Université de la Méditerranée
(Aix Marseille II)
Faculté des Sciences de Luminy

Université de Tunis El-Manar
Faculté des Sciences de Tunis

École Doctorale de Mathématiques et Informatiques E.D. 184

THÈSE

pour obtenir le grade de

DOCTEUR
de l'Université de la Méditerranée et de l'Université de Tunis El-Manar

Discipline : Mathématiques

présentée et soutenue publiquement le 26 Juin 2007
par

Adnen SBOUI

Titre

Détermination des Poids des Codes de Reed-Muller Généralisés

Directeurs de Thèse : François RODIER et Hikma SMIDA

JURY

M. Houcine Chebli	Professeur, Université Tunis El-Manar, Tunisie
M. Johan P. Hansen	Professeur, University of Ny Munkegade, Danemark
M. James W. P. Hirschfeld	Professeur, University of Sussex Brighton, RU. Angleterre (Rapporteur)
M. François Rodier	Directeur de Recherche, CNRS Marseille, France
M. Robert Rolland	MdC (HDR), Université de la Méditerranée Marseille, France
Mme. Hikma Smida	Professeur, Université Tunis El-Manar, Tunisie
M. Leo Storme	Professeur, Université Gent Galglaan 2, Belgique (Rapporteur)

Remerciements

Je remercie vivement mes directeurs de Thèse, M. Rodier et Mme Smida, pour la confiance qu'ils m'ont accordée en me confiant cette tache de thèse en cotutelle.
Je tiens à exprimer ma gratitude à Monsieur Rodier, dont l'étendue des connaissances et la disponibilité m'ont permis de mener à bien ce travail. Je le remercie de m'avoir bien accueilli à l'Institut de Mathématique de Luminy. Il est évident que je lui dois ma formation de chercheur.

Je tiens à remercier infiniment les professeurs James W. P. Hirschfeld et Leo Storme pour s'être intéressés à mon travail et avoir accepté d'en être les rapporteurs.

Je remercie chaleureusement Robert Rolland pour les discussions intéressantes et fructueuses que nous avons eues ensemble concernant des différentes parties de mon travail et pour sa présence en tant que membre de jury.

Je remercie tout particulièrement les professeurs Houcine Chebli et Johan Hansen de s'être intéressés à mon travail, en venant de l'étranger à Marseille. Leur présence en tant que membres de jury est un honneur en plus de l'encouragement.

Pour son soutien et l'intérêt qu'il donne à mon travail, toute ma reconnaissance va à Gilles Lachaud, avec l'honneur que cette thèse puisse représenter un travail de plus publié par l'IML à l'occasion de son 60 ème anniversaire.

Merci aussi à tous les membres et thésards de l'Institut de Mathématiques de Luminy, et spécialement les membres de l'équipe Arithmétiques et théorie de l'Information (ATI) Serge Vladut, Michael Tsfasman, Yves, Stéphane, Christophe, Frédéric et Alexey.

Parmi les contacts scientifique et humains qui ont marqué mon parcours mathématique pendant cette thèse, je veux citer, Patrick Solé, Jean Marc Couveigne, Alexis Bonnecaze et Ferruh Ozbudak et leur exprimer ma vive reconnaissance.

Merci à tous mes frères et mes amis pour leurs encouragements.

Hommage : Il est évident que la vie privée n'est pas indépendante de la vie Universitaire ; deux événements dramatiques et navrants auront marqué cette thèse : le décès de ma mère après une longue maladie suivi récemment par le décès de mon cher frère Lotfi, victime d'un douloureux accident de voiture. Ce qui a engendré des sentiments exacerbés accompagnant mon cursus scientifique depuis mon DEA. C'étaient des épreuves, en parallèle de la thèse, pour comprendre et accepter des choses dépassant les mathématiques.
Tant qu'ils vivent toujours dans le coeur et dans l'esprit, par cette thèse, je tiens à leur rendre hommage, avec ma reconnaissance, de leur soutien durant mon cursus et au bon souvenir de notre vie ensemble.

Table des matières

Chapitre 1

Codes de Reed-Muller généralisés, Approche polynomial à plusieurs indéterminées et approche géométrique

1.1 Résultats et Publications des Travaux de cette Thèse, Introduction générale

Nous étudions dans cette thèse la distribution des poids des codes de Reed-Muller Généralisés et nous présentons des nouveaux résultats sur le spectre de poids de ces codes. Ces résultats donnent des réponses à certaines questions posés dans ce cadre, en particulier aux questions ouvertes dans l'article [6] de Jean Pierre Cherdieu et Robert Rolland intitulé " On the number of points of some Hypersurfaces in $\mathbb{F}_q^n$" qui est paru dans Finite Fields and Their Applications, vol. **2** (1996), 214-224.
Nous rappelons que les poids d'un code (linéaire) mesurent en particulier l'efficacité du code et que leur connaissance sert dans une procédure de décodage.
L'idéal serait de déterminer le polynôme de poids. Sa détermination entière constitue un problème extrêmement difficile. Tout revient à déterminer une hiérarchie sur les nombres de zéros des polynômes définissant le code. On est même loin de pouvoir caractériser tous les poids de ce code. On connaît cependant le poids minimum des mots de code, donnant la distance minimale.

La distance minimale des codes de Reed Muller projectifs généralisés d'ordre d et de lon-

gueur Π_n sur $\mathbb{F}_q$ ($PRM(q,d,n)$) est donnée par une hypersurface qui est une réunion de d hyperplans se coupant tous en une même sous variété linéaire de codimension 2. C'était une conjecture de M. Tsfasman prouvée par J-P. Serre. D'autres poids de ces codes pourraient être déterminés si on connait les configurations géométriques de d hyperplans donnant les nombres correspondants de points rationnels.

Pour un code de Reed-Muller généralisé $GRM(q,d,n)$ d'ordre d défini sur $\mathbb{F}_q^n$, le poids minimal a été donné par Kasami, Lin et Peterson [11]. Il a été déterminé aussi par Delsarte, Goethals et Mac Williams [7] en considérant une présentation à plusieurs indéterminées de ces codes et une approche géométrique.
Pour le cas $d = 2$, le polynôme de poids est entièrement donné par F.J. McEliece [15]. Mais pour $d > 2$, même la détermination du deuxième poids, qui est juste le poids au dessus de la distance minimale, est généralement non résolue. Ce poids est calculé sous certaines conditions, par J.P. Cherdieu et R. Rolland [6]. Dans cet article, les auteurs donnent le second poids avec la restriction q relativement grand par rapport à d, ce qui peut être écrit sous forme simplifiée :

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

Le travail de cette thèse a commencé par la recherche sur ce point autour des pistes suivantes :
- Soit trouver des polynômes contenant des facteurs absolument irréductibles et donnant un poids plus petit que celui calculé par Cherdieu et Rolland.
- Soit supprimer la condition (1) ci-dessus qui est assez large.
Par la suite, nous avons travaillé sur une partie importante du spectre de poids dans le cas projectif, à partir duquel nous avons ensuite déduit les poids correspondants dans le cadre affine (voir annexe).
Les travaux de cette thèse ont abouti à ce niveau à produire quatre papiers dont deux sont déjà publiés. Néanmoins beaucoup de questions restent ouvertes sur le sujet.
1)Le premier, intitulé "Second highest number of points of hypersurfaces in $\mathbb{F}_q^n$", paru dans Finite Fields and Their Applications **13** (2007) (communiqué par Gary L. Mullen).
Dans ce papier, d'une part, nous cherchons à trouver des hypersurfaces non réunions d'hyperplans et qui peuvent donner un nombre de points supérieur à $N_2^\ell = dq^{n-1} - (d-1)q^{n-2}$. D'autre part, nous étudions la dissection de certaines hypersurfaces par des hyperplans et nous cherchons à prouver qu'une hypersurface contenant au moins N_2^ℓ points est un arrangement d'hyperplans. Par des méthodes de combinatoire et de géométrie des incidences, nous avons obtenu des résultats sur le deuxième poids des codes de Reed-Muller généralisés, ce qui lève une grande partie des restrictions de Cherdieu et Rolland [6]. Ce travail ne demande aucun prérequis de théorie des codes.

2)Le deuxième, intitulé "Les Arrangements Minimaux et Maximaux d'Hyperplans dans $\mathbb{P}^n(\mathbb{F}_q)$", paru dans C. R. Acad. Sc. Paris, Ser. I 344 (2007) (présenté par Jean-Pierre Serre). Ce papier étudie les arrangements d'hyperplans dans un espace projectif tels que le nombre de points rationnels de la réunion de ces hyperplans soit minimal. Ce travail a donné comme résultat :
-la détermination du nombre de points minimum donné par un arrangement d'hyperplans, et la configuration géométrique de ces arrangements d'hyperplans.
- Une condition entre q et d pour que ce nombre représente une borne supérieure pour le nombre de points d'une hypersurface quelconque de $\mathbb{P}^n(\mathbb{F}_q)$.
-Une condition nécessaire et suffisante pour qu'un poids d'un mot de code de Reed-Muller d'ordre d sur $\mathbb{P}^n(\mathbb{F}_q)$ soit donné par un arrangement de d hyperplans.

3)Le troisième, intitulé "Special Numbers of Rational Points on Hypersurfaces in the n-dimensional Projective space over a Finite Field", est soumis au "journal of Discrete Mathematics". Nous y donnons une liste d'arrangements d'hyperplans donnant une partie du spectre de poids pour le cas des codes de Reed-Muller Projectifs. Puis nous donnons des bornes sur le nombre de points d'une hypersurfaces quelconque (non composée d'un arrangement d'hyperplans), éventuellement des hypersurfaces absolument irréductibles. L'une de ces bornes est bien comparable avec la borne de Weil sur le nombre de zéros d'un polynôme absolument irréductible.

4)Le quatrième, intitulé "Sur le Nombre de Points Rationnels d'une Courbe Projective Plane sur un Corps Fini ", c'est un papier à soumettre dont une copie rédigé en français est disponible en ligne dans les preprints de l'institut de Mathématiques de Luminy ; http ://iml.univ-mrs.fr/editions/preprint2007/preprint2007.html. Dans ce papier nous restreignons le travail sur les hypersurfaces de l'article 3 précédent aux courbes. Le but est d'améliorer les résultats trouvés dans le cadre des hypersurfaces et d'étudier la possibilité de supprimer les conditions entre q et d pour le deuxième et le troisième grand nombre de zéros. Parmi les résultats trouvés :
- On montre que sur un corps premier $\mathbb{F}_p$ on peut supprimer la condition $d \leq \left[\frac{q}{2}\right]$ pour confirmer le deuxième poids déjà trouvé ; ce qui répond à la question posée sur ce poids en dehors de cette condition.
-On construit des courbes contenant des facteurs non linéaires qui atteignent le troisième grand nombre de zéros N_3^ℓ. Evidemment, ces courbes ont plus de points que N_i^ℓ, pour $i \geq 4$ et que N_{min}^ℓ.
Ceci lève la question sur l'existence de courbes qui ne sont pas composées entièrement de droites et qui peuvent donner des nombres de points dépassant ceux donnés par certaines courbes composées seulement de droites.

1.2 Codes de Reed-Muller généralisés, distribution des Poids

1.2.1 Définitions et notations

On note par :
– $\mathbb{F}_q$ un corps fini à q éléments (q une puissance d'un nombre premier p).

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

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

– $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \cup \{0\}$ 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 $n \geq 2$.

Cadre projectif On rappelle qu'un code de Reed-Muller projectif $PRM(q, d, n)$ est l'image d'une application

$$\begin{array}{rccc} \Phi: & \mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \cup \{0\} & \longrightarrow & \mathbb{F}_q^{\pi_n} \\ & f & \longmapsto & (\mathrm{ev}f(v))_{v \in \mathbb{P}^n(\mathbb{F}_q)} \end{array}$$

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

avec x_i est la première composante non nulle de $v = (x_0 : ... : x_n)$.

Cette application est injective lorsque $d < q$ (on peut le voir facilement par récurrence sur n). Parmi les paramètres de ce code, on a :
longueur $(PRM(q, d, n)) = \Pi_n$ et dimension$(PRM(q, d, n)) = \binom{n+d}{d}$.

– un mot de code $c \in PRM(q,d,n)$ est défini par le vecteur :
$c = (\mathrm{ev}f(v_1), ..., \mathrm{ev}f(v_{\pi_n}))$; 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 définit par f, noté aussi $\#S$.

– $N_1 = \max_{f \in \mathbb{F}_q[X_0,X_1,...,X_n]_d^h} \#Z_q(f)$;

– $\mathcal{P}_1$: l'ensemble des polynômes $f \in \mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ tel que $\#Z_q(f) = N_1$.

– $N_i = \max_{f \in \mathbb{F}_q[X_0,X_1,...,X_n]_d^h \setminus \{\mathcal{P}_1 \cup ... \cup \mathcal{P}_{i-1}\}} \#Z_q(f)$, 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 $f \in \mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ tel que $\#Z_q(f) = N_i$.

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

Cas affine Un code de Reed-Muller généralisé classique $GRM(q,d,n)$ peut être défini comme image de l'application injective

$$\begin{array}{rccc} \Phi : & \mathcal{P}_{(q,d,n)} & \longrightarrow & \mathbb{F}_q^{q^n} \\ & f & \longmapsto & (f(v))_{v \in \mathbb{F}_q^n} \end{array}$$

Parmi les paramètres de ce code, on a :
longueur $(PRM(q,d,n)) = q^n$ et dimension$(PRM(q,d,n)) = \binom{n+d}{d}$.
On parlera de la distance minimale dans le paragraphe suivant consacré à la distribution des poids.

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.

1.3 Résultats sur la distribution des poids

1.3.1 Distance minimale

Cas Affine La distance minimale est donnée dans deux cas à partir de [13] (R.Lidl, H. Niederreiter, théorème 6.13 p 275) lorsque $d \leq q$ et de [11] (Kasami, Lin and Peterson Théorème 5 p. 192).

Théorème 1.3.1. – *Si $d \leq q$ la distance minimale du code $GRM(q, d, n)$ est*

$$d_{min} = w_1 = (q-d)q^{n-1}.$$

De façon plus générale :

– *(Kasami, Lin and Peterson (1968))*
Si $0 < d < n(q-1)$, la distance minimale du code de Reed-Muller Généralisé $GRM(q, d, n)$ est

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

avec $d = r(q-1) + s$ et $s < q-1$.

Un peu plus tard dans [7], les auteurs de cet article caractérisent les polynômes donnant $N_1 = q^n - w_1$ zéros ce qui donne la liste des mots du code $GRM(q, d, n)$ atteignant la distance minimale.

Theorem 1.3.1. *(Delsarte, Goethals et Mac Williams (1970))*

(a) Tout mot de code dont le poids est égal à la distance minimale peut être obtenu par un polynôme de cette 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 des permutations du groupe des automorphismes (le groupe général linéaire non homogène GLNNH(q,n)) sur les x_i (cf : [7] P.410).
Le degré est $d = r(q-1) + s$, avec les t_j sont distincts, et les w_i arbitraires, comme éléments de $\mathbb{F}_q$.

(b) Le nombre de mots de code ayant la distance minimale d_{min} est

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

Remarque 1. *L'hypersurface définie par un polynôme comme ci-dessus est une réunion d'hyperplans dont la configuration géométrique est la suivante :*
r directions dans chacune il y à $q-1$ hyperplans parallèles,
et une $(r+1)$-ème direction où il y a s hyperplans parallèles.

Cas projectif La distance minimale est donnée dans deux cas à partir de deux résultats. J.-P. Serre ([26]) et indépendamment, A. B. Sørensen ([28, 29]) ont donné une borne supérieure sur le nombre de points d'une hypersurface de degré d de $\mathbb{P}^n(\mathbb{F}_q)$. 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 $d-1 = r(q-1)+s$, $0 \leq s < q-1$. Dans le cas $(d < q)$, cette borne est atteinte par une hypersurface qui est une réunion de d hyperplans se coupant tous en une même sous-variété linéaire de codimension 2. Cet arrangement d'hyperplans, qu'on appelle ici maximal, donne la distance minimale des codes de Reed-Muller projectifs d'ordre d pour $d < q$:

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

Pour plus de détail, on peut consulter par exemple l'article de G. Lachaud [12].

1.3.2 Poids au dessus de la distance minimale

Avant de parler de poids au-dessus de la distance minimale, je voudrais citer la notion de poids généralisés (Higher Weights) introduite par Wei dans [35] pour un objectif cryptographique (codes for wire-tap channels of typeII, voir [17]). Pour voir cette notion ainsi que son aspect géométrique, j'invite le lecteur à lire l'article [34] de M. Tsfasman et S. Vladut intitulé "Geometric Approch to Higher Weights". Dans ce cadre, il est intéressant de remarquer que le premier poids généralisé coïncide avec la distance minimale, à savoir le premier poids classique. Nous avons consacré une partie de ce travail pour le calcul du deuxième poids classique dans la majorité des cas. Pour éviter toute ambiguïté et pour attirer l'attention du lecteur, il est à noter que le deuxième poids généralisé pour les codes de Reed-Muller est calculé dans le cas affine par P. Heijnen et R. Pellikaan [10] et par M. Boguslavsky dans le cas projectif [3].

Revenons-en maintenant à notre sujet : Pour $d = 2$, le polynôme de poids est entièrement calculé par McEliece [15].

Pour le cas général $d > 2$:
Des progrès ont été réalisés pour déterminer le spectre de poids des codes de Reed-Muller généralisés. Citons les articles de J.-P. Cherdieu et R. Rolland [6] et de A. Sboui [22, 23], qui déterminent le deuxième et le troisième poids. Un poids particulier est en outre donné dans [18] : il s'agit du plus grand poids des mots définis par les polynômes à facteurs linéaires. Pour le spectre de poids défini par tous les polynômes, il y a plus de précision et beaucoup moins de restriction dans l'article [24].

Deuxième poids

Rappelons l'origine de ce travail : les questions ouvertes posées par R. Rolland et J.-P. Cherdieu dans leur papier [6]. En complément, rappelons les principaux résultats de leur article intitulé " On the number of Points of Some Hypersurfaces in $\mathbb{F}_q^n$".

Théorème 1.3.2. *(J.-P. Cherdieu et R. Rolland [6])*

(i) Le deuxième grand nombre de zéros pour les fonctions polynomiales sur $\mathbb{F}_q$ à n variable et de degré total au plus d, produits de facteurs linéaires, est

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

(ii) Les fonctions polynomiales sur $\mathbb{F}_q$ à n variables et de degré total au plus d, qui sont produits de facteurs linéaires et admettant N_2^ℓ zéros, sont les fonctions polynomiales définissant les arrangements d'hyperplans suivants :
(a) $\mathcal{A}_1^d$; $d-1$ hyperplans parallèles et le d-ème hyperplan les coupe,
(b) $\mathcal{A}_2^d$; d hyperplans se coupent en une même sous-variété linéaire de co-dimension 2.
Le Nombre de fonctions polynomiales sur $\mathbb{F}_q$ à n variables et de degré total au plus d, qui sont produits de facteurs linéaires atteignant la borne N_2^ℓ est

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

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

A partir d'un résultat de W. Schmidt [25] (Theorem 5A, P. 210) améliorant une borne de A. Weil et S. Lang sur le nombre de points d'une hypersurface, on obtient le deuxième poids des codes de Reed-Muller généralisés lorsque q est assez grand :

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

En résumé du travail de Cherdieu et Rolland dans leur article [6] sur le deuxième poids, le cas d'un polynôme ayant un facteur absolument irréductible exige la condition que q soit assez grand relativement à d.

1.3.3 L'apport de cette thèse sur le deuxième poids w_2

La question ouverte posée par Cherdieu et Rolland dans leur article [6] se pose sur la possibilité de lever la restriction q soit assez grand par rapport à d (à savoir la condition (1)). Indépendamment des techniques ayant servi précédemment, nous abordons le problème avec une approche plus géométrique. Par des méthodes de combinatoire et de géométrie

des incidences, nous avons obtenu des résultats pour $q \geq 2d$ qui lèvent une grande partie des restrictions de Cherdieu et Rolland. Le résultat est présenté dans le chapitre 1, qui est l'objet du premier article publié dans Finite Fields and Their Applications.
Nous montrons que pour $q \geq 2d$, le deuxième grand nombre de points rationnels des hypersurfaces dans $\mathbb{F}_q^n$ est seulement donné par des hypersurfaces sous forme d'arrangement d'hyperplans de type $\mathcal{A}_1^d$ et $\mathcal{A}_2^d$ présentés précédemment dans le théorème 1.3.2. Ceci permet d'obtenir le deuxième poids ainsi le nombre de mots atteignant ce poids, les résultats sont trouvés dans la majorités des cas où les codes de Reed-Muller sont définis. L'outil essentiel utilisé commence par le lemme suivant :
Lemme 1.3.3. *Soit S une hypersurface de $\mathcal{H}_{(q,d,n)}$ (l'ensemble des hypersurfaces associées à $\mathcal{P}_{(q,d,n)}$), 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 $\mathrm{A}_{m+1} \supset \mathrm{A}_m$.*

A ce niveau, nous voudrions attirer l'attention du lecteur s'intéressant à ces techniques sur un outil décrit dans un article de E. Ballico [2] (Theorem 1.1) qui ressemble aux techniques de descente par sous-variétés linéaires de ce lemme et qui utilise d'autres arguments de géométrique pour les hypersurfaces cubiques :
Théorème 1.3.4. *Pour un entier t fixé, soit Y une hypersurface cubique irreductible de $\mathbb{P}^n(\mathbb{F}_q)$, $n \geq 2t+6$. Pour toute sous-variété linéaire $D \subset Y$ de dimension $t-1$, définie sur $\mathbb{F}_q$, il existe une sous-variété linéaire M de dimension t, définie sur $\mathbb{F}_q$ avec $D \subset M \subset Y$.*

1.4 Arrangement d'hyperplans et poids des codes de Reed-Muller projectifs

Nous avons présenté dans le cadre projectif des outils simples pour montrer certaines bornes ainsi que des calculs sur le nombre de points de certains arrangement d'hyperplans. Les résultats sont vérifiés par d'autres méthodes mieux connues : diagramme de "Hasse", le principe de "Deletion-Restriction" et les fonctions de Möbius. Il y a également des méthodes de calculs utilisant les nombres de "Betti". On propose au lecteur s'intéressant à ces outils les références [5, 16, 30].
La détermination de certains poids des codes de Reed-Muller Projectifs commence par un travail sur des configurations géométriques de d hyperplans donnant des nombres particuliers de points rationnels.

L'étude des configurations géométriques de certains arrangements d'hyperplans sur $\mathbb{F}_q$ permet d'avoir des idées préliminaires sur certains poids. Ainsi, sous certaines conditions entre q et d, on peut déterminer le nombre de mots du code atteignant un tel poids déjà calculé. Les travaux dans le cas général d'une hypersurface quelconque, donnent des bornes sur le

nombre de points des autres hypersurfaces qui ne sont pas des arrangements d'hyperplans, éventuellement des hypersurfaces absolument irréductibles.
Le deuxième et le troisième poids ainsi le nombre de mots ayant ces poids sont donnés dans le théorème et le corollaire suivants.

Théorème 1.4.1. *Soient $PRM(q,d,n)$ le code de Reed-Muller projectif avec $q \geq 3(d-2)$ et $d \geq 5$.*
On déduit la distance minimale de l'article de J.-P. Serre [26] :

$$d_{min} = w_1 = q^n - (d-1)q^{n-1}.$$

Le deuxième et le troisième poids sont tels que :

$$\begin{aligned} w_2 &= w_1 + (d-2)q^{n-2}, \\ w_3 &= w_1 + 2(d-3)q^{n-2}, \\ &= w_2 + (d-4)q^{n-2}. \end{aligned}$$

Corollaire 1.4.2. *Les nombres de mots de code $PRM(q,d,n)$ atteignant le i-ème poids w_i, $2 \leqslant i \leqslant 3$, qui sont aussi les nombres $\#\mathcal{P}_i$ des polynômes homogènes de $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ atteignant les i-ème nombres de zéros correspondants N_i, $2 \leqslant i \leqslant 3$, avec $q \geq 3(d-2)$ et $d \geq 5$, sont tels que :*

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

$$(ii) \quad \textit{pour } d > 7, \quad \#\mathcal{P}_3 = \binom{q}{d-3} \frac{q^2(q-1)^2}{2} \Pi_n \Pi_{n-1} \Pi_{n-2}.$$

Tout un travail sur les arrangements d'hyperplans d'une part et sur les autres hypersurfaces, non réunions complètes d'hyperplans, d'autre part est faite dans le troisième article, pour arriver à ces résultats. Nous mentionnons ici que les hypersurfaces associées aux ensembles des polynômes $\mathcal{P}_i$ atteignant les poids w_i, $i = 2, 3$ sont composées des arrangements d'hyperplans dont les configurations géométriques sont telles que :

(i) Arrangement de type $\mathcal{A}_2^d$: $d-1$ hyperplans se coupent (sont concourants) en une même sous-variété linéaire de co-dimension 2.

