq g \Leftrightarrow \overline{g} \leq \overline{f}$
- On a les équivalences suivantes : $S_n(f) \subseteq S_n(g) \Leftrightarrow f \leq g \Leftrightarrow f + g = g \Leftrightarrow f.g = f \Leftrightarrow [f \Rightarrow g \equiv 1] \Leftrightarrow \exists h, f + h = g$

Proposition (Monômes conjonctifs)

Soient m_1 et m_2 deux monômes conjonctifs de $\mathbb{F}_n$ alors $m_1 \leq m_2$ si et seulement si $\exists m_3$ un monôme conjonctif de $\mathbb{F}_n$ vérifiant $m_1 = m_2 m_3$

Définition : Monôme maximal

Soit $f \in \mathbb{F}_n$ et m un monôme conjonctif de $\mathbb{F}_n$. On dit que m est maximal pour f si et seulement si $m \leq f$ et $\forall m', m'$ monôme conjonctif de $\mathbb{F}_n$ et $m \leq m' \leq f \Rightarrow m' = m$

Théorème :

Soient $f \in \mathbb{F}_n$ et $M(f)$ l'ensemble des monômes maximaux de f.

- Si m est un monôme conjonctif de f on a : $m \leq f \Rightarrow \exists m' \in M(f), m \leq m' \leq f$
- On a $f = \sum_{m \in M(f)} m$

Définition : (Monômes centraux)

Soient $f \in \mathbb{F}_n$ et $M(f)$ l'ensemble des monômes maximaux de f. $m \in M(f)$ est un monôme central si et seulement si m n'est pas majoré par la somme des autres monômes maximaux de $M(f)$. On note $C(f)$ l'ensemble des monômes centraux de f.

$$m \in C(f) \Leftrightarrow m \in M(f) \;\; et \;\; m \nleq \sum_{m' \in M(f)} m'$$

Proposition :

$$f \in \mathbb{F}_n \;\; et \;\; E \subseteq M(f) \;\; si \;\; f = \sum_{m \in E} m \;\; alors \;\; C(f) \subseteq E$$

Cette proposition montre que les monômes centraux sont indispensables dans l'écriture de f.