Université Paris VII -
Denis Diderot

École Doctorale Paris Centre

Thèse de doctorat

Discipline : Mathématiques

présentée par

Elodie Leducq

Autour des codes de Reed-Muller généralisés

---

dirigée par Jean-François Mestre

Soutenue le 02 décembre 2011 devant le jury composé de :

M. Yves Aubry (Université du Sud Toulon-Var)	Examinateur
M. Claude Carlet (Université Paris 8)	Rapporteur
M. Régis De La Bretèche (Université Paris 7)	Examinateur
M. Loïc Mérel (Université Paris 7)	Examinateur
M. Jean-François Mestre (Université Paris 7)	Directeur
M. François Rodier (Université Aix-Marseille II)	Rapporteur

Institut de Mathématiques de Jussieu
175, rue du chevaleret
75 013 Paris

École doctorale Paris centre Case 188
4 place Jussieu
75 252 Paris cedex 05

A mes parents,
A Mathieu.

Remerciements

Si les remerciements peuvent sembler être la partie la plus simple à écrire d'une thèse, ils constituent cependant un exercice délicat. Il n'est pas toujours évident de trouver les mots justes pour remercier toutes les personnes qui ont contribué d'une manière ou d'une autre à l'aboutissement d'une thèse. Je commence donc par m'excuser auprès de ceux que je vais oublier et auprès de ceux qui ne seront pas remerciés à leur juste valeur.

Je tiens d'abord à remercier chaleureusement Jean-François Mestre, mon directeur de thèse, qui au cours de mon année de Master et de ces trois ans de thèse a accepté de partager ses vastes connaissances mathématiques et son expérience de la recherche (la "technique des mots croisés" s'est avérée payante). Il a non seulement guidé mon chemin dans le domaine des codes correcteurs et de la cryptographie, mais j'ai également pu apprécier au cours de ces années sa disponibilité et sa gentillesse. Il a toujours pris le temps de répondre à mes questions, de m'encourager et de me rassurer dans les moments difficiles de cette thèse.

Je suis honorée que Claude Carlet et François Rodier aient accepté de relire cette thèse. Je les remercie pour leur lecture attentive et leurs remarques judicieuses qui m'ont permis d'améliorer ce manuscrit. Je suis aussi très heureuse qu'ils aient accepté de faire partie de mon jury.

Je tiens à remercier Yves Aubry, Loïc Merel et Régis de la Bretèche d'avoir accepté de faire partie de mon jury. Yves Aubry m'a si bien accueillie au CIRM pour l'AGCT 13 en mars 2011, c'est un réel plaisir de le retrouver à ma soutenance.

Je tiens à remercier Anne Canteaut d'avoir pris le temps de répondre si clairement et si rapidement à mes questions pendant la rédaction de ma thèse.

En parallèle de cette thèse, j'ai eu le plaisir d'enseigner. Merci à François Liret et Thierry Joly d'avoir accompagné mes premiers pas dans cette fabuleuse expérience.

L'institut de mathématiques de Jussieu m'a fourni d'excellentes conditions de travail. Merci à toute l'équipe de théorie des nombres de l'Institut de Mathématiques de Jussieu de m'avoir si bien accueillie et en particulier à Marc Hindry pour sa gentillesse. Un grand merci à Pascal Chietinni, Michel Wasse, Alice Dupouy, et Régine Guittard, leur grande compétence, leur disponibilité et leur gentillesse ont facilité ma vie administrative au sein de l'institut.

Je tiens maintenant à remercier mes compagnons de route, les thésards qui sont passés par le plateau 7C (ou le bureau 3D18) de Chevaleret où, à coup de pauses thé et de conversations plus ou moins mathématiques, ils ont su mettre une ambiance si particulière, le tout sous l'oeil bienveillant d'Easy-Door.

Je commencerais donc par les plus anciens qui m'ont initiée aux pauses thé, aidée à dompter la photocopieuse et les clients légers et si bien accueillie dans cette grande équipe

que sont les thésards, sans oublier leur moitié grands chasseurs de mammouths ou constructeurs de citadelles : Jérôme (l'autre irréductible du 7C04, parce que les aventures de Lise, du crédit ou de la voiture sont autant de bonnes excuses quand on n'a pas envie de travailler), Fabien (toujours un plaisir de te voir entre deux exposés), Manu (expert informatique), Cécile (ma première soutenance de thèse en tant que spectatrice, il y a trois ans déjà), les membres du 7C10 où on pouvait toujours trouver du bon chocolat Banafsheh, Benjamin C., Luc et Mirjam et enfin Ismaël S..

Si le déménagement les a envoyés vers de lointains horizons (Jussieu), il m'a aussi permis d'apprendre à connaitre d'autres thésards : Robert (qui partage toujours avec plaisir ses folles aventures), Christophe (un autre fan des aventures de Robert), Victoria (qui apprend doucement à filtrer), Hoël (que j'ai laissé sans bouilloire), Mathieu (qui a le bureau le mieux rangé de Chevaleret), Alex (générateur de blagues), Loulou et Lukas (deux experts en répartition de bureaux), Paloma (qui fait des collections de vaisselle), Ismaël B. (qui s'y connait aussi en physique), Pierre-Guy et Julie (qui m'ont fait gouter le pouding chômeur), Amaury (qui a pris la relève en MM1), Arnaud (parce qu'on retrouve des Ker-Lannais partout), Olivier (organisateur de Bingo), Johan (qu'on entend si souvent rire dans le couloir) et Sarah (parce qu'il faut bien une post-doc). J'ai une pensée particulière pour mon petit frère mathématiques Yvan et pour ceux qui ont partagé un de mes nombreux bureaux et que je n'ai pas encore cité : Bora (7C04), Wen (7C04), Benjamin W. (7C04), Martin Gr. (7B04 et 3D18), Yong (7C06), Martin Ga.(7C06), Jeremy (7C06), Michael (7C06), Renaud (7C06 et 3D18). Merci aussi à Abed, Bertrand, Claire, Clémence, Dragos, François, Julien, Juliette, Lara, Laura, Philippe, Ruchi, Sary, Xin, Yohan... et pardon à ceux que j'oublie.

Comme il y a une vie avant la thèse, je vais maintenant remercier mes amis d'Orsay, Arnault avec qui j'ai partagé toutes ses années mathématiques depuis la licence mais qui m'a lâchement abandonnée pour ces trois dernières années, Christophe sur qui je peux toujours compter, Julien qui n'est jamais le dernier pour trouver un truc drôle (stupide?) à faire, Fabien qui a le meilleur décodeur du monde. Ils m'ont appris à bien surveiller mes chaussures, mes élastiques, mes crayons, mes feuilles, mes sacs, bref tout ce qui peut se mettre suffisamment haut pour que je ne puisse pas l'attraper (je sais, c'est pas très dur). Merci à vous pour tous ces jolis souvenirs.

