Institut de Mathématiques de Luminy
DEA de Mathématiques Discrètes et Fondements de l'Informatique

Fonctions puissance

Étudiant:
E. Zălinescu

Coordonateur:
Prof. Ph. Langevin

Juin 2004

Sommaire

1 Introduction

Le sujet de ce memoire est, en grand, les fonctions "puissance", c'est-à-dire les fonctions $x \mapsto x^s$ définies sur une extension de degré m du corps de Galois à deux éléments. On s'intéresse aux exposants qui sont "bons" dans le sens que la nonlinearité des fonctions booléennes correspondantes est maximale. En fait une problématique similaire se pose dans des autres contextes: ce des m-séquences, des codes cyclique á deux zéros, des ensembles à différences ou dans la cryptographie. Par exemple, dans le cas des séquences on se demande quels sont les entiers s pour lesquels l'intercorrélation entre une m-séquence est sa décimation par s est minimale.

Dans les années 60-70, quatre exposants, qui sont appelés de type Gold, Kasami, Welch et Niho respectivement, ont été conjecturés comme bons, dans le cas où m est impair. Si pour les deux premiers les preuves ont été données rapidement, pour ceux de type Welch et Niho la confirmation est venue autour de l'année 2000, dans les travaux [2] et [10]. Les deux preuves suivent le même chemin jusqu'à un point: la détermination d'un minimum ν_s. La méthode utilisée dans l'article [10] est assez puissante et permet d'établir la propriété dont nous sommes intéressés pour tous les quatre exposants. La détermination de l'ensemble J_s des éléments pour lesquels ce minumum est atteint semble importante aussi. Dans le cas Gold cette ensemble se "voit" et a une description simple. Pour les autres exposants ce n'est plus le cas. Nous donnons la forme de cet ensemble pour l'exposant de type Kasami. Une description équivalente dans un certain sens a été donnée par Dillon dans [5].

Après la présentation des notations et du cadre de travail, on définit la non-linéarité des fonctions booléennes et on précise qui sont les fonctions qui ont une distance maximale aux applications affines dans le cas où m est pair. On les appellent courbes et elles ont le spectre de Fourier réduit à deux valeurs $\pm\sqrt{q}$, où q est l'ordre du corps sur lequel on travaille.

Ensuite on se place dans le contexte cryptographique. On présente deux classes des fonctions qui fournissent la meilleure résistance aux méthodes de cryptanalyse differentielle, respectivement linéaire. Cette approche nous permet d'obtenir une borne inférieure de la linéarité et de définir les fonctions presque courbes, qui ont le spectre de Fourier réduit à trois valeurs 0 et $\pm\sqrt{2q}$. Les bons exposants pour m impair sont ceux pour lesquels les fonction puissance correspondantes sont presque courbes. On donne une caracatérisation de ces fonctions dans laquelle intervient la haute divisibilité des coefficients de Fourier des fonctions en cause.

Puis on décrit comment on peut arriver à une caractérisation de cette divisibilité en termes du minimum ν_s, en utilisant les sommes de Gauss et les congruences de Stickelberger. On présente aussi autres propriétés des fonctions puissance et une étude des quelques paramètres pour l'exposant de type Gold.

Dans la dernière section on présente l'algorithme de multiplication modulaire qui est à la base de la méthode de Hollmann et Xiang pour la détermination de la valeur ν_s. Ensuite on fait l'analyse compléte de ce point de vue pour les cas Gold et Kasami, en finissant par préciser, dans ce dernier cas, la forme de l'ensemble J_s avec l'aide d'un graphe orienté.

2 Notions préliminaires

2.1 Transformée de Fourier

Les notions suivantes apparaissent avec une fréquence irrégulière dans la suite, mais on préfère de les présenter ensemble ici, car elles sont lies á la transformée de Fourier discréte.

Soit G un groupe de ordre fini n. Un *caractère* de G est un homomorphisme de G dans le groupe multiplicatif $\mathbb{C}^*$. Si μ est identiquement 1, alors μ s'appelle *caractère trivial*. Le caractère $\overline{\mu}$, donné par $\overline{\mu}(x) := \overline{\mu(x)}$, s'appele le *caractère conjugué* de μ, où $\overline{a}$ est le complexe conjugué de $a \in \mathbb{C}$. Les valeurs d'un caractère sont les racines n-ièmes de l'unité. L'ensemble des caractères de G s'appelle le *dual* de G et on le note $\widehat{G}$. Les groupes G et $\widehat{G}$ sont isomorphes et par conséquent ont le même cardinal.

Pour μ un caractère non trivial de G on la *relation d'orthogonalité*:

$$\sum x \in G \mu(x) = 0.$$

La *transformé de Fourier* de $f : G \to \mathbb{C}^*$ est $\widehat{f} : \widehat{G} \to \mathbb{C}^*$ définie par $\widehat{f}(\mu) := \sum_{a \in G} f(a)\overline{\mu(a)}$. Et on aussi une *formule d'inversion*:

$$f(x) = \sum_{\mu \in \widehat{G}} \widehat{f}(\mu)\mu(x).$$

On mentionne aussi la formule $\widehat{\widehat{f}}(x) = nf(-x), \forall x \in G$. Soit T_t l'operateur de translation sur l'ensemble de fonctions de G en $\mathbb{C}^*$, définie par $T_t(f)(x) := f(x+t)$. Alors on dispose de l'egalité suivante:

$$\widehat{T_t(f)}(\mu) = \mu(t)\widehat{f}(\mu).$$

Soit $f, g : G \to \mathbb{C}^*$ deux fonction. Alors la *convolée* de f et de g est la fonction $f * g$ donnée par: $(f * g)(z) := \sum_{x+y=z} f(x)g(y)$. L'opération $*$ s'appelle *produit de convolution*. On définit aussi la *fonction de corrélation* de f et g, donnée par: $(f \times g)(z) := \sum_{x-y=z} f(x)\overline{g(y)}$. L'opération $\times$ s'appelle *produit de corrélation* et on les formules suivantes:

$$\widehat{f} \times \widehat{g} = n\widehat{f\overline{g}}$$
$$\widehat{f \times g} = \widehat{f}\,\overline{\widehat{g}}$$

Si H est un sous-groupe de G alors on définit l'*orthogonal* de H par $H^\perp := \{\mu \in \widehat{G} | \mu(h) = 1, \forall h \in H\}$. Le groupe $H^\perp$ est isomorphe $\widehat{G/H}$ et par conséquent $|S^\perp| = |G|/|H|$. L'identité suivante est connue comme la *formule de Poisson:*

$$\frac{1}{|H^\perp|} \sum_{\mu \in H^\perp} \widehat{f}(\mu)\mu(z) = \sum_{x \in H+z} f(x).$$

2.2 Cadre de travail

On présente maintenant les notions et notations qui vont se mentenir tout au long de ce travail.

Soit $K := \mathbb{F}_2$ le corps Galois à deux éléments et soit L une extension de degré m de K. On note q l'ordre de L. Nous allons identifier le corps L et l'espace vectoriel K^m à travers une base de L sur K. On note par Tr_L la fonction *trace* de L, $\mathrm{Tr}(x) := x + x^2 + x^{2^2} + \cdots + x^{2^{m-1}}$.

Si a est un élément de K^m alors on note $(a_1, a_2, \ldots, a_m)$ sa représentation vectorielle. Aussi on note avec $a.b$ le produit scalaire $a_1b_1+a_2b_2+\cdots+a_mb_m$, où $a, b \in K^m$. Pour une fonction $F : K^m \to K^{m'}$ et pour $c \in K^{m'}$ on note $c.F : K^m \to K$ la fonction donné par $x \mapsto c.F(x)$.

On note par χ le caractère additif canonique de L. Il est définit par $\chi(x) := (-1)^{\mathrm{Tr}_L(x)}$. Soit $f : L \to K$ une fonction booléenne. On note $f_\chi(x) := \chi(f(x)) = (-1)^{f(x)}$ la représentation binaire en valeurs ± 1 de f.

Comme on travaille en caractéristique 2, la transformée de Fourier de f prend la forme $\widehat{f}(a) := \sum_{x\in L} f(x)(-1)^{\mathrm{Tr}_L(ax)}$ (ou $\widehat{f}(a) = \sum_{x\in K^m} f(x)(-1)^{a.x}$). Elle s'appelle la *transformé de Hadamard-Walsh*. Précisons que la somme est sur $\mathbb{Z}$; $\widehat{f}$ prend donc des valeurs entières. On peut écrire $\widehat{f_\chi}(a)$ comme $\sum_{x\in L} \chi(f(x) + ax)$.

Soit $F : L \to L$ une fonction. Comme pour les fonctions booléennes, on note $F_\chi(x) := \chi(F(x)) = (-1)^{\mathrm{Tr}_L(F(x))}$. On a donc $\widehat{F_\chi}(x) = \sum_{x\in L} \chi(F(x) + ax)$.

Une autre notation utilisée est $\overline{1, m} := \{1, 2, \ldots, m\}$, où $m \in \mathbb{N}^*$. Et $\#E$ ou $|E|$ dénote le cardinal d'un ensemble E.

2.3 Fonctions booléennes

Pour $a \in L$, on note $\delta_a : L \to K$ l'application de Dirac, donnée par:

$$\delta_a(x) := \begin{cases} 1, & \text{si } x = a; \\ 0, & \text{si } x \neq a. \end{cases}$$

L'ensemble de fonctions de L dans K est un espace vectoriel sur K.

Théorème 2.1 *La famille $(\delta_a)_{a\in L}$ est une base de l'ensemble des fonctions booléennes.*

Preuve. Soit f une fonction booléenne. Alors $f = \sum_{a\in L} f(a)\delta_a$. On suppose qu'il y a une famille $(\lambda_a)_{a\in K^m} \in K^q$ telle que $\sum_{a\in G} \lambda_a\delta_a = 0$. Alors pour chaque $x \in L$ on a $\sum_{a\in L} \lambda_a\delta_a(x) = 0$, et donc $\lambda_x = 0$. □

Corollaire 2.2 *Les fonctions booléennes forment un espace vectoriel de dimension 2^m sur K.*

Théorème 2.3 *Toute fonction booléenne possède une représentation polynomiale de degré partiel 1 en chaque variable.*

Preuve. Soit $f : K^m \to K$. On peut écrire δ_0 comme $\delta_0(x) = (1+x_1)(1+x_2)\dots(1+x_m)$. Alors $\delta_a(x) = \delta_0(a+x) = \prod_{i=1}^{m}(1+a_i+x_i)$ est un polynôme de degré partiel 1 en chaque variable. Comme $f(x) = \sum_{a\in K^m} f(a)\delta_a(x)$ on arrive à la représentation desirée. □

On peut donc écrire $f : L \to K$ sous la forme suivante:

$$f(x) = \sum_{J\subseteq\overline{1,m}} \alpha_J x_J, \tag{1}$$

où $\alpha_J \in K$ et $x_J = \prod_{j\in J} x_j$. On dit que f est écrite sous la *forme algébrique normale*. Le *degré* d'une fonction booléenne f est le degré polynômial de la forme algébrique normale de f, et est noté $\deg(f)$.

