CHAPITRE 2.

INTRODUCTION AUX FONCTIONS BOOLÉENNES

http://math.univ-lyon1.fr/~roblot/masterpro.html

Définition. Une **fonction booléenne** est une fonction

$$f : \{0,1\}^n \to \{0,1\}$$

Exemple. La fonction suivante de $\{0,1\}^3 \to \{0,1\}$

0	0	0	0	1	0	0	0
0	0	1	0	1	0	1	1
0	1	0	1	1	1	0	0
0	1	1	1	1	1	1	0

C'est la **table de vérité** de la fonction f.

Théorème. Il y a $2^{(2^n)}$ fonctions booléennes sur $\{0,1\}^n$.

Exemple. Pour $n = 5$, il y a $4\,294\,967\,296$ fonctions. Pour $n = 7$, il y a $\approx 10^{38}$ fonctions. (Soit 10^{22} années à 1 milliard de fonctions/seconde.)

Fonctions booléennes et opérateurs logiques

On rappelle les **opérateurs logiques** : non, et, ou, ou exclusif

négation

a	$\neg a$
0	1
1	0

ou

$a \vee b$	0	1
0	0	1
1	1	1

et

$a \wedge b$	0	1
0	0	0
1	0	1

ou exclusif

$a \oplus b$	0	1
0	0	1
1	1	0

Ils permettent de construire des fonctions booléennes.

Exercice. On considère la fonction sur $\{0,1\}^3$

$$f(a,b,c) = (\neg a \vee c) \oplus (\neg(b \vee c \vee (a \wedge \neg b)))$$

Construire sa table de vérité.

Attention à l'ordre des opérateurs. $\neg$ a la plus forte priorité, mais il n'y a pas d'ordre entre $\wedge$ et $\vee$. L'expression suivante est ambigüe

$$\neg a \wedge b \vee a$$

Exercice. Donner les deux écritures non ambigües de cette expression et démontrer qu'elles ne sont pas égales.

Fonctions booléennes et opérateurs logiques

Théorème de représentation normale logique

Toute fonction booléenne peut s'exprimer uniquement à l'aide des opérateurs logiques $\neg$, $\vee$ et $\wedge$, et même uniquement $\neg$ et $\wedge$ (ou $\neg$ et $\vee$).

Preuve. Pour chaque ligne de la table de vérité qui donne la valeur 1, on construit à l'aide de $\neg$ et $\wedge$ une expression qui vaut 1 uniquement pour les entrées correspondantes. Puis, on assemble ces expressions avec des $\vee$.

Pour le deuxième point, on utilise la loi de DeMorgan

$$(a_1 \vee a_2 \vee \cdots \vee a_n) = \neg(\neg a_1 \wedge \neg a_2 \wedge \cdots \wedge \neg a_n)$$

Exercice. Construire une représentation normale logique pour la fonction booléenne suivante

0	0	0	0	1	0	0	0
0	0	1	0	1	0	1	1
0	1	0	1	1	1	0	0
0	1	1	1	1	1	1	1

Règles de calcul logique

Associativité	$(a \wedge b) \wedge c = a \wedge (b \wedge c)$	$(a \vee b) \vee c = a \vee (b \vee c)$
Commutativité	$a \wedge b = b \wedge a$	$a \vee b = b \vee a$
Distributivité	$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$	$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
Idempotent	$a \wedge a = a$	$a \vee a = a$
Double négation	$\neg\neg a = a$	
Loi de DeMorgan	$\neg(a \wedge b) = \neg a \vee \neg b$	$\neg(a \vee b) = \neg a \wedge \neg b$
Absorption	$a \vee (a \wedge b) = a$	$a \wedge (a \vee b) = a$
Valeurs constantes	$a \wedge 0 = 0 \quad a \wedge 1 = a$	$a \vee 1 = 1 \quad a \vee 0 = a$
Valeurs opposées	$a \wedge \neg a = 0$	$a \vee \neg a = 1$

Exercice. Démontrer ces formules.

Exercice. Utiliser les règles de calcul et la représentation trouvée précédemment pour démontrer que la fonction booléenne suivante

0	0	0	0	1	0	0	0
0	0	1	0	1	0	1	1
0	1	0	1	1	1	0	0
0	1	1	1	1	1	1	1

est en fait la fonction $(\neg a \wedge b) \vee (a \wedge c)$.

Indication. Partager l'expression en deux parties. Utiliser la distributivité, puis l'absorption.

Fonctions booléennes et polynômes dans $\mathbb{F}_2[X_1, \ldots, X_n]$

Définition. Un polynôme de $\mathbb{F}_2[X_1, \ldots, X_n]$ est une somme finie de termes monômiaux de la forme (où $\mathbb{F}_2$ est le corps à deux éléments)

$$X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n} \quad \text{avec} \quad a_1, \ldots, a_n \geq 0$$

Exemple. $X_1^3 + X_1^2 X_2 + X_1^5 X_3^7$ est un élément de $\mathbb{F}_2[X_1, X_2, X_3]$

Degré. On définit le degré du terme monômial $X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$ par $a_1 + \cdots + a_n$. Et le degré d'un polynôme comme le maximum des degrés de ses termes monômiaux.

