

Fonctions maximalement non linéaires sur un corps fini

Robert Rolland

26 Mars 2000

R. Rolland, C.N.R.S. Institut de Mathématiques de Luminy
Luminy Case 930, F13288 Marseille CEDEX 9
e-mail : rolland@iml.univ-mrs.fr

1 Notations

Soit $q = p^s$ une puissance d'un nombre premier p . Nous noterons \mathbb{F}_q le corps fini à q éléments.

Si $u = (u_1, \dots, u_m)$ et $v = (v_1, \dots, v_m)$ sont deux éléments de \mathbb{F}_q^m on pose

$$\langle u, v \rangle = \sum_{i=1}^m u_i v_i.$$

Ainsi $\langle u, v \rangle$ est un élément de \mathbb{F}_q .

Lorsque $v \in \mathbb{F}_q^m \setminus \{0\}$ et $t \in \mathbb{F}_q$, notons $H_{v,t}$ l'hyperplan de \mathbb{F}_q^m constitué des point $u \in \mathbb{F}_q^m$ tels que $\langle v, u \rangle + t = 0$.

Nous noterons $\mathcal{F}_{(q,m)}$ l'algèbre des fonctions de \mathbb{F}_q^m dans \mathbb{F}_q .

À toute fonction $f \in \mathcal{F}_{(q,m)}$ on associe le mot

$$\left(f(u) \right)_{u \in \mathbb{F}_q^m}.$$

Le code de Reed-Muller d'ordre 1 est le sous espace des mots associés aux fonctions polynomiales de degré 1, c'est à dire aux fonctions

$$f_{v,t}(u) = \langle v, u \rangle + t,$$

où $v \in \mathbb{F}_q^m$ et $t \in \mathbb{F}_q$.

2 Fonctions de \mathbb{F}_q^m dans l'algèbre du groupe \mathbb{F}_q

2.1 Algèbre de groupe

Soit $\mathbb{C}\mathbb{F}_q$ l'algèbre sur le corps des complexes du groupe additif de \mathbb{F}_q , c'est-à-dire l'algèbre des combinaisons linéaires formelles à coefficients dans \mathbb{C}

$$\sum_{t \in \mathbb{F}_q} \alpha_t Z^t$$

où les opérations sont définies par

$$\sum_{t \in \mathbb{F}_q} \alpha_t Z^t + \sum_{t \in \mathbb{F}_q} \beta_t Z^t = \sum_{t \in \mathbb{F}_q} (\alpha_t + \beta_t) Z^t,$$

$$\lambda \left(\sum_{t \in \mathbb{F}_q} \alpha_t Z^t \right) = \sum_{t \in \mathbb{F}_q} (\lambda \alpha_t) Z^t,$$

$$\left(\sum_{t \in \mathbb{F}_q} \alpha_t Z^t \right) \left(\sum_{t \in \mathbb{F}_q} \beta_t Z^t \right) = \sum_{t \in \mathbb{F}_q} \left(\sum_{r+s=t} (\alpha_r \beta_s) \right) Z^t.$$

- $\mathbb{C}\mathbb{F}_p \simeq \mathbb{C}[Z]/(Z^p - 1)$.
- Si $q = p^s$ alors $\mathbb{C}\mathbb{F}_q \simeq \mathbb{C}[Z_1, \dots, Z_s]/(Z_1^p - 1, \dots, Z_s^p - 1)$.

2.2 Les fonctions de \mathbb{F}_q^m dans $\mathbb{C}\mathbb{F}_q$

Soit $\mathcal{G}_{(q,m)}$ l'algèbre des fonctions de \mathbb{F}_q^m dans $\mathbb{C}\mathbb{F}_q$. Si ϕ est une fonction de $\mathcal{G}_{(q,m)}$, on peut écrire pour tout $u \in \mathbb{F}_q^m$

$$\phi(u) = \sum_{t \in \mathbb{F}_q} C_t(\phi)(u) Z^t,$$

ce qui nous permet de définir à partir de la fonction ϕ les fonctions composantes $C_t(\phi)$ de \mathbb{F}_q^m dans \mathbb{C} .