Proposition 2.4 *Les coefficients de x_J dans l'équation (1), où $J \subseteq \overline{1,m}$, sont $\alpha_J = \sum_{\mathrm{Supp}(a)\subseteq J} f(a)$, où $\mathrm{Supp}(x) := \{i \in \overline{1,m} | x_i = 1\}, \forall x \in K^m$.*

Preuve. Si $a = (a_1, a_2, \dots, a_m) \in K^m$ alors on note $\overline{a} = (\overline{a_1}, \overline{a_2}, \dots, \overline{a_m})$, où $\overline{x} = 1 + x$, pour $x \in K$. On a

$$\begin{aligned} f(x) &= \sum_{a\in K^m} f(a)\delta_a(x) = \sum_{a\in K^m} f(a)\delta_0(a+x) \\ &= \sum_{a\in K^m} f(a)\prod_{i=1}^{m}(\overline{a_i}+x_i) = \sum_{a\in K^m} f(a)\sum_{J\subseteq\overline{1,m}} \overline{a}_{\overline{1,m}\setminus J}x_J \\ &= \sum_{J\subseteq\overline{1,m}} x_J \sum_{a\in K^m} \overline{a}_{\overline{1,m}\setminus J} f(a). \end{aligned}$$

Mais $\overline{a}_{\overline{1,m}\setminus J} = 1 \iff \prod_{i\in\overline{1,m}\setminus J}(1+a_i) = 1 \iff a_i = 0, \forall i \in \overline{1,m}\setminus J \iff \mathrm{Supp}(a) \subseteq J$. □

Proposition 2.5 *Soient $f : L \to K$ et $v \in \overline{1,m}$. Si $2^v | \widehat{f_\chi}(a), \forall a \in K^m$ alors $\deg(f) \leq m - v + 1$.*

Preuve. On a vu dans la proposition précédente que f s'écrit

$$f(x) = \sum_{J\subseteq\overline{1,m}} x_J \sum_{\mathrm{Supp}(a)\subseteq J} f(a).$$

Par conséquent

$$\deg(f) = \max\{\#J | J \subseteq \overline{1,m} \text{ et } \sum_{s\in S} f(s) \equiv 1 (\mathrm{mod}\, 2)\}.$$

Notons avec d le degré de f. Soient $J \subseteq \overline{1,m}$ un ensemble tel que $|J| = d$ et S_J le sous-espace vectoriel $S_J := \{b \in K^m | \mathrm{Supp}(b) \subseteq J\}$. On a que $|S_J^\perp| = |K^m|/|S_J| = 2^{m-|J|}$.

La formule de Poisson nous dit

$$\sum_{\mu \in S_J^\perp} \widehat{f}(\mu) = 2^{m-d} \sum_{s \in S_J} f(s).$$

Comme $\widehat{f_\chi}(0) = 2^m - 2\widehat{f}(0)$ et $\widehat{f_\chi}(a) = 2\widehat{f}(a)$, pour $a \neq 0$, on a que $2^v | \widehat{f_\chi}(a) \iff 2^{v-1} | \widehat{f}(a)$. Et alors $2^{v-1} | 2^{m-d} \sum_{s \in S} f(s)$.

On suppose $d > m-v+1$, c'est-à-dire $v-1-m+d > 0$. Alors $2^{v-1-m+d} | \sum_{s \in S} f(s)$. Mais ça implique $\sum_{s \in S} f(s) \equiv 0 (\mathrm{mod}\, 2)$, qui contredit la supposition que d est le degré de f. Donc $\deg(f) \leq m - v + 1$. □

On définit la *distance de Hamming* entre deux fonctions booléennes f et g comme le nombre des valeurs différentes qu'elles prennent. On la note $\mathrm{d}(f, g)$.

Une fonction $f : K^m \to K$ est dite *équilibrée* si elle prend autant de valeurs 0 que de valeurs 1, (*i.e.*, 2^{m-1}) ou, autrement dit, si $\sum_{x \in K^m} (-1)^{f(x)} = 0$.

3 Nonlinéarité

La *nonlinéarité* de $f : L \to K$, notée $\mathcal{NL}(f)$, est la distance minimale entre la fonction booléenne f et l'ensemble des fonctions affines $x \mapsto \mathrm{Tr}(ax) + b$, où $a \in L, b \in K$.

Proposition 3.1 *Soient $f : K^m \to K$ une fonction booléenne et les éléments $a \in K^m$ et $b \in K$. On a*

$$\mathrm{d}\left(f,\, x \mapsto \mathrm{Tr}(ax) + b\right) = 2^{m-1} - \frac{(-1)^b}{2} \widehat{f_\chi}(a).$$

Preuve. On note A_0 respectivement A_1 le nombre de 0 respectivement de 1 de la fonction $f(x) + \mathrm{Tr}(ax)$. On voit que $\widehat{f_\chi}(a) = A_0 - A_1 = (2^m - A_1) - A_1 = 2^m - 2A_1$. D'où $A_1 = 2^{m-1} - \frac{1}{2}\widehat{f_\chi}(a)$.

Soit $g(x) := \mathrm{Tr}(ax)$ et $g'(x) := \mathrm{Tr}(ax) + 1$. On note par $\mathbf{0}$ et $\mathbf{1}$ les fonctions constantes de valeur 0, respectivement 1. On a $\mathrm{d}(f, g) = \mathrm{d}(f + g, \mathbf{0}) = A_1 = 2^{m-1} - \frac{1}{2}\widehat{f_\chi}(a)$. Et $\mathrm{d}(f, g') = \mathrm{d}(f + g', \mathbf{0}) = \mathrm{d}(f + g, \mathbf{1}) = A_0 = 2^{m-1} + \frac{1}{2}\widehat{f_\chi}(a)$. □

Le *spectre de Fourier* de f est l'ensemble des valeurs des coefficients de $\widehat{f_\chi}$. L'*amplitude spectrale* de f est

$$\mathcal{R}(f) := \max_{a \in L} |\widehat{f_\chi}(a)|.$$

La liaison entre l'amplitude spectrale et la nonlinéarité de f est donnée par:

$$\mathcal{NL}(f) = 2^{m-1} - \frac{1}{2}\mathcal{R}(f).$$

En effet, on a

$$\begin{aligned}\mathcal{NL}(f) &= \min_{g \text{ affine}} \mathrm{d}(f,g) \\ &= \min_{a\in K^m, b\in K}(2^{m-1} + \frac{(-1)^b}{2}\widehat{f}_\chi(a)) \\ &= 2^{m-1} - \tfrac{1}{2}\max_a |\widehat{f}_\chi(a)| \\ &= 2^{m-1} - \tfrac{1}{2}\mathcal{R}(f).\end{aligned}$$

On définit $\mathcal{R}(F) := \max_{a\in L, b\in L^*} |\widehat{b.F}_\chi(a)|$ et $\mathcal{NL}(F) := \min_{b\in L^*} \mathcal{NL}(b.F)$. Évidemment, $\mathcal{NL}(F) = 2^{m-1} - \frac{1}{2}\mathcal{R}(F)$. On s'intéresse aux fonctions avec une grande nonlinéarité, *i.e.*, avec une amplitude spectrale basse. On définit donc

$$\mathcal{R}(m) := \min_{F\in L^L} \mathcal{R}(F),$$

où L^L est l'ensemble de fonctions de L dans L. On dit que la fonction F est *hautement nonlinéaire* si $\mathcal{R}(F) = \mathcal{R}(m)$.

Proposition 3.2 (Identité de Parseval) *Pour une fonction $f : L \to K$ on l'identité suivante:*

$$\sum_{a\in L} \left(\widehat{f}_\chi(a)\right)^2 = 2^{2m}. \tag{2}$$

Preuve. On a

$$\begin{aligned}\sum_{a\in L}(\widehat{f}_\chi(a))^2 &= \sum_{a\in L}\sum_{x\in L}(-1)^{f(x)+\mathrm{Tr}(ax)}\sum_{y\in L}(-1)^{f(y)+\mathrm{Tr}(ay)} \\ &= \sum_{x,y\in L}(-1)^{f(x)+f(y)}\sum_{a\in L}(-1)^{\mathrm{Tr}(a(x+y))} \\ &= 2^m\sum_{x\in L}(-1)^{f(x)+f(x)} = 2^{2m}.\end{aligned}$$

Pour la troisième égalité on a utilisé le fait que la fonction $x \mapsto \mathrm{Tr}(ax)$ est equilibré si $a \neq 0$. □

On obtient ainsi la borne inférieure suivante:

$$\mathcal{R}(f) \geq 2^{\frac{m}{2}}. \tag{3}$$

3.1 Formes quadratiques

Soit $\phi : L \to K$ une forme quadratique. Par définition $\phi(x+y) = \phi(x) + \phi(y) + \varphi(x,y)$, où φ est une forme bilinéaire symétrique. On observe que φ est aussi une

forme symplectique, c'est-à-dire $\varphi(x,x)=0$, pout tout x dans L. On s'intéresse à

$$\begin{aligned}|\widehat{\phi_\chi}(a)|^2 &= \sum_{x\in L}(-1)^{\phi(x)+\mathrm{Tr}(ax)}\sum_{y\in L}(-1)^{\phi(y)+\mathrm{Tr}(ay)}\\ &= \sum_{x\in L}\sum_{y\in L}(-1)^{\phi(x+y)+\varphi(x,y)+\mathrm{Tr}(a(x+y))}\\ &= \sum_{z\in L}\sum_{y\in L}(-1)^{\phi(z)+\varphi(y+z,y)+\mathrm{Tr}(az)}\\ &= \sum_{z\in L}(-1)^{\phi(z)+\mathrm{Tr}(az)}\sum_{y\in L}(-1)^{\varphi(z,y)}.\end{aligned}$$

Soit $\mathrm{Ker}(\phi):=\{x\in L|\varphi(x,y)=0,\forall y\in L\}$. On l'appelle le *noyau* de ϕ. C'est un sous-espace vectoriel de L, de dimension, disons, k. L'application $y\mapsto(-1)^{\varphi(z,y)}$ est un caractère additif. Les relations d'orthogonalité des caractères nous disent que la somme des images d'un caractère non trivial (*i.e.,* pas identiquement 1) vaut zéro. Dans notre cas

$$\sum_{y\in L}(-1)^{\varphi(z,y)}=\begin{cases}2^m, & \text{si } z\in\mathrm{Ker}(\phi);\\ 0, & \text{sinon.}\end{cases}$$

Par conséquence $|\widehat{\phi_\chi}(a)|^2=2^m\sum_{z\in\mathrm{Ker}(\phi)}(-1)^{\phi(z)+\mathrm{Tr}(az)}$. Mais $z\mapsto(-1)^{\phi(z)+\mathrm{Tr}(az)}$ est aussi un caractère de $\mathrm{Ker}(\phi)$, car $\phi(x+y)=\phi(x)+\phi(y),\forall x,y\in\mathrm{Ker}(\phi)$. Alors on a

$$\sum_{z\in\mathrm{Ker}(\phi)}(-1)^{\phi(z)+\mathrm{Tr}(az)}=\begin{cases}2^k, & \text{si } \phi|_{\mathrm{Ker}(\phi)}(z)=\mathrm{Tr}(az),\forall z\in\mathrm{Ker}(\phi);\\ 0, & \text{sinon.}\end{cases}$$

et donc

$$|\widehat{\phi_\chi}(a)|=\begin{cases}2^{\frac{m+k}{2}}, & \text{si } \phi|_{\mathrm{Ker}(\phi)}(z)=\mathrm{Tr}(az),\forall z\in\mathrm{Ker}(\phi);\\ 0, & \text{sinon.}\end{cases}\tag{4}$$

Comme $\phi|_{\mathrm{Ker}(\phi)}$ est linéaire sur $\mathrm{Ker}(\phi)$, on a que $\exists a\in L$ tel que $\phi|_{\mathrm{Ker}(\phi)}(z)=\mathrm{Tr}(az)$. Donc

$$\mathcal{R}(\phi)=2^{\frac{m+k}{2}}.\tag{5}$$

Remarquons que $m+k$ est forcément pair, car $\mathcal{R}(\phi)$ est un entier.