Exercice. Déterminer le degré du polynôme $X_1^3 + X_1^2 X_2 + X_1^5 X_3^7$.

Construction. Une polynôme dans $\mathbb{F}_2[X_1, \ldots, X_n]$ permet de construire une fonction booléenne de $\{0,1\}^n$ en considérant 0 et 1 comme les éléments de $\mathbb{F}_2$.

Exercice. Construire la table de vérité de la fonction correspondant au polynôme $X_1^3 + X_1^2 X_2 + X_1^5 X_3^7$.

Remarque. Puisque $1^n = 1$ et $0^n = 0$, pour tout $n \geq 1$, on peut remplacer X_i^n par X_i sans changer les valeurs.

Exemple. Le polynôme

$$X_1 + X_1 X_2 + X_1 X_3$$

définit la même fonction booléenne que le polynôme

$$X_1^3 + X_1^2 X_2 + X_1^5 X_3^7$$

Polynômes réduits

Définition. Un polynôme dont tous les termes monômiaux sont de la forme

$$X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n} \quad \text{avec} \quad a_1, \ldots, a_n = 0 \text{ ou } 1$$

est un polynôme **réduit**.

Exemple. Le polynôme suivant est réduit

$$X_1 X_3 + X_2 X_3 + X_3$$

Théorème de représentation normale algébrique

Toute fonction booléenne peut s'exprimer *de manière unique* comme un polynôme réduit.

Exercice. Preuve du théorème

1ère partie. Soit P un polynôme réduit dans $\mathbb{F}_2[X_1, \ldots, X_n]$, non nul. On montre qu'il existe $(a_1, \ldots, a_n) \in \{0,1\}^n$ tel que

$$P(a_1, \ldots, a_n) \neq 0.$$

1. Démontrer le résultat pour $n = 1$.
2. Soit $n \geq 1$. On suppose que le résultat est vrai pour tout polynôme dans $\mathbb{F}_2[X_1, \ldots, X_n]$. Soit P un polynôme dans $\mathbb{F}_2[X_1, \ldots, X_{n+1}]$.
   1. Montrer qu'il existe $S, T \in \mathbb{F}_2[X_1, \ldots, X_n]$ tels que
   $$P(X_1, \ldots, X_{n+1}) = X_{n+1} S(X_1, \ldots, X_n) + T(X_1, \ldots, X_n)$$
   2. En déduire qu'il existe $(a_1, \ldots, a_{n+1}) \in \{0,1\}^{n+1}$ tel que
   $$P(a_1, \ldots, a_{n+1}) \neq 0.$$
   Indication. Commencer avec $(a_1, \ldots, a_n) \in \{0,1\}^n$ tel que
   $$S(a_1, \ldots, a_n) \neq 0 \text{ ou } T(a_1, \ldots, a_n) \neq 0$$
3. Conclure.

Exercice. Preuve du théorème

Exercice. Trouver un élément de $\{0,1\}^4$ qui n'annule pas

$$X_1X_2X_4 + X_1X_3X_4 + X_2X_4 + X_3X_4 + X_4$$

2ème partie. Soit $n \geq 1$ et soient P et Q deux polynômes réduits *distincts* dans $\mathbb{F}_2[X_1, \ldots, X_n]$.

Montrer, en utilisant la première partie, qu'ils définissent deux fonctions booléennes différentes.

3ème partie. Soit M un monôme d'un polynôme réduit dans $\mathbb{F}_2[X_1, \ldots, X_n]$.

1. Montrer que M est de la forme
$$X_{i_1} \cdots X_{i_s} \quad \text{où } 0 \leq s \leq n \text{ et } 1 \leq i_1 < \cdots < i_s \leq n$$
2. Compter le nombre de monômes de cette forme.
3. En déduire le nombre de polynômes réduits dans $\mathbb{F}_2[X_1, \ldots, X_n]$.
4. Conclure.

Conversion entre représentations normales

Monômes. Un monôme correspond à un 'et logique' entre les variables du monôme

$$X_1X_3X_5 \leftrightarrow x_1 \wedge x_3 \wedge x_5$$

Addition. L'addition correspond au 'ou exclusif'

$$X_1X_2 + X_1X_3 \leftrightarrow x_1 \wedge x_2 \oplus x_1 \wedge x_3$$

Exercice. Ecrire la représentation normale logique correspondant à la fonction booléenne définie par

$$X_1X_2 + X_2 + X_1X_3$$

Conversion entre représentations normales

Exercice : Construction de la représentation algébrique.