(ii) Arrangement de type $\mathcal{A}_3^d$: $(d-2)$ hyperplans $H_1, ..., H_{d-2}$ se coupent en une même sous-variété linéaire K_1 de co-dimension 2, les deux hyperplans, H_{d-1} et H_d se coupent en une sous-variété linéaire K_2 ($\neq K_1$) de co-dimension 2, tel que K_2 est contenue dans l'un des H_i, pour $1 \leq i \leq d-2$.

Il est intéressant de remarquer qu'à partir de l'arrangement $\mathcal{A}_2^d$, on peut obtenir les deux arrangements du cas affine donnés par Cherdieu et Rolland [6] qui atteignent le deuxième poids. Il revient à prendre $d+1$ hyperplans de type $\mathcal{A}_2^{d+1}$ et envoyer un hyperplans parmi

eux à l'infini, on distingue deux cas qui donnent les deux arrangements correspondants du cas affine.
Au cours de ce travail, une question qui était posée : quel est le dernier poids (autrement dit le plus grand poids) donné par un polynôme composé (produit) de facteurs linéaires ? Ce poids sera noté w^{ℓ}_{min} et l'arrangement d'hyperplans atteignant ce poids sera appelé minimal, noté $\mathcal{A}^d_{min}$.
Une analyse précise des configurations d'hyperplans, obtenue par récurrence à partir de la trace d'une configuration sur un hyperplan, nous a donné la configuration géométrique de l'arrangement minimal de d hyperplans. C'est le travail du deuxième article dans lequel on étudie les arrangements d'hyperplans dans un espace projectif tels que le nombre de points rationnels de la réunion de ces hyperplans soit minimal. Nous montrons de passage que la trace d'un sous-arrangement minimal sur l'un de ses hyperplans est un arrangement de Serre-Tsfasman donnant le premier poids qui est la distance minimale. Nous présentons ici le résultat donnant le nombre de points d'un arrangement minimal, ainsi que les conséquences sur le nombres de points d'une hypersurface contenant des composantes irréductibles. D'autre part, nous donnons un corollaire qui représente une conséquence de ce travail sur le spectre de poids linéaires des codes de Reed-Muller projectifs, à savoir le spectre défini par les polynômes produits de facteurs linéaires.

Théorème 1.4.3. *Un arrangement de d hyperplans minimal $\mathcal{A}^d_{min}$ 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 toutes distinctes entre elles.*
Pour tout arrangement de d hyperplans A, non de type $\mathcal{A}^d_{min}$, on a

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

Le nombre de points de la réunion des hyperplans appartenant à un arrangement de d hyperplans de type $\mathcal{A}^d_{min}$ est

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

En plus nous montrons, sous une condition raisonnable entre q et d, que le nombre de points d'un arrangement minimal représente une borne supérieure pour le nombre de points d'une hypersurface quelconque de degré d de $\mathbb{P}^n(\mathbb{F}_q)$ qui n'est pas une réunion d'hyperplans, cette borne est bien comparable avec une certaine borne connue de Weil sur le nombre de zéros d'un polynôme absolument irréductible.

Théorème 1.4.4. *Soit S une hypersurface définie sur $\mathbb{F}_q$ qui ne soit pas réunion d'hyperplans. Pour $q > \frac{d(d-1)}{2}$ le nombre N de points rationnels de cette hypersurface vérifie*

$$N < dq^{n-1} + \Pi_{n-2} - \frac{(d-1)(d-2)}{2} q^{n-2}.$$

Ce travail permet de déduire une condition nécessaire et suffisante pour qu'un poids soit atteint par un polynôme composé de facteurs linéaires (par un arrangement d'hyperplans).

Corollaire 1.4.5. *Si $q > \frac{d(d-1)}{2}$, pour qu'un poids d'un mot d'un code de Reed-Muller d'ordre d sur $\mathbb{P}^n(\mathbb{F}_q)$ soit inférieur ou égal à $q^n - (d-1)q^{n-1} + \frac{(d-1)(d-2)}{2} q^{n-2}$, il faut et il suffit qu'il soit donné par un arrangement de d hyperplans.*

1.5 Courbes projectives planes et codes de Reed-Muller sur $\mathbb{P}^2(\mathbb{F}_q)$

Nous nous intéressons par l'étude du nombre de points des courbes projectives planes, afin d'améliorer les résultats des nombres particuliers, déjà trouvés dans le cadre général des hypersurfaces. On distingue deux cas pour étudier le nombre de points des courbes qui ne sont pas entièrement composées de droites :

(i) Courbes ne contenant pas de droites.

(ii) Courbes contenant des composantes irréductibles (peuvent contenir des droites).

Pour le premier cas on utilise un travail récent de Carlin et Voloch [4], valable sur un corps premier $\mathbb{F}_p$ et qui permet d'améliorer les conditions entre p et d pour le deuxième et le troisième poids ainsi le poids w_{min} donné par un arrangement minimal de d droites.

Théorème 1.5.1 (Carlin et Voloch [4])**.** *Soient C une courbe algébrique plane définie sur $\mathbb{F}_p$ (p premier) de degré $d < p$, où on n'exclut pas qu'elle puisse être réductible. Supposons que C ne contient pas de composante linéaire définie sur $\mathbb{F}_p$. Alors*

$$\#C \leq \frac{d(d+p-1)}{2}.$$

Si $\#C \geq \frac{d(d+p-1)}{2} - (d-1)$, alors C est absolument irréductible.

Le résultat existe déjà sur un corps $\mathbb{F}_q$ quelconque sous d'autres conditions, voir l'article [31] (theorem 0.1). Dans leur article [19], Rodriguez, Voloch et Zagier donnent des courbes atteignant cette borne.

Par la suite, à partir d'une étude plus fine sur le cas des courbes contenant des composantes irréductibles (peuvent contenir un nombre $k < d$ de droites), nous arrivons à lever complètement la restriction sur le deuxième grand nombre de points dans ce cadre :
Théorème 1.5.2. *Soient C une courbe plane projective, non réunion complète de d droites, avec $d < p$, alors*

$$\#C < N_2^\ell,$$

et on a

$$N_2 = N_2^\ell.$$

Ce qui permet de confirmer le deuxième poids des codes de Reed-Muller définis pour $d < p$ sur $\mathbb{P}^2(\mathbb{F}_p)$. Ensuite une analyse sur les conique et les cubiques irréductibles, leurs intersection avec un faisceau de droites, nous a permis d'améliorer nettement le résultat sur le troisième grand nombre de points N_3, trouvé dans le cas des hypersurfaces. On trouve que $N_3 = N_3^\ell$ pour $d < p - 2$.

Théorème 1.5.3. *Soient C une courbe projective plane de degré d, non réunion complète de d droites avec $d < p - 2$, $p > 2$, alors*

$$\#C \leq N_3^\ell,$$

et on a

$$N_3 = N_3^\ell.$$

L'inégalité est stricte, sauf si la courbe C est constituée de $d-2$ droites issues d'un même point et d'une conique et que $d \geq \frac{p+5}{2}$.

Dans ce travail qui constitue une grande partie du quatrième article, on démontre de façon constructive l'existence des courbes sur $\mathbb{F}_q^n$ atteignant le nombre N_3^ℓ et nous donnons enfin un exemple illustrant un des trois cas où on peut atteindre N_3^ℓ. Evidemment, ces courbes ont plus de points que N_i^ℓ, pour $i \geq 4$ et que N_{min}^ℓ. Ce qui lève la question sur l'existence de polynômes ayant des facteurs non linéaires irréductibles et qui peuvent donner des nombres de zéros dépassant certains nombres donnés par des polynômes composées seulement de facteurs linéaires.

Chapitre 2

Spectre de Poids des Codes de Reed-Muller Généralisés affines

2.1 Relation entre arrangements d'hyperplans affines et projectifs

Notre but dans ce chapitre est de déterminer dans le cas affine, les poids particuliers w_i, $1 \leq i \leq 3$, ainsi que w_{min} déterminés dans le deuxième et le troisième article [18, 23] dans le cas projectif. Ceci revient en premier lieu à déterminer les arrangements affines correspondants aux arrangements projectifs donnant les nombres N_i^ℓ, $1 \leq i \leq 3$ et N_{min}^ℓ. Et pour finir le travail, on doit étudier le cas général des hypersurfaces affines qui ne sont pas entièrement constituées d'arrangements d'hyperplans.
Les notations des objets mathématiques utilisés dans ce chapitre sont définies dans le deuxième et le troisième chapitre.

> Connaissant les arrangements projectifs de type $\bar{\mathcal{A}}_i^d$ ayant N_i^ℓ points, on va chercher comment on peut déterminer les arrangements affines correspondants donnant le i-ème nombre de points N_i^ℓ dans le cas affine.

On note $\alpha : \mathbb{F}_q^n \hookrightarrow \mathbb{P}^n(\mathbb{F}_q)$ l'inclusion naturelle dans l'espace projectif et H_∞ l'hyperplan projectif $\mathbb{P}^n(\mathbb{F}_q) \setminus \mathbb{F}_q^n$. À un arrangement $\mathrm{A} = (H_i)_{i\in I}$ d'hyperplans affines dans $\mathbb{F}_q^n$, on associe l'arrangement projectif $\bar{\mathrm{A}} = (\bar{H}_i)_{i\in \bar{I}}$; $\bar{H}_i$ est l'adhérence de H_i dans $\mathbb{P}^n(\mathbb{F}_q)$ pour $i \in I$ et $\bar{I} = I \cup \{\infty\}$.
Inversement, à partir d'un arrangement de d+1 hyperplans projectifs $\bar{\mathrm{A}}^{d+1} = \{\bar{H}_1, \ldots, \bar{H}_{d+1}\}$, on peut obtenir un arrangement de d hyperplans affines $\{H_1, \ldots, H_d\}$. Il revient à considérer un quelconque des d+1 hyperplans comme hyperplan à l'infini, soit $\bar{H}_k = H_\infty$, $1 \leq k \leq d$+1. L'arrangement affine $\mathrm{A}^d = \{H_1, \ldots, H_d\}$ est obtenu en prenant la partie complémentaire

de l'arrangement projectif $\bar{\mathrm{A}}^d = \{\bar{H}_1, \ldots, \bar{H}_{k-1}, \bar{H}_{k+1}, \ldots \bar{H}_{d+1}\}$ par rapport à $\bar{H}_k$, avec $\bar{H}_k$ est vue ici comme hyperplan à l'infini. On peut choisir $k = d+1$, dans ce cas on peut écrire $H_i = \bar{H}_i \backslash (\bar{H}_{d+1} \cap \bar{H}_i)$, pour $1 \leq i \leq d$. On note $\complement_{\bar{H}_{d+1}}(\bar{A}^{d+1}) = A^d$, $\complement_{\bar{H}_{d+1}}$ l'application qui à $\bar{\mathrm{A}}^{d+1}$ fait correspondre A^d. Le nombre de points dans un arrangement projectif et celui dans l'arrangement affine correspondant, sont reliés par la formule : $N(\bar{\mathrm{A}}^{d+1}) = N(\mathrm{A}^d) + \#H_\infty$. La différence entre les deux nombres est fixe $(= \Pi_{n-1})$; ce qui explique le fait que la correspondance ci-dessus entre arrangements projectifs et arrangements affines conserve l'ordre sur le nombre de points.

> Ainsi, on obtient simplement un arrangement affine de type $\mathcal{A}_i^d$ à partir d'un arrangement projectif de $d+1$ hyperplans de type $\bar{\mathcal{A}}_i^{d+1}$ en supprimant un de ces hyperplans (considéré comme hyperplan à l'infini).

Rappelons les trois configurations géométriques d'arrangements de $d+1$ hyperplans projectifs donnat les trois premiers grands nombres de points ainsi la configuration géométrique d'un arrangement minimal (voir chapitre 3 en remplaçant d par $d+1$)

(i) Arrangement de type $\bar{\mathcal{A}}_1^{d+1}$: tous les hyperplans se coupent (sont concourants) en une même sous-variété linéaire de co-dimension 2.

(ii) Arrangement de type $\bar{\mathcal{A}}_2^{d+1}$: seulement d hyperplans se coupent (sont concourants) en une même sous-variété linéaire E de co-dimension 2, le $(d+1)$-ème hyperplan coupe E en une sous-variété linéaire F de co-dimension 3.

(iii) Arrangement de type $\bar{\mathcal{A}}_3^{d+1}$: $(d-1)$ hyperplans $H_1, ..., H_{d-1}$ se coupent en une même sous-variété linéaire K_1 de co-dimension 2, les deux hyperplans, H_d et H_{d+1} se coupent en une sous-variété linéaire K_2 $(\neq K_1)$ de co-dimension 2, telle que K_2 est contenue dans l'un des H_i, pour $1 \leq i \leq d-1$, soit $H_i = H_{d-1}$.

(iv) Arrangement de type $\bar{\mathcal{A}}_{min}^{d+1}$: tous les hyperplans contiennent une même sous-variété linéaire de co-dimension 3 et les intersections $H_i \cap H_j$ pour $i \neq j$ sont toutes distinctes entre elles.

A partir des quatre configurations projectives ci-dessus, on obtient les configurations affines suivantes de d hyperplans donnant, dans le cas affine, les nombres N_i^ℓ, $1 \leq i \leq 3$, ainsi le nombre N_{min}^ℓ :

Proposition 2.1.1. *Pour $3 < d \leq q$ et $n \geq 2$,*

(i) à partir d'un arrangement projectif de type $\bar{\mathcal{A}}_1^{d+1}$ on obtient un arrangement de type :

$\mathcal{A}_1^d$ *: tous les hyperplans sont parallèles.*

Le nombre de points est :

$$N(\mathrm{A}_1^d) = N_1^\ell = N_1 = dq^{n-1}.$$

On retrouve le résultat donné dans [13] (R.Lidl, H. Niederreiter [4], théorème 6.13 p 275).

(ii) à partir d'un arrangement projectif de type $\bar{\mathcal{A}}_2^{d+1}$ on obtient un arrangement de type :

(1) $\mathcal{A}^d_{2.a}$ *; $d-1$ hyperplans parallèles coupés par le d-ème hyperplan, soit H_d.*
(2) $\mathcal{A}^d_{2.b}$ *; tous les hyperplans se coupent (sont concourants) en une même sous-variété affine de co-dimension 2.*

Le nombre de points d'un arrangement A^d_2 ayant l'une de ces deux configurations est :

$$N(\mathrm{A}^d_2) = N^\ell_2 = dq^{n-1} - (d-1)q^{n-2}.$$

On retrouve ainsi le résultat donné dans [6] (théorèmes 2.1 et 2.2).

(iii) à partir d'un arrangement projectif de type $\bar{\mathcal{A}}^{d+1}_3$ on obtient un arrangement de type

(1) $\mathcal{A}^d_{3.a}$ *: $d-2$ hyperplans parallèles coupés par H_{d-1} et H_d qui sont eux mêmes parallèles selon une autre direction.*
(2) $\mathcal{A}^d_{3.b}$ *: $d-2$ hyperplans parallèles coupés par H_{d-1} et H_d, tel que H_{d-2}, H_{d-1} et H_d se coupent (sont concourants) en une même sous-variété affine de co-dimension 2.*
(3) $\mathcal{A}^d_{3.c}$ *: $d-1$ hyperplans se coupent en une même sous-variété affine de codimension 2 et le d-ème hyperplan est parallèle à l'un d'eux; soit $H_1, \ldots, H_{d-1}$ concourant et $H_d // H_{d-1}$.*

Le nombre de points d'un arrangement A^d_3 ayant une de ces trois configurations géométriques est :

$$N(\mathrm{A}^d_3) = N^\ell_3 = dq^{n-1} - 2(d-2)q^{n-2}.$$

(iv) à partir d'un arrangement projectif de type $\bar{\mathcal{A}}^{d+1}_{min}$ on obtient un arrangement de type :

$\mathcal{A}^d_{min}$: les intersections $H_i \cap H_j$ pour $i \neq j$ sont toutes disjointes entre elles. (i.e. tous les hyperplans se coupent deux à deux selon $\frac{d(d-1)}{2}$ sous-variétés affines disjointes).

Le nombre de points d'un arrangement A^d_{min} ayant ce type de configuration est :

$$N(\mathrm{A}^d_{min}) = N^\ell_{min} = dq^{n-1} - \frac{d(d-1)}{2}q^{n-2}.$$

Démonstration. Etant donné un arrangement projectif de $d+1$ hyperplans de type $\bar{\mathcal{A}}^{d+1}_i$, pour obtenir la ou les configurations de d hyperplans affines correspondantes dans chaque cas, il s'agit de voir toutes les possibilités pour le choix de l'hyperplan à l'infini.

Dans un arrangement projectif de $d+1$ hyperplans de type $\bar{\mathcal{A}}^{d+1}_1$ ou $\bar{\mathcal{A}}^{d+1}_{min}$, tous les hyperplans sont en positions symétriques entre eux (on ne distingue pas une position d'un hyperplan par rapport aux autres). Dans ces deux cas, pour n'importe quel hyperplan choisi comme H_∞, on obtient un seul type d'arrangement de d hyperplans affines, qui sont décrits dans les deux cas (i) et (iv).

(a) Dans un arrangement de type $\bar{\mathcal{A}}^{d+1}_2$, parmi les $d+1$ hyperplans, on distingue deux positions pour le choix de l'hyperplan à l'infini. On peut choisir :
- soit un quelconque des d premiers hyperplans qui sont concourants, et sont en position

symétrique ;
- soit l'hyperplan $\bar{H}_{d+1}$ qui ne passe pas par la sous-variété linéaire commune $\cap_{i=1}^{d}\bar{H}_i$.

(1) Dans le premier cas, on obtient $d-1$ hyperplans affines parallèles (car leur ensemble d'intersection est à l'infini) et le dernier hyperplan les coupe en des sous-variétés affines disjointes. Ce qui est le cas de la configuration affine $\mathcal{A}^d_{2.a}$; on écrit $\mathsf{C}_{\bar{H}_i}(\bar{A}_2^{d+1}) = A^d_{2.a}$, $1 \leq i \leq d$.
(2) Dans le deuxième cas on obtient d hyperplans affines se coupant en une même sous variété affine de co-dimension 2 (une partie de leur ensemble d'intersection qui est une sous-variété linéaire de co-dimension 3 est à l'infini). Ce qui est le cas de la configuration affine $\mathcal{A}^d_{2.b}$, on écrit $\mathsf{C}_{\bar{H}_{d+1}}(\bar{A}_2^{d+1}) = A^d_{2.b}$.

(b) Dans un arrangement de type $\bar{\mathcal{A}}_3^{d+1}$, parmi les $d+1$ hyperplans, on distingue trois positions pour le choix de l'hyperplan à l'infini. On peut choisir :
- soit l'hyperplan $\bar{H}_{d-1}$ qui a une sous-variété linéaire en commun avec les $d-2$ premiers $\bar{H}_i$ et qui a aussi une autre sous variété linéaire en commun avec $\bar{H}_d$ et $\bar{H}_{d+1}$;
- soit un quelconque des $d-2$ premiers hyperplans qui sont concourants (en position symétrique) ;
- soit l'un des deux hyperplans $\bar{H}_d$ et $\bar{H}_{d+1}$ (en position symétrique).

(1) Dans le premier cas on obtient $d-2$ hyperplans affines parallèles (car leur ensemble d'intersection est à l'infini) et de même pour les deux derniers. Ce qui est le cas de la configuration affine $\mathcal{A}^d_{3.a}$, on écrit $\mathsf{C}_{\bar{H}_{d-1}}(\bar{A}_3^{d+1}) = A^d_{3.a}$.
(2) Dans le deuxième cas on obtient $d-2$ hyperplans affines parallèles et les deux derniers sont concourants avec l'un des $d-2$ premiers hyperplans ; dans ce cas (selon les notations utilisées) c'est l'hyperplan affine $\bar{H}_{d-1} \setminus (H_\infty \cap \bar{H}_{d-1}))$. Ce qui est le cas de la configuration affine $\mathcal{A}^d_{3.b}$, on écrit $\mathsf{C}_{\bar{H}_i}(\bar{A}_3^{d+1}) = A^d_{3.b}$, $1 \leq i \leq d-2$.
(3) Dans le troisième cas on obtient $d-1$ hyperplans affines (concourants) se coupant en une même sous-variété affine de co-dimension 2, et le dernier est parallèle à H_{d-1}. Ce qui est le cas de la configuration affine $\mathcal{A}^d_{3.c}$, on écrit $\mathsf{C}_{\bar{H}_i}(\bar{A}_3^{d+1}) = A^d_{3.c}$, $i = d$ ou $d+1$.

Pour déterminer les nombres de points N_i^ℓ dans chaque cas, on doit rappeler ces nombres dans le cas projectif en remplaçant d par $d+1$:
Pour $3 < d \leq q$ et $n \geq 2$, le nombre de points N_i^ℓ d'un arrangement A_i^{d+1} de type $\mathcal{A}_i^{d+1}$, $1 \leq i \leq 3$, ainsi le nombre N^ℓ_{min} de points d'un arrangement minimal de $d+1$ hyperplans sont tels que :

$$\text{(i)} \quad N_1^\ell = (d+1)q^{n-1} + \Pi_{n-2},$$
$$\text{(ii)} \quad N_2^\ell = (d+1)q^{n-1} + \Pi_{n-2} - (d-1)q^{n-2},$$
$$\text{(iii)} \quad N_3^\ell = (d+1)q^{n-1} + \Pi_{n-2} - 2(d-2)q^{n-2},$$
$$\text{(iv)} \quad N^\ell_{min} = (d+1)q^{n-1} + \Pi_{n-2} - \frac{d(d-1)}{2}q^{n-2}.$$

Dans chaque cas nous retranchons $\Pi_{n-1} = q^{n-1} + \Pi_{n-2}$ qui est le nombre de points de l'hyperplan à l'infini, on trouve les nombres correspondants dans le cas affine. □

2.2 Cas général : Hypersurfaces définies par tous les Polynômes de $\mathbb{F}_q[X_1, ..., X_n]_d$

Dans cette section on va chercher s'il existe des hypersurfaces de degré d définies par des polynômes dans $\mathbb{F}_q[X_1, ..., X_n]_d$, non produits de facteurs linéaires, ayant un nombre de points plus grand que N_2^ℓ, N_3^ℓ, ou N_{min}^ℓ. Le résultat obtenu prouve, en particulier, que les hypersurfaces composées par des arrangements d'hyperplans contiennent plus de points que les autres lorsque $q > \frac{d(d+1)}{2}$. Le lemme suivant constitue un outil important pour montrer qu'une hypersurface ayant suffisamment de points est réunion d'hyperplans.