Merci à mes compagnons d'Agreg : Anne qui sait doser le rhum et qui a un canapé confortable, Maud et Raphaël (et Thomas) qui organisent des soirées post-oraux blancs assez mémorables, Camille qui nous a hébergés quand on revenait à Rennes, Adrien (mathémaçon et boursicocotteur). Merci pour ces soirées jeux, pour m'avoir laissé squatter vos canapés, offert à manger et m'avoir fait découvrir le couleur café.

Enfin Gwen, pour toutes ces heures passées en cours, en vacances, autour d'un bon repas et surtout au téléphone à parler de choses importantes et de choses moins importantes, pour m'avoir écoutée parler de maths auxquelles tu ne comprenais pas toujours tout, évacuer ma frustration et parfois mon trop plein d'enthousiasme, pour être toujours là dans les bons comme dans les mauvais moments, il est difficile d'exprimer ici toute ma gratitude alors je me contenterai juste d'un très grand MERCI.

Il est temps de remercier maintenant ma famille. Merci à ma belle famille Annette, Pierre, François et Simon pour m'avoir si bien accueillie il y a quatre ans déjà.

Un grand merci à mes grands-parents, même si cette thèse ne m'a pas laissé le temps de les voir aussi souvent que je le souhaitais, les vacances à la mer se sont toujours avérées ressourçantes. Merci à mon frère et ma soeur, Hervé pour ces trop rares conversations autour de la table de la cuisine, c'est toujours un véritable plaisir et Amandine parce que

j'adore donner des cours de maths par téléphone et comme il n' y a pas que les maths dans la vie pour toutes ces parties de trains, vous faites tous les deux partie de mon univers non-mathématiques si indispensable à mon équilibre.

Enfin, parce qu'il est temps de conclure, je terminerais par les personnes à qui cette thèse est dédiée. Mes parents d'abord qui, il y a bien longtemps m'ont dit que si je voulais faire un métier que j'aime je devais bien travailler à l'école. Je ne suis pas sûre qu'ils imaginaient que la leçon porterait si bien ses fruits. Ils m'ont cependant permis d'aborder ces longues années d'études le plus sereinement possible. Sans leurs encouragements, leur soutien affectif et matériel je n'aurais sûrement pas pu aller aussi loin. Merci infiniment.

Je terminerai par Mathieu qui a participé à l'élaboration de cette thèse de tellement de manières différentes. Je lui dois d'abord un peu près toutes les virgules de ce manuscrit, merci pour cette relecture attentive. Mais surtout, il a été d'un constant soutien pendant ces trois années, il a su avoir une oreille attentive dans les moments difficiles et il a supporté mon enthousiasme chatouillant dans les bons jours. Mathieu, j'ai été très heureuse de partager avec toi cette grande aventure qu'est la thèse même si elle se termine pour tous les deux maintenant mais je suis encore plus heureuse de partager cette encore plus grande aventure qu'est la vie à deux, celle-ci puisse-t-elle encore durer de très nombreuses années. Merci de tout mon coeur.

Résumé

Résumé

Les codes de Reed-Muller et les fonctions presque parfaitement non linéaires ont particulièrement été étudiés sur le corps fini à deux éléments pour leur utilisation en cryptographie. Dans cette thèse, on généralise un certain nombre des résultats obtenus à la caractéristique impaire.

Dans un premier temps, on rappelle la définition et les propriétés des codes de Reed-Muller généralisés. En particulier, on donne une nouvelle preuve du théorème de Delsarte, Goethals et Mac Williams qui donnent les mots de poids minimal de ces codes. On s'intéresse ensuite au rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1. On en donne un encadrement, ce qui nous permet d'en déduire la valeur exacte pour un nombre pair de variables. De plus, à l'aide du logiciel Magma, on obtient des résultats plus précis sur le corps fini à trois éléments. Enfin, on donne une méthode de décodage des codes de Reed-Muller généralisés.

Dans un deuxième temps, on étudie les fonctions presque parfaitement non linéaires et parfaitement non linéaires. Après avoir rappelé les définitions et les résultats connus, on démontre des conjectures de Dobbertin, Mills, Müller, Pott et Willems sur des familles de fonctions presque parfaitement non linéaires en caractéristique 3 et on donne une nouvelle famille de fonctions presque parfaitement non linéaires en caractéristique cinq. Par la suite, on s'intéresse aux fonctions puissances parfaitement non linéaires sur une infinité d'extensions d'un corps fini. En utilisant des méthodes de Jedlicka, Hernando et McGuire, on démontre que les seuls entiers congrus à 1 modulo un nombre premier p qui sont des nombres exceptionnels sont de la forme $1 + p^l$.

Mots-clefs

Codes de Reed-Muller généralisés, rayon de recouvrement, fonctions presque parfaitement non linéaires, fonctions parfaitement non linéaires, nombres exceptionnels, fonctions sur un corps fini.

Around generalized Reed-Muller codes

Abstract

Reed-Muller codes and almost perfect nonlinear functions have been studied mostly for the field with two elements because of their utilization in cryptography. This thesis generalize some results to odd charactéristic.

In a first time, we recall the definition and properties of generalized Reed-Muller codes. Particularly, we give a new proof of Delsarte, Goethals and Mac Williams' theorem which gives the minimal weight codewords of these codes. Then we study the covering radius of the first order generalized Reed-Muller codes. We find upper and lower bounds which give the value of the covering radius for an even number of variables. Furthermore, with Magma, we manage to get more precise results for the field with three elements. Finally, we give a decoding method for generalized Reed-Muller codes.

In a second time, we are interested in almost perfectly nonlinear functions and perfectly nonlinear functions. We recall definitions and already known results. Then, we prove two conjectures of Dobbertin, Mills, Müller, Pott and Willems about families of almost perfectly nonlinear power mappings in characteristic three and we give a new family of almost perfectly nonlinear power mappings in characteristic five. Finally, we study exceptional numbers in odd characteristic that is to say power mappings which are perfectly nonlinear on an infinity of extensions of a finite field. Using methods from Jedlicka, Hernando and McGuire, we prove that the only exceptional numbers congruent to 1 modulo a prime number p are of the form $1 + p^l$.

Keywords

Generalized Reed-Muller codes, covering radius, almost perfectly nonlinear functions, perfectly nonlinear functions, exceptional numbers, functions over finite fields.