Considérons le cas *pair* (*i.e., m* est pair). Soit $\phi(x)=x_1x_2+x_3x_4+\cdots+x_{m-1}x_m$. Alors

$$\varphi(x,y)=x_1y_2+x_2y_1+x_3y_4+x_4y_3+\cdots+x_{m-1}y_m+x_my_{m-1}$$

On remarque que pour chaque $x\neq 0$ on peut trouver un y tel que $\varphi(x,y)=1$. Donc $\mathrm{Ker}(\phi)=\{0\}$ ou, autrement dit, $k=0$. Comme on a trouvé un ϕ tel que $\mathcal{R}(\phi)=2^{m/2}$ on a que

$$\mathcal{R}(m)=2^{\frac{m}{2}}.$$

Les fonctions booléennes f pour lesquelles on a $\mathcal{R}(f)=2^{m/2}$ s'appellent *fonctions courbes*. Tenant compte de l'identité de Parseval on a la caractérisation suivante: f

est courbe si et seulement si $\widehat{f_\chi}(a) = \pm 2^{m/2}, \forall a \in L$. En effet, si $\mathcal{R}(f) = 2^{m/2}$ alors $|\widehat{f_\chi}(a)| \leq 2^{m/2}$. Si il y a un a tel que $|\widehat{f_\chi}(a)| < 2^{m/2}$ alors $\sum_{a \in L}(\widehat{f_\chi}(a))^2 < 2^{2m}$. Donc en le cas pair les fonctions booléennes hautement nonlinéaires sont les fonctions courbes.

Dans le cas *impair* on prend $\phi(x) = x_1x_2 + x_3x_4 + \cdots + x_{m-2}x_{m-1} + x_m$. On trouve le même $\varphi(x, y)$ que dans le cas pair. Il existe un y tel que $\varphi(x, y)$ n'est pas nulle seulement pour les deux éléments x tel que $x_i = 0, \forall i \in \overline{1, m-1}$. Donc $k = 1$ et ça nous donne l'inégalité:

$$2^{\frac{m}{2}} \leq \mathcal{R}(m) \leq 2^{\frac{m+1}{2}}.$$

On a que pour $m \in \{1, 3, 5, 7\}$, $\mathcal{R}(m) = 2^{(m+1)/2}$. $\mathcal{R}(9)$ n'est pas encore connu. Mykkelveit a conjecturé en 1980 que $\mathcal{R}(m) = 2^{(m+1)/2}$ pour chaque m impair. Mais en 1983, Patterson et Wiedemann ont prouvé que $\mathcal{R}(15) \leq 216 < 256 = 2^{(15+1)/2}$. La conjecture de ce cas est maintenant la suivante:

Conjecture 1 *Pour m impair $\mathcal{R}(m)$ est asymptotiquement égale à $2^{m/2}$.*

4 Paramètres cryptographiques

Les attaques les plus réussies sur l'algorithme DES – le plus employé schéma de chiffrement par blocs – utilisent la structure linéaire de la fonction de ronde. Il s'agit de méthodes de cryptanalyse différentielle (voir [1]) et linéaire (voir [13]). Des études (voir [14], [15]) sur les propriétés de la transformation substutionnelle de DES ont conduit à la description des certains critères qu'un algorithme cryptographique de type DES doit satisfaire. Nous présentons ensuite deux classes de fonctions qui sont parmis les plus difficiles à cryptanalyser par les deux méthodes mentionneés, la référence principale étant [4].

Soit $F : K^m \to K^{m'}$ une fonction. Les deux ensembles suivantes sont utilisées par la cryptanalyse différentielle, respectivement linéaire:

$$\begin{aligned} D_F(a, b) &:= \{x \in K^m | F(x + a) + F(x) = b\}, \\ L_F(a, b) &:= \{x \in K^m | a.x + b.F(x) = 0\}, \end{aligned}$$

où $a \in K^m$ et $b \in K^{m'}$. Soient les deux paramètres

$$\begin{aligned} \delta_F(a, b) &:= \#D_F(a, b), \\ \lambda_F(a, b) &:= \#L_F(a, b) - \tfrac{1}{2}\left|K^m\right|. \end{aligned}$$

La résistence de F peut être mesurée par:

$$\begin{aligned} \Delta_F &:= \max_{a \neq 0, b} \delta_F(a, b), \\ \Lambda_F &:= \max_{a, b \neq 0} \left|\lambda_F(a, b)\right|. \end{aligned}$$

Plus ces valeurs sont petites plus la fonction F est résistante aux méthodes de cryptanalyse différentielle et linéaire.

Pour une fonction $F : L \to L'$ on note $\theta_F : L \times L' \to K$ la fonction caractéristique de F:

$$\theta_F(x,y) := \begin{cases} 1, & \text{si } y = F(x); \\ 0, & \text{si } y \neq F(x). \end{cases}$$

Une fonction vectorielle $F : K^m \to K^{m'}$ est *courbe* si pour tous $c \in K^{m'} \backslash \{0\}$ la fonction booléenne $x \mapsto c.F(x)$ est courbe. Une définition équivalente est la suivante: F est courbe si $|\widehat{\theta_F}(a,c)| = 2^{m/2}, \forall a \in K^m, \forall c \in K^{m'} \backslash \{0\}$. En effet, comme

$$\begin{aligned} \widehat{\theta_F}(a,c) &= \sum_{x \in K^m, y \in K^{m'}} \theta_F(x,y)(-1)^{a.x+c.y} \\ &= \sum_{x \in K^m} (-1)^{a.x+c.F(x)} \\ &= \widehat{c.F}_\chi(a), \end{aligned}$$

les deux definitions expriment la même chose.

Si f et g sont deux fonctions booleennes sur K^m alors on note $f \times g$ le produit de corrélation

$$(f \times g)(z) = \sum_{x \in K^m} f(x)g(z+x), \quad \forall z \in K^m.$$

Lemme 4.1 *On a* $\delta_F(a,b) = (\theta_F \times \theta_F)(a,b), \forall (a,b) \in K^m \times K^{m'}$.

Théorème 4.2 *Pour une fonction* $F : K^m \to K^{m'}$, *on a* $\Delta_F \geq 2^{m-m'}$.

Preuve. On voit que, en fixant a, $\bigcup_{b \in K^{m'}} D_F(a,b) = K^m$ et donc $\sum_{b \in K^{m'}} \delta_F(a,b) = 2^m$. Si $\delta_F(a,b) < 2^{m-m'}, \forall b$ alors $\sum_b \delta_F(a,b) < 2^{m'} 2^{m-m'} = 2^m$. On a donc le résultat énoncé. □

On a aussi $\Delta_F \geq 2$ car si x est une solution pour l'équation $F(x+a) + F(x) = b$ alors $x + a$ est toujours une autre solution . Et comme $\sum_b \delta_F(a,b) = 2^m$ on a au moins une paire (a,b) pour laquelle l'équation a des solutions.

On observe que si F est telle que $\Delta_F = 2^{m-m'}$ alors $\delta_F(a,b) = 2^{m-m'}$, $\forall a \in K^m \backslash \{0\}, \forall b \in K^{m'}$. En effet, si $\exists a, b$ tels que $\delta_F(a,b) < 2^{m-m'}$ alors $\sum_{b'} \delta_F(a,b') < 2^m$ ce qu'est impossible.

Une fonction vectorielle $F : K^m \to K^{m'}$, avec $m > m'$, est *parfaitement non-linéaire* si $\Delta_F = 2^{m-m'}$. La restriction $m > m'$ tient compte des observations précédentes.

On appelle la fonction $Der_a F : K^m \to K^{m'}$, donnée par $x \mapsto F(a+x) + F(x)$ la *dérivé de F dans la direction de a*. On voit que F est parfaitement nonlinéaire si et seulement si, pour chaque $a \in K^m \backslash \{0\}$ fixé, la fonction $Der_a F$ prend chaque valeur exactement $2^{m-m'}$ fois. Quand $m' = 1$ ça signifie que $Der_a F$ est équilibrée pour chaque $a \in K^m \backslash \{0\}$.

Lemme 4.3 *On a* $\lambda_F(a,b) = \frac{1}{2}\widehat{\theta_F}(a,b)$ *pour tous* $(a,b) \in K^m \times K^{m'}$.

On a vu que $\max_{a,b} |\widehat{\theta_F}(a,b)| \geq 2^{m/2}$ et donc, dans le cas que m et m' sont tels que cette borne inférieure peut être atteinte, les fonctions F pour lesquelles Λ_F est minimal sont les fonctions courbes. La valeur de Λ_F dans ce cas est $2^{\frac{m}{2}-1}$.

Le lemme suivant fournit un lien entre les deux paramètres cryptographiques.

Lemme 4.4 *On a l'identité:*

$$2^4 \sum_{(a,b)\in K^m \times K^{m'}} \lambda_F(a,b)^4 = 2^{m+m'} \sum_{(a,b)\in K^m \times K^{m'}} \delta_F(a,b)^2.$$

Preuve. On a, par les lemmes précédentes, que $\lambda_F(a,b) = \frac{1}{2}\widehat{\theta_F}(a,b)$ et $\delta_F(a,b) = (\theta_F \times \theta_F)(a,b)$.

Il suffit alors de démontrer, que pour une fonction $f : K^s \to K$, on a

$$\sum_{x\in K^s} \widehat{f}(x)^4 = 2^s \sum_{x\in K^s} (f \times f)(x)^2.$$

On note $g(x) := (f \times f)(x)$. On a donc

$$\begin{aligned}\sum_{x\in K^s} \widehat{f}(x)^4 &= \sum_{x\in K^s} \widehat{(f \times f)}(x)^2 = \sum_{x\in K^s} \widehat{g}^2(x) \\ &= \sum_{x\in K^s} \widehat{(\widehat{g}^2)}(0) = 2^s \widehat{\widehat{g \times g}}(0) \\ &= 2^s (g \times g)(0) = 2^s \sum_{x\in K^s} g(x)^2.\end{aligned}$$

□

Théorème 4.5 *Une fonction est parfaitement nonlinéaire si et seulement si elle est courbe.*

Théorème 4.6 *Les fonctions* $F : K^m \to K^{m'}$ *courbes existent seulement pour* m *pair et* $m \geq 2m'$.

Donc pour m pair et $m \geq 2m'$ la resistance à la cryptanalyse linéaire est équivalente à la resistance à la cryptanalyse différentielle. Pour les autres cas on doit trouver autres bornes.

On a vu que $\Delta_F \geq 2$. On appelle une fonction pour laquelle $\Delta_F = 2$ une fonction *presque parfaitement nonlinéaire* ou *APN* (de "almost perfect nonlinear").

Comme $\Delta_F \geq 2^{m-m'}$ les fonctions APN peuvent exister seulement si $m' \geq m$ (on ne considère pas le cas $m = 2$ et $m' = 1$, car il est trivial). On va voir que cette borne (c'est-à-dire 2) est atteinte; et donc, les fonctions résistantes à la cryptanalyse différentielle, dans ce cas, sont les fonctions APN.

Théorème 4.7 *Pour les fonctions $F : K^m \to K^m$ on a:*

$$\Lambda(F) \geq 2^{\frac{m-1}{2}}.$$

On a égalité si et seulement si F est APN et $\lambda_F(a,b) \in \{0, \pm 2^{(m-1)/2}\}, \forall a, b \neq 0$.

Quand on a égalité, on appelle F fonction *presque courbe* ou AB (de "almost bent"). On voit que, pour avoir égalité, m est nécessairement impair. On observe aussi l'analogie avec les fonctions courbes: le spectre de Fourier d'une fonction courbe prend exactement deux valeurs, celui d'une fonction AB presque courbe prend exactement trois valeurs.

Théorème 4.8 *Si une fonction $F : K^m \to K^m$ est invertible alors $\Lambda(F^{-1}) = \Lambda(F)$ et $\Delta(F^{-1}) = \Delta(F)$.*

On dit qu'une fonction F est *v-divisible* si $2^v | \widehat{F_\chi}(x), \forall x \in L$.

Proposition 4.9 *Une fonction $F : K^m \to K^m$ est AB si et seulement si elle est APN et $\frac{m+1}{2}$-divisible.*

Preuve. Si F est AB alors, par définition, F est APN et on a $\widehat{b.F_\chi}(a) \in \{0, \pm 2^{(m+1)/2}\}$, $\forall b \in K^m \backslash \{0\}, \forall a \in K^m$. Donc F est $\frac{m+1}{2}$-divisible.