Le \mathbb{C} -espace vectoriel $\mathcal{G}_{(q,m)}$ est de dimension q^{m+1} , une base de cet espace étant donnée par la famille de fonctions $(e_{u,t})_{u \in \mathbb{F}_q^m, t \in \mathbb{F}_q}$ où

$$e_{u,t}(v) = \begin{cases} Z^t & \text{si } v = u \\ 0 & \text{si } v \neq u. \end{cases}$$

Dans cette base toute fonction $\phi \in \mathcal{G}_{(q,m)}$ se décompose sous la forme

$$\phi = \sum_{u \in \mathbb{F}_q^m, t \in \mathbb{F}_q} C_t(\phi)(u) e_{u,t}.$$

Exemple 2.2.1: Soit $v \in \mathbb{F}_q^m \setminus \{0\}$. Posons

$$\gamma_v(u) = Z^{\langle v, u \rangle}.$$

Dans cet exemple

$$C_t(\gamma_v)(u) = \begin{cases} 0 & \text{si } t \neq \langle v, u \rangle \\ 1 & \text{si } t = \langle v, u \rangle \end{cases}$$

Donc

$$\gamma_v = \sum_{t \in \mathbb{F}_q} \sum_{u \in H_{v,-t}} e_{u,t}.$$

Exemple 2.2.2: Plus généralement, soit f une fonction de $\mathcal{F}_{(q,m)}$. Définissons alors la fonction ϕ en posant

$$\phi(u) = Z^{f(u)}.$$

Dans cet exemple

$$C_t(\phi)(u) = \begin{cases} 0 & \text{si } t \neq f(u) \\ 1 & \text{si } t = f(u) \end{cases}$$

Exemple 2.2.3: Posons pour tout u

$$\phi(u) = \sum_{t \in \mathbb{F}_q} \alpha_t Z^t,$$

où $\alpha_t \in \mathbb{C}$.

Pour tout t , la fonction $C_t(\phi)$ est la fonction constante α_t . Si bien que

$$\phi = \sum_{t \in \mathbb{F}_q} \alpha_t \sum_{u \in \mathbb{F}_q^m} e_{u,t}.$$

En particulier si $\phi(u) = Z^t$ alors

$$\phi = \sum_{u \in \mathbb{F}_q^m} e_{u,t}.$$

2.3 La transformation $T_{(q,m)}$

Soit $T_{(q,m)}$ l'endomorphisme du \mathbb{C} -espace vectoriel $\mathcal{G}_{(q,m)}$ qui à toute fonction ϕ fait correspondre la fonction $T_{(q,m)}(\phi)$ définie par

$$T_{(q,m)}(\phi)(v) = \sum_{u \in \mathbb{F}_q^m} \phi(u) Z^{-\langle u, v \rangle}.$$

Lemme 2.1 Soit $\phi \in \mathcal{G}_{(q,m)}$ et $\psi = T_{(q,m)}(\phi)$ la transformée de ϕ . Alors pour tout $\tau \in \mathbb{F}_q$

$$C_\tau(\psi)(v) = \sum_{u \in \mathbb{F}_q^m} C_{\langle u, v \rangle + \tau}(\phi)(u).$$

Preuve : Exprimons $\phi(u)$ sous la forme

$$\phi(u) = \sum_{t \in \mathbb{F}_q} C_t(\phi)(u) Z^t,$$

ce qui nous permet d'écrire

$$\psi(v) = \sum_{u \in \mathbb{F}_q^m} \sum_{t \in \mathbb{F}_q} C_t(\phi)(u) Z^{t - \langle u, v \rangle},$$

soit encore

$$\psi(v) = \sum_{\tau \in \mathbb{F}_q} \left(\sum_{u \in \mathbb{F}_q^m} C_{\langle u, v \rangle + \tau}(\phi)(u) \right) Z^\tau,$$

ce qui démontre la formule attendue. \square

Exemple 2.3.1: Soit $\phi \in \mathcal{G}_{(q,m)}$ définie pour tout u par $\phi(u) = Z^0$. Dans ces conditions

$$\psi(v) = \sum_{u \in \mathbb{F}_q^m} Z^{-\langle u, v \rangle}.$$

Si bien que

- Si $v = 0$ alors $\psi(v) = q^m Z^0$.
- Si $v \neq 0$ alors l'application de \mathbb{F}_q^m dans \mathbb{F}_q qui à u associe $-\langle u, v \rangle$ est une forme linéaire surjective. Son noyau est donc un hyperplan. On en conclut que $\psi(v) = q^{m-1} \sum_{t \in \mathbb{F}_q} Z^t$.