Lemma 2.2.1. *Soit ϕ un polynôme de $\mathbb{F}_q[X_1, ..., X_n]_d$ et S l'hypersurface définie par ϕ, tel que son nombre de points est plus grand ou égal à $\eta_t = dq^{n-1} - tq^{n-2}$, avec $q > d + t$, et 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 $A_{m+1} \supset A_m$.*

Démonstration. La démonstration peut être tirée de celle du cas projectif faite dans l'article [23] (Lemma 4.1.), en considérant variété affine au lieu de variété projective linéaire et en tenant compte des formules d'incidences du cas affine. Après vérification, ce qu'il faut remarquer essentiellement, c'est que le résultat dans le cas affine est donné sous la condition : $q > d + t$, tant dis que pour le cas projectif on a $q > d - 1 + t$. Ce qui est bien prévu. □

Théorème 2.2.1. *Soit f un polynôme, non produit de facteurs linéaires, dans $\mathbb{F}_q[X_1, ..., X_n]_d$ avec $d \geq 4$.*

(i) On retrouve le résultat du premier article [22], à savoir :

si $q \geqslant 2d$, alors

$$\#Z_q(f) < N_2^\ell,$$

ainsi

$$N_2 = N_2^\ell.$$

(ii) Si $q \geqslant 3(d-1)$, alors

$$\#Z_q(f) < N_3^\ell,$$

et par suite

$$N_3 = N_3^\ell.$$

(iii) Si $q > \frac{d(d+1)}{2}$, alors

$$\#Z_q(f) < N_{min}^\ell.$$

Démonstration. Soit f un polynôme de $\mathbb{F}_q[X_1, ..., X_n]_d$, S son hypersurface associée, tel que son nombre de points est supérieur ou égal à : $\eta_t = dq^{n-1} - tq^{n-2}$, avec $q > t + d$. Avec le lemme précédent nous prouvons par récurrence sur m que chaque point P dans S (vue comme sous-variété affine de dimension $m = 0$) est contenu dans un hyperplan de $\mathbb{F}_q^n$ qui est contenu dans S. Par conséquent S est une réunion d'hyperplans. C'est le cas des hypersurfaces particulières composées par des arrangements de d hyperplans.
Considérant les nombres N_2^ℓ, N_3^ℓ et N_{min}^ℓ dans la proposition 2.1.1, ces nombres coïncident avec η_t, respectivement, pour $t = d - 1$, $t = 2(d - 2)$ et $t = \frac{d(d-1)}{2}$. D'où on en tire les résultats (i), (ii) et (iii). □

La distance minimale et le deuxième poids, w_2, ainsi le nombre de mots atteignant w_2, sont donnés dans le premier article [22]. Nous donnons ici le troisième poids w_3 ainsi que le nombre de mots atteignant ce poids.
Corollaire 2.2.2. *Soient $GRM(q, d, n)$ le code de Reed-Muller généralisé d'ordre d sur $\mathbb{F}_q^n$, avec $q \geq 3(d - 1)$ on a :*
(i) Pour $d \geq 4$, le troisième poids w_3 est

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

(ii) Pour $d > 6$, le nombre de mots atteignant w_3, qui est aussi le nombre $\#\mathcal{P}_3$ de polynômes dans $\mathbb{F}_q[X_1, ..., X_n]_d$ ayant N_3 zéros est :

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

Démonstration. (i) Le nombre $w_3 = q^n - N_3$ est obtenu à partir des résultats précédents de la proposition 2.1.1 et du théorème 2.2.1.

(ii) Vu que le nombre N_3 est donné par les arrangements de types $\mathcal{A}_{3.a}^d$, $\mathcal{A}_{3.b}^d$ et $\mathcal{A}_{3.c}^d$ donnés dans la proposition 2.1.1, on va calculer le nombre d'arrangements de d hyperplans de chacun de ces trois types, puis on multiplie chaque nombre par $(q - 1)$ pour obtenir le nombre de polynômes associés. La somme des nombres de polynômes associés à ces trois types d'arrangements donne le nombre de mots de poids w_3.
Pour chaque type d'arrangement on va donner une méthode pour construire la configuration géométrique, ce qui nous donne le nombre de choix possibles de chaque étape. On peut ainsi calculer tous les arrangements possibles. En effet :
(a) Pour $\mathcal{A}_{3.a}^d$: on a $\frac{(q^n-1)}{(q-1)}$ directions possibles pour les $(d - 2)$ hyperplans parallèles, puis $\binom{q}{d-2}$ choix pour $d - 2$ hyperplans dans cette direction. Ensuite, pour choisir une autre direction, il nous reste $\frac{(q^n-q)}{(q-1)}$ cas possibles, puis $\binom{q}{2}$ choix de deux hyperplans dans cette

direction. D'où, le nombre de polynômes $\#\mathcal{P}_{3.a}$ associés aux arrangements de type $\mathcal{A}^d_{3.a}$ est :

$$\#\mathcal{P}_{3.a} = \binom{q}{d-2}\frac{q^2}{2}(q^n-1)(q^{n-1}-1).$$

(b) Pour $\mathcal{A}^d_{3.b}$: on a $\frac{(q^n-1)}{(q-1)}$ directions possibles pour les $(d-2)$ hyperplans parallèles, puis $\binom{q}{d-2}$ choix pour $d-2$ hyperplans dans cette direction. Ensuite, $(d-2)$ choix d'un hyperplan parmi les $(d-2)$ déjà choisis, notons H_k cet hyperplan, $1 \leq k \leq d-2$. Par la suite on fixe une sous-variété affine E_{n-2} de co-dimension 2 dans ce dernier hyperplan, où on a $q\frac{(q^{n-1}-1)}{(q-1)}$ choix. Enfin, parmi les q hyperplans autres que H_k passant par E_{n-2}, on a $\binom{q}{2}$ choix possibles de deux hyperplans passant par cette sous-variété affine de co-dimension 2. Alors le nombre de polynômes $\#\mathcal{P}_{3.b}$ associés aux arrangements de type $\mathcal{A}^d_{3.b}$, est :

$$\#\mathcal{P}_{3.b} = \binom{q}{d-2}\frac{q^2(d-2)}{2}(q^n-1)(q^{n-1}-1).$$

(c) Pour $\mathcal{A}^d_{3.c}$: on a $q^2\frac{(q^n-1)(q^n-q)}{(q^2-1)(q^2-q)}$ choix possibles pour fixer une sous-variété affine A_{n-2} de co-dimension 2. Par cette sous-variété, on a $\binom{q+1}{d-1}$ choix pour faire passer $d-1$ hyperplans. Choisissons ensuite un hyperplan H_i, $1 \leq i \leq d-1$, parmi ces $d-1$ hyperplans (d-1 choix possibles). Enfin, on a $q-1$ choix possibles pour le d-ième hyperplan qui soit parallèle à H_i. D'où, le nombre de polynômes $\#\mathcal{P}_{3.c}$ associés aux arrangements de type $\mathcal{A}^d_{3.c}$ est :

$$\#\mathcal{P}_{3.c} = \binom{q}{d-2}q^2(q^n-1)(q^{n-1}-1).$$

La somme des trois nombres donnés dans les trois cas (i), (ii) et (iii) donne le nombre $\#\mathcal{P}_3$ de mots de code de poids w_3. Reste à remarquer que la condition $d > 6$ est du au fait que le résultat provient du cas projectif ($d > 7$), ([23], Corollary 4.3. (II) (iii)).

□

On remarque bien que le nombre $\#\mathcal{P}_3$ est supérieur à $\#\mathcal{P}_2 = \binom{q}{d-1}\frac{d+1}{d}\frac{q^2(q^n-1)(q^{n-1}-1)}{(q-1)}$ (donné dans [6, 22]), qui est supérieur au nombre de mots atteignant la distance minimale, à savoir $\#\mathcal{P}_1 = \binom{q}{d}(q^n-1)$ (facile à calculer). Soit $\{w_n^\ell\}$ l'ensemble des poids donnés par les polynômes à facteurs linéaires ; si on note $(\#\mathcal{P}_n)$ la suite donnant les nombres de mots atteignant les poids (w_n^ℓ), la suite $(\#\mathcal{P}_n)$ semble croissante comme c'est le cas de la suite (w_n^ℓ).
Ceci s'interprète par le fait qu'en passant d'un poids au suivant, les configurations d'hyperplans correspondantes comportent moins d'hyperplans parallèles et d'hyperplans concourants. Ce qui donne plus de choix pour construire les configurations correspondantes à un

poids donné. En plus, à un certain moment d'autres hypersurfaces, ayant des composantes absolument irréductibles, entrent en jeux et atteignent certains poids de la famille $\{w_n^\ell\}$. Ce qui est le cas du troisième poids des codes de Reed-Muller projectifs, (cf : [24]), construits sur un plan projectif.

Bibliographie

[1] Y. Aubry : Reed-Muller codes associated to projective algebraic varieties, "Coding Theory and Algebraic geometry", Proceedings, Luminy 1991, Lecture Notes in Math. **1518** (1992), 4-17.

[2] E. Ballico : Geometry of Cubic and Quartic Hypersurfaces Over Finite Fields, Finite Fields and Their applications, **8** (2002), 554-569.

[3] M. Boguslavsky, On the number of solutions of polynomial systems, Finite Fields Appl. 3, no. 4 (1997), 287–299.

[4] M.-L. Carlin and J.-P. Voloch : Plane Curves with many Points over Finite Fields, Rocky Mountain Journal of Math., 34 (2004), 1255-1259.

[5] P. Cartier : les arrangements d'hyperplans, un chapitre de géométrie combinatoire, "séminaire Bourbaki", Lecture Notes in Mathematics, Vol. 901, Springer-Verlag, Berlin/New York.

[6] J. P. Cherdieu and R. Rolland, On the number of points of some Hypersurfaces in $\mathbb{F}_q^n$, Finite Fields and Their applications, **2** (1996), 214-224.

[7] P. Delsarte, J.M Goethals, and F.J Mac Williams : on generalized Reed-Muller codes and their relatives, Inform. Control **16** (1970).

[8] J. W. P. Hirschfeld : Projective Geometry over Finite Fields (Second Edition), Oxford University Press Inc., New York 1998.

[9] J.W.P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces : update 2001. Finite Geometries, Developments in Mathematics, Kluwer, Boston, 2001, pp. 201-246.

[10] P. Heijnen and R. Pellikaan : Generalized Hamming Weights of q-ary Reed-Muller Codes, IEEE trans. Inform. Theory, vol. 44, pp. 181-196, 1998.

[11] T. Kasami, S. Lin, and W. Peterson : New Generalizations of the Reed-Muller codes. I. primitive codes, IEEE Trans.Inform. Theory **I T -14**, N¡. 2 (1968)

[12] G. Lachaud : The parametres of projective Reed-Muller codes, Discrete Mathematics **81** (1990), 217-221.

[13] R. Lidl, H. Niederreiter : Finite Fields, Encyclopedia of Mathematics and its Applications, **vol 20**, Cambridge University Press (1983).

[14] Y. I. Manin and S. Vladut : Linear codes and modular curves, Itogi Nauki Tekhniki 25 (1984) 209-257 J. Soviet Math. **30** (1985) 2611-2643.

[15] R.J. McEliece, Quadratic forms over finite fields and second-order Reed-Muller codes, JPL Space Programs Summary, **37-58, vol.III.**

[16] P. Orlik and H. Terao : Arrangements of Hyperplanes, Springer-Verlag, Berlin/New York, 1992.

[17] L. H. Ozarow and A. D. Wyner : Wire-tap channel II, AT&T Bell Lab. Tech. J., vol. 63, pp. 665-680, 1984.

[18] F. Rodier, A. Sboui : Les arrangements minimaux et maximaux d'hyperplans dans $P^n(\mathbb{F}_q)$, **C. R. Acad. Sc. Paris, Ser. I 344 (2007)**.

[19] F. Rodriguez Villegas, J. F. Voloch and D. Zagier : Constructions of plane curves with many points, ACTA ARITHMETICA, XCIX.1 (2001).

[20] R. Rolland : The number of MDS[7,3] codes on finite fields of characteristic 2. AAECC 3, no.4, 301-310 (1992)

[21] P. Samuel : Géométrie Projective, Presses Universitaires de France, 1986.

[22] A. Sboui : Second Highest Number of Points of Hypersurfaces In $\mathbb{F}_q^n$, Finite Fields and Their Applications, FFA **13** (2007).

[23] A. Sboui : Special Numbers of Rational Points on Hypersurfaces in the n-dimensional Projective Space over a Finite Field, http ://iml.univ-mrs.fr/editions/preprint2006/preprint2006.html

[24] A. Sboui : Sur le Nombre de Points Rationnels d'une Courbe Projective Plane sur un Corps Fini, http ://iml.univ-mrs.fr/editions/preprint2007/preprint2007.html

[25] W. M. Schmidt : Equations over Finite Fields An Elementary Approach, Springer-Verlag, Berlin/New York, 1976.

[26] J.-P. Serre : Lettre *à* M. Tsfasman du 24 Juillet 1989, in journées Arithmétiques de Luminy 17-21 Juillet 1989, Astérisque **198-199-200** (1991).

[27] A.-N. Skorobogatov : Linear codes, strata of Grassmannians and the problems of Segre. Proceedings of AGCT-3, Luminy, 1991, Lecture Notes in Math. 1518, Springer-Verlag, Berlin 1992, 210-223.

[28] A.-B. Sørensen : On the number of rational points on codimension-1 algebraic sets in $\mathbb{P}^n(\mathbb{F}_q)$, Discrete Mathematics **135** (1994), 321-334.

[29] A.B. Sørensen : Projective Reed-Muller codes ; IEEE Transactions on Information Theory, Vol **37**, No. 6, November 1991

[30] R. P. Stanley : An Introduction To Hyperplane Arrangements, IAS/Parck City Mathematics Series (2005).

[31] K.-O. Stöhr and J. F. Voloch : Weierstrass points and curves over finite fields, Proc. London Math. Soc. (3) 52 (1986), 1-19.

[32] K. Thas : On the Number of points of Hypersurface In Finite Projective space (after J-P Serre) http :// Cage-rug. ac.be/˜K. Thas / ; submitted to J. Algebraic Geom.

[33] K. Thas : Topics in Finite and Algebraic Geometry, 92 pages, Atti Sem. Mat. Fis. Univ. Modena, to appear.

[34] M. Tsfasman and S. Vladut, "Geometric Approch to Higher Weights, IEEE trans. Inform. Theory, vol. 41, pp. 1564-1588, 1995.

[35] V. K. Wei, Generalized Hamming Weights for linear codes, IEEE trans. Inform. Theory, vol. 37, pp. 1412-1418, 1991.

[36] E. J. Weldon : New Generalizations of the Reed-Muller codes -Part II ; Nonprimitive codes, IEEE Trans.Inform. Theory **I T -14**, N¡. 2 (1968)

Chapitre 3

Deuxième grand nombre de points des Hypersurfaces de $\mathbb{F}_q^n$

Second Highest Number of Points of Hypersurfaces In $\mathbb{F}_q^n$

Adnen SBOUI

CNRS-IML, UPR 9016 - 163, Av. de Luminy - Case 907,
13288 Marseille 09 - France.
and
Département de Mathématiques, Faculté des Sciences
de Tunis 1060, Tunisie.

Abstract

For Generalized Reed-Muller, $GRM(q, d, n)$, codes, the determination of the second weight is still generally insolved, it is an open question of Cherdieu - Rolland [1]. In order to answer this question, we study some maximal hypersurfaces and we compute the second weight of $GRM(q, d, n)$ codes with the restriction that $q \geqslant 2d$.

subjclass[2000]: 11T71, 14J70, 05B25

keywords hypersurfaces, weight, Reed-Muller codes

1 Introduction

Let $q = p^t$ (q a power of a prime p, $p > 2$), and $\mathbb{F}_q$ the finite field with q elements. For the dth-order generalized Reed-Muller codes $GRM(q, d, n)$ defined over $\mathbb{F}_q^n$, an important problem is the determination of the weight distribution. The minimum weight was given by Kasami, Lin and Peterson [3], and also by Delsarte, Goethals and Mac Williams [2]. For the case $d = 2$, the weight polynomial is entirely computed by F.-J. McEliece [5]. But when $d > 2$, even the determination of the second weight, which is just the weight above

Email addresses: sboui@iml.univ-mrs.fr, Tel : (0033) 4 91 26 95 72, Fax (0033) 4 91 26 96 55 (Adnen SBOUI).

[1]

the minimal distance, is still generally insolved. This weight is computed, with some conditions, by J.P. Cherdieu and R. Rolland [1]. In this article the authors give the second weight under the restriction that q is large relatively to d, which can be written roughly in the form:

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

which is large enough.
In this paper, by using some methods of combinatorial and incidence geometry, and some techniques used by J-P. Serre [6] and K. Thas [7] in the projective space $P^n(\mathbb{F}_q)$, we prove that the second highest number of points of hypersurfaces of degree at most d in $\mathbb{F}_q^n$ is reached only by particular hypersurfaces which are unions of hyperplanes in the case $q \geq 2d$. In this case we obtained the second weight of the $GRM(q,d,n)$ codes.

2 Definitions and Notations

We denote by $\mathcal{P}_{(q,d,n)}$ the space of polynomials in n variables with coefficients in $\mathbb{F}_q$ and of total degree at most d. In this paper we suppose that $n \geq 2$, $d \geq 2$, and $q \geq 2d$.

We recall that the generalized Reed-Muller codes $GRM(q,d,n)$ is the image of the map

$$\begin{array}{rccc} \Phi: & \mathcal{P}_{(q,d,n)} & \longrightarrow & \mathbb{F}_q^{q^n} \\ & f & \longmapsto & (f(v))_{v\in\mathbb{F}_q^n} \end{array}$$

- a codeword $c \in GRM(q,d,n)$ is defined by the vector:
  $c = (f(v_1), ..., f(v_{q^n}))$; with $f \in \mathcal{P}_{(q,d,n)}$.
- The weight of c is the number of its non-zero coordinates.

- $Z_q(f)$ the set of zeros of f, $\#Z_q(f)$ is the number of points of the hypersurface S defined by f, denoted also $\#S$.

- $N_1 = \max_{f\in\mathcal{P}^*_{(q,d,n)}} \#Z_q(f)$; $\mathcal{P}^*_{(q,d,n)}$ is the set of non-zero polynomials in $\mathcal{P}_{(q,d,n)}$.
- The minimum weight is: $W_1 = q^n - N_1$.

- $\mathcal{P}_1$: the set of polynomials $f \in \mathcal{P}_{(q,d,n)}$ such that $Z_q(f) = N_1$.

- $N_2 = \max_{f \in \mathcal{P}^*_{(q,d,n)} \setminus \mathcal{P}_1} \#Z_q(f)$.
- The second weight is: $W_2 = q^n - N_2$.
- $\mathcal{P}_2$: the set of polynomials $f \in \mathcal{P}_{(q,d,n)}$ such that $Z_q(f) = N_2$.
- $\mathcal{H}_{(q,d,n)}$: the set of hypersurfaces defineds by the polynomials of $\mathcal{P}_{(q,d,n)}$.
- $\mathcal{H}_1$: the set of hypersurfaces $S \in \mathcal{H}_{(q,d,n)}$ such that $\#S = N_1$.
- $\mathcal{H}_2$: the set of hypersurfaces $S \in \mathcal{H}_{(q,d,n)}$ such that $\#S = N_2$.

Let us remark here that $\#\mathcal{P}_i = (q-1)\#\mathcal{H}_i$, for $i = 1, 2$, because each hypersurface can be defined by $(q-1)$ different defining polynomials.

3 Special Hypersurfaces

In this section we consider a special type of hypersurfaces, which are arrangements of some hyperplanes. The following theorems collects results of Kasami, Lin and Peterson [3], Delsarte, Goethals and Mac Williams [2], and J. P. Cherdieu and R. Rolland [1].

Theorem 3.1. *The minimum weight of the $GRM(q, d, n)$ codes, where $q > d$, which we call also minimal distance, is*

$$W_1 = q^n - dq^{n-1}$$

Proof. The result is easily deduced from Kasami, Lin and Peterson [3] (theorem 5), and Delsarte, Goethals and Mac Williams [2] (theorem 2.6.2). □

Moreover, Delsarte et al. [2] characterise all the polynomials defining codewords of minimal weight. These polynomials are products of linear factors and the associated hypersurfaces are unions of d parallel hyperplanes.

In the next theorem we consider hypersurfaces of degree d which are the union of d, not all parallel, hyperplanes. The maximal number of points in this case is the second highest number of zeros, if we restrict the polynomials to be products of linear factors. We will denote it by N_2^l.

Theorem 3.2. *(i) For hypersurfaces in $GF(q)^n$ which are the union of d, not all parallel, hyperplanes, the maximal number of points is given by the two configurations:*

(a) *all the hyperplanes but one are parallel;*
(b) *all the hyperplanes meet in a common subspace of codimension* 2.

(ii) $N_2^l = dq^{n-1} - (d-1)q^{n-2}$ *for* $n \geq 2$ *and* $2 \leq d < q$.

Proof. J. P. Cherdieu and R. Rolland [1] (theorems 2.1 - 2.2 p 216). □

4 Maximal Hypersurfaces

We will search if it exists hypersurfaces from $\mathcal{H}_{(q,d,n)} \setminus \mathcal{H}_1$ which have at least N_2^l points.
The result obtained, with $q \geqslant 2d$, prove that the number N_2^l is not exceeded. Furthermore the hypersurfaces reaching this number of points, called here maximal hypersurfaces, are unions of hyperplanes.

Theorem 4.1. *(i) Let* S *an hypersurface of degree* d *which is not the union of* d *parallel hyperplans (i.e.* $S \in \mathcal{H}_{(q,d,n)} \setminus \mathcal{H}_1$*), defined by a polynomial* $f \in \mathcal{P}_{(q,d,n)} \setminus \mathcal{P}_1$*, with* $q \geqslant 2d$*, then :*

$$\#S \leqslant N_2^l,$$

and so

$$N_2 = N_2^l.$$

(ii) The second weight of the $GRM(q,d,n)$ *codes (when* $q \geqslant 2d$*) is*

$$W_2 = q^n - dq^{n-1} + (d-1)q^{n-2}.$$

Lemma 4.2. *If* S *is an hypersurface in* $\mathcal{H}_{(q,d,n)}$*, such that its number of points is greater or equal to* N_2^ℓ*, (i.e.* $\#S \geqslant N_2^\ell$*), and* S *contains an affine subspace* A_m *of dimension* m *with* $0 \leqslant m \leqslant n-2$*, then* S *contains an affine subspace* A_{m+1} *of dimension* $m+1$ *such that* $\mathrm{A}_{m+1} \supset \mathrm{A}_m$.

Proof. Let A_m an affine subspace of dimension m contained in S. For an affine subspace A_{m+1}, of dimension $m+1$ of $\mathbb{F}_q^n$, containing A_m, two cases can appears.
(i) A_{m+1} is contained in S. In this case $\#(\mathrm{A}_{m+1} \cap S) = q^{m+1}$ as the restriction to S of the associated polynomial is identically zero ($f_{/S} = 0$);
(ii) $\mathrm{A}_{m+1} \setminus \mathrm{A}_m$ meets $S \setminus \mathrm{A}_m$ in at most $(d-1)q^m$ points, since $f_{/\mathrm{A}_{m+1}}$ have at most dq^m zeros (see R.Lidl, H. Niederreiter [4], theorem 6.13 p 275), and A_m

is made of zeros of f.
Recall that the number of A_{m+1} in $\mathbb{F}_q^n$ containing a fixed A_m is :

$$\frac{q^n - q^m}{q^{m+1} - q^m}.$$

We denote with b the number of A_{m+1}, containing A_m, and contained in S. Then the number of points of S is such that :

$$\#S \leqslant (d-1)q^m(\frac{q^n - q^m}{q^{m+1} - q^m} - b) + (q^{m+1} - q^m)b + q^m.$$

With the hypothesis that $\#S \geqslant N_2^l$, we have :

$$(d-1)\frac{q^n - q^m}{q-1} - b(d-1)q^m + (q^{m+1} - q^m)b + q^m \geqslant dq^{n-1} - (d-1)q^{n-2},$$

which is equivalent to :

$$b \geqslant \frac{\gamma_m}{(q-d)(q-1)},$$

where

$$\gamma_m = q^{n-m} - (2d-1)q^{n-1-m} + (d-1)q^{n-2-m} + (d-q).$$

we write γ_m in the form :

$$\gamma_m = q^{n-m-1}(q - (2d-1)) + (d-1)q^{n-2-m} + (d-q).$$

We remark that, the map $m \longrightarrow \gamma_m$ is decreasing in m, therefore $\gamma_m \geqslant \gamma_{n-2}$, for $0 \leqslant m \leqslant n-2$, and $q \geqslant 2d$.

We have

$$\gamma_{n-2} = q^2 - 2dq + 2d - 1 = (q-1)(q-(2d-1)),$$

so,

$$b \geqslant \frac{q-(2d-1)}{(q-d)} > 0, \text{since } q > 2d-1,$$

but b is an integer, hence $b \geqslant 1$.