Si F est APN et $\frac{m+1}{2}$-divisible, alors $\delta_F(a,b) \leq 2, \forall a \in K^m \backslash \{0\}, \forall b \in K^m$ et $2^{(m+1)/2} | \widehat{b.F_\chi}(a,b), \forall a \in K^m, \forall b \in K^m \backslash \{0\}$.

Alors, pour chaque a et $b \neq 0$ on peut écrire $\widehat{b.F_\chi}(a) = 2^{(m+1)/2} z_b(a)$, où $z_b(a)$ est un entier.

La relation de Parseval nous dit que, $\forall b \neq 0$,

$$\begin{aligned} \sum_{a \in K^m} \widehat{b.F_\chi}(a)^2 = 2^{2m} &\iff \sum_a 2^{m+1} z_b(a)^2 = 2^{2m} \\ &\iff \sum_a z_b(a)^2 = 2^{m-1} \\ &\implies \sum_{b \neq 0, a} z_b(a)^2 = 2^{m-1}(2^m - 1). \end{aligned} \tag{6}$$

On a obtenu, dans la preuve du théorème 4.7, que

$$\sum_{a,b \neq 0} \widehat{b.F_\chi}(a)^4 \geq 2^{4m+1} - 2^{3m+1} = 2^{2m+2} \times 2^{m-1} \times (2^m - 1).$$

Tenant compte que l'égalité s'obtient quand F est APN, et que nous sommes dans ce cas, on a

$$\sum_{b \neq 0, a} z_b(a)^4 = 2^{m-1}(2^m - 1). \tag{7}$$

De (6) et (7) on voit que

$$\sum_{b\neq 0,a} z_b(a)^2 = \sum_{b\neq 0,a} z_b(a)^4.$$

Mais on peut avoir cette égalité si et seulement si $z_b(a)^2 \in \{0,1\}, \forall a, b \neq 0$. C'est-à-dire on doit avoir $\widehat{b.F_\chi}(a) \in \{0, \pm 2^{(m+1)/2}\}, \forall a, b \neq 0$, ou encore, F doit être AB. □

5 Fonctions puissance

On considère dans cette section les fonctions puissance: $F_s(x) = x^s, \forall x \in L$. On oublie parfois l'indice s, car il n'y a pas de risques de confusion.

En ce qui concerne la nonlinéarité des fonctions puissance la situation est inverse que dans le cas général. Dans le sens que on connaît sa valeur dans le cas impair et on ne le connaît pas dans le cas pair. Dans ce cas il existe la conjecture suivante, énoncée en 1980 dans [16].

Conjecture 2 *Soit m pair et $(s, 2^m - 1) = 1$. Alors $\mathcal{R}(F_s) \geq 2^{\frac{m}{2}+1}$.*

Proposition 5.1 *On a*

$$\min_s \mathcal{R}(F_s) = 2^{\frac{m+1}{2}} \text{ si } m \text{ est impair;}$$
$$\min_s \mathcal{R}(F_s) \leq 2^{\frac{m}{2}+1} \text{ si } m \text{ est pair.}$$

Preuve. On a montré dans le théorème 4.7 que $\Lambda_F \geq 2^{(m-1)/2}$, ou équivalentement, $\mathcal{R}(F) \geq 2^{(m+1)/2}$. Mais on va voir que, dans le cas impair, il existe des s tel que $\mathcal{R}(F_s) = 2^{(m+1)/2}$.

Dans le cas pair il existe s tel que $\mathcal{R}(F_s) = 2^{\frac{m}{2}+1}$ (voir [6] pour une liste, conjecturée complète). □

Si la fonction F_s est telle que $\mathcal{R}(F_s) = \min_{s'} \mathcal{R}(F_{s'})$ alors on appelle s un *bon exposant*. Si m est impair de proposition 5.1 découle que s est un bon exposant si et seulement si il est un AB-exposant. Rappelons que dans le cas pair il n'y a pas de fonctions AB.

Si s est invertible alors la fonction $x \mapsto x^s$ est une permutation de L. On déduit que si s est un bon exposant alors s^{-1} est un bon exposant, et si F_s est APN alors $F_{s^{-1}}$ est APN. L'automorphisme de Fröbenius, $x \mapsto x^2$, montre que le spectre de Fourier de F_s ne depend pas de la classe cyclotomique de s modulo $2^m - 1$, et aussi, que F_s et F_{2s} ont le même caractère APN. En vu de ces observations, on dit que deux exposants s et s' sont *équivalents* si s' et s, ou s' et s^{-1} appartiennent à la même classe cyclotomique.

Le tableau suivant contient la liste des bons exposants connus dans le cas impair, à équivalence près, avec la mention que, dans le cas Gold et Kasami, les exposants correspondants à r et $m - r$ sont équivalents.

cas	s	condition	référence
Gold	2^r+1	$(r,m)=1$	[9]
Kasami	$2^{2r}-2^r+1$	$(r,m)=1$	[11]
Welch	$2^{(m-1)/2}+3$		[2]
Niho	$2^{2r}+2^r-1$	$4r \equiv 1 (\mathrm{mod}\, m)$	[10]

Tableau 1: Les bons exposants connus pour m impair.

Conjecture 3 (Dobbertin) *Si m est impair et s est un bon exposant alors s est de type Gold, Kasami, Welch ou Niho.*

On note avec $f_s : L \to K$ la fonction booléenne associée à F_s, $f_s(x) := \mathrm{Tr}(F_s(x))$, $\forall x \in L$. Aussi, pour quelconque $a \in \mathbb{Z}$ on note par $\mathrm{w}_2(a)$, la somme des chiffres du résidue de a modulo 2^m-1. La proposition suivante nous dit quel est le degré de cette fonction.

Proposition 5.2 *Soit $c \in L^*$. Si F_s n'est pas identiquement nulle alors*

$$\deg\big(\mathrm{Tr} \circ (cF_s)\big) = \mathrm{w}_2(s).$$

Preuve. Soit $(\beta_1, \beta_2, \ldots, \beta_m)$ une base normale primitive de L sur K. On écrit $s = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_w}$ où $w = \mathrm{w}_2(s)$ et $r_i \in \overline{1,m}, \forall i \in \overline{1,w}$. On a

$$\begin{aligned}
\mathrm{Tr}\big(aF_s(x)\big) &= \mathrm{Tr}\left(c(x_1\beta_1 + x_2\beta_2 + \cdots + x_m\beta_m)^{2^{r_1}+2^{r_2}+\cdots+2^{r_w}}\right) \\
&= \mathrm{Tr}\left(c\prod_{i=1}^{w}\left(x_1\beta_1^{2^{r_i}} + x_2\beta_2^{2^{r_i}} + \cdots + x_m\beta_m^{2^{r_i}}\right)\right) \\
&= \mathrm{Tr}\left(c\sum_{i_1,i_2,\ldots,i_w} x_{i_1}x_{i_2}\ldots x_{i_w}\beta_{i_1}^{2^{r_1}}\beta_{i_2}^{2^{r_2}}\ldots\beta_{i_w}^{2^{r_w}}\right) \\
&= \sum_{i_1,i_2,\ldots,i_w} x_{i_1}x_{i_2}\ldots x_{i_w}\,\mathrm{Tr}\left(c\beta_{i_1}^{2^{r_1}}\beta_{i_2}^{2^{r_2}}\ldots\beta_{i_w}^{2^{r_w}}\right) \\
&= \sum_{i_1,i_2,\ldots,i_w} \mathrm{Tr}\left(c\beta^{2^{i_1}+r_1}\beta^{2^{i_2}+r_2}\ldots\beta^{2^{i_w}+r_w}\right)x_{i_1}x_{i_2}\ldots x_{i_w}.
\end{aligned}$$

D'où on voit que le degré de $\mathrm{Tr} \circ (cF_s)$ est au plus w. On omet la démonstration de l'égalité, qui peut être trouvée dans [3]. □

Cette proposition nous montre que pour les exposants de type Gold et Welch, la fonctions booléenne associée est une forme quadratique, respectivement cubique. En fait, aussi dans les cas de Kasami et Niho on peut trouver des liaisons avec la théorie des formes quadratiques, respectivement cubiques.

Une autre conséquence de la proposition précédente et que, pour m impair, si s est un bon exposant, alors $\mathrm{w}_2(s) \leq (m+1)/2$. En effet, si F_s est AB alors $2^{(m+1)/2} \mid \widehat{f_\chi}(a), \forall a \in L$, et l'inégalité découle de la proposition 2.5.

Si $(s, 2^m - 1) = 1$ alors

$$\begin{aligned}\widehat{(c.F_s)}_\chi(a) &= \sum_x \chi\big(\operatorname{Tr}(cx^s + ax)\big) \\ &= \sum_x \chi\Big(\operatorname{Tr}\big(c(c^{-s^{-1}}x)^s + a(c^{-s^{-1}}x)\big)\Big) \\ &= \sum_x \chi\big(\operatorname{Tr}(x^s + ac^{-s^{-1}}x)\big) \\ &= \widehat{F_\chi}\big(ac^{-s^{-1}}\big),\end{aligned}$$

car $x \mapsto cx^{-s^{-1}}$ est un permutation pour $c \neq 0$. Donc, dans ce cas, on a

$$\mathcal{R}(F_s) = \max_a |\widehat{F_{s\chi}}(a)|.$$

5.1 Divisibilité

Dans l'étude des fonctions puissance, la divisibilité des coefficients de Fourier est importante. Dans le contexte de codes, un théorème de McEliece sur la divisibilité des poids des mots d'un code cyclique permet d'obtenir une caractérisation intéressante. Pour démontrer les conjectures de Welch et Niho, c'est ce théorème et la proprieté APN des fonctions correspondentes (voir [8], respectivement [7]) qui ont été utilisés. Mais on peut obtenir la même caractérisation en utilisant les sommes de Gauss et le théorème de Stickelberger (voir [12]). Dans cette section nous présentons cette approche et quelques proprietés qui y suivent.

On représente le corps L comme $\mathbb{Z}[\zeta]/\mathcal{P}$, où ζ est la racine principale d'ordre $2^m - 1$ de l'unité et $\mathcal{P}$ est un idéal premier de $\mathbb{Z}[\zeta]$ tel que $2 \in \mathcal{P}$. Soit

$$G_L(\psi) := \sum_{x \in L^*} \psi(x)\chi(x)$$

la *somme de Gauss* associée au caractère multiplicatif ψ de L^*, χ étant le caractère additif canonique de L. Comme $G_L(\psi)$ peut être vue comme la transformé de Fourier de χ dans ψ, on a, par la formule d'inversion, que:

$$\chi(x) = \frac{1}{n} \sum_{\psi \in \widehat{L^*}} G_L(\psi)\overline{\psi(x)}.$$

On peut écrire

$$\begin{aligned}
\widehat{F_{s\chi}}(a) &= \sum_{x\in L}\chi(x^s+ax) = 1+\sum_{x\in L^*}\chi(ax)\chi(x^s)\\
&= 1+\frac{1}{q-1}\sum_{x\in L^*}\chi(ax)\Big(\sum_{\psi\in\widehat{L^*}}G_L(\psi)\overline{\psi(x^s)}\Big)\\
&= 1+\frac{1}{q-1}\sum_{\psi\in\widehat{L^*}}G_L(\psi)\sum_{x\in L^*}\chi(ax)\overline{\psi}^s(x)\overline{\psi}^s(a)\psi^s(a)\\
&= 1+\frac{1}{q-1}\sum_{\psi\in\widehat{L^*}}G_L(\psi)\psi^s(a)\sum_{x\in L^*}\chi(ax)\overline{\psi}^s(ax)\\
&= 1+\frac{1}{q-1}\sum_{\psi\in\widehat{L^*}}G_L(\psi)\psi^s(a)G_L(\overline{\psi}^s)\\
&= 1+\frac{1}{q-1}\sum_{j=0}^{q-2}G_L(\overline{\omega}^j)G_L(\overline{\omega}^{-jd})\overline{\omega}^{jd}(a),
\end{aligned}$$

où ω est *le caractère de Teichmüller*, c'est-à-dire $\omega : \mathbb{Z}[\zeta]/\mathcal{P} \to \mathbb{Z}[\zeta]$, donnée par $[a]_{\mathcal{P}} \mapsto a$.