Table des matières

Introduction **15**

Notations **19**

1 Codes de Reed-Muller généralisés **21**

1.1 Rappels sur les codes 21
1.2 Définition et premières propriétés 26
1.2.1 Fonctions de $\mathbb{F}_q^m$ dans $\mathbb{F}_q$ 26
1.2.2 Codes de Reed-Muller 28
1.2.3 Codes de Reed-Muller généralisés 29
1.2.4 Codes de Reed-Muller généralisés et codes cycliques 31
1.3 Distance minimale 34
1.3.1 Distance minimale des codes de Reed-Muller généralisés 35
1.3.2 Mots qui atteignent la distance minimale pour $q = 2$ 36
1.3.3 Mots qui atteignent la distance minimale pour $q \neq 2$ 36
1.3.4 Les codes de Reed-Muller généralisés sur $\mathbb{F}_p$ sont engendrés par les mots de poids minimal 39
1.4 Groupe des automorphismes 41
1.4.1 Preuve du théorème 1.4.1 dans le cas $q = 2$ 41
1.4.2 Preuve du théorème 1.4.1 dans le cas $q \neq 2$ 42

2 Rayon de recouvrement **47**

2.1 Notations 47
2.2 Rappels sur les formes quadratiques en toute caractéristique 47
2.2.1 Définitions 47
2.2.2 Un théorème de réduction 48
2.2.3 Zéros d'une forme quadratique 50
2.3 Rayon de recouvrement des codes de Reed-Muller d'ordre 1 51
2.4 Une borne supérieure pour $\rho(1, m)$ pour les codes de Reed-Muller généralisés 53
2.4.1 Un théorème général 53
2.4.2 Application aux codes de Reed-Muller généralisés 55
2.5 Une borne inférieure pour $\rho(1, m)$ 56
2.5.1 Rayon de recouvrement de $R_q(1, m)$ dans $R_q(2, m)$ 56
2.5.2 Une borne inférieure pour $\rho(1, m)$ 59
2.6 Le cas $q = 3$ 59
2.6.1 Calcul du rayon de recouvrement pour $m = 3$ 59
2.6.2 Mots qui atteignent le rayon de recouvrement 60
2.6.3 Amélioration de la borne inférieure 63

3 Fonctions presque parfaitement non linéaires et parfaitement non linéaires **67**
3.1 Résultats préliminaires . . . 67
3.2 Définitions et premières propriétés . . . 70
3.2.1 Définitions . . . 70
3.2.2 Propriétés . . . 71
3.2.3 Équivalence . . . 72
3.3 Exemples de fonctions presque parfaitement non linéaires et parfaitement non linéaire . . . 74
3.3.1 Fonctions puissances parfaitement non linéaires . . . 74
3.3.2 Fonctions puissances presque parfaitement non linéaires . . . 75
3.3.3 Exemples de fonctions qui ne sont pas des fonctions puissances . . . 82
3.4 Nouvelles familles en caractéristique 3 . . . 85
3.4.1 Deux conjectures de Dobbertin, Mills, Müller, Pott et Willems . . . 85
3.4.2 Une nouvelle famille déduite du théorème 3.3.5 . . . 90
3.5 Nouvelles familles en caractéristique 5 . . . 90
3.5.1 Une conjecture de Dobbertin, Mills, Müller, Pott et Willems . . . 90
3.5.2 Une nouvelle famille . . . 91

4 Nombres exceptionnels **93**
4.1 Préliminaires . . . 93
4.1.1 Un lemme préliminaire . . . 93
4.1.2 Rappels sur les courbes algébriques . . . 94
4.2 Définitions . . . 99
4.2.1 En caractéristique paire . . . 99
4.2.2 En caractéristique impaire . . . 100
4.3 Nombres exceptionnels en caractéristique paire . . . 100
4.4 Les nombres exceptionnels congrus à 1 modulo p en caractéristique impaire 101
4.4.1 Points singuliers et multiplicités . . . 102
4.4.2 Multiplicités d'intersection . . . 106
4.4.3 Preuve du théorème 4.4.1 . . . 110
4.5 Les nombres exceptionnels non congrus à 1 modulo p en caractéristique impaire . . . 114

A Encodage et décodage des codes de Reed-Muller généralisés **117**
A.1 Encodage des codes de Reed-Muller généralisés . . . 117
A.2 Décodage des codes de Reed-Muller . . . 117
A.2.1 Utilisation de la transformée de Hadamard pour les codes de Reed-Muller d'ordre 1 . . . 118
A.2.2 Décodage par vote majoritaire . . . 118
A.3 Décodage des codes de Reed-Muller généralisés . . . 119
A.3.1 Correction d'effacements . . . 119
A.3.2 Correction d'erreurs par vote majoritaire . . . 121
A.4 Complexité . . . 123
A.4.1 Correction d'effacements . . . 123
A.4.2 Corrections d'erreurs par vote majoritaire . . . 123

Bibliographie **125**

Liste des tableaux **131**

Index des notations **132**

Introduction

Les codes de Reed-Muller et les fonctions presque parfaitement non linéaires ont beaucoup été étudiés sur le corps fini à deux éléments pour leur utilisation en cryptographie. Pour présenter une bonne résistance à la cryptanalyse linéaire, une fonction booléenne doit avoir une haute non linéarité, c'est-à-dire être la plus éloignée possible des fonctions affines, au sens de la distance de Hamming. Les fonctions qui atteignent le rayon de recouvrement des codes de Reed-Muller d'ordre 1 sont les fonctions ayant la plus haute non linéarité. Pour cette raison, ce rayon de recouvrement a fait l'objet de nombreuses études. Cependant, on ne dispose que d'un encadrement de ce rayon de recouvrement pour un nombre impair de variables supérieur ou égal à 9. D'autre part, pour résister à la cryptanalyse différentielle, une fonction booléenne doit aussi avoir une faible uniformité, c'est-à-dire qu'il doit y avoir une faible corrélation entre les messages clairs et les messages chiffrés. En caractéristique 2, les fonctions booléennes qui ont la plus faible uniformité sont les fonctions presque parfaitement non linéaires. Dans cette thèse, on généralise un certain nombre de résultats obtenus pour la caractéristique 2 à la caractéristique impaire. On donne notamment un encadrement du rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1. On donne aussi des nouvelles familles de fonctions puissances presque parfaitement non linéaires sur des corps de caractéristique 3 ou 5. Enfin, on utilise des méthodes de Jedlicka, Hernando et McGuire pour déterminer une famille de fonctions puissances parfaitement non linéaires sur une infinité d'extensions d'un corps fini de caractéristique impaire.

Dans le premier chapitre, après avoir rappelé quelques résultats sur les codes de Reed-Muller, on définit les codes de Reed-Muller généralisés de deux manières : une approche à plusieurs variables qui sera celle utilisée dans la grande majorité du manuscrit et une approche en une variable, les codes de Reed-Muller généralisés étant vu comme des codes cycliques étendus. On s'intéresse aussi à la distance minimale de ces codes et plus particulièrement aux mots de code de poids minimal. Plus précisément, on redémontre le théorème suivant de Delsarte, Goethals et MacWilliams [DGM70] en utilisant des arguments de géométrie affine [1] (voir [Led10a]).