Therefore S contains an affine subspace A_{m+1} such that $\mathrm{A}_{m+1} \supset \mathrm{A}_m$.

□

Proof of Theorem (4.1). Let S an hypersurface as in the theorem and let P a point in S. With this lemma we have proved by induction on m that the point P (viewed as an affine subspace of dimension 0) is contained in an hyperplane of $\mathbb{F}_q^n$ which is contained in S. This is the case for all points of S (because, P

can be chosen arbitrarily in S). Consequently S is the union of hyperplanes. So we are in the case of special hypersurfaces which are arrangements of d hyperplanes.
We conclude that the maximal number of points of hypersurfaces belonging to $\mathcal{H}_{(q,d,n)} \setminus \mathcal{H}_1$ is acheived by the two cases (a) and (b) of theorem (3.2).
So we obtain finally,

$$N_2 = N_2^l$$

and

$$W_2 = q^n - N_2 = q^n - dq^{n-1} + (d-1)q^{n-2}.$$

□

Corollary 4.3. *(i) The number of hypersurfaces from $\mathcal{H}_{(q,d,n)}$ reaching the bound N_2, for $q \geqslant 2d \geqslant 1$ is*

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

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

(ii) The number of codewords of $GRM(q,d,n)$ reaching the second weight w_2, which is also the number of polynomials of $\mathcal{P}_{(q,d,n)}$ reaching the second highest number of zeros N_2 is:

$$\#\mathcal{P}_2 = (q-1)\#\mathcal{H}_2.$$

Proof. This numbers are obtained with some combinatorial geometry in [1] (corollary 2.1. p 217) for the case of polynomials wich are products of linear factors, and the theorem (4.1) prove that the number N_2 is not exceeded with polynomials in $\mathcal{P}_{(q,d,n)} \setminus \mathcal{P}_1$ and is reached only by polynomials which are products of linear factors. This prove the result for $q \geqslant 2d \geqslant 1$.

□

References

[1] J. P. Cherdieu and R. Rolland, On the number of points of some Hypersurfaces in $\mathbb{F}_q^n$, Finite Fields and Their applications, **2** (1996), 214-224.

[2] P. Delsarte, J.M Goethals, and F.J Mac Williams: on generalized Reed-Muller codes and their relatives, Inform. Control **16** (1970).

[3] T. Kasami, S.Lin, and W. Peterson : New Generalizations of the Reed-Muller codes. I. primitive codes, IEEE Trans.Inform. Theory **I T -14**, N¡. 2 (1968)

[4] R. Lidl, H. Niederreiter: Finite Fields, Encyclopedia of Mathematics and its Applications, **vol 20**, Cambridge University Press (1983).

[5] R.J. McEliece, Quadratic forms over finite fields and second-order Reed-Muller codes, JPL Space Programs Summary, **37-58, vol.III.**

[6] J-P. Serre: Lettre *à* M. Tsfasman du 24 Juillet 1989, in journées Arithmétiques de Luminy 17-21 Juillet 1989, Astérisque **198-199-200** (1991).

[7] K. Thas : On the Number of points of Hypersurface In Finite Projective space (after J-P Serre) http:// Cage-rug. ac.be/˜K. Thas /; submitted to J. Algebraic Geom.

Chapitre 4

Les Arrangements Minimaux et Maximaux d'Hyperplans dans $\mathbb{P}^n(\mathbb{F}_q)$

Les Arrangements Minimaux et Maximaux d'Hyperplans dans $\mathbb{P}^n(\mathbb{F}_q)$

François RODIER, Adnen SBOUI

CNRS-IML, UMR 6206 - 163, Av. de Luminy - Case 907, 13288 Marseille 09, France.

Reçu le 24 juin 2006 ; accepté après révision le 6 janvier 2007
Disponible sur Internet le 15 fvrier 2007

Présenté par Jean Pierre Serre

Résumé

Dans cette note on étudie les arrangements d'hyperplans dans un espace projectif tels que le nombre de points rationnels de la réunion de ces hyperplans soit minimal. Ces résultats ont des applications en théorie des codes.

Pour citer cet article : F. Rodier, A. Sboui, C. R.Acad. Sci. Paris, Ser. I 344 (2007).

Abstract

Minimal and Maximal Arrangements of Hyperplanes in $\mathbb{P}^n(\mathbb{F}_q)$.

In this note we study the arrangements of hyperplanes in a projective space such that the number of rational points of the union of these hyperplanes is minimal. These results apply to coding theory.

To cite this article: F. Rodier, A. Sboui, C. R. Acad. Sci. Paris, Ser. I 344 (2007).

1 Introduction

J.-P. Serre ([Se]) et indépendamment A. B. Sørensen ([Sø]) ont donné une borne supérieure sur le nombre de points d'une hypersurface de degré d de $\mathbb{P}^n(\mathbb{F}_q)$. Cette borne est atteinte par une hypersurface qui est une réunion de d

Email addresses: rodier@iml.univ-mrs.fr (François RODIER), sboui@iml.univ-mrs.fr (Adnen SBOUI).

hyperplans se coupant tous en une même sous-variété linéaire de codimension 2. Cet arrangement d'hyperplans, qu'on appelle ici maximal, donne la distance minimale des codes de Reed-Muller projectifs d'ordre d pour $d < q$: $d_{\min} = q^n - (d-1)q^{n-1}$. On peut consulter par exemple l'article de G. Lachaud [La]. Peu de progrès ont été réalisés depuis pour déterminer le spectre des codes de Reed-Muller généralisés projectifs. Citons les articles de J.-P. Cherdieu et R. Rolland [CR] et de A. Sboui [Sb1,Sb2], qui déterminent le deuxième et le troisième poids. M. Boguslavsky détermine, lui, le deuxième poids généralisé de ce code [Bo].

Dans cette note on présente l'arrangement (dit minimal) de d hyperplans qui nous donne un autre poids de ces codes. On montre que lorsque $q > \frac{d(d-1)}{2}$, le nombre de points de la réunion des d hyperplans formant un arrangement minimal représente une borne supérieure pour le nombre de points d'une hypersurface quelconque de degré d de $\mathbb{P}^n(\mathbb{F}_q)$ qui n'est pas une réunion d'hyperplans.

2 Notations

On supposera ici que p est un nombre premier, $q = p^s$ où s est un entier strictement positif et d est un entier compris entre 3 et $q+1$. On note par $\mathbb{F}_q$ un corps fini à q éléments, $\mathbb{P}^n(\mathbb{F}_q)$ l'espace projectif de dimension n sur $\mathbb{F}_q$, $\Pi_n = \frac{q^{n+1}-1}{q-1}$ le nombre de points rationnels de $\mathbb{P}^n(\mathbb{F}_q)$.

3 Arrangements d'Hyperplans

Un arrangement de d hyperplans de $\mathbb{P}^n(\mathbb{F}_q)$ est un ensemble de d hyperplans H_i distincts ; on note $N(\mathrm{A})$ le nombre de points de la réunion des hyperplans appartenant à l'arrangement A. On distingue deux types d'arrangements de d hyperplans de $\mathbb{P}^n(\mathbb{F}_q)$, notés $\mathcal{A}_1^d$ et $\mathcal{A}_2^d$.

(1) Arrangement de type $\mathcal{A}_1^d$: tous les hyperplans contiennent une même sous-variété linéaire de codimension 2.
(2) Arrangement de type $\mathcal{A}_2^d$: 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 toutes distinctes entre elles.

3.1 Arrangement Maximal

On peut déduire le résultat suivant de la lettre de Serre [Se] (Théorème et Remarque (2)).

Proposition 3.1. *(i) Le nombre de points de la réunion des hyperplans appartenant à un arrangement de type $\mathcal{A}_1^d$ est $dq^{n-1} + \Pi_{n-2}$.*

(ii) Pour un arrangement de d hyperplans A *qui n'est pas de type $\mathcal{A}_1^d$ on a, pour $d \leq q$:*

$$N(\mathrm{A}) < dq^{n-1} + \Pi_{n-2}.$$

3.2 Arrangement Minimal

Définissons d'abord la trace d'un arrangement. Soit A un arrangement de d hyperplans H_i dans $\mathbb{P}^n(\mathbb{F}_q)$.

Définition 3.2. *La trace de l'arrangement* A *sur un hyperplan H distinct des H_i est l'arrangement, noté $tr_H(\mathrm{A})$, dans l'espace projectif H de dimension $n-1$, formé par les sous-variétés linéaires $H \cap H_i$.*

Les arrangements de type $\mathcal{A}_1^d$ et $\mathcal{A}_2^d$ sont liés par la proposition suivante qu'il est facile de démontrer (cf. [Sb2], proposition 2.3).

Proposition 3.3. *Les propriétés suivantes sont équivalentes :*

(i) $\mathrm{A} = \{H_1, \ldots, H_d\}$ *est un arrangement de type $\mathcal{A}_2^d$.*

(ii) Pour chaque $1 \leq i \leq d$, la trace de l'arrangement $\mathrm{A} - \{H_i\}$ sur H_i est un arrangement de type $\mathcal{A}_1^{d-1}$ dans l'hyperplan H_i.

Le théorème suivant justifie le nom d'arrangement minimal pour les arrangement de type $\mathcal{A}_2^d$.

Théorème 3.4. *(i) Le nombre de points de la réunion des hyperplans appartenant à un arrangement* A_2 *de type $\mathcal{A}_2^d$ est*

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

(ii) Pour tout arrangement de d hyperplans A*, non de type $\mathcal{A}_2^d$, on a*

$$N(\mathrm{A}) > N(\mathrm{A}_2).$$

Démonstration. (i) La formule suivante permet de compter sans répétition les points de la réunion d'hyperplans d'un arrangement $\mathrm{A}_2 = \{H_1, \ldots, H_d\}$:

$$N(\mathrm{A}_2) = \#H_1 + \sum_{j=1}^{d-1} \Big(\#H_{j+1} - N(tr_{H_{j+1}}\{H_1, \ldots, H_j\}) \Big). \qquad (1)$$

L'arrangement $\{H_1, \ldots, H_{j+1}\}$, étant une partie d'un arrangement d'hyperplans de type $\mathcal{A}_2^d$, est un arrangement du même type. La proposition 3.3 montre alors que la trace de l'arrangement $\{H_1, \ldots, H_j\}$ sur l'hyperplan H_{j+1} est un arrangement de type $\mathcal{A}_1^j$ dans H_{j+1}.

(ii) On va procéder par récurrence sur d.

Pour $d = 3$, le résultat est clair.

En supposant que le résultat soit vrai pour $d-1$ prouvons le pour d.

Soit A un arrangement de d hyperplans H_i qui ne soit pas de type $\mathcal{A}_2^d$. D'après la proposition 3.3, il existe au moins un i_0 compris entre 1 et d, tel que $tr_{H_{i_0}}(\mathrm{A} - H_{i_0})$ forme un arrangement d'au plus $d-1$ hyperplans dans H_{i_0}, qui ne soit pas de type $\mathcal{A}_1^{d-1}$. La proposition 3.1-(ii) implique que

$$N\Big(tr_{H_{i_0}}(\mathrm{A} - H_{i_0})\Big) < (d-1)q^{n-2} + \Pi_{n-3}. \tag{2}$$

Le nombre de points de la réunion des hyperplans appartenant à A est tels que :

$$N(\mathrm{A}) = \#(\bigcup_{\substack{i=1 \\ i \neq i_0}}^{d} H_i) + \#H_{i_0} - N\Big(tr_{H_{i_0}}(\mathrm{A} - H_{i_0})\Big). \tag{3}$$

D'après l'hypothèse de récurrence, on a

$$\#(\bigcup_{\substack{i=1 \\ i \neq i_0}}^{d} H_i) \geq (d-1)q^{n-1} + \Pi_{n-2} - \frac{(d-2)(d-3)}{2} q^{n-2}, \tag{4}$$

d'où le résultat.

□

3.3 Existence

Par dualité entre espaces projectifs, un arrangement de type $\mathcal{A}_2^d$ dans $\mathbb{P}^n(\mathbb{F}_q)$ correspond à un ensemble de d points contenus dans un plan dans l'espace projectif dual $\mathbb{P}^n(\mathbb{F}_q)^\perp$, tel que 3 points ne soient pas alignés, autrement dit un d-arc dans ce plan selon la terminologie de la géométrie des espaces projectifs finis (*voir* [HS]). Un ensemble de d points rationnels d'une conique forme un d-arc pour tout $d \leq q+1$. Par dualité, il provient d'un arrangement de type $\mathcal{A}_2^d$ dans $\mathbb{P}^n(\mathbb{F}_q)$. En caractéristique impaire, tout ensemble de d droites tangentes à une conique est un arrangement minimal dans $\mathbb{P}^2(\mathbb{F}_q)$.

On peut prolonger cette construction à $\mathbb{P}^n(\mathbb{F}_q)$: on vérifie facilement qu'étant données une sous-variété linéaire Z de codimension 3 dans $\mathbb{P}^n(\mathbb{F}_q)$ et un arrangement A de droite de type $\mathcal{A}_2^d$ dans un plan disjoint de Z, tout ensemble

de d hyperplans engendrés par Z et par une droite de l'arrangement A est un arrangement minimal pour tout $d \leq q+1$.

4 Cas Général : les hypersurfaces

On montre qu'il n'existe pas d'hypersurface qui ne soit pas réunion d'hyperplans, et qui ait un nombre de points plus grand qu'un arrangement minimal de d hyperplans, lorsque $q > \frac{d(d-1)}{2}$.

Théorème 4.1. *Soit S une hypersurface définie sur $\mathbb{F}_q$ qui ne soit pas réunion d'hyperplans. Pour $q > \frac{d(d-1)}{2}$ le nombre N de points rationnels de cette hypersurface vérifie*

$$N < dq^{n-1} + \Pi_{n-2} - \frac{(d-1)(d-2)}{2} q^{n-2}.$$

Ce résultat se déduit du lemme suivant.

Lemme 4.2. *Soit S une hypersurface contenant au moins $dq^{n-1} + \Pi_{n-2} - \frac{(d-1)(d-2)}{2} q^{n-2}$ points rationnels, avec $q > \frac{d(d-1)}{2}$. Supposons que S contient un sous-espace linéaire E_m de dimension m avec $0 \leqslant m \leqslant n-2$, alors S contient un sous-espace linéaire E_{m+1} de dimension $m+1$ tel que $E_{m+1} \supset E_m$.*

Démonstration. Le résultat est démontré dans un cadre plus général dans [Sb2], lemma (4.1). □

Le théorème se montre alors par récurrence sur m. Si S est comme dans le lemme, chaque point P est contenu dans un hyperplan de $\mathbb{P}^n(\mathbb{F}_q)$ qui est contenu dans S. Par conséquent S est réunion d'hyperplans.

On en déduit le résultat suivant sur les codes de Reed-Muller.

Corollaire 4.3. *Si $q > \frac{d(d-1)}{2}$, pour qu'un poids d'un mot d'un code de Reed-Muller d'ordre d sur $\mathbb{P}^n(\mathbb{F}_q)$ soit inférieur ou égal à $q^n - (d-1)q^{n-1} + \frac{(d-1)(d-2)}{2} q^{n-2}$, il faut et il suffit qu'il soit donné par un arrangement de d hyperplans.*

Références

[Bo] M. Boguslavsky, On the number of solutions of polynomial systems, Finite Fields Appl. 3, no. 4 (1997), 287–299.

[CR] J.-P. Cherdieu, R. Rolland, On the number of points of some hypersurfaces in $\mathbb{F}_q^n$, Finite Fields Appl. 2, no. 2 (1996), 214–224.

[HS] J.W.P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces : update 2001. Finite Geometries, Developments in Mathematics, Kluwer, Boston, 2001, pp. 201 246.

[La] G. Lachaud, The parameters of projective Reed-Muller codes, Discrete Math. 81, no. 2 (1990), 217–221.

[Sb1] A. Sboui, Second highest number of points of hypersurfaces in $\mathbb{F}_q^n$, Finite Fields and Their Applications, FFA **13** (2007).

[Sb2] A. Sboui, Special numbers of rational points on hypersurfaces in the n-dimensional projective space over a finite field, soumis au Journal of Discrete Mathematics, disponible sur Internet à l'adresse <http ://iml.univ-mrs.fr/editions/preprint2006/preprint2006.html>

[Se] J.-P. Serre, Lettre à M. Tsfasman, in : Journées Arithmétiques de Luminy, 17-21 juillet 1989, Astérisque **198-199-200**, 1991, 351–353.

[Sø] A. B. Sørensen, Projective Reed-Muller codes, IEEE Trans. Inform. Theory 37, no. 6 (1991), 1567–1576.

Modifications effectuées

– L'expert a écrit : *It is not clear what sort of consequences these two results have for the spectrum of projective Reed-Muller codes. (...)*
In general, the note gives a very little indication of the coding theoretic motivation and/or consequences of their work. (...)
The authors should at least add the works mentioned in this report.
J'ai mentionné dans l'introduction, l'état des connaissances sur le spectre des codes de Reed-Muller généralisés, et je l'ai complété par plus de références.
J'ai également ajouté un corollaire au théorème 4.1, pour indiquer les conséquence de ce résultat sur le spectre des codes de Reed-Muller.

– L'expert a écrit : *I believe Section 4 concerning duality and its consequences needs greater elaboration or at least a pointed reference to a forthcoming paper where details about the claims made can be found.*
J'ai présenté cette section (devenue la sous-section 3.3) de manière plus simple et adaptée au cas des arrangements d'hyperplans.

– L'expert a écrit : *Minor corrections*
Elles ont été toutes faites

– *Autres modifications*
J'ai supprimé la Remarque 1 et j'ai inséré son contenu où elle était utile, à savoir la démonstration du Théorème 3.4, (i).

Chapitre 5

Nombres particuliers de Points Rationnels des Hypersurfaces sur un espace Projectif de dimension n sur un Corps Fini (dans $\mathbb{P}^n(\mathbb{F}_q)$)

Special Numbers of Rational Points on Hypersurfaces in the n-dimensional Projective space over a Finite Field

Adnen SBOUI

CNRS-IML, UMR 6206, Campus Univ. de Luminy - Case 907,
13288 Marseille 09 - France.
and
Département de Mathématiques, Faculté des Sciences
de Tunis 1060, Tunisie.

Abstract

We study first some arrangements of hyperplanes in the n-dimensional projective space $\mathbb{P}^n(\mathbb{F}_q)$. Then we compute, in particular, the second and the third highest numbers of rational points on hypersurfaces of degree d. As application of our results we obtain some weights of the Generalized Projective Reed-Muller codes $PRM(q, d, n)$. And we also list all the homogeneous polynomials reaching such numbers of zeros and giving the correspondent weights.

Key words: Hyperplane arrangements, Hypersurfaces, Rational points, Homogeneous Polynomials, Projective Reed-Muller Codes.
Subjclass[2000] (MSC): 11T71, 14J70, 05B25

1 Introduction

The determination of the number of points in certain hypersurfaces of degree d in the n-dimentional affine and projective space over a finite field $\mathbb{F}_q$, gives results on the weight distribution of the generalized Reed-Muller codes. The d-th order generalized Reed-Muller codes $GRM(q, d, n)$ was introduced firstly

Email addresses: sboui@iml.univ-mrs.fr, Tel : (0033) 4 91 26 95 72, Fax (0033) 4 91 26 96 55 (Adnen SBOUI).

[1]

in the affine case by Kasami, Lin and Peterson [4], studied in detail by connection between the multivariable and one variable approch by Delsarte, Goethals and Mac Williams [3]. Moreover Lachaud [5] following Manin and Vladut [6], has considered projective Reed-Muller codes $PRM(q, d, n)$ i.e. the d-th order Reed-Muller codes defined over the projective space $\mathbb{P}^n(\mathbb{F}_q)$. As another presentation, in his paper [1] Y. Aubry studied the case of Reed-Muller codes associated to projective algebraic varieties.
As in the affine case, a difficult problem is the determination of the weight polynomial. The only known weight is the first, called the minimum distance and it has been proven independently by Sørensen [10] and Serre [8].
However, in the affine case, for the classical generalized Reed-Muller codes the second weight was computed by Cherdieu and Rolland [2] under a condition between q and d. Recently, I [7] resolved a large part of the restriction of Cherdieu and Rolland and proved the result of the second wieght in the majority of cases.
In this paper, by using some methods of combinatorial and incidence geometry in the projective space $\mathbb{P}^n(\mathbb{F}_q)$, we compute in particular, the second and the third highest numbers of points of hypersurfaces which are associated to homogeneous polynomials in $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$.
We start with the case of homogeneous polynomials which are products of linear factors. In this case we give the three first highest numbers of zeros and the last one. In the following we study the general case of homogeneous polynomials in $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ and we obtain some weights of $PRM(q, d, n)$ codes. In each case we compute the number of codewords reaching the correspondent weights.

2 Definitions and Notations

We denote by :

- $\mathbb{F}_q$ a finite field with q elements (q a power of a prime p).
- $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \cup \{0\}$ the vector space of homogeneous polynomials in $n+1$ variables with coefficients in $\mathbb{F}_q$ and of degree d.
- $\mathbb{P}^n(\mathbb{F}_q)$ the n-dimensional projective space over $\mathbb{F}_q$.
- $\Pi_n = \#\mathbb{P}^n(\mathbb{F}_q) = \frac{q^{n+1}-1}{q-1}$, the number of rational points of $\mathbb{P}^n(\mathbb{F}_q)$.
- $\Pi_{-1} = 0$ (by convention, which meaning the number of points in the empty set).

In this paper we suppose that $2 \leq d \leq q$ and $n \geq 2$. We recall that the projective Reed-Muller codes $PRM(q,d,n)$ is the image of the map

$$\begin{array}{rccc} \Phi : \mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \cup \{0\} & \longrightarrow & \mathbb{F}_q^{\pi_n} \\ f & \longmapsto & (\mathrm{ev}f(v))_{v \in \mathbb{P}^n(\mathbb{F}_q)} \end{array}$$

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

where x_i is the first non-zero component of $v = (x_0 : ... : x_n)$.

- A codeword $c \in PRM(q,d,n)$ is defined by the vector :
  $c = (\mathrm{ev}f(v_1), ..., \mathrm{ev}f(v_{\pi_n}))$; with $f \in \mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \cup \{0\}$.

- The weight of c is the number of its non-zero coordinates.

- $Z_q(f)$ the set of zeros of f, $\#Z_q(f)$ is the number of points of the hypersurface S defined by f, denoted also $\#S$.

- $N_1 = \max\limits_{f \in \mathbb{F}_q[X_0,X_1,...,X_n]_d^h} \#Z_q(f)$;

- $\mathcal{P}_1$: the set of polynomials $f \in \mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ such that $\#Z_q(f) = N_1$.

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

- $\mathcal{P}_i$: the set of polynomials $f \in \mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ such that $\#Z_q(f) = N_i$.

- The i-th weight is $w_i = \Pi_n - N_i$, for $i \geq 1$.

3 Hyperplane Arrangements

An arrangement of d hyperplanes in $\mathbb{P}^n(\mathbb{F}_q)$ is a set, $\mathrm{A}^d = \{H_1, \ldots, H_d\}$, of d hyperplanes. From the geometrical point of view, a set of zeros of a homogeneous polynomial product of d distinct linear factors is a particular hypersurface formed by an arrangement of d hyperplanes.
The maximal number of $\mathbb{F}_q$-rational points on a hypersurface of degree d in the n-dimensional projective space $\mathbb{P}^n(\mathbb{F}_q)$ is obtained by hypersurfaces splits

into d distinct hyperplanes having a certain geometrical configuration, what is given by Serre [8] for $d \leq q$ and by Sørensen [9] for $d \leq n(q-1)$.
It is of interest to find other configurations of hyperplanes with many points, in order to determine other weights of certain classes of codes. It would be desirable to classify arrangements of d hyperplanes according to theirs numbers of points. However, it comes that is possible to classify them for small values of d, which is not obvious for large value.
For any value of d, less than q, we present the three first arrangements of d hyperplanes, having the first three highest numbers of points, which is the subject of subsection (3.3) and the last one which is the bulk of the following subsection (3.1), what will be called minimal arrangement, that is the arrangement with the minimum number of points.
For an arrangement $\mathrm{A}^d = \{H_1, \ldots, H_d\}$, the number of points in the union $\bigcup_{i=1}^{d} H_i$ is called the number of points of the arrangement A^d, denoted by $N(\mathrm{A}^d)$ and by $\#\bigcup_{i=1}^{d} H_i$ in certain cases.
We describe five configurations of arrangements of d hyperplanes in the projective space $\mathbb{P}^n(\mathbb{F}_q)$ denoted by $\mathcal{A}_i^d$, $1 \leq i \leq 5$, and we will denote by A_i^d an arrangement of type $\mathcal{A}_i^d$. Sometimes, by abuse of brevity we say $\mathcal{A}_i^d$-arrangement for an arrangement A_i^d of type $\mathcal{A}_i^d$.