Exemple 2.3.2: Plus généralement si $\phi(u) = \sum_{t \in \mathbb{F}_q} \alpha_t Z^t$ alors

- Si $v = 0$ alors $\psi(v) = q^m \sum_{t \in \mathbb{F}_q} \alpha_t Z^t$.
- Si $v \neq 0$ alors $\psi(v) = q^{m-1} \left(\sum_{t \in \mathbb{F}_q} \alpha_t \right) \sum_{t \in \mathbb{F}_q} Z^t$.

Exemple 2.3.3: Cherchons la transformée $\epsilon_{a,t}$ de la fonction $e_{a,t}$.

$$\epsilon_{a,t}(v) = \sum_{u \in \mathbb{F}_q^m} e_{a,t}(u) Z^{-\langle u,v \rangle},$$

ce qui donne

$$\epsilon_{a,t}(v) = Z^{t-\langle a,v \rangle}.$$

Décomposons $\epsilon_{a,t}$ dans la base $(e_{u,t})_{u \in \mathbb{F}_q^m, t \in \mathbb{F}_q}$.

Si $a = 0$ alors

$$\epsilon_{0,t} = \sum_{v \in \mathbb{F}_q^m} e_{v,t}.$$

Si $a \neq 0$ alors

$$\epsilon_{a,t} = \sum_{\tau \in \mathbb{F}_q} \sum_{v \in H_{a,\tau-t}} e_{v,\tau}.$$

En particulier

$$\epsilon_{a,0} = \gamma_{-a}.$$

Exemple 2.3.4: Cherchons la transformée de la fonction γ_a .

$$T_{(q,m)}(\gamma_a)(v) = \sum_{u \in \mathbb{F}_q^m} \gamma_a(u) Z^{-\langle u,v \rangle},$$

ou encore

$$T_{(q,m)}(\gamma_a)(v) = \sum_{u \in \mathbb{F}_q^m} Z^{\langle a,u \rangle} Z^{-\langle u,v \rangle},$$

c'est-à-dire

$$T_{(q,m)}(\gamma_a)(v) = \sum_{u \in \mathbb{F}_q^m} Z^{\langle a-v,u \rangle}.$$

Par suite

$$T_{(q,m)}(\gamma_a)(v) = \begin{cases} q^m Z^0 & \text{si } v = a \\ q^{m-1} \sum_{t \in \mathbb{F}_q} Z^t & \text{si } v \neq a. \end{cases}$$

Exemple 2.3.5: Remarquons que la fonction $\epsilon_{a,t}$ s'exprime sous la forme

$$\epsilon_{a,t} = Z^t \gamma_{-a},$$

si bien que

$$T_{(q,m)}(\epsilon_{a,t})(v) = \begin{cases} q^m Z^t & \text{si } v = -a \\ q^{m-1} \sum_{t \in \mathbb{F}_q} Z^t & \text{si } v \neq -a. \end{cases}$$

Exemple 2.3.6: Remarquons que lorsque $a \neq 0$ et $t_1 \neq t_2$,

$$\{(v, \tau) \mid \langle a, v \rangle + t_1 - \tau = 0\} \cap \{(v, \tau) \mid \langle a, v \rangle + t_2 - \tau = 0\} = \emptyset.$$

On voit aussi que chacun de ces ensembles a q^m éléments. On en conclut que

$$\sum_{t \in \mathbb{F}_q} \epsilon_{a,t} = \sum_{u \in \mathbb{F}_q^m, t \in \mathbb{F}_q} e_{u,t}.$$

Compte tenu du calcul déjà effectué des fonctions $\epsilon_{0,t}$, cette égalité vaut aussi pour $a = 0$.

À partir de là il est facile de construire deux fonctions distinctes ayant la même transformée. Il suffit de choisir par exemple deux éléments distincts a et b dans \mathbb{F}_q^n et de considérer les deux fonctions distinctes $\sum_{t \in \mathbb{F}_q} e_{a,t}$ et $\sum_{t \in \mathbb{F}_q} e_{b,t}$. Leurs transformées sont $\sum_{t \in \mathbb{F}_q} \epsilon_{a,t}$ et $\sum_{t \in \mathbb{F}_q} \epsilon_{b,t}$ qui sont toutes deux égales à $\sum_{u \in \mathbb{F}_q^m, t \in \mathbb{F}_q} e_{u,t}$.