Soient

$$\begin{aligned}
\nu_s :=&\ \min_{0<j<2^m-1}\big(\mathrm{w}_2(-js)+\mathrm{w}_2(j)\big),\\
J_s :=&\ \big\{j|0<j<2^m-1 \text{ et } \mathrm{w}_2(-js)+\mathrm{w}_2(j)=\nu_s\big\},\\
P_s(X) :=&\ \textstyle\sum_{j\in J_s}X^j,\ P\in L[X].
\end{aligned}$$

Proposition 5.3 *La fonction puissance $x \mapsto x^s$ est ν_s-divisible mais pas plus.*

Preuve. Les congruences de Stickelberger affirment que

$$-G_L(\overline{\omega}^j) \equiv (-2)^{\mathrm{w}_2(j)} (\mathrm{mod}\, \mathcal{P}^{\mathrm{w}_2(j)+1}).$$

Alors on obtient que

$$\sum_{j=1}^{q-2}G_L(\overline{\omega}^j)G_L(\overline{\omega}^{-js})\overline{\omega}^{js}(a) \equiv (-2)^{\nu_s}\sum_{j\in J_s}\overline{\omega}^{js}(a)(\mathrm{mod}\,\mathcal{P}^{\nu_s+1}).$$

Pour un entier t multiple de $q-1$ on a $\frac{t}{q-1} \equiv -t(\mathrm{mod}\, q)$. Et comme $(-2)^{\nu_s} \equiv -2^{\nu_s}(\mathrm{mod}\,\mathcal{P}^{\nu_s+1})$, car $2 \in \mathcal{P}$, alors on obtient les suivantes:

$$\begin{aligned}
\widehat{f}_\chi(a) &= \frac{q}{q-1}+\frac{1}{q-1}\sum_{j=1}^{q-2}G_L(\overline{\omega}^j)G_L(\overline{\omega}^{-js})\overline{\omega}^{js}(a)\\
&\equiv \frac{1}{q-1}\big(q+(-2)^{\nu_s}\sum_{j\in J_s}\overline{\omega}^{js}(a)\big)(\mathrm{mod}\,\mathcal{P}^{\nu_s+1})\\
&\equiv 2^{\nu_s}\sum_{j\in J_s}\overline{\omega}^{js}(a)(\mathrm{mod}\,\mathcal{P}^{\nu_s+1}).
\end{aligned}$$

Donc $\widehat{f_\chi}(a) \equiv 2^{\nu_s} P_s(a^{-s}) (\mathrm{mod}\, \mathcal{P}^{\nu_s+1})$ et par conséquent, $2^{\nu_s} | \widehat{f_\chi}(a), \forall a \in L$.

Comme $P_s(X^s)$ n'est pas identiquement nul sur L, il existe un $a \in L$ tel que $P_s(a^{-s}) \neq 0$ et donc $2^{\nu_s+1} \nmid \widehat{f_\chi}(a)$. □

On considère dans ce qui suit que m est *impair*.

On observe que $\mathrm{w}_2(2j) = \mathrm{w}_2(j)$ et on déduit que J_s est une réunion de classes cyclotomiques. Pour un entier $0 < k < 2^m - 1$ soit C_k la classe cyclotomique qu'il génère. On note $m_k := |C_k|$ et $d_k := m/m_k$. Alors pour $j \in C_k$ on a

$$\mathrm{Tr}(x^j) = \sum_{l=0}^{d_k-1} \sum_{i=0}^{m_k-1} (x^{2^i})^{j 2^{l m_k}} = d_k \sum_{i=0}^{m_k-1} x^{j 2^i} = \sum_{i=0}^{m_k-1} x^{j 2^i} = \sum_{l \in C_k} x^l,$$

car $2^{m_k} j \equiv j (\mathrm{mod}\, 2^m - 1)$ et d_k est impair. On peut définir alors

$$Q_s(X) := \sum_{j \in J_s^0} X^j,$$

où J_s^0 est l'ensemble des représentants minimaux de chaque classe cyclotomique de J_s. On voit que $P_s(X) = \mathrm{Tr}_L\big(Q_s(X)\big)$.

Si $P_s(a) = 1$ alors $\widehat{f_\chi}(a) \equiv 2^{\nu_s} (\mathrm{mod}\, 2^{\nu_s+1})$. Et comme, évidemment, si $P_s(a^{-s}) = 0$ alors $2^{\nu_s+1} | \widehat{f_\chi}(a)$, on a l'équivalence

$$P_s(a^{-s}) = 0 \iff 2^{\nu_s+1} | \widehat{f_\chi}(a). \tag{8}$$

Si F_s est AB alors on peut dire encore plus, c'est-à-dire

$$P_s(a^{-s}) = 0 \iff \widehat{f_\chi}(a) = 0. \tag{9}$$

On peut donc, si s est un bon exposant, caracatériser le support de $\widehat{f_\chi}$ en fonction de J_s:

$$\mathrm{Supp}(\widehat{f_\chi}) := \{a \in L | \widehat{f_\chi}(a) \neq 0\} = \{a \in L | \, \mathrm{Tr}\Big(\sum_{j \in J_s^0} a^{-js}\Big) = 1\}. \tag{10}$$

Lemme 5.4 *Si la fonction puissance x^s est $\frac{m+1}{2}$-divisible alors s est invertible.*

Preuve. Si s n'est pas invertible alors il existe $t \neq 0$ tel que $st \equiv 0 (\mathrm{mod}\, n)$. Comme dans notre hypothèse on a $\mathrm{w}_2(-js) + \mathrm{w}_2(j) \geq (m+1)/2$, $\forall j$, $0 < j < 2^m - 1$, on déduit $\mathrm{w}_2(t) \geq (m+1)/2$ et $\mathrm{w}_2(-t) \geq (m+1)/2$. Mais ça n'est pas possible car $\mathrm{w}_2(t) + \mathrm{w}_2(-t) = m$. □

Corollaire 5.5 *Si la fonction F_s est AB alors $(s, 2^m - 1) = 1$.*

La propriété analogue de l'assertion précédente pour les fonctions APN est aussi vraie.

Proposition 5.6 *Si la fonction F_s est APN alors $(s, 2^m - 1) = 1$.*

Théorème 5.7 *L'entier s est un bon exposant si et seulement si $\nu_s = (m+1)/2$ et $P_s(X)$ a 2^{m-1} racines dans L.*

Preuve. Soit $z(a)$ le nombre entier tel que $\widehat{f_\chi}(a) = z(a)2^{\nu_s}$. Par la relation de Parseval on a que $\sum_{a\in L} z^2(a)2^{2\nu_s} = 2^{2m}$, d'où $\sum_{a\in L} z^2(a) = 2^{2m-2\nu_s}$.

On suppose que $\nu_s = (m+1)/2$ et $P_s(X)$ a 2^{m-1} racines. Comme de $2^{\nu_s+1} \mid \widehat{f_\chi}(a)$ résulte que $z(a)$ est pair, l'équivalence (8) et le lemme 5.4 nous montrent que exactement un demi des $z(a)$ sont pairs. Par conséquent, il y a 2^{m-1} des $z(a)$ impairs. Alors

$$2^{m-1} = \sum_{a\in L} z^2(a) \geq \sum_{z(a)\equiv 1 (\mathrm{mod}\, 2)} z^2(a) = 2^{m-1}.$$

On doit avoir egalité, ce que implique $z(a) \in \{0, \pm 1\}, \forall a \in L$. Donc F_s est AB.

Réciproquement, on suppose $z(a) \in \{0, \pm 1\}, \forall a \in L$. Alors $\sum_{a\in L} z(a)^2 = 2^{m-1}$, d'où on voit qu'il y a $2^m - 1$ des $z(a)$ égaux à 0. Comme la relation (9) est équivalente à: $|z(a)| = 0 \Leftrightarrow P_s(a^{-s}) = 0$, on voit que $P_s(X)$ a 2^{m-1} racines dans L. □

Corollaire 5.8 *Soit s un nombre entier. Si $\nu_s = (m+1)/2$ et la fonction polynomiale associée à $Q_s(X)$ est une permutation alors s est un bon exposant.*

Preuve. Dans ce cas $P_s(X) = \mathrm{Tr}_L\left(Q_s(X)\right)$ a 2^{m-1} racines dans L car la fonction trace est une fonction équilibrée. □

On observe que si $\nu_s = (m+1)/2$ et J_s est réduit à une seule classe cyclotomique alors s est un bon exposant, car en ce cas s est invertible et donc $Q_s(X)$ est une permutation. On a verifié expérimentalement pour $m \leq 39$ que les seuls exposants pour lesquels $|J_s^0| = 1$ sont ceux de type Gold et un certain exposant de type Kasami si $3 \nmid m$. Dans le sens invers: si s est dans un de ces cas, alors $|J_s^0| = 1$, on sait que l'affirmation est vrai (voir la section suivante pour le cas Gold et la remarque 2 à la page 27 pour le cas Kasami).

5.2 Le cas Gold

Les deux théorèmes suivants donnent les propriétés des fonctions puissance d'exposant de type Gold. Le premier théorème est énoncé pour m quelconque, tandis que le deuxième pour m impair.

Théorème 5.9 *Soit $s = 2^r + 1$. Alors*

$$\Delta_{F_s} = 2^{(r,m)}$$

et si $(s, 2^m - 1) = 1$ alors

$$\mathcal{R}(F_s) = 2^{\frac{m+(2r,m)}{2}}.$$

Preuve. Soit $a, b \in L, a \neq 0$. L'équation

$$(x+a)^{2^r+1} + x^{2^r+1} = b$$

a zéro ou au moins deux solution. On suppose qu'elle a au moins deux solutions x et y. On a

$$\begin{aligned} (x+a)^{2^r+1} + x^{2^r+1} = b \quad &\Longleftrightarrow \\ (x+a)(x^{2^r} + a^{2^r}) + x^{2^r+1} = b \quad &\Longleftrightarrow \\ xa^{2^r} + ax^{2^r} = a^{2^r+1} + b. & \end{aligned}$$

Et pareillement pour y, d'où, en sommant,

$$\begin{aligned} (x+y)a^{2^r} + a(x+y)^{2^r} = 0 \quad &\Longleftrightarrow \\ (x+y)^{2^r-1} = a^{2^r-1}. & \end{aligned}$$

D'ici on voit que $((x+y)a^{-1})^{2^r-1} = 1$. Comme $((x+y)a^{-1})^{2^m-1} = 1$ et $(2^m-1, 2^r-1) = 2^{(m,r)}-1$ on a que $(x+y)a^{-1} \in \mathbb{F}^*_{2^{(m,r)}}$, ou équivalentement, $(x+y) \in a\mathbb{F}^*_{2^{(m,r)}}$. Donc étant donné une solution x_0 l'ensemble de toutes les solutions est $x_0 + a\mathbb{F}_{2^{(m,r)}}$ qui est de cardinal $2^{(m,r)}$. Ainsi on a $\Delta_{F_s} = 2^{(r,m)}$.