(1) Arrangement of type $\mathcal{A}_1^d$: all the hyperplanes meet in a common subspace of codimension 2.

(2) Arrangement of type $\mathcal{A}_2^d$: $(d-1)$ hyperplanes meet in a common subspace K of codimension 2 and the d-th hyperplane meet K in a subspace E of codimension 3.

(3) Arrangement of type $\mathcal{A}_3^d$: $(d-2)$ hyperplanes $H_1, ..., H_{d-2}$ meet in a common subspace K_1 of codimension 2, the last two hyperplanes, H_{d-1} and H_d meet in a subspace K_2 $(\neq K_1)$, such that K_2 is contained in one H_i, for $1 \leq i \leq d-2$.

(4) Arrangement of type $\mathcal{A}_4^d$: for each $1 \leq i, j \leq d$ and $i \neq j$, we have $H_i \cap H_j = K_j^i$, where the K_j^i are $\binom{d}{2}$ linear subspaces of codimension 2 all distinct and meet in a common linear subspace M of codimension 3.

(5) Arrangement of type $\mathcal{A}_5^d$: the remainding cases.

Remark 1. *It is clear that the different configurations are distincts when* $d \geq 5$.

Indeed : If $d = 3$ there are two possible configurations $\mathcal{A}_1^3$ and $\mathcal{A}_2^3$.
For $d = 4$ it is clear that $\mathcal{A}_2^4$ and $\mathcal{A}_3^4$ are confused.
Remark 2. *Let* $\mathrm{A}^d = \{H_1, H_2, ..., H_d\}$ *an* $\mathcal{A}_k^d$*-arrangement,* $k = 1$ *or* 4. *If*

we extract m hyperplanes $H_{i_1}, H_{i_2}, ..., H_{i_m}$ from A^d, then the arrangement $\{H_{i_j}; j = 1, \ldots, m\}$ is also of type $\mathcal{A}_k^m$.
(In other words : a subset of A_k^d, $k = 1$ or 4, is an arrangement of the same type).

Indeed : In an arrangement of type $\mathcal{A}_k^d$, $k = 1$ or 4, there is no distinguished position of a hyperplane relatively to the others (all have symmetrical positions between them).
Proposition 3.1. *(i) The number of points in an $\mathcal{A}_1^d$-arrangement is*

$$N(\mathrm{A}_1^d) = dq^{n-1} + \Pi_{n-2}.$$

(ii) For an arrangement A^d not of the type $\mathcal{A}_1^d$ we have

$$N(\mathrm{A}^d) < dq^{n-1} + \Pi_{n-2}.$$

Démonstration. (i) Let $\mathrm{A}_1^d = \{H_1, \ldots, H_d\}$ such that $\bigcap_{i=1}^d H_i = K$ a linear subspace of codimension 2 then $N(\mathrm{A}_1^d) = \#K + d\#(H_1 \setminus K) = \Pi_{n-2} + dq^{n-1}$.
(ii) We can deduce the result from Serre's letter [8] (Theorem and Remark (2)).

□

3.1 The Minimal Arrangement

Definition 3.2. *Let $\mathrm{A}^d = \{H_1, \ldots, H_d\}$ an arrangement of d hyperplanes in $\mathbb{P}^n(\mathbb{F}_q)$. For a hyperplane H in $\mathbb{P}^n(\mathbb{F}_q)$, distinct from the H_i, we call $\{H_1 \cap H, \ldots, H_d \cap H\}$ the arrangement trace of A^d on H, which will be denote by $tr_H(\mathrm{A}^d)$.*
Proposition 3.3. *Let $\mathrm{A}^d = \{H_1, \ldots, H_d\}$ an arrangement of d hyperplanes in $\mathbb{P}^n(\mathbb{F}_q)$. The following properties are equivalent :*
(i) A^d is an arrangement of type $\mathcal{A}_4^d$.

(ii) For each $1 \leq i \leq d$, the arrangement trace of $\mathrm{A}^d \setminus \{H_i\} = \{H_1, \ldots, H_{i-1}, H_{i+1}, \ldots, H_d\}$ on H_i is an $\mathcal{A}_1^{d-1}$-arrangement in $\mathbb{P}^{n-1}(\mathbb{F}_q)$.

(iii) for each i, j and k distincts we have $H_i \cap H_j \neq H_i \cap H_k$ and all the H_i contain a common linear subvariety of codimension 3.

Démonstration. (i) $\Rightarrow$(iii) : This comes immediately from the definition of $\mathcal{A}_4^d$.

(iii) $\Rightarrow$(ii) : For a fixed $1 \leq i \leq d$, we must have that $tr_{H_i}(\mathrm{A}^d \setminus \{H_i\}) = \{H_1 \cap H_i, \ldots, H_{i-1} \cap H_i, H_{i+1} \cap H_i, \ldots, H_d \cap H_i\}$ is an arrangement of $d-1$ linear subvarieties of codimension 2 meeting in a common linear subvariety of codimension 3. Since for each i, j and k distincts we have $H_i \cap H_j \neq H_i \cap H_k$, then the $d-1$ linear subvarieties $H_i \cap H_j$, for $1 \leq j \leq d$ and $j \neq i$, are distinct and meet in a linear subvariety of codimension 3. Therefore $\{H_1 \cap H_i, \ldots, H_{i-1} \cap H_i, H_{i+1} \cap H_i, \ldots, H_d \cap H_i\}$ is an $\mathcal{A}_1^{d-1}$-arrangement in H_i which is a projective space of dimension $n-1$.

(ii) $\Rightarrow$(i) : Let $\mathrm{A}^d = \{H_1, \ldots, H_d\}$ an arrangement satisfying the property (ii). It is easily seen that all the H_i, $1 \leq i \leq d$ contain a linear subvariety M of codimension 3. It remains to prove that $H_i \cap H_j \neq H_k \cap H_l$ for $(i,j) \neq (k,l)$. For this, it is sufficient to show that $(H_i \cap H_j) \cap (H_k \cap H_l)$ is a subvariety of codimension larger than 2 in $\mathbb{P}^n(\mathbb{F}_q)$.
Writing $(H_i \cap H_j) \cap (H_k \cap H_l) = (H_i \cap H_j) \cap (H_i \cap H_k) \cap (H_i \cap H_l)$, we have from (ii) and Remark (2), that $(H_i \cap H_j), (H_i \cap H_k)$ and $(H_i \cap H_l)$ form an $\mathcal{A}_1^3$-arrangement in H_i, therefore $(H_i \cap H_j) \cap (H_k \cap H_l)$ is a linear subvariety of codimension 2 in H_i, so it is of codimension 3 in $\mathbb{P}^n(\mathbb{F}_q)$. Hence $(H_i \cap H_j) \neq (H_k \cap H_l)$.

□

Theorem 3.4. *(i) The number of points of an arrangement A_4^d of type $\mathcal{A}_4^d$ is*

$$N(\mathrm{A}_4^d) = dq^{n-1} + \Pi_{n-2} - \frac{(d-1)(d-2)}{2} q^{n-2}.$$

(ii) For any hyperplane arrangement A^d, not of the type $\mathcal{A}_4^d$, we have

$$N(\mathrm{A}^d) > N(\mathrm{A}_4^d).$$

Démonstration. (i) The following sum counts every point in a hyperplane arrangement A^d exactly once,

$$N(\mathrm{A}^d) = \#H_1 + \sum_{j=1}^{d-1} [\#H_{j+1} - \# \bigcup_{i=1}^{j} (H_i \cap H_{j+1})]. \tag{1}$$

Let us consider an arrangement $\mathrm{A}_4^d = \{H_1, ..., H_d\}$, the subarrangement $\{H_1, \ldots, H_{j+1}\}$ is an $\mathcal{A}_4^{j+1}$-arrangement (Remark 2). From the proposition 3.3, the trace $\{H_1 \cap H_{j+1}, \ldots, H_j \cap H_{j+1}\}$ of $\{H_1, \ldots, H_j\}$ on H_{j+1} form an $\mathcal{A}_1^j$-arrangement in H_{j+1} which is a projective space of dimension $n-1$. Then we have, from proposition 3.1-(i),

$$\# \bigcup_{i=1}^{j} (H_i \cap H_{j+1}) = \Pi_{n-3} + jq^{n-2},$$

hence, from formula (1) we get

$$\begin{aligned} N(\mathrm{A}_4^d) &= \Pi_{n-1} + \sum_{j=1}^{d-1} [\Pi_{n-1} - (\Pi_{n-3} + jq^{n-2})] \\ &= dq^{n-1} + \Pi_{n-2} - \frac{(d-1)(d-2)}{2} q^{n-2}. \end{aligned}$$

(ii) We will proceed by recurrence on d.
For $d = 3$, let $\mathrm{A}^3 = \{H_1, H_2, H_3\}$ an arrangement of three hyperplanes such that $H_1 \cap H_2 = K$ a linear subspace of codimension 2. There are two possible positions for H_3 relatively to K :

- H_3 contains K, in this case A^3 is an $\mathcal{A}_1^3$-arrangement and $N(\mathrm{A}^3) = 3q^{n-1} + \Pi_{n-2}$,
- H_3 intersects K in a linear subspace L of codimension 3. With a simple calculation one has

$$\begin{aligned} N(\mathrm{A}^3) &= 2q^{n-1} + \Pi_{n-2} + \Pi_{n-1} - (\Pi_{n-3} + 2q^{n-2}) \\ &= 3q^{n-1} + \Pi_{n-2} - q^{n-2}, \end{aligned}$$

what gives $N(\mathrm{A}_4^3)$, and then the result is satisfied for $d = 3$.

Let us suppose now that the result is true for $d-1$ and let us prove it for d. Let $\mathrm{A}^d = \{H_1, \ldots, H_d\}$ a hyperplane arrangement not of the type $\mathcal{A}_4^d$. From the proposition 3.3 there exists at least one $1 \leq i_0 \leq d$, such that the trace of $\{H_1, \ldots, H_{i_0-1}, H_{i_0+1}, \ldots, H_d\}$ on H_{i_0}, $tr_{H_{i_0}}(\mathrm{A}^d \setminus \{H_{i_0}\})$, form an arrangement of $d-1$ hyperplanes in $\mathbb{P}^{n-1}(\mathbb{F}_q)$, not of the type $\mathcal{A}_1^{d-1}$.
So, from proposition 3.1-(ii), we get

$$\# \bigcup_{\substack{i=1 \\ i \neq i_0}}^{d} (H_i \cap H_{i_0}) < (d-1)q^{n-2} + \Pi_{n-3}. \tag{2}$$

The number of points in A^d can be represented as follows :

$$N(\mathrm{A}^d) = \# \bigcup_{\substack{i=1 \\ i \neq i_0}}^{d} H_i + \#H_{i_0} - \# \bigcup_{\substack{i=1 \\ i \neq i_0}}^{d} (H_i \cap H_{i_0}). \tag{3}$$

For $\mathrm{A}^d \setminus \{H_{i_0}\}$ which is an arrangement of $d-1$ hyperplanes, considering (i) and by the recurrence hypothesis, we get

$$N(\mathrm{A}^d \setminus \{H_{i_0}\}) = \# \bigcup_{\substack{i=1 \\ i \neq i_0}}^{d} H_i \geq (d-1)q^{n-1} + \Pi_{n-2} - \frac{(d-2)(d-3)}{2} q^{n-2}. \tag{4}$$

Then, by formulas (2), (3) and (4) one obtains

$$N(\mathrm{A}^d) > (d-1)q^{n-1} + \Pi_{n-2} - \frac{(d-2)(d-3)}{2} q^{n-2} + \Pi_{n-1} - (d-1)q^{n-2} - \Pi_{n-3},$$

so the result

$$N(\mathrm{A}^d) > dq^{n-1} + \Pi_{n-2} - \frac{(d-1)(d-2)}{2} q^{n-2}.$$

□

Considering the last result, from now on, we may denote A^d_{min} an arrangement A^d_4 and by N^ℓ_{min} its number of points, denoted by $N(\mathrm{A}^d_4)$ previously. This notation with the symbol"ℓ" and "min" means that one speaks here about minimal number of zeros of polynomials in $\mathbb{F}_q[X_0, X_1, ..., X_n]^h_d$ wich are product of linear factors, the associated hypersurfaces are unions of hyperplanes giving the type $\mathcal{A}^d_4$ of hyperplane arrangements.

3.2 Particular Arrangements

Lemma 3.5. *Let $\mathrm{A}^m = \{H_1, ..., H_m\}$ be an $\mathcal{A}^m_1$-arrangement in $\mathbb{P}^n(\mathbb{F}_q)$. If H is a hyperplane in $\mathbb{P}^n(\mathbb{F}_q)$ not containing $\bigcap_{i=1}^m H_i$, then $tr_H(\mathrm{A}^m)$ is an $\mathcal{A}^m_1$-arrangement in $\mathbb{P}^{n-1}(\mathbb{F}_q)$, and we have*

$$N(tr_H(\mathrm{A}^m)) = \#\bigcup_{i=1}^m (H_i \cap H) = \Pi_{n-3} + mq^{n-2}.$$

Démonstration. In $\mathbb{P}^n(\mathbb{F}_q)$, if H is a hyperplane and E is a subspace of dimension $t > 0$, then $E \cap H$ has dimension t or $t-1$.
The linear subvariety $\bigcap_{i=1}^m H_i = K$ is of codimension 2 (A^m is an $\mathcal{A}^m_1$-arrangement).
As H does not contain K, the $H_i \cap H$ are m distinct linear subvarieties of codimension 2 meeting in a linear subspaces, $H \cap K$, of codimension 3.
Therefore $tr_H(\mathrm{A}^m) = \{H_1 \cap H, \ldots, H_m \cap H\}$ form an $\mathcal{A}^m_1$-arrangement in H which is a projective space of dimension $n-1$. It follows from proposition 3.1 that

$$N(tr_H(\mathrm{A}^m)) = \Pi_{n-3} + mq^{n-2}.$$

□

Definition 3.6. *Let $\mathrm{A}^d_{[r]} = \{H_1, \ldots, H_d\}$ a hyperplane arrangement such that : r hyperplanes $H_1, H_2, ..., H_r$ meet in a common linear subspace K of codimension 2, (i.e. $\{H_1, \ldots, H_r\}$ is an $\mathcal{A}^r_1$-arrangement) and no hyperplane among the $d-r$ others contains K.*
Lemma 3.7. *The number of points of an arrangement $\mathrm{A}^d_{[r]}$ is such that*

$$N(\mathrm{A}^d_{[r]}) \leq dq^{n-1} + \Pi_{n-2} - (d-r)(r-1)q^{n-2}. \tag{5}$$

Démonstration. Let us write the number of points of an arrangement $\mathrm{A}^d_{[r]}$ in the following way

$$N(\mathrm{A}^d_{[r]}) = \#\bigcup_{i=1}^{r} H_i + \sum_{j=r+1}^{d} [\#H_j - \#\bigcup_{i=1}^{j-1}(H_i \cap H_j)].$$

Therefore

$$N(\mathrm{A}^d_{[r]}) \leq \#\bigcup_{i=1}^{r} H_i + \sum_{j=r+1}^{d} [\#H_j - \#\bigcup_{i=1}^{r}(H_i \cap H_j)]. \tag{6}$$

the arrangement $\{H_1, \ldots, H_r\}$ is of type $\mathcal{A}^r_1$, from proposition 3.1 we get

$$\#\bigcup_{i=1}^{r} H_i = rq^{n-1} + \Pi_{n-2},$$

from lemma 3.5 we have

$$\#\bigcup_{i=1}^{r}(H_i \cap H_j) = \Pi_{n-3} + rq^{n-2};$$

thus, the formula (6) give

$$N(\mathrm{A}^d_{[r]}) \leq rq^{n-1} + \Pi_{n-2} + \sum_{j=r+1}^{d} [\Pi_{n-1} - (\Pi_{n-3} + rq^{n-2})],$$

hence

$$N(\mathrm{A}^d_{[r]}) \leq dq^{n-1} + \Pi_{n-2} - (d-r)(r-1)q^{n-2}.$$

□

Definition 3.8. *Let* $\mathrm{A}^d_{(r,d-r)}$, $2 \leq r \leq d-2$, *an arrangement of* d *hyperplanes such that :*
r *hyperplanes* $H_1, H_2, ..., H_r$ *meet in a common linear subspace* K *of codimension* 2;
$d-r$ *hyperplanes* $H_{r+1}, H_{r+2}, ..., H_d$ *meet in a common linear subspace* K' *of codimension* 2 *with* $K' \neq K$.

The following proposition (case (a)) give a set of arrangements reaching the bound of (5) in the last lemma 3.7.
Proposition 3.9. *Let us consider the arrangement* $\mathrm{A}^d_{(r,d-r)}$ *defined as above.*

(a) If K' is contained in one H_i, $1 \leq i \leq r$, then

$$N(\mathrm{A}^d_{(r,d-r)}) = dq^{n-1} + \Pi_{n-2} - (d-r)(r-1)q^{n-2}.$$

(b) Let us suppose that K (resp. K') is not contained in any H_j, $r+1 \leq j \leq d$ (resp. H_i, $1 \leq i \leq r$).

(1) If $K \cap K' = \emptyset$, which is possible for $n \leq 3$, then

$$N(\mathrm{A}^d_{(r,d-r)}) = dq^{n-1} + \Pi_{n-2} - \Big(r(d-r)-1\Big)q^{n-2} + (r-1)(d-r-1)\Pi_{n-3}.$$

(2) If $K \cap K' = N$ a linear subspace of codimension 4, which is possible for $n \geq 4$, then

$$N(\mathrm{A}^d_{(r,d-r)}) = dq^{n-1} + \Pi_{n-2} - \Big(r(d-r)-1\Big)q^{n-2} + (r-1)(d-r-1)q^{n-3}.$$

(3) If $K \cap K^{'} = M$ a linear subspace of codimension 3, then

$$N(\mathrm{A}^d_{(r,d-r)}) = dq^{n-1} + \Pi_{n-2} - \Big(r(d-r)-1\Big)q^{n-2}.$$

Démonstration. We may compute the number of points in $\mathrm{A}^d_{(r,d-r)}$ as follows

$$N(\mathrm{A}^d_{(r,d-r)}) = \#\bigcup_{i=1}^{r} H_i + \#\bigcup_{j=r+1}^{d} H_j - \#[(\bigcup_{i=1}^{r} H_i) \cap (\bigcup_{j=r+1}^{d} H_j)]. \tag{7}$$

As $\{H_1, \ldots, H_r\}$ is an $\mathcal{A}^r_1$-arrangement, we have

$$\#\bigcup_{i=1}^{r} H_i = rq^{n-1} + \Pi_{n-2} \tag{8}$$

which is the same case for the arrangement $\{H_{r+1}, \ldots, H_d\}$, so

$$\#\bigcup_{j=r+1}^{d} H_j = (d-r)q^{n-1} + \Pi_{n-2}. \tag{9}$$

In the different situations we will compute

$$\chi = \#\Big[(\bigcup_{i=1}^{r} H_i) \cap (\bigcup_{j=r+1}^{d} H_j)\Big], \tag{10}$$

which may be written as

$$\chi = \#\Big[H_r \cap (\bigcup_{j=r+1}^{d} H_j)\Big] + \sum_{i=1}^{r-1} \#\Big[(H_i \setminus K) \cap (\bigcup_{j=r+1}^{d} H_j)\Big].$$

For $1 \leq i \leq r-1$, it is clear that

$$\#\Big[(H_i \setminus K) \cap (\bigcup_{j=r+1}^{d} H_j)\Big] = \#\Big[H_i \cap (\bigcup_{j=r+1}^{d} H_j)\Big] - \#\Big[K \cap (\bigcup_{j=r+1}^{d} H_j)\Big],$$

so

$$\chi = \#\Big[H_r \cap (\bigcup_{j=r+1}^{d} H_j)\Big] + \sum_{i=1}^{r-1} \Big[\#\Big(H_i \cap (\bigcup_{j=r+1}^{d} H_j)\Big) - \#\Big(K \cap (\bigcup_{j=r+1}^{d} H_j)\Big)\Big]. \tag{11}$$

By lemma 3.5, for all hyperplane H_i not containing K', we have

$$\#\Big[H_i \cap (\bigcup_{j=r+1}^{d} H_j)\Big] = \#\bigcup_{j=r+1}^{d} (H_j \cap H_i) = \Pi_{n-3} + (d-r)q^{n-2}. \tag{12}$$

(a) We may suppose that K' is contained in H_r. In this case $K \cap K' = L$ a linear subspace of codimension 3 because $K \neq K'$ and $(K \cup K') \subset H_r$.

Then

$$\#[H_r \cap (\bigcup_{j=r+1}^{d} H_j)] = \#K' = \Pi_{n-2}, \tag{13}$$

and

$$\#[K \cap (\bigcup_{j=r+1}^{d} H_j)] = \#(K \cap K') = \#L = \Pi_{n-3}. \tag{14}$$

Combining (12) which is valid for $1 \leq i \leq r-1$, (13) and (14), from (11) we get

$$\chi = \Pi_{n-2} + (r-1)(d-r)q^{n-2}. \tag{15}$$

Therefore, from equations (7), (8), (9), (10) and (15) we get

$$N(\mathrm{A}^d_{(r,d-r)}) = dq^{n-1} + \Pi_{n-2} - (d-r)(r-1)q^{n-2}.$$

(b) Since no H_i contains K', then the equation (12) is valid for $1 \leq i \leq r$. To calculate χ, it remains to calculate $\#[K \cap (\bigcup_{j=r+1}^{d} H_j)]$.

