Détermination du Spectre de Poids des Codes de Reed-Muller Généralisés

Adnen SBOUI

Institut de Mathématiques de Luminy (IML)

Journées Informatique et Géométrie
Nice, 14 et 15 juin 2007

On note par :

- $\mathbb{F}_q$ un corps fini à q éléments (q une puissance d'un nombre premier p).
- $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \cup \{0\}$ l'espace vectoriel des polynômes homogènes à $n+1$ variables avec coefficients dans $\mathbb{F}_q$ et de degré d.
- $\mathbb{P}^n(\mathbb{F}_q)$ l'espace projectif de dimension n sur $\mathbb{F}_q$.
- $\Pi_n = \#\mathbb{P}^n(\mathbb{F}_q) = \frac{q^{n+1}-1}{q-1}$, le nombre de points rationnels de $\mathbb{P}^n(\mathbb{F}_q)$.
- $\Pi_{-1} = 0$ (par convention, qui signifie le nombre de points de l'ensemble vide).

On suppose que $2 \leq d \leq q$ et $n \geq 2$.

Pour tout polynôme f de $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \cup \{0\}$, soit ev$f$ la fonction polynomiale d'évaluation de f sur les éléments de $\mathbb{P}^n(\mathbb{F}_q)$, définie par :

$$\begin{array}{rcl} ev f : \mathbb{P}^n(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_q \\ v = (x_0 : ... : x_n) & \longmapsto & \frac{f(x_0,...,x_n)}{x_i^d} \end{array}$$

avec x_i la première composante non nulle de v.

Le code de Reed-Muller projectif $PRM(q, d, n)$ est l'image de l'application :

$$\begin{array}{rccc} \Phi : & \mathbb{F}_q[X_0, X_1, ..., X_n]_d^h & \longrightarrow & \mathbb{F}_q^{\pi_n} \\ & f & \longmapsto & (evf(v))_{v \in \mathbb{P}^n(\mathbb{F}_q)} \end{array}$$

- un mot de code $c \in PRM(q, d, n)$ est défini par le vecteur : $c = (\text{ev}f(v_1), ..., \text{ev}f(v_{\pi_n}))$; avec $f \in \mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \cup \{0\}$.
- Le poids de c est le nombre de ces composantes non nulles.

- $Z_q(f)$ l'ensemble des zéros de f
- $\#Z_q(f)$ est le nombre de points de l'hypersurface S défini par f, noté aussi $\#S$.
- $N_1 = \max_{f \in \mathbb{F}_q[X_0, X_1, \ldots, X_n]_d^h} \#Z_q(f)$;
- $\mathcal{P}_1 = \{f \in \mathbb{F}_q[X_0, X_1, \ldots, X_n]_d^h \text{ tel que } \#Z_q(f) = N_1\}$

- $N_2 = \max_{f \in \mathbb{F}_q[X_0, X_1, \ldots, X_n]_d^h \setminus \mathcal{P}_1} \#Z_q(f)$
- $\mathcal{P}_2 = \{f \in \mathbb{F}_q[X_0, X_1, \ldots, X_n]_d^h / \#Z_q(f) = N_2\}$
- Le deuxième poids est : $w_2 = \Pi_n - N_2$.

- $N_i = \max_{f \in \mathbb{F}_q[X_0, X_1, \ldots, X_n]_d^h \setminus \{\mathcal{P}_1 \cup \ldots \cup \mathcal{P}_{i-1}\}} \#Z_q(f)$, pour $i \geq 2$;

  Si on considère l'ensemble des polynômes qui sont produits de facteurs linéaires, on définit de la même façon les nombres N_i^{ℓ}.

- $\mathcal{P}_i$: l'ensemble des polynômes $f \in \mathbb{F}_q[X_0, X_1, \ldots, X_n]_d^h$ tel que $\#Z_q(f) = N_i$.

- Le i-ème poids est $\boxed{w_i = \Pi_n - N_i}$, pour $i \geq 1$.

Cas Affine

➤ $\mathcal{P}_{(q,d,n)} = \mathbb{F}_q[X_1, ..., X_n]_d$ l'espace des polynômes à n variables avec coefficients dans $\mathbb{F}_q$ et de degré total au plus d.

➤$\mathcal{H}_{(q,d,n)}$: l'ensemble des hypersurfaces définies par les polynômes de $\mathcal{P}_{(q,d,n)}$.

$\mathbb{F}_q^n$ l'espace affine de dimension n sur $\mathbb{F}_q$.

En remplaçant $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \cup \{0\}$ par $\mathcal{P}_{(q,d,n)}$, on définit de la même façon un mot de code, son poids, les nombres N_i, N_i^ℓ, $\mathcal{P}_i$ et les poids w_i pour le cas affine.