Théorème 0.0.1. *Soit $0 \leq r \leq m(q-1)-1$, $r = t(q-1)+s$, $0 \leq s \leq q-2$. Les mots de poids minimal de $R_q(r,m)$ sont les mots de $R_q(r,m)$ dont le support est l'union de $q-s$ sous-espaces affines de $\mathbb{F}_q^m$ parallèles de codimension $t+1$ tous inclus dans un sous-espace affine de codimension t.*

Enfin, on rappelle le groupe des automorphismes des codes de Reed-Muller généralisés.

Dans le deuxième chapitre, on s'intéresse au rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1. Après avoir rappelé les résultats connus pour $q = 2$, on démontre les résultats suivants pour tout q (voir [Led11]).

1. "The authors hasten to point out that it would be very desirable to find a more sophisticated and shorter proof" [DGM70, Appendix]

Théorème 0.0.2. *Pour tout q, $m \geq 1$, le rayon de recouvrement du code de Reed-Muller généralisé d'ordre 1 $R_q(1,m)$ vérifie :*

$$(q-1)q^{m-1} - q^{\lceil \frac{m}{2} \rceil - 1} \leq \rho(1,m) \leq (q-1)q^{m-1} - q^{\frac{m}{2}-1}.$$

Cet encadrement découle d'un théorème plus général sur le rayon de recouvrement des codes et d'un résultat sur le rayon de recouvrement partiel des codes de Reed-Muller généralisés d'ordre 1 :

Théorème 0.0.3. *Soit C un code sur $\mathbb{F}_q$ de longueur n auto-complémentaire et de force 2 alors*

$$\rho(C) \leq \frac{(q-1)}{q}n - \frac{\sqrt{n}}{q}.$$

Théorème 0.0.4. *Pour tout m et tout q, $\rho_2(1,m) = (q-1)q^{m-1} - q^{\lceil \frac{m}{2} \rceil - 1}$.*

La preuve de ce dernier résultat repose sur une étude des zéros des formes quadratiques. Enfin avec l'aide du logiciel Magma, on obtient le résultat suivant pour $q = 3$.

Théorème 0.0.5. *Pour $q = 3$, $\rho(1,3) = 16$.*

On en déduit

Théorème 0.0.6. *Pour $q = 3$ et m un entier impair,*

$$\rho(1,m) \geq (q-1)q^{m-1} - \frac{2}{3}q^{\lceil \frac{m}{2} \rceil - 1}.$$

Dans le chapitre 3, on étudie les fonctions presque parfaitement et parfaitement non linéaires. Après avoir rappelé des résultats connus, on démontre deux conjectures faites dans [DMM+03] qui donnent de nouvelles familles de fonctions presque parfaitement non linéaires en caractéristique 3.

Conjecture 0.0.7. *Pour $e \geq 5$ impair, la fonction $x \mapsto x^d$ est presque parfaitement non linéaire sur $\mathbb{F}_{3^e}$ pour*

$$d = \begin{cases} \frac{3^{\frac{e+1}{2}}-1}{2} & \text{si } e \equiv 3 \mod 4 \\ \frac{3^{\frac{e+1}{2}}-1}{2} + \frac{3^e-1}{2} & \text{si } e \equiv 1 \mod 4 \end{cases}.$$

Conjecture 0.0.8. *Pour $e \geq 5$ impair, la fonction $x \mapsto x^d$ est presque parfaitement non linéaire sur $\mathbb{F}_{3^e}$ pour*

$$d = \begin{cases} \frac{3^{e+1}-1}{8} & \text{si } e \equiv 3 \mod 4 \\ \frac{3^{e+1}-1}{8} + \frac{3^e-1}{2} & \text{si } e \equiv 1 \mod 4 \end{cases}.$$

On donne également une preuve d'une troisième conjecture de [DMM+03] différente de celle donnée par Zha et Wang dans [ZW10].

Conjecture 0.0.9. *Soit e un entier impair. La fonction $x \mapsto x^d$ est presque parfaitement non linéaire sur $\mathbb{F}_{5^e}$ pour*

$$d = \frac{5^e - 1}{4} + \frac{5^{\frac{e+1}{2}} - 1}{2}.$$

Finalement, on donne une nouvelle famille de fonctions presque parfaitement non linéaires en caractéristique 5.

Théorème 0.0.10. *Soit $l \geq 2$ et e un entier tel que $e \equiv -1 \mod 2^l$, alors la fonction $x \mapsto x^d$ est presque parfaitement non linéaire sur $\mathbb{F}_{5^e}$ pour*

$$d = \frac{1}{2}\frac{5^{e+1}-1}{5^{\frac{e+1}{2^l}}+1} + \frac{5^e-1}{4}.$$

On peut trouver tous les nouveaux résultats de ce chapitre dans [Led10b].

Dans le dernier chapitre, on s'intéresse aux fonctions parfaitement non linéaires sur une infinité d'extensions de $\mathbb{F}_p$. Dans [Jed07, HM09], Jedlicka, Hernando et McGuire utilisent le théorème de Bézout pour démontrer que les seules fonctions puissances qui sont presque parfaitement non linéaires sur une infinité d'extensions de $\mathbb{F}_2$ sont celles données par Gold et Kasami. En utilisant les mêmes méthodes, on démontre le résultat suivant (voir [Led10c]) :

Théorème 0.0.11. *Les seuls $d \equiv 1 \mod p$, tels que $x \mapsto x^d$ soit parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_p$ sont de la forme $d = 1 + p^l$.*

Enfin, en annexe, on donne une méthode de décodage des codes de Reed-Muller généralisés.

Notations

Les notations suivantes sont valables pour la totalité du manuscrit.

- p désigne un nombre premier.
- $q = p^e$ désigne une puissance d'un nombre premier.
- $\mathbb{F}_q$ est le corps fini à q éléments.
- $\mathbb{F}_q[x_1, \ldots, x_m]$ est l'anneau des polynômes en m variables à coefficients dans $\mathbb{F}_q$. On note $\deg(f)$ le degré d'un polynôme f de $\mathbb{F}_q[x_1, \ldots, x_m]$.
- Pour m un entier, $\mathrm{GL}_m(\mathbb{F}_q)$ désigne le groupe linéaire de $\mathbb{F}_q^m$ et $\mathrm{GA}_m(\mathbb{F}_q)$ le groupe affine de $\mathbb{F}_q^m$.
- Si A est une partie d'un ensemble E, on note $\#A$ son cardinal et A^c son complémentaire dans E.
- Soit m un entier et f une fonction de $\mathbb{F}_q^m$ dans $\mathbb{F}_q$. On note $\mathrm{Supp}(f)$ le support de f, c'est-à-dire $\{x \in \mathbb{F}_q^m : f(x) \neq 0\}$.
- Soit C un code linéaire de longueur n. Pour tout $c \in C$, on note son poids de Hamming
$$|c| := \#\{1 \leq i \leq n : c_i \neq 0\}.$$
- On note $d(.,.)$ la distance de Hamming.
- Si $n \in \mathbb{N}$, on note $\mathcal{S}_n$ le groupe des permutations de $\{1, \ldots, n\}$.
- Si $x \in \mathbb{R}$, on note $\lfloor x \rfloor$ sa partie entière inférieure et $\lceil x \rceil$ sa partie entière supérieure.
- Si a et b sont deux éléments d'un anneau principal, $\mathrm{pgcd}(a, b)$ désigne leur plus grand diviseur commun.
- Si p est un nombre premier, a un entier, le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut 0 si $a \equiv 0 \mod p$, 1 si a est un carré dans $\mathbb{F}_p$ et -1 si a n'est pas un carré dans $\mathbb{F}_p$.