Ainsi l'application $T_{(q,m)}$ n'est pas injective et nous nous proposons d'en déterminer le noyau.

Soit ϕ un élément de $\mathcal{G}_{(q,m)}$, $\psi = T_{(q,m)}(\phi)$ sa transformée, et $\theta = T_{(q,m)}(\psi)$ la transformée de ψ .

Proposition 2.1 *Avec les notations précédentes on a la relation*

$$\theta(w) = q^{m-1} \sum_{t \in \mathbb{F}_q} (Z^0 - Z^t) \phi(-w) + \left(q^{m-1} \sum_{t \in \mathbb{F}_q} Z^t \right) \psi(0).$$

Preuve : On a successivement

$$\theta(w) = \sum_{v \in \mathbb{F}_q^m} \left(\sum_{u \in \mathbb{F}_q^m} \phi(u) Z^{-\langle u, v \rangle} \right) Z^{-\langle v, w \rangle},$$

$$\theta(w) = \sum_{v \in \mathbb{F}_q^m} \sum_{u \in \mathbb{F}_q^m} \phi(u) Z^{-\langle u+w, v \rangle},$$

$$\theta(w) = \sum_{u \in \mathbb{F}_q^m} \phi(u) \sum_{v \in \mathbb{F}_q^m} Z^{-\langle u+w, v \rangle},$$

et en utilisant l'exemple 2.3.3

$$\theta(w) = q^m \phi(-w) + \left(q^{m-1} \sum_{t \in \mathbb{F}_q} Z^t \right) \sum_{u \in \mathbb{F}_q^m \setminus \{-w\}} \phi(u).$$

Mais

$$\sum_{u \in \mathbb{F}_q^m \setminus \{-w\}} \phi(u) = \sum_{u \in \mathbb{F}_q^m} \phi(u) - \phi(-w) = \psi(0) - \phi(-w).$$

On déduit des calculs précédents la formule attendue. \square

Lemme 2.2 *Pour qu'une fonction $\phi \in \mathcal{G}_{(q,m)}$ vérifie pour tout $w \in \mathbb{F}_q^m$ la relation*

$$\phi(w) \cdot \left(q - \sum_{t \in \mathbb{F}_q} Z^t \right) = 0,$$

il faut et il suffit que

$$\phi(w) = \lambda(w) \sum_{t \in \mathbb{F}_q} Z^t,$$

où λ est une fonction de \mathbb{F}_q^m dans \mathbb{C} .

Preuve : La condition est nécessaire, en effet en écrivant ϕ sous la forme

$$\phi(w) = \sum_{t \in \mathbb{F}_q} C_t(\phi)(w) Z^t,$$

on calcule

$$\phi(w) \cdot \left(q - \sum_{t \in \mathbb{F}_q} Z^t \right) = q\phi(w) - \left(\sum_{t \in \mathbb{F}_q} C_t(\phi)(w) \right) \left(\sum_{t \in \mathbb{F}_q} Z^t \right),$$

et donc en supposant la nullité du produit on déduit

$$\phi(w) = (1/q) \left(\sum_{t \in \mathbb{F}_q} C_t(\phi)(w) \right) \left(\sum_{t \in \mathbb{F}_q} Z^t \right).$$

D'autre part le simple calcul de

$$\left(\lambda(w) \sum_{t \in \mathbb{F}_q} Z^t \right) \cdot \left(q - \sum_{t \in \mathbb{F}_q} Z^t \right)$$

montre que la condition est suffisante. \square

Proposition 2.2 *Le noyau de $T_{q,m}$ est le sous espace des fonctions ϕ telles que pour tout $w \in \mathbb{F}_q^m$*

$$\phi(w) = \lambda(w) \sum_{t \in \mathbb{F}_q} Z^t$$

où λ est toute fonction de \mathbb{F}_q^m dans \mathbb{C} qui vérifie

$$\sum_{u \in \mathbb{F}_q^m} \lambda(u) = 0.$$

Ce sous espace est de dimension $q^m - 1$.