La distance minimale est donnée par :
R.Lidl, H. Niederreiter ($d \leq q$),
Kasami, Lin et Peterson (1968) pour $0 < d < n(q-1)$.

Distance minimale du code $GRM(q, d, n)$

- Si $d \leq q$,
$$d_{min} = w_1 = (q-d)q^{n-1}.$$
- Si $0 < d < n(q-1)$, avec $d = r(q-1) + s$, $s < q-1$:
$$d_{min} = w_1 = (q-s)q^{n-r-1}.$$

Delsarte, Goethals and Mac Williams (1970) :
Tout mot, du code $GRM(q, d, n)$, de poids w_1 peut être obtenu par un polynôme de la forme :

$$P(x_1, ..., x_n) = \lambda \prod_{i=1}^{r} [1 - (x_i - w_i)^{q-1}] \prod_{j=1}^{s} (x_{r+1} - t_j),$$

modulo l'action, sur les x_i, des permutations du groupe GLNH(q,n) (le groupe général linéaire non homogène sur $\mathbb{F}_q^n$).

Le degré est $d = r(q-1) + s$, avec les t_j sont distincts, et les w_i arbitraires, comme éléments de $\mathbb{F}_q$.

Les hyperplans de Delsarte, Goethals et Mc Williams

L'hypersurface définie par un polynôme comme ci-dessus est une réunion d'hyperplans dont la configuration géométrique est :

r directions, dans chacune il y à $q-1$ hyperplans parallèles et une $(r+1)$-ème direction où il y à s hyperplans parallèles.

on calcule le nombre d'hypersurfaces de ce type, on obtient par la suite :

Nombre de mots atteignant la distance minimale

$$\#\mathcal{P}_1 = \binom{q}{s}(q^{n-r}-1)q^r \frac{(q^n-1)(q^{n-1}-1)...(q^{r+1}-1)}{(q^{n-r}-1)(q^{n-r-1}-1)...(q-1)}$$

➢ Pour $d = 2$, le polynôme de poids est entièrement calculé par McEliece
cf : "Quadratic forms over finite fields and second-order Reed-Muller codes", JPL Space Programs Summary, 37-58, vol.III.

Pour le cas général :
➢Lorsque $d > 2$, même la détermination du deuxième poids, est non généralement résolue !

Arrangements d'hyperplans de Cherdieu et Rolland

Théorème

Le deuxième grand nombre de zéros des polynômes de $\mathcal{P}^{\ell}_{(q,d,n)}$, est

$$N_2^{\ell} = dq^{n-1} - (d-1)q^{n-2}.$$

Ce nombre est donné par des polynômes définissant les arrangements d'hyperplans suivants :

(a) *$\mathcal{A}^d_{2.a}$; $d-1$ hyperplans parallèles et le d-ème hyperplan les coupe,*

(b) *$\mathcal{A}^d_{2.b}$; d hyperplans se coupent en une même sous-variété linéaire de co-dimension 2.*

Cherdieu et Rolland (1996) :
A partir d'un résultat de W. Schmidt, améliorant une borne de A. Weil et S. Lang sur le nombre de points d'une hypersurface ; on obtient le nombre N_2 et le deuxième poids w_2 des codes $GRM(q, d, n)$ lorsque q est assez grand relativement à d :

- $N_2 = dq^{n-1} - (d-1)q^{n-2}$.
- $w_2 = q^n - dq^{n-1} + (d-1)q^{n-2}$,

sous la condition

$$q \geq q_1 \geq 4d^2\left(\frac{d(d+1)}{2}\right)^{2^{\frac{d(d+1)}{2}}}$$

Contribution sur le deuxième poids

Indépendamment des techniques ayant servi avant, nous abordons le problème avec une approche plus géométrique.
L'outil essentiel utilisé commence par le lemme suivant :

Lemme

Soit S une hypersurface de $\mathcal{H}_{(q,d,n)}$, telle que son nombre de points est supérieur ou égal à N_2^ℓ, (i.e. $\#S \geqslant N_2^\ell$).

Pour $q \geq 2d$, si S contient une sous-variété affine A_m, de dimension m avec $0 \leqslant m \leqslant n-2$, alors S contient une sous-variété affine A_{m+1} de dimension $m+1$ tel que $\mathrm{A}_{m+1} \supset \mathrm{A}_m$.