- On note χ le caractère quadratique sur $\mathbb{F}_q$ défini par :

$$\forall x \in \mathbb{F}_q, \qquad \chi(x) = \begin{cases} 1 & \text{si } x \text{ est un carré dans } \mathbb{F}_q^* \\ -1 & \text{si } x \text{ n'est pas un carré dans } \mathbb{F}_q^* \\ 0 & \text{si } x = 0 \end{cases} .$$

Chapitre 1

Codes de Reed-Muller généralisés

Dans ce chapitre, on donne une généralisation des codes de Reed-Muller définis sur $\mathbb{F}_2$ introduits par Reed en 1954 [Ree54] en étendant la définition à tout corps fini $\mathbb{F}_q$. Cette généralisation a d'abord été introduite par Kasami, Lin et Peterson dans [KLP68] et Weldon dans [Wel68]. Les principales références pour les codes de Reed-Muller généralisés sont [PHB98] et [DGM70].

Dans ce chapitre, m est un entier naturel strictement positif.

1.1 Rappels sur les codes

Avant d'étudier les codes de Reed-Muller généralisés plus en détails, on commence par faire quelques rappels sur les codes en général. Une référence pour cette section est [vL99].

Soit A un ensemble fini non vide, appelé alphabet et n un entier naturel.

Proposition 1.1.1. *L'application de $A^n \times A^n$ dans $\mathbb{N}$ définie par*

$$\forall x,\ y \in A^n,\ d(x,y) = \#\{i : 1 \leq i \leq n, x_i \neq y_i\}$$

est une distance appelée la distance de Hamming.

Définition 1.1.2. Un code de longueur n est un sous-ensemble de A^n.

On s'intéresse à la distance minimale d'un code car elle permet de déterminer sa capacité de correction.

Définition 1.1.3. Soit C un code de longueur n tel que $\#C \geq 2$. La distance minimale de C est

$$d := \min(d(x,y) : x \in C, y \in C, x \neq y)$$

Proposition 1.1.4. *Soit C un code de longueur n et de distance minimale d. Alors*

$$\#C \leq (\#A)^{n-d+1} \text{ (inégalité de Singleton)}$$

et on peut retrouver au moins $d-1$ effacements et corriger au moins $\lceil \frac{d}{2} \rceil - 1$ erreurs.

Démonstration. Soit $i_1, \ldots, i_{d-1} \in \{1, \ldots, n\}$. On considère la projection de A^n sur A^{n-d+1} suivante :

$$\varphi : \begin{array}{ccc} A^n & \to & A^{n-d+1} \\ (x_i)_{i\in\{1,\ldots,n\}} & \mapsto & (x_i)_{i\in\{1,\ldots,n\}\setminus\{i_1,\ldots,i_{d-1}\}} \end{array}$$

Soit x, $y \in C$ tels que $\varphi(x) = \varphi(y)$. Alors $d(x, y) \leq d - 1$. Comme la distance minimale de C est d, nécessairement $x = y$ et φ est injective sur C. D'où $\#C \leq (\#A)^{n-d+1}$ et on peut corriger au moins $d - 1$ effacements.
Soit c_0 un mot du code. Supposons qu'en envoyant c_0, on reçoive $x \in A^n$ tel que

$$d(x, c_0) < \frac{d}{2}.$$

Si c est un mot de code différent de c_0, $d(x, c) \geq d(c, c_0) - d(x, c_0) > d - \frac{d}{2}$. Donc il existe un seul mot de code à distance inférieure à $\frac{d}{2}$ de x, c'est le mot de code envoyé. □

Groupe des automorphismes

On trouve la proposition suivante dans [BON84].

Proposition 1.1.5. *Les isométries de l'espace métrique (A^n, d) sont de la forme :*

$$\phi_{\Pi,\sigma} : \begin{array}{ccc} A^n & \to & A^n \\ (a_i) & \mapsto & (\pi_i(a_{\sigma^{-1}(i)})) \end{array}$$

où $\sigma \in \mathcal{S}_n$ et $\Pi = (\pi_1, \ldots, \pi_n)$ est une famille de permutations de A.

Démonstration. On commence par remarquer que les applications décrites ci-dessus sont bien des isométries.
Pour tout $i \in \{1, \ldots, n\}$, $a \in A$ et $x \in A^n$, on note $\Lambda_{a,i}(x)$ l'élément de A^n obtenu en remplaçant la $i$ème coordonnée de x par a.
Soit f une isométrie de (A^n, d) et $x_0 \in A^n$. Pour tout $i \in \{1, \ldots, n\}$ et $a \in A \setminus \{x_{0,i}\}$, $f(\Lambda_{a,i}(x_0))$ est à distance 1 de $f(x_0)$ puisque f est une isométrie. Il existe donc un unique $(b, j) \in A \times \{1, \ldots, n\}$ tel que $f(\Lambda_{a,i}(x_0)) = \Lambda_{b,j}(f(x_0))$ avec $b \neq f(x_0)_j$. Soit $a' \in A \setminus \{x_{0,i}\}$, $a' \neq a$ et (b', j') l'unique couple tel que $f(\Lambda_{a',i}(x_0)) = \Lambda_{b',j'}(f(x_0))$. Si $j \neq j'$ alors $d(f(\Lambda_{a',i}(x_0)), f(\Lambda_{a,i}(x_0))) = 2$ ce qui est absurde puisque f est une isométrie. Donc pour chaque i et quelque soit a, il correspond un unique j. On pose $j = \sigma(i)$, $\pi_j(a) = b$ et $\pi_j(x_{0,i}) = f(x_0)_j$. Comme f est une isométrie, chaque π_j est une permutation. On pose alors $g = \phi_{\Pi,\sigma}^{-1} \circ f$. Par construction, x_0 et tous les éléments de A^n à distance 1 de x_0 sont fixés par g. Soit $i \geq 2$. Supposons que pour tout $x \in A^n$ tel que $d(x_0, x) < i$, $g(x) = x$. Soit $x \in A^n$ tel que $d(x, x_0) = i$. Supposons, quitte à modifier l'ordre des coordonnées, que $x_1 \neq x_{0,1}$ et $x_2 \neq x_{0,2}$. On considère $y = (x_{0,1}, x_2, \ldots, x_n)$, $z = (x_1, x_{0,2}, x_3, \ldots, x_n)$ et $w = (x_{0,1}, x_{0,2}, x_3, \ldots, x_n)$. Alors $d(x_0, y) < i$, $d(x_0, z) < i$ et $d(x_0, w) < i$. D'où par hypothèse de récurrence, $g(y) = y$, $g(z) = z$ et $g(w) = w$. De plus, comme g est une isométrie, $g(x)$ doit être à distance 1 de y et z et à distance 2 de w. La seule possibilité est $g(x) = x$. Finalement $f = \phi_{\Pi,\sigma}$. □

Le groupe $\mathcal{S}_n$ est donc un sous-groupe du groupe des isométries de (A^n, d).