Preuve : Remarquons que si ϕ est une fonction de transformée nulle alors en vertu de la proposition 2.1

$$\phi(w) \cdot \left(q - \sum_{t \in \mathbb{F}_q} Z^t \right) = 0,$$

et le lemme 2.2 montre que

$$\phi(w) = \lambda(w) \sum_{t \in \mathbb{F}_q} Z^t.$$

Dans ces conditions, pour tout $t \in \mathbb{F}_q$ nous avons

$$C_t(\phi)(w) = \lambda(w).$$

Si on note ψ la transformée de ϕ on sait que

$$C_t(\psi)(w) = \sum_{u \in \mathbb{F}_q^m} C_{\langle u, w \rangle + t}(\phi)(u),$$

c'est-à-dire ici

$$C_t(\psi)(w) = \sum_{u \in \mathbb{F}_q^m} \lambda(u).$$

Le résultat en découle. \square

Remarque : Il est facile de voir que les fonctions

$$\delta_a = \sum_{t \in \mathbb{F}_q} (e_{0,t} - e_{a,t})$$

où $a \in \mathbb{F}_q^m \setminus \{0\}$ constituent une base du noyau de $T_{(q,m)}$.

Remarque : Une base d'un supplémentaire dans $\mathcal{G}_{(q,m)}$ du noyau de $T_{(q,m)}$ est donnée par les vecteurs $(e_{a,t})$ où :

$$a \neq 0 \text{ et } t \neq t_0$$

ou

$$a = 0,$$

(t_0 est un élément fixé dans \mathbb{F}_q).

On a ainsi $q^{m+1} - q^m + 1$ vecteurs, et les vecteurs $e_{a,t}$ correspondants forment une base de l'image de $T_{(q,m)}$.

2.4 Le calcul de la transformation

Si ϕ est une fonction de $\mathcal{G}_{(q,m)}$ alors ϕ est déterminée par le $\mathbb{C}\mathbb{F}_q$ -vecteur $(\phi(u))_{u \in \mathbb{F}_q^m}$.

Considérons la $\mathbb{C}\mathbb{F}_q$ -matrice

$$\mathcal{T}_{(q,m)} = (Z^{-\langle u,v \rangle})_{\substack{u \in \mathbb{F}_q^m \\ v \in \mathbb{F}_q^m}}.$$

Alors la fonction $T_{(q,m)}(\phi)$ est donnée par le $\mathbb{C}\mathbb{F}_q$ -vecteur

$$(T_{(q,m)}(\phi)(u))_{u \in \mathbb{F}_q^m} = \mathcal{T}_{(q,m)} \cdot (\phi(u))_{u \in \mathbb{F}_q^m}.$$

La question qui se pose est donc de trouver un algorithme performant pour calculer le produit d'un $\mathbb{C}\mathbb{F}_q$ -vecteur par la $\mathbb{C}\mathbb{F}_q$ -matrice $\mathcal{T}_{(q,m)}$.

2.4.1 Etude plus précise de la matrice de la transformation

Proposition 2.3 *La matrice $\mathcal{T}_{(q,m)}$ se décompose sous la forme*

$$\mathcal{T}_{(q,m)} = \underbrace{\mathcal{T}_{(q,1)} \otimes \mathcal{T}_{(q,1)} \otimes \cdots \otimes \mathcal{T}_{(q,1)}}_{m \text{ termes}}.$$

Preuve : Se prouve immédiatement par récurrence. La proposition est vraie pour $m = 1$. Supposons la vraie à l'ordre m . Alors

$$\begin{aligned} (Z^{-\langle u,v \rangle})_{\substack{u \in \mathbb{F}_q^m \\ v \in \mathbb{F}_q^n}} \otimes \mathcal{T}_{(q,1)} &= \\ (Z^{-\langle u,v \rangle - ab})_{\substack{u \in \mathbb{F}_q^m, a \in \mathbb{F}_q \\ v \in \mathbb{F}_q^n, b \in \mathbb{F}_q}} &= (Z^{-\langle u,v \rangle})_{\substack{u \in \mathbb{F}_q^{m+1} \\ v \in \mathbb{F}_q^{n+1}}} . \square \end{aligned}$$