Corollaire

Soit S une hypersurface de degré d, non réunion de d hyperplans parallèles (i.e. $S \in \mathcal{H}_{(q,d,n)} \setminus \mathcal{H}_1$). Pour $q \geqslant 2d$

$$\#S \leqslant N_2^{\ell}.$$

$\Longrightarrow$

- *Le deuxième grand nombre de points sur les hypersurfaces de $\mathbb{F}_q^n$ est*

$$N_2 = N_2^{\ell}$$

- *Le deuxième poids des codes $GRM(q, d, n)$ est*

$$w_2 = q^n - dq^{n-1} + (d-1)q^{n-2}$$

Nombre de mots de poids w_2

Pour $q \geq 2d$, $\#\mathcal{P}_2 = (q-1)\#\mathcal{H}_2$

$$\#\mathcal{P}_2 = \binom{q}{d-1} \frac{d+1}{d} \frac{q^2(q^n-1)(q^{n-1}-1)}{(q-1)} \text{ if } d > 2,$$

$$\#\mathcal{P}_2 = \frac{q^3(q^n-1)(q^{n-1}-1)}{2(q-1)} \text{ if } d = 2.$$

La distance minimale est donnée dans deux cas :

- Pour le cas $d \leq n(q-1)$, A. B. Sørensen prouve à partir du résultat dans le cas affine que

$$d_{min} = w_1 = (q-s)q^{n-r-1},$$

avec $d-1 = r(q-1)+s$, $0 \leq s < q-1$.

- J.-P. Serre, le cas $(d < q)$, $N_1 = dq^{n-1} + \Pi_{n-2}$,

$$d_{\min} = q^n - (d-1)q^{n-1}.$$

N_1, est atteint seulement par un arrangement de d hyperplans de type :
$\mathcal{A}_1^d$, d hyperplans se coupant tous en une même sous-variété linéaire de codimension 2.

Le nombre de mots atteignant le premier poids w_1 est

$$\#\mathcal{P}_1 = \binom{q+1}{d} \frac{q-1}{q+1} \Pi_n \Pi_{n-1}$$

Théorème : $PRM(q, d, n)$ avec $q \geq 2(d-1)$

- (i) Soit f un polynôme homogène de $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \setminus \mathcal{P}_1$, on a

$$\#Z_q(f) \leq dq^{n-1} + \Pi_{n-2} - (d-2)q^{n-2},$$

et

$$N_2 = N_2^{\ell} = dq^{n-1} + \Pi_{n-2} - (d-2)q^{n-2}.$$

- (ii)Le deuxième poids est

$$w_2 = q^n - (d-1)q^{n-1} + (d-2)q^{n-2}.$$

Le nombre N_2 est atteint par des hypersurfaces de type :

➤ $\mathcal{A}_2^d$, $(d-1)$ hyperplans qui se coupent en un même sous-espace K de codimension 2 et le d-ème hyperplan coupe K en un sous-espace E de codimension 3.

$\Longrightarrow$ On retrouve les arrangements de Cherdieu et Rolland $\mathcal{A}_{2.a}^d$ et $\mathcal{A}_{2.b}^d$

Corollaire

Le nombre de mots de $PRM(q, d, n)$ admettant le poids w_i, $1 \leq i \leq 2$, qui est encore le nombre $\#\mathcal{P}_i$ de polynômes homogènes de $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ ayant N_i zéros, est

$$(i) \qquad \#\mathcal{P}_1 = \binom{q+1}{d} \frac{q-1}{q+1} \Pi_n \Pi_{n-1}$$

$$(ii) \qquad \#\mathcal{P}_2 = \binom{q+1}{d-1} \frac{q^2(q-1)}{q+1} \Pi_n \Pi_{n-1} \Pi_{n-2}$$

Cas projectif

$\mathcal{A}_3^d$: les $(d-2)$ hyperplans $H_1, ..., H_{d-2}$ forment un arrangement de type $\mathcal{A}_1^{d-2}$. les trois hyperplans H_{d-2}, H_{d-1} et H_d se coupent en une même sous-variété linéaire de codimension 2, distincte de $\cap_{i=1}^{d-2} H_i$.

Cas projectif

$\mathcal{A}_3^d$: les $(d-2)$ hyperplans $H_1, ..., H_{d-2}$ forment un arrangement de type $\mathcal{A}_1^{d-2}$. les trois hyperplans H_{d-2}, H_{d-1} et H_d se coupent en une même sous-variété linéaire de codimension 2, distincte de $\cap_{i=1}^{d-2} H_i$.

Cas affine

(1) $\mathcal{A}_{3.a}^d$: $d-2$ hyperplans $H_1, \ldots, H_{d-1}$ sont parallèles, coupés par H_{d-1} et H_d qui sont eux mêmes parallèles.

(2) $\mathcal{A}_{3.b}^d$: $d-2$ hyperplans parallèles coupés par H_{d-1} et H_d, tel que H_{d-2}, H_{d-1} et H_d sont concourants.