On a déjà remarqué que f_s est une forme quadratique. On pourrait alors déterminer $\mathcal{R}(F_s)$ avec (5), à partir de la dimension de

$$\mathrm{Ker}(f_s) = \{x \in L | \, \mathrm{Tr}\left(xy^{2^r} + yx^{2^r}\right) = 0, \forall y \in L\}.$$

Soit $x \in \mathrm{Ker}(f_s)$. On a $\mathrm{Tr}(xy^{2^r}) = \mathrm{Tr}(x^{2^r}y) = \mathrm{Tr}(x^{2^{2r}}y^{2^r}), \forall y \in L$. Comme $y \mapsto y^{2^r}$ est une permutation de L, on doit avoir $x = x^{2^{2r}}$, c'est-à-dire $x \in \mathbb{F}_{2^{(m,2r)}}$. Ici on a utilisé la propriété suivante de la fonction trace: si $\mathrm{Tr}(az) = 0, \forall z \in L$ alors $a = 0$. Donc on a que $\dim\left(\mathrm{Ker}(f_s)\right) = (m, 2r)$, d'où $\mathcal{R}(F_s) = 2^{(m+(2r,m))/2}$. □

Théorème 5.10 *Soit s un exposant tel que $(s, 2^m-1) = 1$. L'exposant s est de type Gold,* i.e., *$s = 2^r+1$ et $(r, m) = 1$, si et seulement si $\nu_s = (m+1)/2$ et J_s est égal à la classe cyclotomique de $-s^{-1}$.*

Preuve. On suppose d'abord que s est de type Gold. Comme $(r, m) = 1$ et m est impair, s est un bon exposant et donc $\nu_s = (m+1)/2$. On a vu plus haut que F_s est une forme quadratique et que son noyau est $\{x \in L | x^{2^{2r}} = x\} = K$, car $(2r, m) = 1$. Alors le coefficient de Fourier de f_χ, donné par (4), est

$$|\widehat{f_\chi}(a)| = \begin{cases} 2^{\frac{m+1}{2}}, & \text{si } f|_K(z) = Tr(az), \forall z \in K; \\ 0, & \text{sinon.} \end{cases}$$

C'est-à-dire $\widehat{f_\chi}(a) = 2^{(m+1)/2} \Leftrightarrow \mathrm{Tr}(a) = 1$. Et encore, en vu de l'équivalence (9), $P_s(a^{-s}) = 0 \Leftrightarrow \mathrm{Tr}(a) = 0, \forall a \in L$. Donc les deux polynômes sont égaux, c'est-à-dire $\{-js | j \in J\} = C_1$, d'où $J_s = C_{-s^{-1}}$.

□

6 Algorithme de multiplication modulaire

Dans cette section on considère toujours m impair et s un exposant tel que $(s, 2^m - 1) = 1$. On a vu dans la section précédente que la divisibilité de la fonction puissance d'exposant s est liée à la quantité

$$\nu_s = \min_{0<a<2^m-1} \big(\mathrm{w}_2(-sa) + \mathrm{w}_2(a) \big).$$

Pour etudier ν_s on préfère une forme équivalente obtenue en observant que $\mathrm{w}_2(-sa) = m - \mathrm{w}_2(sa)$. On définit alors

$$\eta_s := \max_{0<a<2^m-1} \big(\mathrm{w}_2(sa) - \mathrm{w}_2(a) \big).$$

On voit que $\nu_s + \eta_s = m$.

Hollman et Xiang décrivent dans l'article [10] une approche pour l'étude de η_s avec l'aide d'un algorithme de type "addition avec transport" pour la multiplication modulaire. Cette méthode leur permet de montrer que $\eta_s = (m-1)/2$ pour les quatre bons exposants dans le cas impair, et de prouver ainsi les conjectures de Welch et Niho. Nous suivons la ligne de cet article, en présentant cette approche et la détermination de η_s dans le cas des exposants Gold et Kasami. En plus, pour ces exposants nous caractérisons l'ensemble J_s. Pour le cas Gold, nous avons vu dans la section précédente qu'on arrive à décrire cet ensemble, mais avec l'aide des outils différentes. Pour l'exposant de type Kasami une description équivalente dans le sens de la relation (10) a été donnée par Dillon dans [5]. La démonstration du lemme 6.1 a été esquissée par Langevin.

Pour un entier quelconque a, $0 \le a \le 2^m - 1$, on note avec $a_{m-1}, \ldots, a_1, a_0$, sa représentation binaire, c'est-à-dire $a = 2^{m-1}a_{m-1} + \cdots + 2a_1 + a_0$. On identifie souvent a avec la suite de longueur m: $a_{m-1}, \ldots, a_1, a_0$ ou avec la suite périodique infinie de période m qui s'en déduit. C'est pour cette raison qu'on prend toujours dans cette section les indices modulo m.

Pour une suite périodique d'entiers $(a_i)_{i\in\mathbb{Z}}$, de période m, on note

$$a^{[k]} := \sum_{i=0}^{m-1} a_{i+k} 2^i.$$

Si a est un entier, $0 \le a \le 2^m - 1$, alors $a^{[k]}$ signifie le décalage cyclique à droite de ses chiffres binaires avec k positions. Observons que la multiplication modulo $2^m - 1$ de a par 2 est équivalente avec un décalage cyclique à gauche avec une position. En effet:

$$2a = a_{m-1} + 2a_0 + 2^2 a_1 + \cdots + 2^{m-1}a_{m-2} + (2^m - 1)a_{m-1} \equiv a^{[m-1]} (\mathrm{mod}\, 2^m - 1).$$

Et en itérant on voit que $2^k a \equiv a^{[m-k]} (\mathrm{mod}\, 2^m - 1), \forall k \ge 0$.

Lemme 6.1 *Soit $(d_i)_{i\in\mathbb{Z}}$ une suite périodique de nombres entiers, de période m. Alors il existe une unique suite $(u_i)_{i\in\mathbb{Z}}$ de nombres entiers satisfaisant*

$$2c_{i+1} = d_i + c_i \tag{11}$$

pout tout i si et seulement si $d^{[0]} \equiv 0 (\mathrm{mod}\, 2^m - 1)$. Si c'est le cas alors pout tout i

$$c_i = \frac{d^{[i]}}{(2^m - 1)}. \tag{12}$$

Preuve. Soit (b_i) la suite donnée par $b_i = 2^i, \forall i \in \overline{0, m-1}$. Puisque on peut voir les suites de longueur m comme des fonctions de $\mathbb{Z}/m\mathbb{Z}$ à valeurs dans $\mathbb{C}$, on peut utiliser les outils de l'analyse de Fourier. On voit ainsi que $d^{[i]} = \sum_{l=0}^{m-1} d_{i+l} b_i = (d \times b)(i)$, où $\times$ dénote le produit de corrélation.

Soit μ un caractère additif de $\mathbb{Z}/m\mathbb{Z}$. Alors $\exists j \in \overline{0, m-1}$ tel que $\mu(i) = (\zeta^j)^i, \forall i \in \overline{0, m-1}$, où ζ est une racine primitive m-ième de l'unité. On a

$$\overline{\widehat{b}(\mu)} = \sum_{i=0}^{m-1} b_i \mu(i) = \sum_{i=0}^{m-1} 2^i \zeta^{ji} = \frac{(2\zeta^j)^m - 1}{2\zeta^j - 1} = \frac{2^m - 1}{2\mu(1) - 1}.$$

Alors

$$\widehat{d}(\mu) = \frac{\widehat{(d \times b)}(\mu)}{\overline{\widehat{b}(\mu)}} = (2\mu(1) - 1)\frac{\widehat{(d \times b)}(\mu)}{2^m - 1}.$$

On voit facilement que la suite des nombres $d^{[i]}/(2^m - 1)$ satisfait la relation (11). Si $d^{[0]} \equiv 0 (\mathrm{mod}\, 2^m - 1)$ alors la suite ne contient pas que d'entiers.

Réciproquement, soit $(c_i)_{i\in\mathbb{Z}}$ une suite telle que $2c_{i+1} = d_i + c_i, \forall i \in \mathbb{Z}$. Alors $2\mu(1)\widehat{c}(\mu) = \widehat{d}(\mu) + \widehat{c}(\mu)$, d'où $\widehat{d}(\mu) = (2\mu(1) - 1)\widehat{c}(\mu)$. En vu de la relation obtenue plus haut, on a

$$\widehat{c}(\mu) = \frac{\widehat{(d \times b)}(\mu)}{2^m - 1}.$$

Et, en appliquant encore une fois la transformée de Fourier, on obtient que

$$c_i = \frac{d^{[i]}}{2^m - 1}.$$

Si on impose que $(c_i)_{i\in\mathbb{Z}}$ soit une suite d'entiers alors on doit avoir $d^{[i]} \equiv 0 (\mathrm{mod}\, 2^m - 1), \forall i \in \mathbb{Z}$. □

Remarque La suite $(c_i)_{i\in\mathbb{Z}}$ satisfaisant la relation (11) est unique. En plus on a $\sum_{i=0}^{m-1} c_i = \sum_{i=0}^{m-1} d_i$.

Théorème 6.2 *Soient $k \in \mathbb{N}^*$ et les nombres $t^{(j)}, b^{(j)} \in \mathbb{Z}$, où $0 \leq b^{(j)} \leq 2^m - 1, \forall j \in \overline{1, k}$. Si $0 \leq u < 2^m - 1$ est tel que*

$$u \equiv \sum_{j=1}^{k} t^{(j)} b^{(j)} (\mathrm{mod}\, 2^m - 1),$$

alors il existe une unique suite d'entiers $(c_i)_{i\in\overline{0,m-1}}$ *telle que, pour tout* i

$$2c_{i+1} + u_i = \sum_{j=1}^{k} t^{(j)} b_i^{(j)} + c_i. \tag{13}$$

En plus, si $\exists j \in \overline{1,k}$ *tel que* $b^{(j)} \not\equiv 0 (\mathrm{mod}\, 2^m - 1)$ *alors pout tout* i

$$t_- \leq c_i < t_+,$$

où $t_- = \sum_{j,t^{(j)}<0} t^{(j)}$ *et* $t_+ = \sum_{j,t^{(j)}>0} t^{(j)}$.

Preuve. Soit $(d_i)_{i\in\overline{0,m-1}}$ la suite suivante:

$$d_i := \sum_{j=1}^{k} t^{(j)} b_i^{(j)} - u_i, \quad \forall i \in \overline{0, m-1}.$$

On voit facilement que le somme $\sum_{i=0}^{m-1} d_i 2^i = \sum_{j=1}^{k} t^{(j)} b^{(j)} - u$, est égale à 0 modulo $2^m - 1$ par hypothèse. On peut alors utiliser le lemme précédent et obtenir ainsi l'existence et l'unicité de la suite (c_i) satisfaisant la relation (13). Et aussi, pour un i quelconque, la formule (12) s'applique:

$$c_i(2^m - 1) = d^{[k]} = \sum_{l=0}^{m-1} 2^l d_{k+l} = \sum_{l=0}^{m-1} 2^l \sum_{j=1}^{k} t^{(j)} b_{k+l}^{(j)} - \sum_{l=0}^{m-1} 2^l u_{k+l}. \tag{14}$$

D'où on déduit les inégalités suivantes:

$$\sum_{j=1}^{k} t^{(j)} \sum_{l=0}^{m-1} 2^l b_{k+l}^{(j)} - (2^m - 1) \leq c_i(2^m - 1) \leq \sum_{j=1}^{k} t^{(j)} \sum_{l=0}^{m-1} 2^l b_{k+l}^{(j)}$$

$$\sum_{j:t^{(j)}<0} t^{(j)} \sum_{l=0}^{m-1} 2^l b_{k+l}^{(j)} - (2^m - 1) \leq c_i(2^m - 1) \leq \sum_{j:t^{(j)}>0} t^{(j)} \sum_{l=0}^{m-1} 2^l b_{k+l}^{(j)}$$

$$t_-(2^m - 1) - (2^m - 1) < c_i(2^m - 1) < t_+(2^m - 1)$$

En simplifiant la dernière inégalité on obtient que $t_- \leq c_i < t_+$. □

Remarque Tenant compte de (14) on a $\sum_{j=1}^{k} t^{(j)} (b^{(j)})^{[i]} = c_i(2^m - 1) + u^{[i]}$. Et comme $0 \leq u < 2^m - 1$ on voit que c_i et $u^{[i]}$ sont le quotient et le reste de la division de $\sum_{j=1}^{k} t^{(j)} (b^{(j)})^{[i]}$ par $2^m - 1$.