Proposition 2.4 *La matrice $\mathcal{T}_{(q,m)}$ se décompose sous la forme*

$$\mathcal{T}_{(q,m)} = M_{q^m}^{(1)} M_{q^m}^{(2)} \cdots M_{q^m}^{(m)}$$

où

$$M_{q^m}^{(i)} = I_{q^{m-i}} \otimes \mathcal{T}_{(q,1)} \otimes I_{q^{i-1}}.$$

Preuve : Pour $m = 1$ on a $M_q^{(1)} = I_1 \otimes \mathcal{T}_{(q,1)} \otimes I_1 = \mathcal{T}_{(q,1)}$, donc le résultat est vrai. Par récurrence supposons le résultat vrai à l'ordre m . Alors pour $1 \leq i \leq m$ on a

$$\begin{aligned} M_{q^{m+1}}^{(i)} &= I_{q^{m+1-i}} \otimes \mathcal{T}_{(q,1)} \otimes I_{q^{i-1}} \\ M_{q^{m+1}}^{(i)} &= I_q \otimes I_{q^{m-i}} \otimes \mathcal{T}_{(q,1)} \otimes I_{q^{i-1}} \\ M_{q^{m+1}}^{(i)} &= I_q \otimes M_{q^m}^{(i)} \end{aligned}$$

et aussi

$$M_{q^{m+1}}^{(m+1)} = \mathcal{T}_{(q,1)} \otimes I_{q^m}.$$

Donc,

$$\begin{aligned} M_{q^m}^{(1)} M_{q^m}^{(2)} \cdots M_{q^m}^{(m+1)} &= (I_q \otimes M_{q^m}^{(1)}) \cdots (I_q \otimes M_{q^m}^{(m)}) (\mathcal{T}_{(q,1)} \otimes I_{q^m}), \\ M_{q^m}^{(1)} M_{q^m}^{(2)} \cdots M_{q^m}^{(m+1)} &= \mathcal{T}_{(q,1)} \otimes (M_{q^m}^{(1)} M_{q^m}^{(2)} \cdots M_{q^m}^{(m)}), \end{aligned}$$

$$M_{q^m}^{(1)} M_{q^m}^{(2)} \cdots M_{q^m}^{(m+1)} = \mathcal{T}_{(q,1)} \otimes \mathcal{T}_{(q,m)},$$

$$M_{q^m}^{(1)} M_{q^m}^{(2)} \cdots M_{q^m}^{(m+1)} = \mathcal{T}_{(q,m+1)}. \square$$

Remarquons qu'on a aussi

$$\mathcal{T}_{(q,m)} = M_{q^m}^{(m)} M_{q^m}^{(m-1)} \cdots M_{q^m}^{(1)}.$$

La multiplication d'un vecteur de $\mathbb{C}\mathbb{F}_q^n$ par une des matrices $M_{q^m}^{(i)}$ est très simple. Chaque ligne de cette matrice a q éléments non nuls et ces éléments sont de la forme Z^s . La multiplication d'un élément de cette forme par un élément de $\mathbb{C}\mathbb{F}_q$ est un shift. Pour chaque ligne de $M_{q^m}^{(i)}$ il faut donc faire q shifts, $q - 1$ additions dans $\mathbb{C}\mathbb{F}_q$, c'est-à-dire $q(q - 1)$ additions dans \mathbb{Z} . En conséquence la multiplication d'un vecteur de $(\mathbb{C}\mathbb{F}_q)^{q^m}$ par une des matrices $M_{q^m}^{(i)}$ demande $q(q - 1)q^m = q(q - 1)n$ additions (et des shifts).

La multiplication d'un vecteur de $(\mathbb{C}\mathbb{F}_q)^{q^m}$ par $\mathcal{T}_{(q,m)}$ demande donc

$$q(q - 1) \log_q(n)n$$

additions, où $n = q^m$.

2.4.2 La pratique de la transformation

Remarquons que pour transformer un vecteur, la multiplication par la matrice $M_{q^m}^{(m)}$ revêt une importance particulière. En effet on peut réaliser la transformation uniquement avec des produits par des matrices de ce type. Pour cela il suffit de constater que pour multiplier un vecteur $\omega = (\xi_u)_{u \in \mathbb{F}_q^m}$ de longueur q^m par $\mathcal{T}_{(q,m)}$ il suffit de calculer $M_{q^m}^{(m)} \cdot \omega$ puis de couper ce vecteur en q vecteurs de taille q^{m-1} (en prenant dans l'ordre q blocs de $q^{(m-1)}$ composantes), de transformer ces q vecteurs par $\mathcal{T}_{(q,m-1)}$ et de reconstituer le vecteur résultat par juxtaposition des q blocs de composantes résultats. Par récursivité on voit qu'on ne fait dans ce cas que des multiplications par des matrices de la forme $M_{q^i}^{(i)}$.

