Feuille d'exercices 6

Résistance aux corrélations des fonctions booléennes

Une *fonction booléenne* est une fonction $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Son *support* est $\operatorname{supp}(f) = \{\mathbf{x} \in F_2^n \;/\; f(\mathbf{x}) = 1\}$. Son *poids de Hamming* est $\operatorname{wt}(f) = \mid \operatorname{supp}(f) \mid$. Une fonction booléenne $f : \mathbb{F}_2^n \to \mathbb{F}_2$ est *équilibrée* quand $\operatorname{wt}(f) = 2^{n-1}$.
On munit $\mathbb{F}_2$ de l'ordre $\le$ vérifiant $0 \le 1$, et on note $\preceq$ l'ordre produit sur $\mathbb{F}_2^n$, défini par ($\mathbf{u} = (u_1, \ldots, u_n)$, $\mathbf{v} = (v_1, \ldots, v_n)$) :

$$\mathbf{u} \preceq \mathbf{v} \equiv \forall i \in \{1, \ldots, n\}\; u_i \le v_i\ .$$

Soient $X_1, \ldots, X_n$ des variables aléatoires à valeur dans $\mathbb{F}_2$, indépendantes et équilibrées ($P(X_i = 0) = P(X_i = 1) = \frac{1}{2}$). Une fonction $f : \mathbb{F}_2^n \to \mathbb{F}_2$ est *résistante aux corrélations à l'ordre m* quand pour tout sous-ensemble de taille $k \le m$ de $\{1, \ldots, n\}$, soit $M = \{i_1, \ldots, i_k\}$, la variable aléatoire $Z = f(X_1, \ldots, X_n)$ est indépendante des X_i, $i \in M$. Quand Z est également equilibrée, on dit que la fonction f *est m-résiliente*.

Exercice 1. Les fonctions $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ et $g : \mathbb{F}_2^4 \to \mathbb{F}_2$ définies ci-dessous sont elles équilibrées ? Résistent-elles aux corrélations à l'ordre 1 ?

$$f(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3\ ; \quad g(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_3 + x_4\ .$$

Exercice 2 (d'après Siegenthaler 84). Pour $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{u} = (u_1, \ldots, u_n)$, $\mathbf{u} \in \mathbb{F}_2^n$, on convient de noter $\mathbf{x}^{\mathbf{u}}$ le monôme $\mathbf{x}^{\mathbf{u}} = \prod_{i=1}^n x_i^{u_i}$ (où les éléments 0 et 1 de $\mathbb{F}_2$ sont identifiés aux entiers 0 et 1).

1. Soit f une fonction de $\mathbb{F}_2^n$ dans $\mathbb{F}_2$. Rappeler pourquoi f est une fonction polynomiale (à plusieurs variables), et s'écrit de façon unique comme une somme de monômes où chaque variable est de degré au plus 1, appelée *forme algébrique normale*. Le degré de f, noté $\deg(f)$, est le degré de sa forme algébrique normale. On notera :

$$f(\mathbf{x}) = \sum_{\mathbf{u} \in \mathbb{F}_2^n} a_u \mathbf{x}^{\mathbf{u}} \quad \text{(notation conservée pour les questions suivantes).}$$

2. La fonction $a : \mathbf{u} \mapsto a_{\mathbf{u}}$ est une fonction boooléenne à n arguments. Vérifier que la transfomation : $f \mapsto a$ est involutive, plus précisément vérifier que :

$$f(\mathbf{u}) = \sum_{\mathbf{v} \preceq \mathbf{u}} a_{\mathbf{v}} \;\text{ et }\; a_{\mathbf{u}} = \sum_{\mathbf{v} \preceq \mathbf{u}} f(\mathbf{v})\ .$$

3. On pose $\operatorname{supp}_{\mathbf{u}}(f) = \{\mathbf{v} \preceq \mathbf{u} \;/\; f(\mathbf{v}) = 1\}$, $\operatorname{wt}_{\mathbf{u}}(f) = \mid \operatorname{supp}_{\mathbf{u}}(f) \mid$. On note $\mathbf{1}$ le vecteur constant de $\mathbb{F}_2^n$ égal à 1, $\mathbf{1}_{\le k}$ le vecteur de $\mathbb{F}_2^n$ dont les k premiers bits sont à 1 et les suivants à 0. Clairement $\operatorname{supp}_{\mathbf{1}}(f) = \operatorname{supp}(f)$. On note $I_{\mathbf{u}} = \{1 \le i \le n \;/\; u_i = 1\}$. Les variables aléatoires $X_1, \ldots, X_n$ et Z sont comme ci-dessus.
   - **a.** Montrer que $a_u = 1$ si et seulement si $\operatorname{wt}_u(f)$ est impair.
   - **b.** Exprimer $P(Z = 1)$ en fonction de $\operatorname{wt}(f)$, et plus généralement, $P(Z = 1 \mid X_i = 0 \text{ pour } i \notin I_{\mathbf{u}})$ en fonction de $\operatorname{wt}_{\mathbf{u}}(f)$.
   - **c.** En déduire que si f résiste aux corrélations à l'ordre m, et si $n - m \le \mid I_{\mathbf{u}} \mid \le n$, alors

   $$\operatorname{wt}_{\mathbf{u}}(f) = 2^{|I_{\mathbf{u}}| - n} \operatorname{wt}(f) = 2^{|I_u| - (n-m)} \operatorname{wt}_{\mathbf{1}_{\le n-m}}(f)\ .$$