Définition 1.1.6. On appelle groupe des automorphismes du code C le sous-groupe de $\mathcal{S}_n$ défini par :

$$\mathrm{Aut}(C) := \{\sigma \in \mathcal{S}_n, \sigma(C) = C\}$$

où $\sigma(C) = \{\sigma.c, c \in C\}$.

Définition 1.1.7. Un code de longueur n dont le groupe des automorphismes contient le cycle $(1, \ldots, n)$ est appelé un code cyclique.

Définition 1.1.8. Le rayon de recouvrement d'un code C sur un alphabet A de longueur n est le plus petit ρ tel que les boules fermées centrées en des mots de C et de rayon ρ recouvrent A^n. Autrement dit, si on note $\rho(C)$ le rayon de recouvrement de C, on a

$$\rho(C) := \max_{x \in A^n} \min_{c \in C} d(x, c).$$

Codes linéaires

A partir de maintenant, on suppose $A = \mathbb{F}_q$.

Définition 1.1.9. Soit C un code de longueur n. Le poids d'un mot $c \in C$, noté $|c|$, est le nombre de coordonnées non nulles de ce mot, c'est-à-dire la distance de c à 0.

Remarque 1.1.10. Si C est un code de longueur n et x, $y \in C$, alors $d(x, y) = |x - y|$.

On s'intéresse maintenant à un cas particulier : les codes linéaires.

Définition 1.1.11. Un code linéaire sur $\mathbb{F}_q$ de longueur n est un sous-espace vectoriel de $\mathbb{F}_q^n$. Si C est un code linéaire de dimension k on dit que C est un $[n, k]$-code.

Définition 1.1.12. Soit C un $[n, k]$-code. Une matrice à k lignes et n colonnes est une matrice génératrice de C si ses lignes forment une base de C.

Remarque 1.1.13. La distance minimale d'un code linéaire est le plus petit poids des mots non nuls du code, c'est-à-dire $d := \min_{c \in C \setminus \{0\}} |c|$

On dira alors qu'un code linéaire de longueur n, de dimension k et de distance minimale d est un $[n, k, d]$-code.

Définition 1.1.14. Soit C un code de longueur n sur $\mathbb{F}_q$. Le code étendu de C, $\overline{C}$, est le code de longueur $n + 1$ défini par

$$(c_0, c_1, \ldots, c_n) \in \overline{C} \Leftrightarrow (c_1, \ldots, c_n) \in C \text{ et } \sum_{k=0}^{n} c_i = 0.$$

Codes duaux

Définition 1.1.15. Soit C un $[n, k]$-code. Le code dual de C, noté $C^\perp$ est le code linéaire de longueur n défini par :

$$C^\perp := \{x \in \mathbb{F}_q^n : \forall y \in C < x, y >= 0\}$$

où $< x, y >:= \sum_{i=1}^{m} x_i y_i$.

Proposition 1.1.16. *Si C est un $[n, k]$ code, $C^\perp$ est un $(n, n - k)$-code.*

Démonstration. Soit $(e_1, \ldots, e_k)$ une base de C, alors

$$\begin{array}{ccc} \mathbb{F}_q^n & \to & \mathbb{F}_q^k \\ x & \mapsto & (< x, e_1 >, \ldots, < x, e_k >) \end{array}$$

est une application linéaire surjective de noyau $C^\perp$. Par le théorème du rang, on obtient donc le résultat. □

Proposition 1.1.17. *Si C un code linéaire de longueur n, alors*

$$\mathrm{Aut}(C) = \mathrm{Aut}(C^{\perp}).$$

Démonstration. Soit $\sigma \in \mathrm{Aut}(C)$, $c \in C$, $c' \in C^{\perp}$. On a

$$< c, \sigma.c' >= \sum_{i=1}^{n} c_i c'_{\sigma(i)} = \sum_{i=1}^{n} c_{\sigma^{-1}(i)} c'_i =< \sigma^{-1}.c, c' >= 0$$

Donc $\sigma.c' \in C^{\perp}$ et $\mathrm{Aut}(C) \subset \mathrm{Aut}(C^{\perp})$. On procède de même pour l'inclusion inverse. □

Codes cycliques

On a un isomorphisme linéaire entre $\mathbb{F}_q^n$ et $\mathbb{F}_q[x]/(x^n - 1)$:

$$\begin{array}{rcl} \mathbb{F}_q^n & \to & \mathbb{F}_q[x]/(x^n-1) \\ (a_1, \ldots, a_n) & \mapsto & a_1 + a_2 x + \ldots + a_n x^{n-1} \end{array}$$

On peut donc identifier $\mathbb{F}_q^n$ et $\mathbb{F}_q[x]/(x^n - 1)$.

Théorème 1.1.18. *Un code linéaire C sur $\mathbb{F}_q$ de longueur n est cyclique si et seulement si C est un idéal de $\mathbb{F}_q[x]/(x^n - 1)$.*

Démonstration. Supposons que C soit un code cyclique. Soit $c(x) \in C$ alors $xc(x) \in C$ par définition. D'où, pour tout entier i, $x^i c(x) \in C$. Comme C est un code linéaire sur $\mathbb{F}_q$, pour tout $a(x) \in \mathbb{F}_q[x]$, $a(x)c(x) \in C$ et donc C est un idéal.
Réciproquement, supposons que C soit un idéal de $\mathbb{F}_q[x]/(x^n - 1)$. Alors, pour tout $c(x) \in C$, $xc(x) \in C$ donc C est un code cyclique. □

Proposition 1.1.19. *Soit K un corps, $f \in K[x]$ et on considère le morphisme de K-algèbres canonique*

$$\varphi : K[x] \to K[x]/(f).$$

Alors l'application

$$\psi : \begin{array}{ccc} \{\textit{diviseurs unitaires de } f\} & \to & \{\textit{idéaux de } K[X]/(f)\} \\ g & \mapsto & \varphi((g)) \end{array}$$

est une bijection. Si J est un idéal de $K[x]/(f)$, l'unique g tel que $J = \varphi((g))$ s'appelle le polynôme générateur minimal de J.
De plus $\varphi((g))$ est un espace vectoriel de dimension $\deg(f) - \deg(g)$.