La multiplication par $M_{q^m}^{(m)}$ d'un vecteur $\omega = (\xi_u)_{u \in \mathbb{F}_q^m}$ de longueur q^m peut être vue de la façon suivante : à partir du vecteur ω on construit la matrice Ω ayant q lignes et q^{m-1} colonnes où les q lignes de Ω sont formées par les q blocs de q^{m-1} composantes de ω , prises dans l'ordre. Le résultat s'obtient par le produit $\mathcal{T}_{(q,1)} \cdot \Omega$ puis en reconstituant à partir de ce produit un vecteur de longueur q^m .

3 Distance à un code de Reed-Muller.

3.1 Définitions et propriétés élémentaires

À toute fonction $f \in \mathcal{F}_{(q,m)}$ faisons correspondre la fonction F de \mathbb{F}_q^m dans $\mathbb{C}\mathbb{F}_q$ définie par

$$F(u) = Z^{f(u)}.$$

La transformée $T(q, m)(F)$ est donnée par

$$T(q, m)(F)(v) = \sum_{u \in \mathbb{F}_q^m} Z^{f(u) - \langle u, v \rangle},$$

et en regroupant les termes

$$T(q, m)(F)(v) = \sum_{t \in \mathbb{F}_q} N_{v,t}(f) Z^t,$$

où

$$N_{v,t}(f) = \#\{u \in \mathbb{F}_q^m \mid f(u) - \langle u, v \rangle = t\}.$$

Ce regroupement des termes nous permet d'énoncer

Théorème 3.1 *Le nombre $N_{v,t}(f)$ est le nombre de composantes des mots $\left(f(u)\right)_u$ et $\left(\langle u, v \rangle + t\right)_u$ qui coïncident.*

Corollaire 3.1 *La distance de Hamming du mot $\left(f(u)\right)_u$ au code de Reed-Muller d'ordre 1 est*

$$q^m - \text{Max}_{v \in \mathbb{F}_q^m, t \in \mathbb{F}_q} N_{v,t}(f).$$

Définition 3.1 *Les fonctions maximale non linéaires de $\mathcal{F}_{(q,m)}$ sont les fonctions f dont la distance de Hamming au code de Reed-Muller d'ordre 1 est maximale, c'est-à-dire celles pour lesquelles*

$$\text{Max}_{v \in \mathbb{F}_q^m, t \in \mathbb{F}_q} N_{v,t}(f)$$

est minimum.

Nous noterons $\mathcal{B}_{(q,m)}$ l'ensemble des fonctions maximale non linéaires de $\mathcal{F}_{(q,m)}$.

Nous noterons

$$\mu(q, m) = \text{Min}_{f \in \mathcal{F}_{(q,m)}} \text{Max}_{v \in \mathbb{F}_q^m, t \in \mathbb{F}_q} N_{v,t}(f).$$

Le rayon de recouvrement du code de Reed-Muller d'ordre 1 est donc $q^m - \mu(q, m)$.

Théorème 3.2 *Pour tout $v \in \mathbb{F}_q^m$,*

$$\sum_{t \in \mathbb{F}_q} N_{v,t}(f) = q^m.$$

Preuve : Ceci est une conséquence immédiate de la formule

$$T_{(q,m)}(F)(v) = \sum_{u \in \mathbb{F}_q^m} Z^{f(u) - \langle u, v \rangle},$$

qui montre qu'on dispose de q^m termes de la forme Z^τ qu'on regroupe en q blocs ayant $N_{v,t}(f)$ termes.

Remarque : Pour une fonction affine $f(u) = \langle a, u \rangle + b$, si $v \neq a$ alors $N_{v,t} = q^{m-1}$ pour tout t , et si $v = a$, alors si $t \neq b$ $N_{v,t} = 0$ sinon si $t = b$ $N_{v,t} = q^m$. Bien entendu

$$q^m - \text{Max}_{v \in \mathbb{F}_q^m, t \in \mathbb{F}_q} N_{v,t}(f) = 0.$$

Si g et h diffèrent d'une fonction affine leur distance au code de Reed-Muller d'ordre 1 est la même. En fait

$$N_{v,t}(g + \langle a, u \rangle + b) = N_{v-a, t-b}(g).$$

Théorème 3.3 *Il n'existe pas de fonction f pour laquelle tous les $N_{v,t}(f)$ sont égaux à q^{m-1} .*