   - **d.** En déduire que si f résiste aux corrélations à l'ordre m, alors elle est de degré au plus $n - m$, et que si de plus f est equilibrée, alors elle est de degré au plus $n - m - 1$ sauf si $n = m + 1$.

Exercice 3 (d'après Siegenthaler 84).

1. On suppose que f_1 et f_2 sont deux fonctions distinctes de $\mathbb{F}_2^n \to \mathbb{F}_2$ résistantes aux corrélations à l'ordre m équilibrées. Montrez que la fonction $f : \mathbb{F}_2^{n+1} \to \mathbb{F}_2$ est équilibrée et résistante aux corrélations à l'ordre m :

$$f(x_1, \ldots, x_{n+1}) = x_{n+1} f_1(x_1, \ldots, x_n) + (1 + x_{n+1}) f_2(x_1, \ldots, x_n)\ .$$

2. Montrer que pour $n \ge 2$, les fonctions $g_k : \mathbb{F}_2^n \to \mathbb{F}_2$ sont équilibrées et résistent aux corrélations à l'ordre $n - 2$:

$$g_k(x_1, \ldots, x_n) = \sum_{i \ne k} x_i \quad 1 \le k \le n\ .$$

3. Utiliser les résultats des deux questions précédentes et de l'exercice précédent pour montrer que la fonction h est équilibrée et résiste aux corrélations à l'ordre 2, mais pas à l'ordre 3 :

$$h(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2 + x_4 + x_3x_5 + x_4x_5\ .$$

4. Indiquer comment construire une fonction de degré 2 à $n+2$ variables, $n \geq 3$, équilibrée et résistante aux corrélations à l'ordre $n-1$, une fonction de degré k à $n+k$ variables équilibrée et resistante aux corrélations à l'ordre $n-1$.

Pour $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^n$, on note $\mathbf{u} \cdot \mathbf{v}$ le produit scalaire de $\mathbf{u}$ et $\mathbf{v}$:

$$(u_1, \ldots, u_n) \cdot (v_1, \ldots, v_n) = u_1 v_1 + \cdots + u_n v_n \, .$$

Une fonction booléenne linéaire à n arguments s'écrit $\mathbf{u}^* : \mathbf{x} \mapsto \mathbf{u} \cdot \mathbf{x}$ (forme linéaire sur $\mathbb{F}_2^n$).
Sous les mêmes hypothèses sur les X_i qu'en début de feuille, la *corrélation* de deux fonctions f et g de $\mathbb{F}_2^n \to \mathbb{F}_2$ est par définition :

$$C(f,g) = 2P\big(f(X_1, \ldots, X_n) = g(X_1, \ldots, X_n)\big) - 1 \, .$$

On a $C(f,g) \in [-1,1]$, $C(f,g) = 1$ ssi $f = g$, et $C(f,g) = -1$ ssi $f = 1-g$.
Deux fonctions f et g seront dites *corrélées* si $C(f,g) \neq 0$, $|C(f,g)|$ mesure l'amplitude de la corrélation.
À $f : \mathbb{F}_2^n \to \mathbb{F}_2$ on associe la fonction $\hat{f} : \mathbb{F}_2^n \to \mathbb{R}$ définie par $\hat{f}(\mathbf{u}) = 1$ si $f(\mathbf{u}) = 0$, et $\hat{f}(\mathbf{u}) = -1$ si $f(\mathbf{u}) = 1$. On note aussi $\hat{f}(\mathbf{u}) = (-1)^{f(\mathbf{u})}$.
Étant données deux fonctions $\alpha, \beta : \mathbb{F}_2^n \to \mathbb{R}$ on note $\langle \alpha, \beta \rangle = \sum_{\mathbf{u} \in \mathbb{F}_2^n} \alpha(\mathbf{u})\beta(\mathbf{u})$, en particulier :

$$\langle \hat{f}, \hat{g} \rangle = \sum_{\mathbf{u} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{u})}(-1)^{g(\mathbf{u})} \quad \text{(avec la convention ci-dessus)}$$

Exercice 4. Vérifier que $(\alpha, \beta) \mapsto \langle \alpha, \beta \rangle$ est un produit scalaire sur l'espace vectoriel réel $\mathbb{R}^{\mathbb{F}_2^n}$ ($\sim \mathbb{R}^{2^n}$) (la norme associée est notée usuellement). Montrer que pour toutes fonctions booléennes f et g à n arguments :

$$\langle \hat{f}, \hat{f} \rangle = 2^n \, ; \;\; C(f,g) = \frac{\langle \hat{f}, \hat{g} \rangle}{2^n} = \frac{\langle \hat{f}, \hat{g} \rangle}{\| \hat{f} \| \| \hat{g} \|} \; (= \cos(\hat{f}, \hat{g})) \, .$$

Exercice 5.

