QUOTIENT DE RAYLEIGH DE FONCTION BOOLÉENNE

PAVLE MICHKO

Résumé. On s'interesse aux quotients de Rayleigh des fonctions booléennes.

1. quotient de Rayleigh

On utilise les notations habituelles : $\mathbb{F}_2$ le corps à deux éléments, le cardinal de $\mathbb{F}_2^m$ est noté q, identifié au corps L. Pour une fonction de $\mathbb{F}_2^m$ dans $\mathbb{F}_2$, le coefficient de Walsh en a vaut :

$$f^{\mathfrak{w}}(a) = \sum_x \mu(f(x) + ax). \tag{1}$$

On dit que f est courbe si

$$f^{\mathfrak{w}}(a) = \pm\sqrt{q} = \mu(\tilde{f}(a)) \times \sqrt{q}$$

L'existence d'une fonction courbe implique que m est pair. On dit que f est autoduale quand $f = \tilde{f}$ et andiduale si $f + 1 = \tilde{f}$. Le coefficient de Rayleigh de f est :

$$\begin{aligned} R(f) &= \sum_{x,y\in\mathbb{F}_2^m} \mu(f(x) + xy + f(y)) \\ &= \sum_a f^{\mathfrak{w}}(x) \times \mu(f(x)) \end{aligned}$$

Il s'agit du quotient de Rayleigh $R(\mathfrak{F}, \mu \circ f)$ du vecteur $\mu \circ f$ par rapport à l'opérateur de Fourier $\mathfrak{F}$ qui possède deux valeurs propres $\pm\sqrt{q}$. On note alors que

$$-\sqrt{q} \leq \frac{1}{q} R(f) = R(\mathfrak{F}, f) \leq \sqrt{q}$$

Les fonctions antiduales et autoduales sont aux frontières de ces inégalités et réciproquement.

On introduit les notations

$$r(f) = \frac{1}{q} R(f), \quad \rho(q) = \sup_f r(f)$$

Problème 1. *Comment de distribuent les nombres $r(f)$?*

En dimension paire $r(q) = \sqrt{q}$. En dimension impaire, il n'existe pas de fonction courbe mais il me semble raisonnable de conjecturer

Date: Automne 2014, dernière compilation 20 septembre 2014.

Conjecture 1.

$$\lim_{q\to\infty}\frac{r(q)}{\sqrt{q}}=1$$

Avec deux fonctions booléennes f et g, on construit une fonction de dimension $m+1$ en posant :

$$(f,g)(x,t)=tf(x)+(t+1)g(x).$$

On a

$$(f,g)^{\mathfrak{w}}(a,t)=f^{\mathfrak{w}}(a)+\mu(t)g^{\mathfrak{w}}(a)$$

Et

$$\begin{aligned}R(f,g)&=\sum_{a,t}(f^{\mathfrak{w}}(a)+\mu(t)g^{\mathfrak{w}}(a))\mu((f,g)(a,t))\\&=\sum_{a}(f^{\mathfrak{w}}(a)+g^{\mathfrak{w}}(a))\mu(g(a))+\sum_{a}(f^{\mathfrak{w}}(a)-g^{\mathfrak{w}}(a))\mu(f(a))\\&=\sum_{a}f^{\mathfrak{w}}(a)(\mu(f(a))+\mu(g(a)))+\sum_{a}g^{\mathfrak{w}}(a))(\mu(f(a))-\mu(g(a)))\end{aligned}$$

en particulier si $f=g$ est autoduale :

$$r(f,f)=2R(f)/2q=\sqrt{q}=\sqrt{2q}/\sqrt{2}$$

en dimension impaire $r(q)\geq\frac{1}{\sqrt{2}}$.