On revient maintenant à notre problème, étudier la quantité $\mathrm{w}_2(sa) - \mathrm{w}_2(a)$, où $0 \leq a \leq 2^m - 1$. On distingue rapidement trois choix qu'on peut faire sur les variables k, t^j, b^j du théorème précédent de tel sort que ceci nous donne d'informations sur le produit modulaire sa:

Si on prend $k = 1$, $t^{(1)} = s$, $b^{(1)} = a$, alors on obtient les suivantes, pour tout i:

$$2c_{i+1} + u_i = sa_i + c_i,$$
$$0 \leq c_i < s < 2^m - 1.$$

Comme $sa = \sum_{j=0}^{m-1} s_j 2^j a$, on peut prendre $k = m$, $t^{(j)} = s_{j-1}$, $b^{(j)} = 2^{j-1}a$. Et alors, pour tout i

$$\begin{aligned} 2c_{i+1} + u_i &= \sum_{j=0}^{m-1} s_j a_{i-j} + c_i \Leftrightarrow \\ 2c_{i+1} + u_i &= (s * a)(i) + c_i, \\ 0 \le c_i &< \mathrm{w}_2(s) < m, \end{aligned}$$

où $*$ est le produit de convolution.

Finalement, pour $k = m$ on peut trouver $t^{(j)} \in \{-1, 0, 1\}$ et $e_j \in \overline{0, m-1}$ tels que $s = \sum_{j=1}^{m} t^{(j)} 2^{e_j}$. En prenant $b^{(j)} \equiv 2^{e_j} a (\mathrm{mod}\, 2^m - 1)$, on a pout tout i

$$\begin{aligned} 2c_{i+1} + u_i &= \sum_{j=1}^{m} t^{(j)} a_{i-e_j} + c_i, \qquad (15) \\ t_- \le c_i &< t_+. \end{aligned}$$

Cette dernière approche a l'avantage que les c_i peuvent prendre un nombre plus petit de valeurs que dans les autres cas, car on peut trouver des t^j tels que $t_+ - t_- \le \mathrm{w}_2(s)$.

6.1 Le cas Gold

Dans cette section on traite le cas de l'exposant de type Gold, c'est-à-dire $s = 2^r + 1$, avec $0 < r < m$. On considère $(r, m) = 1$. Alors $(s, 2^m - 1) = 1$, car en général, $(2^k + 1, 2^m - 1) = 1$ si est seulement si $m/(k, m)$ est impair. Soient a et u tels que $0 < a, u < 2^m - 1$ et $u \equiv sa (\mathrm{mod}\, 2^m - 1)$.

Le théorème 6.2 assure que il existe $c_i \in \{0, 1\}, 0 \le i \le m-1$, tels que

$$2c_i + u_i = a_{i-r} + a_i + c_{i-1}. \qquad (16)$$

En sommant pour tous i, on obtient $\mathrm{w}_2(u) - \mathrm{w}_2(a) = \mathrm{w}_2(a) - \mathrm{w}(c)$, où $\mathrm{w}(c) := \sum_{i=0}^{m-1} c_i$. On définit alors $\alpha_i := a_i - c_i, \forall i \in \overline{0, m-1}$. On voit que $\alpha_i \in \{-1, 0, 1\}$.

Lemme 6.3 *Si $\alpha_i = 1$ alors $\alpha_{i-r} \le 0$.*

Preuve. Si $a_i - c_i = 1$ alors $a_i = 1$ et $c_i = 0$ et (16) devient $u_i = 1 + a_{i-r} + c_{i-1}$. Par conséquent $a_{i-r} = 0$ et donc $\alpha_{i-r} \le 0$. On voit aussi que $u_i = 1$ et $c_{i-1} = 0$. □

On définit

$$\mathrm{w}(\alpha) := \sum_{i=0}^{m-1} \alpha_i = \mathrm{w}_2(sa) - \mathrm{w}_2(a).$$

Soit i un indice quelconque. Le lemme précédent nous dit que $(\alpha_{i-jr}, \alpha_{i-(j+1)r}) \neq (1, 1), \forall j$. Comme $(r, m) = 1$, les indices $i - jr$ avec $j \in \overline{0, m-1}$ énumèrent tous les α_j. Alors en sommant les α_j écrits de cette manière on voit que $\mathrm{w}(\alpha) \le (m-1)/2$.

On suppose que $\mathrm{w}(\alpha) = (m-1)/2$. Alors $\alpha_i \in \{0,1\}, \forall i$. En effet, si $\exists i$ tel que $\alpha_i = -1$ alors $\mathrm{w}(\alpha) \leq -1 + (m-1)/2$. On déduit que la suite α contient $(m+1)/2$ zéros et $(m-1)/2$ de 1. On déduit que $\exists i \in \overline{0, m-1}$ tel que $\alpha_i = \alpha_{i-(m-1)r} = 0$ et pour chaque $j \in \overline{0, m-1}$, $\alpha_{i-jr} = 1$ si et seulement si j est impair. On fixe cet indice i. Alors, comme on a vu dans la preuve du lemme,

$$\forall j \in \overline{1, m-1}, a_{i-jr} = \begin{cases} 1, & \text{si } j \text{ est impair;} \\ 0, & \text{si } j \text{ est pair.} \end{cases}$$

Il reste à déterminer la valeur de a_i. Par la définition de α on a $\mathrm{w}_2(u) = \mathrm{w}(\alpha) + \mathrm{w}_2(a) = (m-1)/2 + a_i + (m-1)/2$. Mais comme $0 < u < 2^m - 1$ la somme des chiffres de u ne peut pas être m et alors $a_i = 0$. Donc, à l'equivalence près, a est égal à

$$1 + 2^{2r} + 2^{4r} + \cdots + 2^{(\frac{m-1}{2}-1)2r} = \frac{2^{r(m-1)} - 1}{2^{2r} - 1}.$$

Soit b ce nombre. On a que

$$\begin{aligned} bs &= \frac{2^{r(m-1)} - 1}{2^{2r} - 1}(2^r + 1) \\ &= \frac{2^{r(m-1)} - 1}{2^r - 1} = \frac{2^{rm} - 1}{2^r - 1} - 2^{r(m-1)} \\ &\equiv -2^{rm}2^{-r} \equiv -2^r 2^{-r} \equiv -1 (\mathrm{mod}\, 2^m - 1). \end{aligned}$$

On a prouvé donc:

Proposition 6.4 *On suppose m impair et soit $s = 2^r + 1$, où $0 < r < m$ et $(r, m) = 1$. Alors $\eta_s = (m-1)/2$ et l'ensemble J_s est égal à la classe cyclotomique de $-s^{-1}$.*

6.2 Le cas Kasami

On considère ici le cas de l'exposant de type Kasami, c'est-à-dire $s = 2^{2r} - 2^r + 1$, avec $0 < r < m$. On considère $(r, m) = 1$. Soient a et u tels que $0 \leq a, u < 2^m - 1$, $a \neq 0$ et $u \equiv sa (\mathrm{mod}\, 2^m - 1)$. Le théorème 6.2, avec la relation (13) écrite sous la forme de (15), nous dit que il existe $c_i \in \{-1, 0, 1\}, 0 \leq i \leq m-1$, tels que

$$2c_i + u_i = a_{i-2r} - a_{i-r} + a_i + c_{i-1} \tag{17}$$

En sommant pour tous les i, on obtient $\mathrm{w}(c) = \mathrm{w}_2(a) - \mathrm{w}_2(u)$, où $\mathrm{w}(c) := \sum_{i=0}^{m-1} c_i$.

Lemme 6.5 *Pour tout i, si $c_i = -1$ alors $c_{i-r} \geq 0$.*

Preuve. On suppose qu'il existe un indice i pour lequel $c_i = c_{i-r} = -1$. En sommant les égalités (17) pour les indices i et $i - r$ on obtient:

$$-4 + u_i + u_{i-r} = a_{i-r} + a_{i-3r} + c_{i-1} + c_{i-r-1}. \tag{18}$$

Mais $u_i + u_{i-r} - a_{i-r} - a_{i-3r} \leq 2$, c'est-à-dire $c_{i-1} + c_{i-r-1} \leq -2$, d'où $c_{i-1} = c_{i-r-1} = -1$. En itérant l'argument on trouve que $c_{j-1} = c_{j-r-1} = -1, \forall j \in \overline{0, m-1}$. Ainsi l'égalité (18) devient

$$u_i + u_{i-r} = a_{i-r} + a_{i-3r} + 2.$$

Par conséquent tous les a_i valent 1. Mais ceci contredit notre supposition $a < 2^m - 1$. □

Le lemme précédent nous dit que $(c_i, c_{i-r}) \neq (-1, -1), \forall i \in \overline{0, m-1}$. Et comme $(r, m) = 1$, alors en énumérant $c_i, c_{i-r}, c_{i-2r}, \ldots, c_{i-(m-1)r}$ et en sommant on obtient la borne $\mathrm{w}(c) \geq -\frac{m-1}{2}$, c'est-à-dire

$$\mathrm{w}_2(sa) - \mathrm{w}_2(a) \leq \frac{m-1}{2}.$$

On verra qu'il existe de a tels que ce maximum est atteint. On s'intéresse à la forme de a en ce cas. On ne suppose plus a fixé et on cherche les solutions du système de m équations (17) où $\mathrm{w}(c) = -(m-1)/2$. Alors pour tout i, $c_i \in \{-1, 0\}$. En effet, si $\exists i \in \overline{0, m-1}$ tel que $c_i = 1$ alors $\mathrm{w}(c) \geq 1 - (m-1)/2$. Ainsi dans la suite (c_i) il y a $(m+1)/2$ zéros et $(m-1)/2$ de 1. On déduit que $\exists i \in \overline{0, m-1}$ tel que $c_i = c_{i-(m-1)r} = 0$ et

$$\forall j \in \overline{0, m-1}, \quad c_{i-jr} = \begin{cases} -1, & \text{si } j \text{ est impair;} \\ 0, & \text{si } j \text{ est pair.} \end{cases}$$

On note pour chaque $j \in \overline{0, m-1}$,

$$b_j := a_{i-jr}, \quad d_j := c_{i-jr}, \quad v_j := u_{i-jr}, \tag{19}$$

où le i est celui trouvé plus haut. Alors les d_j sont les suivantes:

$$\forall j \in \overline{0, m-1}, \quad d_j = \begin{cases} -1, & \text{si } j \text{ est impair;} \\ 0, & \text{si } j \text{ est pair.} \end{cases}$$

Pour chaque j on considère $j' \in \overline{0, m-1}$ tel que $j'r \equiv jr + 1 (\mathrm{mod}\, m)$. L'égalité (17) pour l'indice $i - jr$ s'écrit alors

$$2d_j + v_j = b_{j+2} - b_{j+1} + b_j + d_{j'}. \tag{20}$$

On remarque qu'on peut prendre comme ci-dessus les indices modulo m. Soit r^{-1} l'inverse de r modulo m, $1 \leq r^{-1} \leq m-1$. Les équivalences suivantes nous donnent la forme de j':

$$\begin{aligned} j'r \equiv jr + 1 (\mathrm{mod}\, m) &\iff (j' - j) \equiv r^{-1} (\mathrm{mod}\, m) \\ &\iff j' = \begin{cases} j + r^{-1} & \text{si } j < m - r^{-1}, \\ j + r^{-1} - m & \text{si } j \geq m - r^{-1}. \end{cases} \end{aligned} \tag{21}$$

On suppose r^{-1} impair et on note $k := m - r^{-1}$. Alors k est pair. La relation précédente pour j' nous donne

$$j' \equiv \begin{cases} j+1 (\mathrm{mod}\, 2), & \text{si } 0 \leq j < k; \\ j (\mathrm{mod}\, 2), & \text{si } k \leq j \leq m-1. \end{cases}$$

On considère d'abord $0 \leq j < k$. Si j est impair alors j' est pair et l'équation (20) s'écrit:

$$-2 + v_j + b_{j+1} = b_{j+2} + b_j.$$

Comme les variables présentes sont binares on déduit leurs valeurs:

$$b_j = 0,\ b_{j+1} = 1,\ b_{j+2} = 0,\ \text{et } v_j = 1,$$

qui sont en accord avec l'équation qui correspond au indice pair dans (20):

$$v_{j+1} + b_{j+2} = b_{j+3} + b_{j+1} - 1.$$

Donc tous les b_j sont déterminés pour $1 \leq j \leq k+1$, et aussi tous les v_j pour $1 \leq j \leq k-1$.