Démonstration. On commence par montrer que ψ est injective. Soit g, $h \in K[x]$, unitaires divisant f tels que $\varphi((g)) = \varphi((h))$. Alors il existe k et $j \in K[x]$ tels que

$$g(x) = h(x)j(x) + f(x)k(x).$$

Comme h divise f, h divise g. Par symétrie, on a aussi g divise h et puisque g et h sont unitaires, $g = h$.
Montrons maintenant que ψ est surjective. Soit J un idéal de $K[x]/(f)$. Alors $\varphi^{-1}(J)$ est un idéal de $K[x]$, il existe donc $g \in K[x]$ unitaire tel que $(g) = \varphi^{-1}(J)$. De plus,

$$(f) = \varphi^{-1}(\{0\}) \subset \varphi^{-1}(J) = (g)$$

donc g divise f.
Soit $g \in K[x]$, unitaire et divisant f. Montrons que l'espace vectoriel $\varphi((g))$ est de dimension $\deg(g) - \deg(f)$. Soit $\overline{c}(x) \in \varphi((g))$. On considère $c(x) \in K[x]$, l'unique représentant de $\overline{c}(x)$ de degré strictement plus petit que $\deg(f)$. Alors il existe q et $r \in K[x]$ tel que

$$c(x) = g(x)q(x) + r(x)f(x) = g(x)\left(q(x) + r(x)\frac{f(x)}{g(x)}\right)$$

Comme $\deg(c) < \deg(f)$, $\deg(q(x) + r(x)\frac{f(x)}{g(x)}) < \deg(f) - \deg(g)$. Une base de $\varphi((g))$ est $\varphi(g(x)), \varphi(xg(x)), \ldots, \varphi(x^{\deg(f)-\deg(g)-1}g(x))$. □

Par la proposition précédente, à chaque idéal de $\mathbb{F}_q[x]/(x^n - 1)$ il correspond un unique polynôme générateur minimal. Un code cyclique étant un idéal de $\mathbb{F}_q[x]/(x^n - 1)$, les éléments du code sont les multiples du polynôme générateur minimal correspondant. Ce polynôme est appelé polynôme générateur du code. Le polynôme générateur d'un code cyclique est un diviseur de $x^n - 1$ donc ses racines sont des racines $n$ième de l'unité.

Jusqu'à la fin de cette section, on suppose que $\mathrm{pgcd}(n, q) = 1$

Définition 1.1.20. Si B est un ensemble de racines $n$ième de 1 et C un code cyclique de longueur n, on dit que B est un ensemble définissant pour C si

$$c(x) \in C \Leftrightarrow \forall \xi \in B, \quad c(\xi) = 0.$$

Un exemple : les codes BCH

Définition 1.1.21. Un code cyclique de longueur n sur $\mathbb{F}_q$ est appelé un code BCH de distance assignée δ si son polynôme générateur est le plus petit multiple commun des polynômes minimaux de β^l, $\beta^{l+1}, \ldots, \beta^{l+\delta-2}$ pour un certain l et β une racine $n$ième de l'unité.

Théorème 1.1.22. *La distance minimale d'un code BCH de distance assignée δ est supérieure ou égale à δ.*

Démonstration. Si C est un code BCH, alors il existe un entier l et une racine $n$ième de l'unité β tels que

$$(c_1, \ldots, c_n) \in C \Leftrightarrow \forall l \leq j \leq l + \delta - 2, \quad c_1 + c_2\beta^j + \ldots + c_n\beta^{j(n-1)} = 0.$$

On considère la matrice $H = \begin{pmatrix} 1 & \beta^l & \beta^{2l} & \ldots & \beta^{l(n-1)} \\ 1 & \beta^{l+1} & \beta^{2(l+1)} & \ldots & \beta^{(l+1)(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{l+\delta-2} & \beta^{2(l+\delta-2)} & \ldots & \beta^{(l+\delta-2)(n-1)} \end{pmatrix}$.

Alors

$$c = (c_1, \ldots, c_n) \in C \Leftrightarrow cH^t = 0$$

Considérons $\delta - 1$ colonnes de H :

$$\begin{pmatrix} \beta^{i_1 l} \\ \vdots \\ \beta^{i_1(l+\delta-2)} \end{pmatrix}, \ldots, \begin{pmatrix} \beta^{i_{\delta-1} l} \\ \vdots \\ \beta^{i_{\delta-1}(l+\delta-2)} \end{pmatrix}$$

Leur déterminant vaut :

$$D = \beta^{(i_1+\ldots+i_{\delta-1})l} \begin{vmatrix} 1 & \cdots & 1 \\ \beta^{i_1} & \cdots & \beta^{i_{\delta-1}} \\ \vdots & & \vdots \\ \beta^{i_1(\delta-2)} & \cdots & \beta^{i_{\delta-1}(\delta-2)} \end{vmatrix}.$$

Donc n'importe quelles $\delta-1$ colonnes de H sont linéairement indépendantes et la distance minimale de C est au moins δ. □

1.2 Définition et premières propriétés

1.2.1 Fonctions de $\mathbb{F}_q^m$ dans $\mathbb{F}_q$

On note B_m^q la $\mathbb{F}_q$-algèbre des fonctions de $\mathbb{F}_q^m$ dans $\mathbb{F}_q$.
Pour tout $u \in \mathbb{F}_q^m$, notons 1_u l' élément de B_m^q défini par :

$$1_u(v) = \begin{cases} 1 & \text{si } u = v \\ 0 & \text{sinon} \end{cases}.$$

La famille $(1_u)_{u\in\mathbb{F}_q^m}$ forme une base du $\mathbb{F}_q$-espace vectoriel B_m^q. On peut donc identifier les $\mathbb{F}_q$-algèbres B_m^q et $\mathbb{F}_q^{q^m}$:

$$\begin{array}{rcl} B_m^q & \to & \mathbb{F}_q^{q^m} \\ f & \mapsto & (f(x))_{x\in\mathbb{F}_q^m} \end{array}.$$

Proposition 1.2.1. *Les $\mathbb{F}_q$-algèbres B_m^q et $\mathbb{F}_q[x_1,\ldots,x_m]/(x_1^q - x_1,\ldots,x_m^q - x_m)$ sont isomorphes.*

Démonstration. On définit la famille de fonctions polynomiales suivantes :

$$\forall u = (u_1,\ldots,u_m) \in \mathbb{F}_q^m,\ f_u = \prod_{i=1}^{m}(1-(x_i-u_i)^{q-1}).$$

Comme la famille $(1_u)_{u\in\mathbb{F}_q^m}$ forme une base du $\mathbb{F}_q$-espace vectoriel B_m^q et que la famille $(f_u)_{u\in\mathbb{F}_q^m}$ forme une base du $\mathbb{F}_q$-espace vectoriel des fonctions polynomiales en m variables $\mathrm{Pol}(m,\mathbb{F}_q)$, on obtient l'isomorphisme d'algèbres :

$$\begin{array}{rcl} \mathrm{Pol}(m,\mathbb{F}_q) & \to & B_m^q \\ f_u & \mapsto & 1_u \end{array}$$