(3) $\mathcal{A}_{3.c}^d$: $d-1$ hyperplans $H_1, \ldots, H_{d-1}$ sont concourants et $H_d // H_{d-1}$.

Cas projectif

$$N_3^\ell = dq^{n-1} + \Pi_{n-2} - 2(d-3)q^{n-2}$$

Pour $q \geq 3(d-2)$,

$$N_3 = N_3^\ell$$

$$w_3 = q^n - (d-1)q^{n-1} + 2(d-3)q^{n-2}$$

Pour $d > 7$, le nombre de mots atteignant w_3 est

$$\#\mathcal{P}_3 = \binom{q}{d-3} \frac{q^2(q-1)^2}{2} \Pi_n \Pi_{n-1} \Pi_{n-2}$$

Cas projectif

$$N_3^\ell = dq^{n-1} + \Pi_{n-2} - 2(d-3)q^{n-2}$$

Pour $q \geq 3(d-2)$,

$$N_3 = N_3^\ell$$

$$w_3 = q^n - (d-1)q^{n-1} + 2(d-3)q^{n-2}$$

Pour $d > 7$, le nombre de mots atteignant w_3 est

$$\#\mathcal{P}_3 = \binom{q}{d-3} \frac{q^2(q-1)^2}{2} \Pi_n \Pi_{n-1} \Pi_{n-2}$$

Cas affine

$$N_3^\ell = dq^{n-1} - 2(d-2)q^{n-2}$$

Pour $q \geq 3(d-1)$,

$$N_3 = N_3^\ell$$

$$w_3 = q^n - dq^{n-1} + 2(d-2)q^{n-2}$$

Pour $d > 6$, le nombre de mots atteignant w_3 est

$$\#\mathcal{P}_3 = \binom{q}{d-2} \frac{q^2(d+1)}{2} (q^n - 1)(q^{n-1} - 1)$$

Cas projectif

$\mathcal{A}^d_{min}$: un arrangement de d hyperplans minimal est tel que : tous les hyperplans contiennent une même sous-variété linéaire de codimension 3 et les intersections $H_i \cap H_j$ pour $i \neq j$ sont distinctes deux à deux.

Cas projectif

$\mathcal{A}^d_{min}$: un arrangement de d hyperplans minimal est tel que : tous les hyperplans contiennent une même sous-variété linéaire de codimension 3 et les intersections $H_i \cap H_j$ pour $i \neq j$ sont distinctes deux à deux.

Cas affine

$\mathcal{A}^d_{min}$: un arrangement de d hyperplans minimal est tel que : les intersections $H_i \cap H_j$ pour $i \neq j$ sont disjointes deux à deux.

Cas projectif

Le nombre de points d'un arrangement de d hyperplans de type $\mathcal{A}^d_{min}$ est $N^{\ell}_{min} = dq^{n-1} + \Pi_{n-2} - \frac{(d-1)(d-2)}{2} q^{n-2}$.

Pour tout arrangement de d hyperplans A^d non de type $\mathcal{A}^d_{min}$,

$$N(\mathrm{A}^d) > N^{\ell}_{min}.$$

Pour $q > \frac{d(d-1)}{2}$, on a $w^{\ell}_{min} = q^n - (d-1)q^{n-1} + \frac{(d-1)(d-2)}{2} q^{n-2}$.

Cas projectif

Le nombre de points d'un arrangement de d hyperplans de type $\mathcal{A}^d_{min}$ est
$N^{\ell}_{min} = dq^{n-1} + \Pi_{n-2} - \frac{(d-1)(d-2)}{2} q^{n-2}$.

Pour tout arrangement de d hyperplans A^d non de type $\mathcal{A}^d_{min}$,

$$N(\mathrm{A}^d) > N^{\ell}_{min}.$$

Pour $q > \frac{d(d-1)}{2}$, on a
$w^{\ell}_{min} = q^n - (d-1)q^{n-1} + \frac{(d-1)(d-2)}{2} q^{n-2}$.

Cas affine

Le nombre de points d'un arrangement de d hyperplans de type $\mathcal{A}^d_{min}$ est
$N^{\ell}_{min} = dq^{n-1} - \frac{d(d-1)}{2} q^{n-2}$.

Pour tout arrangement de d hyperplans A^d non de type $\mathcal{A}^d_{min}$,

$$N(\mathrm{A}^d) > N^{\ell}_{min}.$$

Pour $q > \frac{d(d+1)}{2}$, ona
$w^{\ell}_{min} = q^n - dq^{n-1} + \frac{d(d-1)}{2} q^{n-2}$.