(1) $K \cap K^{'} = \emptyset$. Since no H_j contains K, for $r+1 \leq j \leq d$, we have

$$\#(H_j \cap K) = \Pi_{n-3},$$

in addition $H_{j_1} \cap K \cap H_{j_2} \cap K = K' \cap K = \emptyset$, for $r+1 \leq j_1, j_2 \leq d$, $j_1 \neq j_2$, from where

$$\#[K \cap (\bigcup_{j=r+1}^{d} H_j)] = (d-r)\#(K \cap H_d),$$

then

$$\#[K \cap (\bigcup_{j=r+1}^{d} H_j)] = (d-r)\Pi_{n-3}. \tag{16}$$

Using (12) and (16), from (11) we get

$$\chi = \Pi_{n-3} + (d-r)q^{n-2} + \sum_{i=1}^{r-1}[\Pi_{n-3} + (d-r)q^{n-2} - (d-r)\Pi_{n-3}],$$

so

$$\chi = \Pi_{n-2} + \Big(r(d-r)-1\Big)q^{n-2} - (r-1)(d-r-1)\Pi_{n-3}. \tag{17}$$

Therefore, from equations (7), (8), (9), (10) and (17) we get

$$N(\mathrm{A}^d_{(r,d-r)}) = dq^{n-1} + \Pi_{n-2} - \Big(r(d-r)-1\Big)q^{n-2} + (r-1)(d-r-1)\Pi_{n-3}.$$

(2) $K \cap K^{'} = N$ a linear subspace of codimension 4. Since no H_j contains K, for $r+1 \leq j \leq d$, we have

$$\#(H_j \cap K) = \Pi_{n-3},$$

so

$$\#[(H_j \setminus K') \cap K] = q^{n-3},$$

from where

$$\#[K \cap (\bigcup_{j=r+1}^{d} H_j)] = \#(K \cap K^{'}) + (d-r)\#[K \cap (H_d \setminus K')],$$

then

$$\#[K \cap (\bigcup_{j=r+1}^{d} H_j)] = \Pi_{n-4} + (d-r)q^{n-3}. \tag{18}$$

Using (12) and (18), from (11) we get

$$\chi = \Pi_{n-3} + (d-r)q^{n-2} + \sum_{i=1}^{r-1}[\Pi_{n-3} + (d-r)q^{n-2} - \Big(\Pi_{n-4} + (d-r)q^{n-3}\Big)],$$

so

$$\chi = \Pi_{n-2} + \Big(r(d-r)-1\Big)q^{n-2} - (r-1)(d-r-1)q^{n-3}. \tag{19}$$

Therefore, from equations (7), (8), (9), (10) and (19) we get

$$N(\mathrm{A}^d_{(r,d-r)}) = dq^{n-1} + \Pi_{n-2} - \Big(r(d-r)-1\Big)q^{n-2} + (r-1)(d-r-1)q^{n-3}.$$

(3) For $r+1 \leq j \leq d$, no H_j contains K so $H_j \cap K$ is of codimension 3, and $H_j \cap K$ contains $K \cap K^{'}$ which is a linear subspace of codimension 3, then $H_j \cap K = K \cap K^{'}$ and so $K \cap (H_j \setminus K') = \emptyset$, for $r+1 \leq j \leq d$. Thus

$$\#[K \cap (\bigcup_{j=r+1}^{d} H_j)] = \#(K \cap K') = \Pi_{n-3}. \tag{20}$$

From equations (12) and (20), applying (11) we have

$$\chi = \Pi_{n-3} + (d-r)q^{n-2} + \sum_{i=1}^{r-1}(d-r)q^{n-2},$$

so

$$\chi = \Pi_{n-3} + r(d-r)q^{n-2}. \tag{21}$$

Therefore, from equations (7), (8), (9), (10) and (21) we get

$$N(\mathrm{A}^d_{(r,d-r)}) = dq^{n-1} + \Pi_{n-2} - \Big(r(d-r)-1\Big)q^{n-2}.$$

□

Remark 3. *The reader can check easily that largest value of* $N(\mathrm{A}^d_{(r,d-r)})$ *is given by the case (a) of the above proposition.*

3.3 Maximal arrangements

We are able now to specify the three configurations of hyperplanes giving the three first numbers of points. In particular for $1 \leq i \leq 3$, the number of points

$N(\mathrm{A}_i^d)$ we write it briefly N_i^ℓ. What will be justified by the following theorem, and this will be in conformity with the notation N_i of the second section. The letter "ℓ" in this new notation means that one speaks here about maximal numbers of zeros of polynomials in $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ wich are product of linear factors, the associated hypersurfaces are unions of hyperplanes.

Theorem 3.10. *The number of points N_i^ℓ of an arrangement A_i^d of typ $\mathcal{A}_i^d$, $1 \leq i \leq 3$, with $4 < d \leq q$ and $n \geq 2$, is such that :*

(i) $N_1^\ell = dq^{n-1} + \Pi_{n-2}$,
(ii) $N_2^\ell = dq^{n-1} + \Pi_{n-2} - (d-2)q^{n-2}$,
(iii) $N_3^\ell = dq^{n-1} + \Pi_{n-2} - 2(d-3)q^{n-2}$.
(iv) For $d > 7$, we have $N(\mathrm{A}_5^d) < N_3^\ell$.

Démonstration. (i) From the proposition (3.1), an arrangement of type $\mathcal{A}_1^d$ give $dq^{n-1} + \Pi_{n-2}$ points.

(ii) The number of points of an arrangement of type $\mathcal{A}_2^d$ is such that

$$N(\mathrm{A}_2^d) = \#\bigcup_{i=1}^{d-1} H_i + \#H_d - \#[H_d \cap (\bigcup_{i=1}^{d-1} H_i)]$$

From lemma 3.5 with $m = d-1$, we have

$$\#[H_d \cap (\bigcup_{i=1}^{d-1} H_i)] = \#\bigcup_{i=1}^{d-1}(H_i \cap H_d) = \Pi_{n-3} + (d-1)q^{n-2}.$$

$\{H_1, \ldots, H_{d-1}\}$ is an $\mathcal{A}_1^{d-1}$-arrangement, so

$$\#\bigcup_{i=1}^{d-1} H_i = (d-1)q^{n-1} + \Pi_{n-2},$$

thus

$$\begin{aligned} N_2^\ell = N(\mathrm{A}_2^d) &= (d-1)q^{n-1} + \Pi_{n-2} + \Pi_{n-1} - \left(\Pi_{n-3} + (d-1)q^{n-2}\right) \\ &= dq^{n-1} + \Pi_{n-2} - (d-2)q^{n-2}. \end{aligned}$$

(iii) An arrangement A_3^d of type $\mathcal{A}_3^d$ coincides with an arrangement $\mathrm{A}_{(r,d-r)}^d$ when $r = d-2$, which is the case (a) of the proposition 3.9. Then

$$N_3^\ell = N(\mathrm{A}_{(d-2,2)}^d) = dq^{n-1} + \Pi_{n-2} - 2(d-3)q^{n-2}.$$

(iv) We remark that, in the case of an $\mathcal{A}_5^d$-arrangement, the maximum number of hyperplanes meeting in common subspace of codimension 2 is $d-2$.

Because if there exists $(d-1)$ hyperplanes meeting in a common linear subspace K of codimension 2, for the d-th hyperplane two cases can appear :
-H_d contains K which gives an $\mathcal{A}_1^d$-arrangement,
-H_d intersects K in a linear subspace of codimension 3, which gives an $\mathcal{A}_2^d$-arrangement.
We will reason with the maximal number of hyperplanes meeting in a common subspace of codimension 2, let r_m be this number. A hyperplane arrangement A^d of the type $\mathcal{A}_5^d$ can there be regarded as an $\mathrm{A}^d_{[r_m]}$ where $2 \leq r_m \leq d-2$.

(a) If $r_m = d-2$ the proposition 3.9 gives the differents cases and prove the result.

(b) If $4 \leq r_m \leq d-3$, starting from formula (5), the variations of the function $\varphi(r) = (d-r)(r-1)$ between 4 and $d-3$ ($d > 7$) prove that

$$N(\mathrm{A}^d_{[r_m]}) \leq N(\mathrm{A}^d_{[d-3]}).$$

With the lemma 3.7 we have

$$N(\mathrm{A}^d_{[d-3]}) \leq dq^{n-1} + \Pi_{n-2} - 3(d-4)q^{n-2},$$

and since $3(d-4) > 2(d-3)$, when $d \geq 7$, we get

$$N(\mathrm{A}^d_{[r_m]}) < N_3^\ell = dq^{n-1} + \Pi_{n-2} - 2(d-3)q^{n-2}.$$

It remains to see the cases $r_m = 3$ and $r_m = 2$. It is clear that the number of points in one $\mathcal{A}^d_{[r_m]}$-arrangement can be written in the form :

$$N(\mathrm{A}^d_{[r_m]}) = \#\bigcup_{i=1}^{4} H_i + \sum_{j=5}^{d}[\#H_j - \#\left(H_j \cap (\bigcup_{i=1}^{j-1} H_i)\right)],$$

hence

$$N(\mathrm{A}^d_{[r_m]}) \leq \#\bigcup_{i=1}^{4} H_i + \sum_{j=5}^{d}[\#H_j - \#\left(H_j \cap (\bigcup_{i=1}^{4} H_i)\right)]. \tag{22}$$

(c) If $r_m = 3$, the arrangement considered is of type $\mathcal{A}^d_{[3]}$. In fact with the lemma 3.7 we know that,

$$N(\mathrm{A}^d_{[3]}) \leq dq^{n-1} + \Pi_{n-2} - 2(d-3)q^{n-2}.$$

For $d > 7$, we will prove the strict inequality. Let H_1, H_2 and H_3 such that $\bigcap_{i=1}^3 H_i = K$ a linear subspace of codimension 2 (i.e. $\{H_1, H_2, H_3\}$ is an $\mathcal{A}_1^3$-arrangement), then $\{H_1, ..., H_4\}$ is an $\mathcal{A}_2^d$-arrangement,
from (ii) with $d = 4$ we have

$$\#\bigcup_{i=1}^{4} H_i = 4q^{n-1} + \Pi_{n-2} - 2q^{n-2}. \tag{23}$$

Let $K_i = H_4 \cap H_i,\ 1 \leq i \leq 3$, and $H_4 \cap (\bigcap_{i=1}^{3} H_i) = H_4 \cap K = M$ a linear subspace of codimension 3. So $H_4 \cap (\bigcup_{i=1}^{3} H_i) = \bigcup_{i=1}^{3}(H_i \cap H_4) = \bigcup_{i=1}^{3} K_i$, where the K_i are linear subspaces of codimension 2 with a common linear subspace M $(=\bigcap_{i=1}^{3} K_i)$ of codimension 3.

The number of points in the trace of $\{H_1, H_2, H_3)$ on H_4 is given by lemma (3.5) :

$$\#\bigcup_{i=1}^{3}(H_i \cap H_4) = \#(H_4 \cap \bigcup_{i=1}^{3} H_i) = \Pi_{n-3} + 3q^{n-2},$$

and in the same way

$$\#(H_j \cap \bigcup_{i=1}^{3} H_i) = \Pi_{n-3} + 3q^{n-2}, \text{ for } \ j \geq 5. \tag{24}$$

So, for $j \geq 5$ we have the following inequality

$$\#(H_j \cap \bigcup_{i=1}^{4} H_i) \geq \Pi_{n-3} + 3q^{n-2}.$$

Let us suppose that for some $j \geq 5$, one has

$$\#(H_j \cap \bigcup_{i=1}^{4} H_i) = \Pi_{n-3} + 3q^{n-2}, \tag{25}$$

since $H_j \cap (\bigcup_{i=1}^{4} H_i) = [H_j \cap (\bigcup_{i=1}^{3} H_i)] \cup (H_j \cap H_4)$ and from (24) and (25), we get

$$H_j \cap H_4 \subset H_j \cap (\bigcup_{i=1}^{3} H_i) \subset \bigcup_{i=1}^{3} H_i,$$

so

$$H_j \cap H_4 \subset H_4 \cap (\bigcup_{i=1}^{3} H_i) = \bigcup_{i=1}^{3} K_i.$$

Thus for $j \geq 5$ the $H_j \cap H_4$, $j \geq 5$ are among $\{K_1, K_2, K_3\}$. Since $r_m = 3$, a subspace K_i cannot be contained in more than three hyperplanes of this arrangement $\mathrm{A}^d_{[3]}$. For $i = 1, 2, 3$, K_i is contained in H_i, H_4 and an unique hyperplane H_j, with $j \geq 5$, and one can suppose that to each K_i is associated the hyperplane H_{i+4}. Thus, only three hyperplanes H_j, which can be for example H_5, H_6 and H_7 can contain respectively K_1, K_2, and K_3. Hence for all $j \geq 5$, except at most three hyperplanes verifie the equation (25), for the others we have :

$$\#\Big(H_j \cap (\bigcup_{i=1}^{4} H_i)\Big) > \Pi_{n-3} + 3q^{n-2}. \tag{26}$$

Therefore, from (22), (23), (24) and (26), for $d > 7$ we get

$$N(\mathrm{A}^d_{[3]}) < 4q^{n-1} + \Pi_{n-2} - 2q^{n-2} + \sum_{j=5}^{d}[\Pi_{n-1} - (\Pi_{n-3} + 3q^{n-2})],$$

then

$$N(\mathrm{A}^d_{[3]}) < dq^{n-1} + \Pi_{n-2} - 2(d-3)q^{n-2}.$$

(d) If $r_m = 2$, in this case, the considered arrangement $\mathrm{A}^d_{[2]}$ is an arrangement of d hyperplanes such as there does not exist more than two hyperplanes having the same intersection in a linear subspace of codimension two.
We will use formula (22) :

$$N(\mathrm{A}^d_{[r_m]}) \leq \#\bigcup_{i=1}^{4} H_i + \sum_{j=5}^{d}[\#H_j - \#\left(H_j \cap (\bigcup_{i=1}^{4} H_i)\right)].$$

For the term $\#\bigcup_{i=1}^{4} H_i$, let us apply the lemma 3.7 with $d = 4$ and $r = 2$, one obtains

$$\#\bigcup_{i=1}^{4} H_i \leq 4q^{n-1} + \Pi_{n-2} - 2q^{n-2}. \tag{27}$$

For $j \geq 5$, the trace of $\{H_1, ..., H_4\}$ on H_j form an arrangement of 4 hyperplanes in $\mathbb{P}^{n-1}(\mathbb{F}_q)$. Then from theorem 3.4, we have

$$\#[H_j \cap (\bigcup_{i=1}^{4} H_i)] \geq 4q^{n-2} + \Pi_{n-3} - 3q^{n-3},$$

hence

$$\#[H_j \cap (\bigcup_{i=1}^{4} H_i)] > 3q^{n-2} + \Pi_{n-3}, \text{ because } q > 3. \tag{28}$$

Therefore, from (22), (27) and (28) we obtain

$$N(\mathrm{A}^d_{[2]}) < 4q^{n-1} + \Pi_{n-2} - 2q^{n-2} + \sum_{j=5}^{d}[\Pi_{n-1} - (3q^{n-2} + \Pi_{n-3})],$$

finally

$$N(\mathrm{A}_{[2]}) < dq^{n-1} + \Pi_{n-2} - 2(d-3)q^{n-2}.$$

□

Remark 4. *We derive from the preceding proof that for $d \geq 5$ we have a large inequality*

$$N(\mathrm{A}^d_5) \leq N^\ell_3.$$

Indeed : considering the part (iv) of the above demonstration, we have that an arrangement A_5^d it is considered as an arrangement $\mathrm{A}_{[r_m]}^d$, with $2 \leq r_m \leq d-2$. We treat the case $3 \leq r_m \leq d-2$ (what replaces the cases (a), (b) and (c) together), the study of the variations of the function $\varphi(r) = (d-r)(r-1)$ between 3 and $d-2$ ($d \geq 5$) prove that

$$N(\mathrm{A}_{[r_m]}^d) \leq N(\mathrm{A}_{[d-2]}^d).$$

With the lemma 3.7 we have

$$N(\mathrm{A}_{[d-2]}^d) \leq dq^{n-1} + \Pi_{n-2} - 2(d-3)q^{n-2}.$$

For $r_m = 2$, we conserve the same proof which it done without the condition $d > 7$.
Thus, for $d \geq 5$ we get $N(\mathrm{A}_5^d) \leq N_3^\ell$.

4 General Case Of Homogeneous Polynomials In $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$

In this section we will search if there exists homogeneous polynomials from $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$, not product of linear factors, admitting a number of zeros larger than N_2^ℓ, N_3^ℓ, or N_{min}^ℓ. The result obtained prove, in particular, that the hypersurfaces which are unions of hyperplanes contain more points than the others when $q > \frac{d(d-1)}{2}$.
Lemma 4.1. *Let ϕ a homogeneous polynomial in $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ and S the associated hypersurface, such that its number of points is greater or equal to :*
$\eta_t = dq^{n-1} + \Pi_{n-2} - tq^{n-2}$, where $t \leq q-d$, and S contains a linear subspace E_m of dimension m with $0 \leqslant m \leqslant n-2$, then S contains a linear subspace E_{m+1} of dimension $m+1$ such that $E_{m+1} \supset E_m$.

Démonstration. Let E_m an linear subspace of dimension m in $\mathbb{P}^n(\mathbb{F}_q)$ contained in S. For an linear subspace E_{m+1}, of dimension $m+1$ in $\mathbb{P}^n(\mathbb{F}_q)$, containing E_m, two cases may appear.

1) E_{m+1} is contained in S. In this case $\#(E_{m+1} \cap S) = \Pi_{m+1}$ as the restriction to S of the associated polynomial is identically zero ($\phi_{/S} = 0$) ;

2) $E_{m+1} \setminus E_m$ meets $S \setminus E_m$ in at most $dq^m + \Pi_{m-1} - \Pi_m (= (d-1)q^m)$ points, since $\phi_{/E_{m+1}}$ have at most $dq^m + \Pi_{m-1}$ zeros (Serre [8] and Thas [11]), and E_m is made of zeros of ϕ.

Recall that the number of E_{m+1} in $\mathbb{P}^n(\mathbb{F}_q)$ containing a fixed E_m is :

$$\frac{q^{n-m}-1}{q-1}.$$

We denote with α the number of E_{m+1}, containing E_m, and contained in S. Then the number of points of S is such that :

$$\#S \leqslant (d-1)q^m(\frac{q^{n-m}-1}{q-1}-\alpha)+q^{m+1}\alpha+\Pi_m.$$

With the hypothesis that $\#S \geqslant \eta_t$, we have :

$$(d-1)\frac{q^n-q^m}{q-1}-\alpha(d-1)q^m+q^{m+1}\alpha+\Pi_m \geqslant dq^{n-1}+\Pi_{n-2}-tq^{n-2},$$

which is equivalent to :

$$\alpha \geqslant \frac{\delta_m}{(q-(d-1))(q-1)},$$

where

$$\delta_m = q^{n-m}-(d+t-1)q^{n-1-m}+tq^{n-2-m}+(d-q-1).$$

we write δ_m in the form :

$$\delta_m = q^{n-m-1}(q-(d+t-1))+tq^{n-2-m}+(d-q-1).$$

We remark that, the map $m \longrightarrow \delta_m$ is decreasing in m, therefore $\delta_m \geqslant \delta_{n-2}$, for $0 \leqslant m \leqslant n-2$, and $q \geqslant d+t-1$.

We have

$$\delta_{n-2} = q^2-(d+t)q+t+d-1 = (q-1)(q-(t+d-1)),$$

so,

$$\alpha \geqslant \frac{q-(t+d-1)}{(q-d-1)} > 0, \text{since } q > t+d-1,$$

but α is an integer, hence $\alpha \geqslant 1$.

Therefore S contain a linear subspace E_{m+1} such that $E_{m+1} \supset E_m$. □

Theorem 4.2. *Let f a homogeneous polynomial, not product of linear factors, in $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ with $d \geq 5$.*
(i) If $q \geqslant 2(d-1)$, then

$$\#Z_q(f) < N_2^\ell,$$

and so

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

(ii) If $q \geqslant 3(d-2)$*, then*

$$\#Z_q(f) < N_3^{\ell},$$

and so

$$N_3 = N_3^{\ell}.$$

(iii) If $q > \frac{d(d-1)}{2}$*, then*

$$\#Z_q(f) < N_{min}^{\ell}.$$

Démonstration. Let f a homogeneous polynomial in $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ and S the associated hypersurface, such that its number of points is greater or equal to :
$\eta_t = dq^{n-1} + \Pi_{n-2} - tq^{n-2}$, where $q > t + d - 1$. With the previous lemma we have proved by induction on m that each point P in S (viewed as an linear subspace of dimension $m = 0$) is contained in a hyperplane of $\mathbb{P}^n(\mathbb{F}_q)$ which is contained in S. Consequently S is unions of hyperplanes. So we are in the case of special hypersurfaces which are arrangements of d hyperplanes.
Considering the numbers N_2^{ℓ}, N_3^{ℓ} and N_{min}^{ℓ} in theorems 3.10 and 3.4, this numbers coincide with η_t, respectively, for $t = d-2$, $t = 2(d-3)$ and $t = \frac{(d-1)(d-2)}{2}$. Therefore the results (i), (ii) and (iii) follows. □

Corollary 4.3. *Let* $PRM(q, d, n)$ *the projective Reed-Muller codes with* $q \geq 3(d-2)$ *and* $d \geq 5$.
(I) The first three weights are :

$$\begin{aligned} w_1 &= q^n - (d-1)q^{n-1}, \\ w_2 &= q^n - (d-1)q^{n-1} + (d-2)q^{n-2}, \\ w_3 &= q^n - (d-1)q^{n-1} + 2(d-3)q^{n-2}. \end{aligned}$$

(II) The numbers of codewords of $PRM(q, d, n)$ *reaching the correspondent* i*-th weight* w_i*,* $1 \leqslant i \leqslant 3$*, which are also the numbers* $\#\mathcal{P}_i$ *of homogeneous polynomials in* $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ *reaching the* i*-th highest numbers of zeros* N_i*,* $1 \leqslant i \leqslant 3$*, are :*

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

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

$$(iii)\ when\ d > 7, \#\mathcal{P}_3 = \binom{q}{d-3} \frac{q^2(q-1)^2}{2} \Pi_n \Pi_{n-1} \Pi_{n-2}.$$

Démonstration. (I) The numbers $w_i = \Pi_n - N_i$, $1 \leq i \leq 3$, are deduced from the previous results mentioned in theorems (3.10) and (4.2).
(II)These numbers are obtained by using some combinatorial methods from projective geometry. To find each $\#\mathcal{P}_i$ we compute the number of possible $\mathcal{A}_i^d$-arrangments and we multiply the obtained number by $(q-1)$, because each hyperplane arrangment can be defined by $(q-1)$ different defining polynomials. At the beginning, let us recall that the number $\#G_{r+1}^{n+1}$ of r-dimensional linear subspaces E_r in $\mathbb{P}^n(\mathbb{F}_q)$ (i.e. the number of points of the Grassmannians of order r) is :

$$\#G_{r+1}^{n+1} = \frac{(q^{n+1}-1)(q^n-1)...(q^{n+1-r}-1)}{(q^{r+1}-1)(q^r-1)...(q-1)}.$$

To construct an $\mathcal{A}_i^d$- arrangment, $1 \leqslant i \leqslant 3$, we can proceed the following steps.

(i) For $\mathcal{A}_1^d$: we have $\#G_{n-1}^{n+1} = \frac{(q^{n+1}-1)(q^n-1)}{(q^2-1)(q-1)}$ ways of selecting one subspace K of codimension 2 and $\binom{q+1}{d}$ choices for d distinct hyperplanes which common this subspace.

(ii) For $\mathcal{A}_2^d$, we have :
(1) $\#G_{n-1}^{n+1} = \frac{(q^{n+1}-1)(q^n-1)}{(q^2-1)(q-1)}$ ways of selecting one subspace K of codimension 2,
(2) then $\binom{q+1}{d-1}$ choices for $d-1$ distinct hyperplanes which containing K,
(3) then $\#G_{n-2}^{n-1} = \frac{(q^{n-1}-1)}{(q-1)}$ ways of selecting an subspace M of codimension 3 in K,
(4) and then $(q^2+q+1-(q+1) = q^2)$ choices for the d-th hyperplane, because the number of hyperplanes in $\mathbb{P}^n(\mathbb{F}_q)$ containing the fixed linear subspace M is (q^2+q+1), where $(q+1)$ among them through K.

(iii) For $\mathcal{A}_3^d$, we have :
(1) $\#G_{n-1}^{n+1} = \frac{(q^{n+1}-1)(q^n-1)}{(q^2-1)(q-1)}$ ways of selecting a subspace K_1,
(2) then $\binom{q+1}{d-2}$ choices for $d-2$ distinct hyperplanes containing this subspace K_1,
(3) then $(d-2)$ choices for selecting one hyperplane H_i among them,

(4) then $\#G^n_{n-1} - 1 = (\frac{q^n-1}{q-1} - 1)$ ways of selecting a subspace K_2 (which is distinct from K_1 in H_i,
(5) and then $\binom{q}{2}$ choices for 2 distinct hyperplanes (which are distincts from H_i) containing the subspace K_2.
In each case, with a simple calculation the correspondent numbers $\#\mathcal{P}_i$ follows.