1. Montrer que la famille $(\widehat{\mathbf{u}^*})_{u \in \mathbb{F}_2^n}$ est une base orthogonale de $\mathbb{R}^{\mathbb{F}_2^n}$, dont tous les vecteurs ont pour norme $2^{\frac{n}{2}}$.
2. On appelle *transformée de Hadamard-Walsh* d'une fonction $\alpha : \mathbb{F}_2^n \to \mathbb{R}$, la fonction $W_\alpha : \mathbb{F}_2^n \to \mathbb{R}$ qui à $\mathbf{u}$ associe la coordonnée de α associée à $\mathbf{u}$ dans la base $(2^{-n}\widehat{\mathbf{u}^*})_{\mathbf{u} \in \mathbb{F}_2^n}$ (W_α détermine donc α) :

$$\forall \mathbf{x} \in \mathbb{F}_2^n \;\; \alpha(\mathbf{x}) = \frac{1}{2^n} \sum_{\mathbf{u} \in \mathbb{F}_2^n} W_\alpha(\mathbf{u})(-1)^{\mathbf{u} \cdot \mathbf{x}} \, .$$

   Montrer que :

$$\forall \mathbf{u} \in \mathbb{F}_2^n \;\; W_\alpha(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \alpha(\mathbf{x})(-1)^{\mathbf{u} \cdot \mathbf{x}}$$

   et que pour toute fonction $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $W_{\hat{f}}(\mathbf{u}) = 2^n C(f, \mathbf{u}^*)$, c'est-à-dire que $W_{\hat{f}}(\mathbf{u})$ est une mesure de la corrélation entre f et la fonction booléenne u^*.
3. Montrer que pour toute fonction $f : \mathbb{F}_2^n \to \mathbb{F}_2$ (calculer la norme de $\hat{f}$ de deux façons) :

$$\sum_{\mathbf{u} \in \mathbb{F}_2^n} C(f, \mathbf{u}^*)^2 = 1 \qquad \textit{(formule de Parseval)}$$

   Cette formule donne une relation entre le nombre de fonctions booléennes linéaires à laquelle f est corrélée et l'amplitude de ces corrélations. Ainsi f est forcément corrélée à au moins une forme linéaire. Pour minimiser la corrélation d'une fonction booléenne aux formes linéaires, on peut choisir, quand n est pair, f telle que $\forall u \in \mathbb{F}_2^n \, C(f, \mathbf{u}^*) = 2^{-\frac{n}{2}}$ (fonction courbe), mais une telle fonction ne peut être équilibrée (exercice).

Exercice 6 (Xiao et Massey 1985). Soit Z une variable aléatoire prenant un nombre fini de valeurs réelles. Soient $X_1, \ldots, X_n$ des variables aléatoires à valeur dans $\mathbb{F}_2$.

1. Montrer que Z est indépendante de $X = (X_1, \ldots, X_n)$ si et seulement si Z est indépendante de toutes les combinaisons linéaires (dans $\mathbb{F}_2$) des X_i (comparer, pour z fixé, les transformées de Walsh de $\alpha : \mathbf{x} \mapsto P(X = \mathbf{x} | Z = z)$ et $\beta : \mathbf{x} \mapsto P(X = \mathbf{x})$).
2. On suppose de plus $X_1, \ldots, X_n$ indépendantes et équilibrées, et $Z = f(X)$ où $f : \mathbb{F}_2^n \to \mathbb{F}_2$, et $\mathbf{u} \in \mathbb{F}_2^n$, $\mathbf{u} \neq \mathbf{0}$. Montrer que Z est indépendante de $\mathbf{u} \cdot X$ ssi $W_{\hat{f}}(\mathbf{u}) = 0$.
3. En déduire que la fonction $f : \mathbb{F}_2^n \to \mathbb{F}_2$ résiste aux corrélations à l'ordre m si et seulement si $W_{\hat{f}}(\mathbf{u}) = 0$ pour tout $\mathbf{u}$ de $\mathbb{F}_2^n$ dont au moins une et au plus m composantes sont non nulles, et que f est équilibrée si et seulement si $W_{\hat{f}}(\mathbf{0}) = 0$.