2. Maiorana-MacFarland

On suppos m pair. L'espace $\mathbb{F}_2^m$ est identifié au produit de $K\times K$, ou K est le corps d'ordre $\sqrt{q}$. Soit π une permutation de K, la fonction définie par :

$$f(x,y)=\operatorname{trace}(x\pi(y))$$

est courbe. Il s'agit d'une fonction de Maiorana-MacFarland, la duale d'obtient par un calcul direct :

$$\begin{aligned}f^{\mathfrak{w}}(a,b)&=\sum_{x,y}\mu(x\pi(y)+ax+by)\\&=\sqrt{q}\sum_{\pi(y)=a}\mu(by)\\&=\sqrt{q}\mu(b.\pi^{-1}(a))\end{aligned}$$

Le coefficient de Rayleigh vaut

$$R(f) = \sqrt{q} \sum_{a,b} \mu(a\pi(b) + b\pi^{-1}(a)$$
$$= \sqrt{q} \sum_{a,b} \mu(\pi(a)\pi(b) + ab)$$

Notons que dans le cas ou π est l'identité, on obtient la valeur $q\sqrt{q}$ qui correspond aux fonctions autoduales.

3. Distribution

Dans le cas d'une inversion $\pi(x) = \frac{c^{1/2}}{x}$, avec c non nul, et la convention $\pi(0) = 0$, on obtient

$$R(f) = \sqrt{q} \sum_{x,y} \mu(\frac{c}{xy} + xy)$$
$$= \sqrt{q}[(\sqrt{q} - 1) \sum_{t} \mu(\frac{c}{t} + t) + q] \quad = q + q\,\mathrm{kloos}\, c - \sqrt{q}\,\mathrm{kloos}\,(c)$$

où $\mathrm{kloos}\,(c)$ est une somme de Kloosterman qui prend toutes les valeurs entières multiples de 4 dans l'intervalle $[-2\sqrt[4]{q}, +2\sqrt[4]{q}]$.

Proposition 1. *Pour tout entier x multiple de 4 dans l'intervalle $[-2\sqrt[4]{q}, +2\sqrt[4]{q}]$, il existe une quantité réelle ϵ de valeur absolue au plus 2 telle que $1 + x + \epsilon$ soit le $r(f)$ d'une fonction courbe.*

Démonstration. Les sommes de Kloosterman vérifient $|\mathrm{kloos}\,(c)| \leq 2\sqrt[4]{q}$. □

4. Quotient faible

On ne suppose rien sur la parité de m.

On considère la fonction $f_c(x) = \mathrm{trace}\,(c/x)$, son quotient de Rayleigh est connecté à une somme de Kloosterman généralisée.

$$R(f_c) = \sum_{x,y} \mu(c/x + c/y + xy)$$
$$= 2 \sum_{y} \mu(c/y) - 1 + \sum_{xyz=1} \mu(c/x + c/y + z)$$
$$= -1 + \sum_{xyz=1} \mu(c/x + c/y + 1/z)$$
$$= -1 + \sum_{xyz=c^2} \mu(x + y + z)$$

On sait que cette somme de Kloosterman généralisée est majorée par $3q$ ce qui conduit à

$$|r(f_c)| \leq 3$$

un comportement moyen.

5. MOYENNE

Tout quadruplet x, y, z, t, conduit à un caractère addifif :

$$\chi_{x,y,z,t}(f) = \mu(f(x) + f(y) + f(z) + f(t)).$$

On suppose V un espace d'application tel que pour tout x, y, z, t :

$$\chi_{x,y,z,t} \perp V \Longrightarrow \sharp\{x, y, z, t\} = 1, 2.$$

On en déduit la moyenne :

$$\sum_{f\in V} R(f) = \sum_{f\in V} \sum_{x,y} \mu(f(x) + f(y) + xy) = |V| \sum_{x} \mu(x^2) = 0$$

et la moyenne quadratique :

$$\begin{aligned}
\sum_{f\in V} R(f)^2 &= \sum_{f\in V} \sum_{x,y,z,t} \mu(f(x) + f(y) + f(z) + f(t) + xy + zt) \\
&= \sum_{f\in V} \sum_{x,y,z,t} \mu(f(x) + f(y) + f(z) + f(t) + xy + zt) \\
&= |V| \, [\sum_{x=y,z=t} \mu(x^2 + z^2) + \sum_{x=z,y=t} \mu(2xy) + \sum_{x=t,y=z} \mu(2xy) - 2 \sum_{x=y=z=t} \mu(2x^2)] \\
&= |V| \, [q^2 - 2q]
\end{aligned}$$

En moyenne

$$|R(f)| \sim q$$