□

Conclusion

We have found the largest numbers of zeros of homogeneous polynomial in $\mathbb{F}_q[X_0, X_1, ..., X_n]^h_d$ reached by homogeneous polynomials which are product of linear factors, the associated hypersurfaces are hyperplane arrangements. According to what precedes, in particular results in the theorem 3.10, theorem 4.2 and the corollary 4.3, for $q > \frac{d(d-1)}{2}$ we distinguish special weights of the projective Reed-Muller codes $PRM(q, d, n)$. The weights w_i of this set, corresponding to codewords c_i, are given only by all the polynomials which are products of linear factors. The total number of corresponding codewords of this set is $(q-1)$ times the number of possible hyperplane arrangements in $\mathbb{P}^n(\mathbb{F}_q)$, because each hyperplane arrangement can be defined by $(q-1)$ defining polynomials :

$$\#\{c_i\} = (q-1)\Pi_n(\Pi_n - 1)...(\Pi_n - d + 1).$$

It is practical to give the total list of this weights for small values of d. For the general case (when d is large enough) we are satisfied here with the first three weights w_1, w_2 and w_3 given by the corollary 4.3 and the last weight of this list, denoted w^ℓ_{min}, which is deduced from the minimal arrangemnt (theorem 3.4) :

$$w^\ell_{min} = \Pi_n - N^\ell_{min} = q^n - (d-1)q^{n-1} + \frac{(d-1)(d-2)}{2}q^{n-2}.$$

Références

[1] Y. Aubry : Reed-Muller codes associated to projective algebraic varieties, "Coding Theory and Algebraic geometry", Proceedings, Luminy 1991, Lecture Notes in Math. **1518** (1992), 4-17.

[2] J.-P. Cherdieu and R. Rolland, On the number of points of some Hypersurfaces in $\mathbb{F}^n_q$, Finite Fields and Their applications, **2** (1996), 214-224.

[3] P. Delsarte, J.M Goethals, and F.J Mac Williams : on generalized Reed-Muller codes and their relatives, Inform. Control **16** (1970).

[4] T. Kasami, S.Lin, and W. Peterson : New Generalizations of the Reed-Muller codes. I. primitive codes, IEEE Trans.Inform. Theory **I T -14**, N¡. 2 (1968)

[5] G. Lachaud : The parametres of projective Reed-Muller codes, Discrete Mathematics **81** (1990), 217-221.

[6] Y. I. Manin and S. Vladut : Linear codes and modular curves, Itogi Nauki Tekhniki 25 (1984) 209-257 J. Soviet Math. **30** (1985) 2611-2643.

[7] A. Sboui : Second Highest Number of Points of Hypersurfaces In $\mathbb{F}_q^n$, Finite Fields and Their applications, article in press, available online 19 december 2005.

[8] J.-P. Serre : Lettre *à* M. Tsfasman du 24 Juillet 1989, in journées Arithmétiques de Luminy 17-21 Juillet 1989, Astérisque **198-199-200** (1991).

[9] A.B. Sørensen : On the number of rational points on codimension-1 algebraic sets in $\mathbb{P}^n(\mathbb{F}_q)$, Discrete Mathematics **135** (1994), 321-334.

[10] A.B. Sørensen : Projective Reed-Muller codes ; IEEE Transactions on Information Theory, Vol **37**, No. 6, November 1991

[11] K. Thas : On the Number of points of Hypersurface In Finite Projective space (after J-P Serre) http :// Cage-rug. ac.be/˜K. Thas / submitted to J. Algebraic Geom.

Chapitre 6

Sur le Nombre de Points Rationnels d'une Courbe Projective Plane sur un Corps Fini

Sur le Nombre de Points Rationnels d'une Courbe Projective Plane sur un Corps Fini

Adnen SBOUI

IML-CNRS, Campus Univ. de Luminy case 907,
13288 Marseille cedex 09 France

Résumé

L'étude du nombre de points sur les hypersurfaces de $\mathbb{P}^n(\mathbb{F}_q)$ dans l'article [5], permet de déduire en particulier que les courbes projectives planes sur $\mathbb{F}_q$ de degré $d < q$ composées entièrement de droites contiennent plus de points que les autres courbes sous une certaine condition entre q et d. On connaît en particulier les trois premiers grands nombres de points rationnels des courbes algébriques sur $\mathbb{P}^2(\mathbb{F}_q)$ qui sont composées de droites seulement, ainsi que le minimum.

On cherche ici à améliorer ces résultats pour la classe des courbes sur $\mathbb{F}_p$, p premier. Dans le cas contraire on donnera quelques exemples de courbes sur $\mathbb{F}_q$ non réunions de composantes linéaires et qui ont des nombres de points plus grands que certains donnés par des courbes qui sont réunions de droites.

1 Introduction

La détermination d'un ensemble de poids des codes de Reed-Muller Généralisés qui sont au dessus de la distance minimale, conduit à établir une certaine hiérarchie sur les nombres de zéros des polynômes définissant ces codes. En particulier, l'étude du nombre de points des courbes planes de degré d sur $\mathbb{F}_q$ permet d'avoir une idée plus claire sur une partie assez large du spectre de poids des codes de Reed-Muller d'ordre d définies sur $\mathbb{P}^2(\mathbb{F}_q)$.

1.1 Notation

– $\mathbb{F}_q$ un corps fini à q éléments (q une puissance d'un nombre premier p).

Email address: sboui@iml.univ-mrs.fr (Adnen SBOUI).

– $\mathbb{P}^n(\mathbb{F}_q)$ l'espace projectif de dimension n sur $\mathbb{F}_q$.

– $\mathcal{C}_{d,q}$: la famille des courbes projectives planes de degré d sur $\mathbb{F}_q$.
– $\mathcal{C}^\ell_{d,q}$: l'ensemble des courbes de $\mathcal{C}_{d,q}$ qui sont composées de d droites distinctes, dites aussi courbes à composantes linéaires.

– Pour une courbe C de $\mathcal{C}_{d,q}$, on note $\#C$ le nombre de points rationnels de C.
– $N_1 = \max\limits_{C\in\mathcal{C}_{d,q}} \#C$;
– $\mathcal{C}_1$: l'ensemble des courbes de $\mathcal{C}_{d,q}$ atteignant le nombre N_1.

– $N_i = \max\limits_{C\in\mathcal{C}_{d,q}\setminus\{\mathcal{C}_1\cup\ldots\cup\mathcal{C}_{i-1}\}} \#C$, pour $i \geq 2$;
– $\mathcal{C}_i$: l'ensemble des courbes de $\mathcal{C}_{d,q}$ atteignant le nombre N_i.

Si on se restreint sur les courbes à composantes linéaires, en remplaçant dans les définitions des nombres N_i précédents $\mathcal{C}_{d,q}$ par $\mathcal{C}^\ell_{d,q}$, on définie de la même façon les nombres analogues N^ℓ_i, $i \geq 1$. Le minimum nombre de points rationnels d'une courbe qui est réunions de d droites distincts, c.à.d le minimum nombre de points pris sur la famille $\mathcal{C}^\ell_{d,q}$, sera noté N^ℓ_{min}.

2 Courbes à composantes linéaires

Considérant en premier lieu la classe des courbes projectives planes de degré d sur un corps fini $\mathbb{F}_q$ qui sont composées de d droites distinctes. Les nombres N^ℓ_1, N^ℓ_2, N^ℓ_3 et N^ℓ_{min} peuvent être obtenus à partir d'un travail récent sur les hypersurfaces sur $\mathbb{P}^n(\mathbb{F}_q)$, voir [5] théorème (3.2, p 12), dont voici le résultat :

Théorème 2.1. *Les trois premiers grands nombres de points N^ℓ_i, $1 \leq i \leq 3$, ainsi que le dernier N^ℓ_{min}, donnés par les courbes à composantes linéaires, i.e. les courbes de l'ensemble $\mathcal{C}^\ell_{d,q}$, sont tels que :*
(i) $N^\ell_1 = dq + 1$;
(ii) $N^\ell_2 = d(q-1) + 3$;
(iii) $N^\ell_3 = d(q-2) + 7$;
(iv) $N^\ell_{min} = dq - \frac{d(d-3)}{2}$.

A partir du travail sur les arrangements d'hyperplans dans [5], on peut déduire aussi les configurations géométriques des courbes atteignants les nombres N^ℓ_i, $1 \leq i \leq 3$ et N^ℓ_{min} :

Corollaire 2.2. *(i) N^ℓ_1 est donné par les courbes de $\mathcal{C}_1$, tels que les d droites sont toutes concourantes en un même point.*

(ii) N_2^ℓ *est donné par les courbes de* $\mathcal{C}_2$ *: tels que, seulement* $d-1$ *droites sont concourantes en un même point.*

(iii) N_3^ℓ *est donné par les courbes de* $\mathcal{C}_3$*, tels que* $d-2$ *droites* $\{\Delta_i, 1 \leq i \leq d-2\}$ *sont concourantes en un même point* P_1 *avec* Δ_{d-2}*,* Δ_{d-1} *et* Δ_d *sont concourantes en un deuxième point* $P_2 \neq P_1$*.*

(iv) N_{min}^ℓ *est donné par les courbes de* $\mathcal{C}_{min}$ *: tels que, aucun trois droites soient concourantes (i.e.* $\Delta_i \cap \Delta_j \neq \Delta_i \cap \Delta_k$ *pour tous* i*,* j *et* k *distincts entre* 1 *et* d*).*

Remarques 1. *(i) Le nombre* N_1^ℓ *qui est le maximum sur l'ensemble des courbes projectives planes à composantes linéaires* $\mathcal{C}_{d,q}^\ell$*, représente aussi le plus grand nombre de points sur l'ensemble entier des courbes projectives planes* $\mathcal{C}_{d,q}$ *:*

$$N_1 = N_1^\ell,$$

ce qui est démontré dans [6] par J.-P. Serre et dans [8] par K. Thas. Ce nombre est atteint par une courbe composée de d droites concourantes en un même point. D'autre part le travail de Sørensen [7] permet aussi de déduire le maximum nombre de points N_1 *pour les courbes de* $\mathcal{C}_{d,q}$ *dans le cas où* $d \leq 2(q-1)$*.*

(ii) Pour le nombre N_2^ℓ*, un travail analogue à été faite dans le cas affine sur les hypersurfaces par Cherdieu et Rolland [1].*

(iii) Il est à remarquer aussi que le nombre N_{min}^ℓ *à été déjà calculé avec une autre méthode par Hirschfeld [3] (Chapitre II Lemma 2.24, p 55).*

Pour les nombres N_2 et N_3 on déduit de [5] (Théorème (4.1, p 17-18)) que ces nombres se confondent avec N_2^ℓ et N_3^ℓ avec les conditions suivantes entre q et d :

Théorème 2.3. *Soient* C *une courbe plane projective, non réunion de* d *facteurs linéaires, (i.e.* $C \in \mathcal{C}_{d,q} \setminus \mathcal{C}_{d,q}^\ell$*) avec* $d > 4$*.*

(i) Si $q \geqslant 2(d-1)$ *(*$d \leq \frac{q}{2}+1$*), alors*

$$\#C < N_2^\ell,$$

et on a

$$N_2 = N_2^\ell.$$

(ii) Si $q \geqslant 3(d-2)$ *(*$d \leq \frac{q}{3}+2$*), alors*

$$\#C < N_3^l,$$

et on a

$$N_3 = N_3^\ell.$$

(iii) Si $q > \frac{d(d-1)}{2}$*, alors*

$$\#C \leq N_{min}^l.$$

Le but de ce travail est d'améliorer ces résultats et de supprimer, si possible, ces conditions entre q et d dans les différents cas, en gardant l'hypothèse du cadre général $d < q$. Dans le cas contraire il s'agit de voir s'il existe des courbes qui ne sont pas réunions complètes de droites et qui peuvent donner des nombres de points supérieurs à N_2^ℓ ou N_3^ℓ ou N_{min}^ℓ. En d'autre termes existe-t-il des courbes de l'ensemble $\mathcal{C}_{d,q} \setminus \mathcal{C}_{d,q}^\ell$ qui peuvent donner des nombres de points intermédiaires entre les N_i^ℓ ?

3 Courbes Particulières avec composante non linéaire et Résultats sur les Coniques et les Cubiques Irréductibles

3.1 Cas d'une courbe C de degré d sur $\mathbb{F}_q$ composée d'une conique $\mathscr{C}$ et de $d-2$ droites concourantes

Soit C une courbe projective plane de degré d sur $\mathbb{F}_q$ composée d'une conique $\mathscr{C}$ (une quadrique irréductible) et de $d-2$ droites concourantes en un même point. Le nombre de points dans une conique sur $\mathbb{F}_q$ est $\#\mathscr{C} = q+1$, voir par exemple [3] (page 156). La détermination du nombre de points de C revient à l'étude de la position de la conique $\mathscr{C}$ relativement aux droites Δ_i, $1 \leq i \leq d-2$, et à leur point de concours ω.

3.1.1 le cas $\omega \in \mathscr{C}$

Dans ce cas on peut facilement calculer le nombre de points sur C :

$$\#C = \begin{cases} (d-1)q - 2d + 6, \text{ ou} \\ (d-1)q - 2d + 7 \end{cases} \tag{1}$$

En effet : parmi les $q+1$ droites de $\mathbb{P}^2(\mathbb{F}_q)$ passant par ω il y à une droite δ_0 qui est tangente, les autres droites recoupent la conique en un autre point. Si on choisit les $d-2$ droites passant par ω distinctes de δ_0, le nombre de points sur C est : $\#C = \#\bigcup_{i=1}^{d-2} \Delta_i + \#\mathscr{C} - \#[\mathscr{C} \cap \bigcup_{i=1}^{d-2} \Delta_i] = (d-2)q+1+q+1-2(d-2) = (d-1)q - 2d + 6$. dans le cas où l'une des Δ_i, $1 \leq i \leq d-2$, coïncide avec δ_0 un calcul analogue donne $\#C = (d-1)q - 2d + 7$.

3.1.2 le cas $\omega \notin \mathscr{C}$

Dans ce cas, chercher les courbes qui ont plus de points, revient à voir combien de droites possibles passent par ω et ne rencontrent pas la conique $\mathscr{C}$. En numérotant les points de $\mathscr{C}$, A_i, $1 \leq i \leq q+1$, le cardinal de l'ensemble des

droites ωA_i, $1 \leq i \leq q+1$, comptées avec répétition, est compris entre $\frac{q+1}{2}$ et $q+1$. La borne supérieure est atteinte dans le cas où toutes les droites ωA_i sont tangentes à $\mathscr{C}$ et la borne inférieure est atteinte lorsque chaque droite ωA_i coupe $\mathscr{C}$ en deux points. Autrement dit, le nombre η de droites issues du point ω et coupant $\mathscr{C}$ est tels que : $\frac{q+1}{2} \leq \eta \leq q+1$. Ce ci nous permet de déduire une borne sur le nombre de droites issues de ω et n'ayant pas d'intersection avec $\mathscr{C}$:
Remarque 1. *Soient $\mathscr{C}$ une conique et ω un point n'appartenant pas à $\mathscr{C}$.*
Le nombre $\bar{\eta}$ de droites issues du point ω et ne coupant pas $\mathscr{C}$ est tels que :

$$\bar{\eta} \leq \frac{q+1}{2}.$$

Pour plus de précision on va étudier les cas q pair et q impair séparément :

3.1.2.1 Cas d'un Corps de Caractéristique 2 La donnée d'une conique $\mathscr{C}$ sur le plan projective $\mathbb{P}^2(\mathbb{F}_q)$, q pair, induit l'existence d'un point particulier qui est le point de concours des $q+1$ tangentes à $\mathscr{C}$, noté Ω appelé souvent le noyau de $\mathscr{C}$ voir [3] (corollary 7.11, page 157). Comme le faisceau de base Ω des $q+1$ tangentes à $\mathscr{C}$ (c.-à-d. les $q+1$ tangentes concourantes en Ω) couvre entièrement le plan, il y a deux cas pour le nombre de droites issues de ω et tangentes à $\mathscr{C}$:

Propriété 1. *(i) Si $\omega = \Omega$, il y a exactement $q+1$ droites issues de ω et tangentes à $\mathscr{C}$ qui sont les droites ωA_i citées si dessus sans répétition dans ce cas. Donc les $q+1$ droites passant par ω coupent la conique $\mathscr{C}$, d'où $\underline{\bar{\eta} = 0}$.*
(ii) Si $\omega \neq \Omega$, c.à.d. ω appartient à une des $q+1$ tangente et une seule, donc il y a exactement une seule tangente issue de ω à $\mathscr{C}$. Dans ce cas une seulement des droites ωA_i est comptée une seule fois (coupe $\mathscr{C}$ en un point), soit ωA_1, les autres droites ωA_i, $2 \leq i \leq q+1$ coupent $\mathscr{C}$ en deux points et comme ça seront comptées deux fois dans cette liste, d'où $\underline{\bar{\eta} = \frac{q}{2}}$.

3.1.2.2 Cas d'un Corps de Caractéristique $p \neq 2$ On sait que sur un corps de caractéristique différent de 2, l'ensemble des droites tangentes à une conique $\mathscr{C}$ forment une conique dans l'espace dual ; voir [4] (Théorème 53 page 136). Ceci permet de dire que par un point n'appartenant pas à $\mathscr{C}$ on peut mener au plus deux tangentes à $\mathscr{C}$. Par suite les tangentes à $\mathscr{C}$ forment un arrangement de $q+1$ droites ayant une configuration géométrique de type $\mathcal{C}_{min}$ suivant la notation dans le Corollaire 2.2. D'après le théorème 2.1 (iv),

le nombre de points dans la réunions de ces droites T_i tangentes à $\mathscr{C}$, est :

$$\#\bigcup_{i=1}^{q+1} T_i = \frac{(q+1)(q+2)}{2}.$$

Fixons une tangente T_{i_0}, les q autres tangentes T_i, $1 \leq i \leq q+1$, $i \neq i_0$, coupent T_{i_0} en q points distincts. Avec ces précisions on tire :

Conséquences :
- (1) Si $\omega \in \bigcup_{i=1}^{q+1} T_i \setminus \mathscr{C}$ (un point sur la réunions des tangentes et non sur $\mathscr{C}$) par ω il passe deux tangentes à $\mathscr{C}$.
- (2) Si $\omega \in \mathbb{P}^2(\mathbb{F}_q) \setminus \bigcup_{i=1}^{q+1} T_i$ on ne peut pas mener de tangente à $\mathscr{C}$ par ω.

Terminologie
- (a) Soit $Ext(\mathscr{C}) = \bigcup_{i=1}^{q+1} T_i \setminus \mathscr{C}$, son nombre de points est : $\#Ext(\mathscr{C}) = \frac{q(q+1)}{2}$.
- (b) Soit $Int(\mathscr{C}) = \mathbb{P}^2(\mathbb{F}_q) \setminus \bigcup_{i=1}^{q+1} T_i$, son nombre de point est : $\#Int(\mathscr{C}) = \frac{q(q-1)}{2}$.

Propriété 2. *Soit ω un point du plan n'appartenant pas à $\mathscr{C}$:*
(i) Si $\omega \in Int(\mathscr{C})$, alors $\eta = \#\{\omega A_i\} = \frac{(q+1)}{2}$, c'est le cas où on ne peut pas mener de tangente de ω à $\mathscr{C}$, par suite $\bar{\eta} = \frac{(q+1)}{2}$
(ii) Si $\omega \in Ext(\mathscr{C})$, alors $\eta = \#\{\omega A_i\} = \frac{(q+3)}{2}$, c'est le cas où on peut mener deux tangentes de ω à $\mathscr{C}$, d'où $\bar{\eta} = \frac{(q-1)}{2}$

Conclusion Pour avoir plus de possibilités de droites passant par ω ne coupant pas $\mathscr{C}$, on a intérêt à minimiser $\eta = \#\{\omega A_i\}$, ce ci revient à placer ω dans le lieu où il y a moins de tangentes qui passent.
Dans le cas q pair il y a $q^2 - 1$ points possibles où on peut mener exactement $\frac{q}{2}$ droites par un point sans couper la conique $\mathscr{C}$ (le cas où $\omega \in \mathbb{P}^2(\mathbb{F}_q) \setminus (\mathscr{C} \cup \{\Omega\})$).
Dans le cas q impair, et comme nous venons de le voir, il y a $\#Int(\mathscr{C}) = \frac{q(q-1)}{2}$ points possibles où on peut mener exactement $\frac{(q+1)}{2}$ droites par un point sans couper la conique $\mathscr{C}$, le cas où $\omega \in Int(\mathscr{C})$, c'est le seul cas où la borne dans la remarque 1 est atteinte.

3.2 Cubiques Irréductibles

Théorème 3.1. *Soit $\mathfrak{C}$ une cubique irréductible projective plane sur $\mathbb{F}_q$:*

(1) Si $\mathfrak{C}$ est non singulière, on a :

$$|\#\mathfrak{C} - (1+q)| \leq 2\sqrt{q}$$

(2) Si $\mathfrak{C}$ est singulière, on a :

$$\#\mathfrak{C} \leq q + 2.$$

Démonstration. le premier cas est donné par le théorème de Hasse-Weil, voir par exemple [3] (corollary 2.29 page 57).
Pour le cas d'une cubique non lisse : notons qu'une cubique non lisse contient un seul point singulier, en effet : s'il y a deux points singuliers, la droite qui passe par ces deux points coupe la cubique en au moins quatre points en comptant les multiplicités, ce qui contredit le fait qu'une droite coupe une cubique irréductible en au plus trois points (en comptant les multiplicités).
Soit alors P le point singulier de $\mathfrak{C}$, on fait pivoter une droite par celui-ci ; puisque ce point est au moins double chaque droite parmi les $q+1$ passant par P recoupe la cubique en un autre point au plus, ainsi le résultat découle. □

Soit C une courbe projective plane de degré d sur $\mathbb{F}_q$ composée d'une cubique $\mathfrak{C}$ irréductible et de $d-3$ droites concourantes. Comme le cas d'une courbe composée de droites et d'une conique, la détermination du nombre de points de C revient à savoir le nombre maximal de droites Δ_i passant par un point ω (non situé sur $\mathfrak{C}$) et qui n'ont pas d'intersection avec $\mathfrak{C}$.

Lemme 3.2. *Soit $\mathfrak{C}$ une cubique irréductible sur $\mathbb{P}^2(\mathbb{F}_q)$ contenant λ points rationnels et soit ω un point n'appartenant pas à $\mathfrak{C}$. Le nombre $\bar{\sigma}$ de droites passant par ω et ne coupant pas $\mathfrak{C}$ est tels que :*

$$\bar{\sigma} \leq q + 1 - \frac{\lambda}{3}.$$

Démonstration. Faisons comme dans le cas de la conique : en numérotant les points de $\mathfrak{C}$, A_i, $1 \leq i \leq \lambda$, le cardinal σ de l'ensemble des droites ωA_i, $1 \leq i \leq \lambda$, est tels que $\sigma \geq \frac{\lambda}{3}$ puisqu'une droite coupe une cubique irréductible en trois points au plus, dans ce cas chacune est comptée au plus trois fois dans la liste. De là on tire la borne supérieur de $\bar{\sigma}$ qui est clairement positive grâce au théorème 3.1. □

4 Courbes sur $\mathbb{F}_p$, p premier

Théorème 4.1 (Carlin et Voloch [2])**.** *Soient C une courbe algébrique plane définie sur $\mathbb{F}_p$ (p premier) de degré $d < p$, où on n'exclut pas qu'elle puisse être réductible. Supposons que C ne contient pas une composante linéaire définie sur $\mathbb{F}_p$. Alors*

$$\#C \leq \frac{d(d+p-1)}{2}.$$

Si $\#C \geq \frac{d(d+p-1)}{2} - (d-1)$, *alors* C *est absolument irréductible.*
Remarques 2. *Reprenons les nombres* N_1^ℓ, N_2^ℓ, N_3^ℓ *et* N_{min}^ℓ *sur un corps* $\mathbb{F}_p$ *et notons* $B_{CV} = \frac{d(d+p-1)}{2}$ *la borne précédente de Carlin et Voloch. Un calcul simple montre que :*
(i) pour $d < p$, $B_{CV} < N_2^\ell = d(p-1) + 3$.
(ii) pour $d < p-2$, $B_{CV} < N_3^\ell = d(p-2) + 7$.
(iii) pour $d < p/2 + 2$, $B_{CV} < N_{min}^\ell = d(p - \frac{d-3}{2})$.

Il reste à étudier le cas des courbes projectives planes de degré d qui contiennent des droites mais qui ne sont pas entièrement composées de d droites distinctes.