1. Soit $(a_1, \ldots, a_n)$ dans $\{0,1\}^n$. Montrer que

$$(x_1 \oplus a_1 \oplus 1) \wedge \cdots \wedge (x_n \oplus a_n \oplus 1) = 1 \iff x_i = a_i \text{ pour } 1 \leq i \leq n$$

2. En déduire que le polynôme suivant est la représentation normale algébrique de la fonction booléenne f sur $\{0,1\}^n$

$$\sum_{\substack{(a_1,\ldots,a_n)\in\{0,1\}^n \\ \text{tels que } f(a_1,\ldots,a_n)=1}} (X_1 + a_1 + 1) \cdots (X_n + a_n + 1)$$

3. Calculer la représentation algébrique normale de la fonction booléenne

0	0	0	0	1	0	0	0
0	0	1	0	1	0	1	1
0	1	0	1	1	1	0	0
0	1	1	1	1	1	1	1

4. Calculer la représentation algébrique normale de la fonction booléenne

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

Distance entre fonctions booléennes

Définition. Soient f et g deux fonctions booléennes de $\{0,1\}^n$, on définit la distance de f à g par

$$d(f,g) = \text{card}\,\{x \in \{0,1\}^n \text{ tel que } f(x) \neq g(x)\}$$

Exercice. Calculer la distance entre les deux fonctions booléennes suivantes :

$$f(a,b) = a \vee \neg b \quad \text{et} \quad g(a,b) = \neg a \oplus b$$

Exercice. Montrer que d est bien une distance, c'est-à-dire qu'elle vérifie pour f, g et h trois fonctions booléennes :

- $d(f,g) = 0$ si et seulement si $f = g$,
- $d(f,g) = d(g,f)$,
- $d(f,h) \leq d(f,g) + d(g,h)$.

Transformée de Fourier et transformée de Walsh

Produit scalaire. Soient $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ deux éléments de $\{0,1\}^n$. On définit le produit scalaire de x et y par

$$\begin{aligned} x * y &= x_1 y_1 + \cdots + x_n y_n \quad (\text{dans } \mathbb{F}_2) \\ &= (x_1 \wedge y_1) \oplus \cdots \oplus (x_n \wedge y_n) \end{aligned}$$

Exercice. Soient $x, y, z \in \{0,1\}^n$. Montrer $x * (y \oplus z) = (x * y) \oplus (x * z)$.

Transformée de Fourier. Soit f une fonction booléenne sur $\{0,1\}^n$, la transformée de Fourier de f est la fonction de $\{0,1\}^n$ dans $\mathbb{Z}$ définie par

$$\hat{f}(u) = \sum_{x \in \{0,1\}^n} (-1)^{x*u} f(x)$$

où les valeurs 0 et 1 de f sont vues comme des entiers.

Exercice. Calculer la transformée de Fourier de la fonction booléenne

$$f(a,b,c) = (a \oplus \neg b) \wedge (a \vee b \vee \neg c)$$

Transformée de Walsh. Soit f une fonction booléenne sur $\{0,1\}^n$, la transformée de Walsh de f est la fonction de $\{0,1\}^n$ dans $\mathbb{Z}$ définie par

$$\tilde{f}(u) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus (x * u)}$$

Exercice. Calculer la transformée de Walsh de la fonction booléenne

$$f(a,b,c) = (a \oplus \neg b) \wedge (a \vee b \vee \neg c)$$

Vérifier qu'on a

$$\tilde{f}(u) = \begin{cases} 2^n - 2\hat{f}(0...0) & \text{si } u = 0...0 \\ -2\hat{f}(u) & \text{sinon} \end{cases}$$

Démonter ce résultat en utilisant le fait que $(-1)^{f(x)} = 1 - 2f(x)$ et

$$\sum_{x \in \{0,1\}^n} (-1)^{x*u} = \begin{cases} 2^n & \text{si } u = 0...0 \\ 0 & \text{sinon} \end{cases}$$

Indication. Pour $u \neq 0...0$, montrer qu'il existe v tel que $u * v = 1$.

Fonctions booléennes vectorielles

Définition. Un fonction booléenne vectorielle (FBV) de $\{0,1\}^n$ dans $\{0,1\}^m$ est un vecteur $(f_1, \ldots, f_m)$ de m fonctions booléennes sur $\{0,1\}^n$. C'est donc une fonction de $\{0,1\}^n$ dans $\{0,1\}^m$ donnée par

$$(a_1, \ldots, a_n) \mapsto \big(f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)\big)$$

Exemple. La fonction suivante est une fonction booléenne vectorielle de $\{0,1\}^3$ dans $\{0,1\}^2$

$$F(a,b,c) = \big((a \wedge b) \oplus \neg c, (\neg a \wedge b) \vee (a \oplus b \oplus c)\big)$$

Fonctions booléennes vectorielles et cryptosystèmes.
Un cryptosystème travaillant sur des blocs de n bits avec une clé de m bits est donné par une fonction booléenne vectorielle de $\{0,1\}^{n+m}$ dans $\{0,1\}^n$, ou de $\{0,1\}^n$ dans $\{0,1\}^n$ *si on considère la clé fixée*.