On observe que si $k = m-1$ alors b est totalement déterminé de cette façon. Mais ce cas est équivalent au cas Gold, car $k = m-1 \Leftrightarrow r^{-1} = 1 \Leftrightarrow r = 1 \Rightarrow s = 3 = 2^1 + 1$.

On considère maintenant $j \geq m - r^{-1}$ et on suppose que $k \leq m-3$. Dans ce cas j et j' ont la même parité et par conséquent l'équation 20 pour un indice pair, respectivement impair, est:

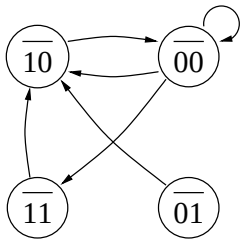
$$\begin{cases} v_j + b_{j+1} = b_{j+2} + b_j, \\ v_{j+1} + b_{j+2} = b_{j+3} + b_{j+1} + 1, \end{cases} \tag{22}$$

où j est pris pair.

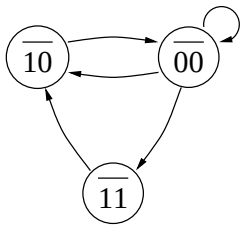
On a obtenu déjà que $b_k = 1$ et $b_{k+1} = 0$. Les égalités (22) correspondantes aux indices k et $k+1$ nous conduisent aux valeurs $b_{k+2} = b_{k+3} = 0$ et $v_k = v_{k+1} = 1$. Ainsi nous sommes conduits à considérer la relation, notée $\rightarrow$, entre les quatre paires (x, y), où $x, y \in \{0, 1\}$, donnée par:

$$(x, y) \rightarrow (z, t) \iff \begin{cases} x + z - y \in \{0, 1\}, \\ 1 + y + t - z \in \{0, 1\}. \end{cases}$$

Les quadruples (x, y, z, t), tel que $(x, y) \rightarrow (z, t)$, sont en correspondance biunivoque avec les quadruples $(b_j, b_{j+1}, b_{j+2}, b_{j+3})$, où j est pair, $k \leq j \leq m-3$, qui satisfont le système (22), c'est-à-dire l'équation (20) pour les indices j et $j+1$. On note par $\overline{00}$ le couple $(0, 0)$ et de même pour les autres paires. On a déjà vu que $\overline{10} \rightarrow \overline{00}$. En analysant toutes les posibilités on obtient le graphe orienté suivant, correspondant à la relation $\rightarrow$:



Tenant compte que $(b_k, b_{k+1}) = (1, 0)$ et que $\#\{(j, j+1) | k \leq j \leq m-1$ et j pair$\} = (r^{-1}+1)/2$, on remarque que chaque chemin de longueur $(r^{-1}+1)/2$ ayant comme sommet de départ $\overline{10}$ conduit à une solution b du système (22), où la longueur d'un chemin est le nombre de sommets qui le composent. Comme on ne peut pas arriver au sommet $\overline{01}$ à partir d'aucun autre sommet, le graphe G qui caractérise les solutions b du système (22) est le suivant:



On verifie facilement, par calcul direct, que la solution ainsi obtenue satisfait l'équation (20) pour les indices $m-1$ et 0. Donc les solutions b du système d'équations (20) sont données par:

$$\begin{cases} b_j = 0, & \text{si } 1 \leq j \leq k+1,\ j \text{ impair}, \\ b_j = 1, & \text{si } 1 \leq j \leq k+1,\ j \text{ pair}, \\ b_k b_{k+1}, b_{k+2} b_{k+3}, \ldots, b_{m-1} b_0 \text{ est un chemin dans le graphe } G. \end{cases} \tag{23}$$

On énonce alors:

Proposition 6.6 *On suppose m impair et soit $s = 2^{2r} - 2^r + 1$, où $0 < r < m$ et $(r, m) = 1$. Alors $\eta_s = (m-1)/2$ et l'ensemble J_s est égal à la réunion des classes cyclotomiques des éléments a qui satisfont*

$$\begin{cases} a_{\varepsilon jr} = 0, & \textit{si } 1 \leq j \leq k+1,\ j \textit{ impair}, \\ a_{\varepsilon jr} = 1, & \textit{si } 1 \leq j \leq k+1,\ j \textit{ pair}, \\ a_\varepsilon a_{\varepsilon - r}, a_{\varepsilon - 2r} a_{\varepsilon - 3r}, \ldots, a_r a_0 \textit{ est un chemin dans le graphe } G, \end{cases}$$

où $\varepsilon := -1$, $k := m - r^{-1}$ si r^{-1} est impair et $\varepsilon := 1$, $k := r^{-1}$ si r^{-1} est pair.

Preuve. Tenant compte de la discussion précédente il nous reste le cas r^{-1} pair et à trouver les classes cyclotomiques des a a partir de (23). Comme les décalages

cycliques d'un élément ne change pas la classe cyclotomique de ceci, alors on peux supposer que $i = 0$ dans (19). Alors on voit que $a_{-jr} = b_j, \forall j \in \mathbb{Z}$. Et comme $-(k+l)r \equiv 1 - lr (\mathrm{mod}\, m), \forall l \in \mathbb{Z}$ on obtient la description énoncée pour r^{-1} impair.

L'exposant s est equivalent à $s' := 2^{2(m-r)} - 2^{m-r} + 1$. En effet, s et s' se trouve dans la même classe cyclotomique car on peut voir que $2^{2r}s' \equiv s (\mathrm{mod}\, 2^m - 1)$. Ainsi les ensembles J_s et J'_s sont égaux. Et on observe que si r^{-1} est pair alors $(m-r)^{-1} = m - r^{-1}$ est impair. En vue de cette observation c'est facile à obtenir la description énoncée pour r^{-1} pair. □

Remarques

1. Les b obtenus par (23) génèrent des classes cyclotomiques différentes, car si on fait un décalage cyclique on ne peut pas tomber sur un élément de l'ensemble J_s parce que la "suite" 1010, présente dans la "partie fixe" de b, ne correspond pas à un chemin dans le graphe G.

   L'expression de j' donnée par (21) nous montre qu'un décalage cyclique de a avec une position correspond à un décalage cyclique de b avec r^{-1} positions. On voit alors que les a correspondants aux b donnés par (23) génèrent, eux aussi, des classes cyclotomiques différentes.

2. Soient x_l, y_l et z_l les nombres des chemins de longueur l dans le graphe G qui ont comme sommet initial $\overline{10}$ et comme sommet terminal $\overline{10}$, $\overline{00}$ et $\overline{11}$ respectivement. En analysant le graphe G on voit que ces nombres sont données par les relations de récurrence suivantes:

$$\begin{cases} x_{l+1} = y_l + z_l, \\ y_{l+1} = x_l + y_l, \\ z_{l+1} = y_l, \end{cases}$$

   avec les valeurs initiales $x_1 = 1$, $y_1 = 0$ et $z_1 = 0$. Ce système de récurrences s'écrit de façon équivalente

$$y_{l+1} = y_l + y_{l-1} + y_{l-2},$$

   avec $y_0 = 0,\ y_1 = 0,\ y_2 = 1$. Le nombre de chemins de longueur l dans le graphe G qui ont comme sommet initial 10 est égale à $x_l + y_l + z_l = y_{l-1} + y_{l-2} + y_l + y_{l-1} = y_{l+1} + y_{l-1}$, si $l > 1$. Tenant compte de la correspondance chemins–solutions décrite plus haut on a

$$|J_s^0| = y_{l_0+1} + y_{l_0-1},$$

   où $l_0 = \frac{1}{2}(r^{-1} + 1)$ et J_s^0 est obtenu en choisissant les représentants minimaux de chaque classe cyclotomique de J_s. On voit aussi que si l_0 est 1 ou 2 alors $|J_s^0| = 1$ et si $l_0 > 2$ alors $|J_s^0| > 1$. Le cas $l_0 = 1$ correspond à $r^{-1} = 1$, c'est-à-dire au cas Gold. Si $l_0 = 2$ alors à $r^{-1} = 3$ et par conséquent $3 \nmid m$. Donc on a qu'il existe un exposant $s \neq 3$ de type Kasami pour lequel l'ensemble J_s est réduit à une seule classe cyclotomique si et seulement si $3 \nmid m$.

3. On observe que l'élément de J_s qui correspond au chemin de G ayant tous les sommets $\overline{00}$ sauf le premier est le plus simple à exprimer sans recourir à sa représentation binaire:

$$2^{\varepsilon 2r} + 2^{\varepsilon 4r} + \cdots + 2^{\varepsilon kr} = 2^{\varepsilon 2r} \frac{2^{\varepsilon kr} - 1}{2^{\varepsilon 2r} - 1}$$

Bibliographie

[1] E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptology **4** (1991), 3–72.

[2] A. Canteaut, P. Charpin and H. Dobbertin, *Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture*, IEEE Trans. Inform. Theory **46** (2000), 4–8.

[3] C. Carlet, *Codes de Reed-Muller, codes de Kerdock et de Preparata*, thèse de doctorat, Paris VI, 1990.

[4] F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis*, Advances in Cryptology–EUROCRYPT'94 (New-York), vol. 950, Springer-Verlag, 1995, pp. 356–365.

[5] J.F. Dillon, *Multiplicative difference sets via additive characters*, Designs, Codes and Cryptography **17** (1999), 225–235.

[6] H. Dobbertin, *One-to-one highly nonlinear power functions on GF*(2^n), AAECC **9** (1998), 139–152.

[7] ———, *Almost perfect nonlinear power functions on GF*(2^n)*: The Niho case*, Inform. and Comput. **151** (1999), 57–72.

[8] ———, *Almost perfect nonlinear power functions on GF*(2^n)*: The Welch case*, IEEE Trans. Inform. Theory **45** (1999), 1271–1275.

[9] R. Gold, *Maximal recursive sequences with 3-valued recursive crosscorrelation functions*, IEEE Transactions of Information Theory **14** (1968), 154–156.

[10] H.D.L. Hollmann and Q. Xiang, *A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences*, Finite Fields and Their Applications **7** (2001), 253–286.

[11] T. Kasami, *The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes*, Inform. and Control **18** (1971), 369–394.

[12] Ph. Langevin and P. Veron, *On the nonlinearity of power functions*, (2004).

[13] M. Matsui, *Linear cryptanalysis method for DES cipher*, Advances in Cryptology–EUROCRYPT'93 (New-York), vol. 765, Springer-Verlag, 1994, pp. 386–397.

[14] K. Nyberg, *Differentially uniform mappings for cryptography*, Advances in Cryptology–EUROCRYPT'93 (New-York), vol. 765, Springer-Verlag, 1994, pp. 55–64.

[15] ———, *S-boxes and round functions with controllable linearity and differential uniformity*, Fast Soft Encryption (New-York), vol. 1008, Springer-Verlag, 1995, pp. 111–129.

[16] D.V. Sarwate and M.B. Pursley, *Crosscorrelation properties of pseudorandom and related sequences*, Proceedings of the IEEE **68** (1980), no. 5, 593–619.