Lemme 4.2. *Soit* C *une courbe projective plane de degré* d *sur* $\mathbb{F}_p$ *contenant* k *droites,* $C = \bigcup_{i=1}^k \Delta_i \cup C'$, *avec* C' *une courbe de degré* $d-k$ *ne contenant pas de droite. Alors*

$$\#C \leq \beta(k) = \frac{1}{2}[k^2 + k(p-2d+1) + d(p+d-1)] + 1.$$

Démonstration. On utilise la borne de Serre (spécialisée pour les courbes, i.e. n=2 dans [6]) pour la première composante qui est la réunion de k droites, d'où $\#\bigcup_{i=1}^k \Delta_i \leq kp + 1$. Pour la deuxième composante C', on utilise la borne de Carlin Voloch B_{CV}, $\#C' \leq \frac{(d-k)(d-k+p-1)}{2}$. Et comme $\#C \leq \#\bigcup_{i=1}^k \Delta_i + \#C'$, un calcul simple donne le résultat. □

4.1 Deuxième grand nombre de points : N_2

Dans cette section on va prouver qu'on peut supprimer la condition $d \leq \frac{p}{2} + 1$ dans le théorème 2.3 (i), ce qui permet de conclure que $N_2 = N_2^\ell$ pour $d < p$.

Théorème 4.3. *Soient* C *une courbe plane projective, non réunion complète de* d *droites, avec* $d < p$, *alors*

$$\#C < N_2^\ell,$$

et on a

$$N_2 = N_2^\ell.$$

Démonstration. Considérons C une courbe projective plane de degré d, non réunion complète de d droites.
Si la courbe C ne contenant pas de droite, la remarque 2 (i) donne le résultat. Il nous reste à étudier le cas d'une courbe C contenant k droites, non réunion complète de droites, avec $1 \leq k \leq d-2$. D'après le lemme 4.2 on a : $\#C \leq \beta(k) = \frac{1}{2}[k^2 + k(p-2d+1) + d(p+d-1)] + 1$. On montre ici que le nombre N_2^ℓ

est supérieur à cette borne $\beta(k)$: soit $\varphi(k) = N_2^\ell - \beta(k)$, l'étude des variations de la fonction $\varphi(k) = -\frac{k^2}{2} - \frac{k}{2}(p-2d+1) - \frac{d}{2}(d-p+1) + 2$ entre 1 et $d-2$ prouve que $N_2^\ell > \beta(k)$ pour $d < p$.
En effet : la dérivée de la fonction $\varphi(k)$ s'annule en $k_0 = d - \frac{p+1}{2}$. Si $k_0 > 0$, on a besoin de vérifier que les valeurs de $\varphi(k)$ en 1 et en $d-2$ sont positives. Si $k_0 < 0$, on a besoin seulement de vérifier que $\varphi(d-2) > 0$.
$\varphi(1) = -\frac{d^2}{2} + \frac{d}{2}(p+1) - \frac{p}{2} + 1$, puisque $2 \leq d \leq p-1$, il est facile à vérifier que ce nombre est positif.
$\varphi(d-2) = -\frac{1}{2}(d-2)^2 - \frac{1}{2}(d-2)(p-2d+1) - \frac{d}{2}(d-p+1) + 2 = p - \frac{d}{2} + 1 > 0$.
D'où $\#C < N_2^\ell$ et on conclut que $N_2 = N_2^\ell$.

□

4.2 Troisième grand nombre de points : N_3

Dans cette section on va prouver que $N_3 = N_3^\ell$ pour $d < p-2$.

Théorème 4.4. *Soient C une courbe projective plane de degré d, non réunion complète de d droites avec $d < p-2$, $p > 2$, alors*

$$\#C \leq N_3^\ell,$$

et on a

$$N_3 = N_3^\ell.$$

L'inégalité est stricte, sauf si la courbe C est constituée de $d-2$ droites issues d'un même point et d'une conique et que $d \geq \frac{p+5}{2}$.

Démonstration. Considérant C une courbe projective plane de degré d, non réunion complète de d droites, qui peut être irréductible.
(A) Si la courbe C ne contient pas de droites, la remarque 2 (ii) donne le résultat.
(B) Cas d'une courbe C contenant k droites, $1 \leq k \leq d-2$.

(1) Le cas $1 \leq k \leq d-4$:
D'après le Lemme 4.2 on a : $\#C \leq \beta(k) = \frac{1}{2}[k^2 + k(p-2d+1) + d(p+d-1)] + 1$. Soit $\psi(k) = N_3^\ell - \beta(k)$, l'étude des variations de la fonction $\psi(k) = -\frac{k^2}{2} - \frac{k}{2}(p-2d+1) - \frac{d}{2}(d-p+3) + 6$ entre 1 et $d-4$, montre que cette fonction prend des valeurs positives, en effet : sa dérivée s'annule en $k_0 = d - \frac{p+1}{2}$. Si $k_0 > 0$, on a besoin de vérifier que les valeurs de $\psi(k)$ en 1 et en $d-4$ sont positives. Si $k_0 < 0$, on a besoin seulement de vérifier que $\varphi(d-4) > 0$.
$\psi(1) = -\frac{d^2}{2} + \frac{d}{2}(p-1) - \frac{p}{2} + 5$, qui est positive pour $2 \leq d \leq p-2$.
$\psi(d-4) = -\frac{1}{2}(d-4)^2 - \frac{1}{2}(d-4)(p-2d+1) - \frac{d}{2}(d-p+3) + 6 = 2(p-d) > 0$.

Ce qui prouve que $N_3^\ell > \beta(k)$ pour $1 \leq k \leq d-4$. Dans ce cas N_3^ℓ est supérieur à $\#C$ dés que $d < p-2$.

(2) Cas d'une courbe contenant $k = d-3$ droites et une cubique $\mathfrak{C}$ irréductible :
Si les $d-3$ droites Δ_i ne sont pas concourantes :
le nombre de points de la réunion $\bigcup_{i=1}^{d-3} \Delta_i$ prend au plus la valeur de N_2^ℓ. En remplaçant d par $d-3$ dans N_2^ℓ, on obtient $\#\bigcup_{i=1}^{d-3} \Delta_i \leq (d-3)p - d + 6$ et d'après le théorème 3.1, $\#\mathfrak{C} \leq (1+p) + 2\sqrt{p}$. Donc $\#C \leq (d-2)p - d + 2\sqrt{p} + 7$ qui est inférieur à N_3^ℓ.
Si les $d-3$ droites Δ_i sont concourantes :
Soient λ le nombre de points rationnels de $\mathfrak{C}$ et b le nombre de droites, parmi les $d-3$, qui coupent $\mathfrak{C}$. Le nombre de points de la courbe $C = \bigcup_{i=1}^{d-3} \Delta_i \cup \mathfrak{C}$ vérifie $\#C \leq \#\bigcup_{i=1}^{d-3} \Delta_i + \#\mathfrak{C} - \#[\mathfrak{C} \cap \bigcup_{i=1}^{d-3} \Delta_i]$. Vu que chaque droite parmi l'ensemble des b droites coupant $\mathfrak{C}$ coupe la cubique au moins en un point, on a $\#(\mathfrak{C} \cap \bigcup_{i=1}^{d-3} \Delta_i) \geq b$. D'où $\#C \leq (d-3)p + 1 + \lambda - b$. D'après le lemme 3.2, le nombre de droites parmi les $d-3$ ne coupant pas $\mathfrak{C}$ vérifie $d-3-b \leq p+1-\frac{\lambda}{3}$, par suite $\#C \leq (d-2)p - d + 5 + \frac{2\lambda}{3}$. D'après le théorème 3.1 on a $\lambda \leq p+1+2\sqrt{p}$, d'où $\#C \leq dp - \frac{4}{3}\sqrt{p}(\sqrt{p}-1) - d + 6$. Cette borne est inférieure à N_3^ℓ, on déduit dans ce cas que $\#C < N_3^\ell$ dés que $d < p$.

(3) Cas d'une courbe contenant $k = d-2$ droites et une quadrique irréductible (une conique) :

(i) Si les $d-2$ droites Δ_i ne sont pas concourantes en un même point :
le nombre de points de la réunion $\bigcup_{i=1}^{d-2} \Delta_i$ prend au plus la valeur de N_2^ℓ. En remplaçant d par $d-2$ dans N_2^ℓ, on obtient $\#\bigcup_{i=1}^{d-2} \Delta_i \leq (d-2)p - d + 5$ et d'autre part $\#\mathscr{C} = p+1$. On utilise une majoration simple : $\#C \leq \#\bigcup_{i=1}^{d-2} \Delta_i + \#\mathscr{C} = (d-1)p - d + 6$, qui est inférieur à N_3^ℓ dés que $d < p$.

(ii) Si les $d-2$ droites Δ_i sont concourantes en ω, $\{\omega\} = \bigcap_{i=1}^{d-2} \Delta_i$, dans ce cas on majore $\#C$ en tenant compte de l'intersection entre la conique et les $d-2$ droites concourantes. Soit

$$\#C = \#\bigcup_{i=1}^{d-2} \Delta_i + \#\mathscr{C} - \#(\mathscr{C} \cap \bigcup_{i=1}^{d-2} \Delta_i) \qquad (2)$$

1er cas $d < \frac{p+1}{2} + 2$: En utilisant la formule (2), on peut écrire $\#C \leq (d-1)p + 2 - b$, avec b le nombre de droites passant par ω et coupant $\mathscr{C}$. D'après la remarque 1, $d-2-b \leq \frac{p+1}{2}$; alors $\#C \leq (d-1)p + \frac{p+1}{2} - d + 4$ qui est inférieur à N_3^ℓ dés que $d < \frac{p+1}{2} + 2$.

2ème cas $d \geq \frac{p+1}{2} + 2$: On peut déduire de (2) que $\#C = (d-1)p + 2 - 2s - t$, avec s le nombre de droites passant par ω et sécantes avec $\mathscr{C}$ et t le nombre de droites passant par ω et tangentes à $\mathscr{C}$.
p, étant premier supérieur ou égal à 3, donc impair :
dans ce cas, la borne est maximale lorsque le maximum de droites parmi les $d-2$ issues de ω ne coupent pas $\mathscr{C}$. D'après la propriété 2, on distingue deux cas $\omega \in Int(\mathscr{C})$ ou $\omega \in Ext(\mathscr{C})$:
Si $\omega \in Int(\mathscr{C})$, soient $\frac{p+1}{2}$ droites issues de ω ne coupent pas $\mathscr{C}$, dans ce cas il y a pas de tangente issue de ω à $\mathscr{C}$. Chacune des $d - 2 - \frac{p+1}{2}$ droites restants coupe $\mathscr{C}$ en deux points. Donc $\#C \leq (d-1)p + 2 - 2(d - 2 - \frac{p+1}{2})$ qui est le nombre N_3^ℓ.
Si $\omega \in Ext(\mathscr{C})$, on a $\frac{p-1}{2}$ droites issues de ω ne coupent pas $\mathscr{C}$, et pour que la courbe C contient plus de points encore, on prend parmi les $d - 2 - \frac{p-1}{2}$ droites qui restent deux tangentes afin de minimiser les droites sécantes à $\mathscr{C}$. D'où $\#C \leq (d-1)p + 2 - 2 - 2(d - 2 - \frac{p-1}{2} - 2)$ qui est le nombre N_3^ℓ. Ce qui achève la démonstration.

□

4.3 Exemples de courbes admettant des facteurs non linéaires et ayant un nombre de points égal à N_3^ℓ sur $\mathbb{F}_q$

Dans les étapes de la démonstration du précédent théorème 4.4, on remarque que l'inégalité $\#C \leq N_3^\ell$ est large dans le cas où $d \geq \frac{p+1}{2} + 2$. Donc il est possible dans ce cas qu'il existe des courbes projectives planes sur $\mathbb{F}_q$ composées de $d-2$ droites concourantes et une conique, ayant un nombre de points égal à N_3^ℓ. Cherchons alors un exemple de courbes de ce type contenant N_3^ℓ points rationnels sur $\mathbb{F}_q$ en tenant compte des propriétés donnés dans la partie 3.1.

Soit $C = \bigcup_{i=1}^{d-2} \Delta_i \cup \mathscr{C}$, réunion de $d-2$ droites concourantes en un point ω et une conique $\mathscr{C}$. On s'intéresse au cas $\omega \notin \mathscr{C}$, car si n'est pas le cas, le nombre de points d'une telle courbe est inférieur à N_3^ℓ, voir la formule (1). On distinguera les deux cas q pair et q impair.

(1) Le cas q pair :

Proposition 4.5. *Soit $d \geq \frac{q}{2} + 3$ et soit C une courbe projective plane de degré d sur $\mathbb{F}_q$, $d = \frac{q}{2} + t$ et $3 \leq t \leq \frac{q}{2}$, composée de $d-2$ droites concourantes en un même point ω et une conique $\mathscr{C}$ de noyau distinct de ω. Si $\frac{q}{2}$ de ces droites ne coupent pas $\mathscr{C}$ et s'il y a une droite tangente, alors $\underline{\#C = N_3^\ell}$.*

Démonstration. Dans le cas q pair, pour avoir plus de points rationnels sur une telle courbe C, on doit avoir le maximum nombre possible de droites parmi les $d-2$ ne coupant pas la conique $\mathscr{C}$, ce qui est le cas (ii) du propriété 1 lorsque $\omega \neq \Omega$ qui est le noyau de $\mathscr{C}$. Dans ce cas il y a $\frac{q}{2}$ droites passant par ω ne coupant pas $\mathscr{C}$ et c'est le maximum possible, on a en plus une droite passant par ω tangente à $\mathscr{C}$. Les $t-3, = d-2-(1+\frac{q}{2})$, droites couperont $\mathscr{C}$ en deux points. Le nombre de points rationnels de C est $\#C = \#\bigcup_{i=1}^{d-2}\Delta_i + \#\mathscr{C} - \#[\mathscr{C} \cap \bigcup_{i=1}^{d-2}\Delta_i]$, le calcul donne $\#C = (d-1)q+7-2t$, ce nombre est égal à N_3^ℓ, $\forall\ t \geq 3$ car $2t = 2d-q$. Ceci montre que dans ce cas, quelque soit le nombre t compris entre 3 et $\frac{q}{2}$, on peut atteindre le nombre N_3^ℓ sans le dépasser avec ce type de courbe. □

(2) le cas q impair :

Proposition 4.6. *Soit $d \geq \frac{q+1}{2}+2$ et soit C une courbe projective plane de degré d sur $\mathbb{F}_q$, $d = \frac{q+1}{2}+t$ avec $2 \leq t \leq \frac{q-1}{2}$, composée de $d-2$ droites concourantes en un même point ω et une conique $\mathscr{C}$.*
Plaçons nous dans les deux cas suivants :

(a) $\omega \in Int(\mathscr{C})$: parmi les $d-2$ droites issues de ω, $\frac{q+1}{2}$ ne coupent pas $\mathscr{C}$.

(b) $\omega \in Ext(\mathscr{C})$: parmi les $d-2$ droites issues de ω, $\frac{q-1}{2}$ droites ne coupent pas $\mathscr{C}$ et il y a deux tangentes.
Dans chacun de ces deux cas on a bien $\underline{\#C = N_3^\ell}$.

Démonstration. (a) Si $\omega \in Int(\mathscr{C})$, chaque droite parmi les $t-2$ droites restant, coupe $\mathscr{C}$ en deux points. Le nombre de points rationnels de C est $\#C = \#\bigcup_{i=1}^{d-2}\Delta_i + \#\mathscr{C} - \#[\mathscr{C} \cap \bigcup_{i=1}^{d-2}\Delta_i]$, le calcul donne $\#C = (d-1)q+6-2t$, ce nombre est égal à N_3^ℓ car $2t = 2d-(q+1)$.

(b) Si $\omega \in Ext(\mathscr{C})$, ici on a exactement $\frac{(q-1)}{2}$ droites issues de ω ne coupant pas la conique, et c'est le cas où on peut mener deux tangentes de ω à $\mathscr{C}$. Chaque droite parmi les $t-3$ restant, coupe $\mathscr{C}$ en deux points. Le nombre de points rationnels de C est $\#C = \#\bigcup_{i=1}^{d-2}\Delta_i + \#\mathscr{C} - \#[\mathscr{C} \cap \bigcup_{i=1}^{d-2}\Delta_i]$, le calcul donne $\#C = (d-1)q-2t+6$, or $2t = 2d-(q+1)$, d'où $\#C = N_3^\ell$.

□

Exemple :
Soient $F(x_0,x_1,x_2) = x_0x_1\prod_{i=1}^{d-4}(x_0-\mu_i x_1)(x_2^2-x_0x_1)$ un polynôme de degré d sur $\mathbb{F}_q$, avec q impair et $d = \frac{(q+1)}{2}+3$. Le lieu géométrique des zéros de ce polynôme est la courbe C composée de la conique $\mathscr{C}$ d'équation $x_2^2-x_0x_1$ et de $d-2$ droites, $\Delta : x_0 = 0$, $\Delta' : x_1 = 0$ et $\Delta_i : x_0-\mu_i x_1 = 0$; $1 \leq i \leq d-4$. Ces $d-2$ droites sont concourantes en même point $\omega(0,0,1)$. Une droite tangente à $\mathscr{C}$ en $Y(y_0,y_1,y_2)$ à pour équation $\frac{\partial F}{\partial x_0}y_0 + \frac{\partial F}{\partial x_1}y_1 + \frac{\partial F}{\partial x_2}y_2 = 2x_2y_2 - x_1y_0 - x_0y_1$.

Les tangentes à $\mathscr{C}$ issues de $\omega(0,0,1)$ sont les tangentes en $Y(y_0,y_1,y_2)$ tel que $y_2=0$ et comme $Y\in\mathscr{C}$ on a $y_2^2=y_0y_1\Rightarrow y_0=0$ ou $y_1=0$. Donc on a deux tangentes issues de $\omega(0,0,1)$ à $\mathscr{C}$ en $Y_1(1,0,0)$ et $Y_2(0,1,0)$, ces deux tangentes sont les droites $\Delta: x_0=0$ et $\Delta': x_1=0$. Les $d-4$ droites $\Delta_i: x_0-\mu_i x_1=0$; $1\leq i\leq d-4$, avec les μ_i sont des non-carrées dans $\mathbb{F}_q$, n'ont pas d'intersection avec $\mathscr{C}$ car le système $\begin{cases} x_2^2=x_0x_1, \\ x_0=\mu_i x_1 \end{cases}$ *n'admet pas de solution.*
Alors $\#C=\#\Delta+\#\Delta'+\#\bigcup_{i=1}^{d-4}\Delta_i+\#\mathscr{C}-\#[\mathscr{C}\cap(\bigcup_{i=1}^{d-2}\Delta_i\cup\Delta\cup\Delta')]=(d-1)q$, *qui est égal à* N_3^ℓ *pour* $d=\frac{(q+1)}{2}+3$.
Cet exemple constitue une illustration du deuxième cas de la proposition 4.6.

Conclusion Dans cette dernière partie du travail, on construit des courbes atteignant le nombre N_3^ℓ. Evidemment, ces courbes ont plus de points que N_i^ℓ, pour $i\geq 4$ et que N_{min}^ℓ.
Ce ci lève la question de départ sur l'existence de courbes qui ne sont pas composées entièrement de droites et qui peuvent donner des nombres de points dépassant certains nombres donnés par les courbes composées seulement de droites.

Références

[1] J.-P. Cherdieu and R. Rolland : On the Number of Points of some Hypersurfaces in $\mathbb{F}_q^n$, Finite Fields and Their Applications, **2** (1996), 214-224.

[2] M.-L. Carlin and J.-P. Voloch : Plane Curves with many Points over Finite Fields, Rocky Mountain Journal of Math., 34 (2004), 1255-1259.

[3] J. W. P. Hirschfeld : Projective Geometry over Finite Fields (Second Edition), Oxford University Press Inc., New York 1998.

[4] P. Samuel : Géométrie Projective, Presses Universitaires de France, 1986.

[5] A. Sboui : Special Numbers of Rational Points on Hypersurfaces in the n-dimensional Projective Space over a Finite Field, http ://iml.univ-mrs.fr/editions/preprint2006/preprint2006.html

[6] J.-P. Serre : Lettre à M. Tsfasman du 24 Juillet 1989, in journées Arithmétiques de Luminy 17-21 Juillet 1989, Astérisque **198-199-200** (1991).

[7] A.B. Sørensen : On the number of rational points on codimension-1 algebraic sets in $\mathbb{P}^n(\mathbb{F}_q)$, Discrete Mathematics **135** (1994), 321-334.

[8] K. Thas : Topics in Finite and Algebraic Geometry, 92 pages, Atti Sem. Mat. Fis. Univ. Modena, to appear.

Historique : Exemple d'application

- Codes de Reed-Muller et Mariner 9

Le 19.01.1972, la sonde spatiale MARINER-9 transmettait des photos du Grand canyon de la planète Mars ♂. La très grande qualité de cette photo avait été obtenue en protégeant la transmission contre les erreurs éventuelles au moyen du Code correcteur de Reed-Muller d'ordre 1 et de longueur 32.

- Codage source du problème

Une photo est découpée en petits rectangles chacun d'entre eux étant assimilé à un point muni d'un niveau d'énergie. Il existe en tout 64 niveaux d'énergie, on a donc besoin de 64 messages à transmettre, chacun représenté par une succession de 6 "bits" (symboles 0 et 1). Pour pouvoir corriger les erreurs de transmission on represente chaque message m de 6 bits par une suite plus longue de 32 bits.

FIG. 6.1 – photo de Mars ♂(1972), communiquée par 'Mariner 9' en utilisant les codes de Reed-Muller binaires d'ordre 1

Résumé

Nous étudions dans cette thèse la distribution des poids des codes de Reed-Muller Généralisés dans les deux cas affine et projectif. Nous obtenons de nouveaux résultats sur le spectre de poids de ces codes, en utilisant comme techniques des outils arithmétiques et géométriques sur un corps fini.
La détermination de certains poids, nécessite une étude assez fine sur les arrangements d'hyperplans. De plus, une analyse précise sur le nombre de points rationnels d'une hypersurface quelconque, nous a permis de dégager les principaux résultats.
Nous caractérisons, en particulier, les trois premiers poids ainsi la liste des mots atteignant ces poids. Ensuite, nous étudions les arrangements d'hyperplans tels que le nombre de points rationnels soit minimal. Le poids donné par un arrangement minimal est particulier, c'est le poids maximal donné par la classe des polynômes qui sont produits de facteurs linéaires.
Enfin, nous nous restreignons aux courbes projectives planes pour étendre les résultats en supprimant certaines restrictions sur les paramètres q et d de ces codes.

Mots Clés : Points rationnels, Courbes projectives planes, Arrangements d'hyperplans, Hypersurfaces sur un Corps fini, Polynômes homogènes, Codes de Reed-Muller généralisés, Spectre de poids.

*

*Reconnaissances : Ce travail n'aurait pu être réalisé sans le soutien inestimable et le support matériel du laboratoire IML-CNRS (l'Institut de Mathématiques de Luminy) et L'IFC (l'institut français de coopération en Tunisie). Ma reconnaissance va particulièrement à Mme Chabbi de l'IFC, Aurélia, Eric et Corine du coté de l'IML.

Title : Determination of the spectrum weight of the generalized Reed-Muller Codes

Abstract

In this thesis, we study the weights distribution of the generalized Reed-Muller codes in the affine and the projective case. The main contributions are presented in four papers. Certain new results give answers to some open questions on the spectrum weight of these codes.

The most used techniques return to arithmetic and finite geometry and some methods of projective geometry over a finite fields.

Some results on the weight distribution are given by the determination of the number of points in certain hypersurfaces. The complete characterization of a linear spectrum weight of these codes, requires a fine study on arrangements of hyperplanes.

We characterize, in particular, the first three weights and the list of the words reaching these weights. Then, we study arrangements of hyperplanes such that the number of rational points is minimal. The weight given by a minimal arrangement is particular, it is the maximum weight given by the class of the polynomials which are product of linear factors.

Lastly, we restrict the work made within the general framework of the hypersurfaces on the curves of which the goal is to extend the results by removing certain restrictions and by improving the conditions on the parameters q and d of these codes.

Keywords : Rational points, Projective plane Curve, Hyperplane arrangement, Hypersurface over finite fields, Homogneous polynomial, Generalized Reed-Muller Codes, Spectrum weight.

†

[†] A chaque nouveau savoir je m'aperçois à quel point je suis loin des réalités !
L'obtention du Doctorat n'empêchera pas de conserver un esprit étudiant, ayant toujours besoin d'apprendre.