Preuve : Sinon nous aurions

$$T_{(q,m)}(F)(v) = q^{m-1} \sum_{t \in \mathbb{F}_q} Z^t.$$

Or nous connaissons une fonction ayant cette transformée, la fonction

$$\Phi(u) = (1/q) \sum_{t \in \mathbb{F}_q} Z^t.$$

Par suite la fonction $F - \Phi$ serait ue fonction du noyau de $T_{(q,m)}$ et donc on aurait

$$F(u) = (1/q + \lambda(u)) \sum_{t \in \mathbb{F}_q} Z^t,$$

qui ne peut en aucun cas être de la forme $Z^{f(u)}$.

Ceci implique que $Max_{v \in \mathbb{F}_q^m, t \in \mathbb{F}_q} N_{v,t}(f) \geq q^{m-1} + 1$ et donc que $\mu(q, m) \geq q^{m-1} + 1$. Par suite le rayon de recouvrement du code de Reed-Muller d'ordre 1 est $\leq q^m - q^{m-1} - 1$.

Cette borne peut être effectivement atteinte pour certaines valeurs de q et de m . Par exemple, prenons $q = 9$, $m = 2$. Soit α racine du polynôme primitif $x^2 + x + 2$. Soit

$$f(u_1, u_2) = \alpha^5 u_1^2 + \alpha^5 u_2^2 + \alpha^2 u_1 u_2.$$

Alors

$$Max_{v \in \mathbb{F}_9^2, t \in \mathbb{F}_9} N_{v,t}(f) = 10.$$

Ce qui donne un rayon de recouvrement de 71.

Ici on constate en plus que la borne est atteinte par une forme quadratique. Enfin remarquons que

Remarque 1 : La classe des fonctions maximalelement non linéaire ne coïncide pas avec celle des fonctions courbes. Considérons par exemple le corps \mathbb{F}_7 et prenons la fonction quadratique sur \mathbb{F}_7^2 :

$$f(x_1, x_2) = x_1^2 + 2x_2^2 + 4x_1x_2.$$

Le déterminant de cette forme quadratique est

$$Det \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = 5.$$

Donc cette fonction est courbe (forme quadratique de déterminant non nul). Pourtant cette fonction n'est pas maximalelement non linéaire. En effet

$$Max_{v \in \mathbb{F}_7^2, t \in \mathbb{F}_7} N_{v,t}(f) = 13,$$

et il y a des fonctions pour lesquelles ce Max est plus petit. Par exemple la fonction quadratique

$$x_1^2 + x_2^2 + 4x_1x_2$$

a un Max qui vaut 8 (ce qui est d'ailleurs forcément le plus petit Max possible puisqu'il vaut $q + 1$).

Remarque 2 : On peut trouver des exemples de fonctions quadratiques dont le déterminant est nul et qui parmi les fonctions quadratiques sont le plus loin des fonctions linéaires. Par exemple prenons $q = 5$ et considérons les fonctions de 3 variables ($m = 3$). La fonction

$$f(x_1, x_2, x_3) = x_2^2 + 4x_3^2 + 2x_2x_3$$

a un déterminant nul, cependant

$$\text{Max}_{v \in \mathbb{F}_5^3, t \in \mathbb{F}_5} N_{v,t}(f) = 30,$$

ce qui est la plus petite valeur pour une forme quadratique et peut être d'ailleurs pour toute fonction.

Références

- [1] **Ambrosimov A.S.** *Properties of bent functions of q -valued logic over finite fields.* Discrete Math. Appl., Vol.4, No.4, pp.341-350 (1994)
- [2] **Ashikhmin A.E., Litsyn S.N.** *Fast Decoding of Non-Binary First Order Reed-Muller Codes.* AAECC 7, 299-308 (1996)
- [3] **Kumar P.V., Scholtz R.A., Welch L.R.** *Generalized Bent Functions and Their Properties.* Journal of Combinatorial Theory, Series A, 40, 90-107 (1985)
- [4] **Lachaud G.** *Exponential sums as discrete Fourier transform with invariant phase functions.* Prétirage de l'IML, No 93-01 (1993)
- [5] **Logachev O.A., Salnikov A.A., Yashchenko V.V.** *Bent functions on a finite Abelian group.* Discrete Math. Appl., Vol.7, No.6, pp.547-564 (1997)