Il reste à montrer que $\mathbb{F}_q[x_1,\ldots,x_m]/(x_1^q - x_1,\ldots,x_m^q - x_m)$ est isomorphe à $\mathrm{Pol}(m,\mathbb{F}_q)$. On considère le morphisme d'algèbres

$$\phi_m : \begin{array}{rcl} \mathbb{F}_q[x_1,\ldots,x_m] & \to & \mathrm{Pol}(m,\mathbb{F}_q) \\ P & \mapsto & (x \mapsto P(x)) \end{array}.$$

Alors $(x_1^q - x_1,\ldots,x_m^q - x_m) \subset \mathrm{Ker}(\phi_m)$ donc ϕ_m induit le morphisme d'algèbres suivant :

$$\overline{\phi_m} : \begin{array}{rcl} \mathbb{F}_q[x_1,\ldots,x_m]/(x_1^q - x_1,\ldots,x_m^q - x_m) & \to & \mathrm{Pol}(m,\mathbb{F}_q) \\ \overline{P} & \mapsto & (x \mapsto P(x)) \end{array};$$

$\overline{\phi_m}$ est surjective, on montre par récurrence sur m qu'elle est injective.
Si $m = 1$. Soit $\overline{P} \in \mathbb{F}_q[x]/(x^q - x)$ tel que $\overline{\phi_1}(\overline{P}) = 0$ et P l'unique représentant de $\overline{P}$

de degré au plus $q-1$. Comme $\overline{P} \in \mathrm{Ker}(\overline{\phi_1})$, pour tout $x \in \mathbb{F}_q$, $P(x) = 0$. De plus, $\deg(P) \leq q-1$ donc $P = 0$.
Soit $m \geq 2$. Supposons que $\overline{\phi_{m-1}}$ soit injective.
Soit $\overline{P} \in \mathbb{F}_q[x_1, \ldots, x_m]/(x_1^q - x_1, \ldots, x_m^q - x_m)$ tel que $\overline{\phi_m}(\overline{P}) = 0$ et P l'unique représentant de $\overline{P}$ de degré au plus $q-1$ en chacune des variables. Soit $x_1, \ldots, x_{m-1} \in \mathbb{F}_q$ fixés,

$$P = \sum_{k=0}^{q-1} x_m^k g_k(x_1, \ldots, x_{m-1}) = P_{x_1,\ldots,x_{m-1}}(x_m).$$

Pour tout $x_m \in \mathbb{F}_q$, $P_{x_1,\ldots,x_{m-1}}(x_m) = 0$. Comme $\deg(P_{x_1,\ldots,x_{m-1}}) \leq q-1$, pour tout $x_1, \ldots, x_{m-1} \in \mathbb{F}_q$, on a $g_k(x_1, \ldots, x_{m-1}) = 0$ pour tout k et pour tout $x_1, \ldots, x_{m-1} \in \mathbb{F}_q$. Par hypothèse de récurrence, $g_k = 0$ et donc $P = 0$. □

On peut maintenant définir le degré d'une fonction de $\mathbb{F}_q^m$ dans $\mathbb{F}_q$.

Définition 1.2.2. Si $f \in B_m^q$, son image dans $\mathbb{F}_q[x_1, \ldots, x_m]/(x_1^q - x_1, \ldots, x_m^q - x_m)$ a un unique représentant de degré au plus $q-1$ en chacune des variables. Le degré de f est alors le degré de ce représentant. On le note $\deg(f)$.

Proposition 1.2.3. *Le degré de $f \in B_m^q$ est strictement plus petit que $m(q-1)$ si et seulement si*

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

Démonstration. On va montrer ce résultat pour chaque monôme. On considère le monôme suivant : $x_1^{i_1} \ldots x_m^{i_m}$.
Si l'un des i_j est nul, on peut supposer qu'il s'agit de i_1 sans perte de généralité. Alors

$$\sum_{x \in \mathbb{F}_q^m} x_1^{i_1} \ldots x_m^{i_m} = q \sum_{(x_2,\ldots,x_m) \in \mathbb{F}_q^{m-1}} x_2^{i_2} \ldots x_m^{i_m} = 0.$$

On suppose maintenant que pour tout $1 \leq j \leq m$, $i_j \neq 0$. Par hypothèse, il existe un i_j tel que $i_j = i \neq q-1$. Il existe donc $y \in \mathbb{F}_q^*$ tel que $y^i \neq 1$. On a alors

$$\sum_{x \in \mathbb{F}_q} x^i = \sum_{x \in \mathbb{F}_q} (yx)^i.$$

D'où, comme $y^i \neq 1$, $\sum_{x \in \mathbb{F}_q} x^i = 0$ et donc

$$\sum_{x \in \mathbb{F}_q^m} x_1^{i_1} \ldots x_m^{i_m} = 0.$$

D'autre part, $\sum_{x \in \mathbb{F}_q^m} x_1^{q-1} \ldots x_m^{q-1} = (-1)^m \neq 0$. □

Action du groupe affine

Soit σ un élément du groupe affine $\mathrm{GA}_m(\mathbb{F}_q)$ défini par

$$\forall x \in \mathbb{F}_q^m, \qquad \sigma(x) = A.x + b$$

où A est une matrice $m \times m$ inversible et b est un élément de $\mathbb{F}_q^m$.
On peut alors définir une action de σ sur $f \in B_m^q$ comme suit :

$$\forall x \in \mathbb{F}_q^m \qquad (\sigma.f)(x) = f(Ax + b).$$

On obtient alors facilement la proposition suivante :

Proposition 1.2.4. *Soit r un entier tel que $0 \leq r \leq m(q-1)$. L'ensemble des fonctions de $\mathbb{F}_q^m$ dans $\mathbb{F}_q$ de degré inférieur ou égal à r est stable sous l'action du groupe affine.*

1.2.2 Codes de Reed-Muller

Dans cette sous-section, on fait quelques rappels sur les codes de Reed-Muller, c'est-à-dire qu'on se place dans le cas où $q = 2$. La plupart des résultats donnés dans cette sous-section peuvent être trouvés dans [MS77b] ou [CH10][Chap. 10].

Définition 1.2.5. Soit r un entier tel que $0 \leq r \leq m$. Le code de Reed-Muller d'ordre r, $R(r, m)$, est le sous-espace des fonctions de B_m^2 de degré au plus r.

Remarque 1.2.6.
- On a $R(0, m) \subset R(1, m) \subset \ldots \subset R(m, m)$.
- Les codes de Reed-Muller sont stables sous l'action du groupe affine (proposition 1.2.4).

Théorème 1.2.7. *Soit $0 \leq r \leq m$. Le code de Reed-Muller d'ordre r est un code linéaire de longueur 2^m et de dimension $\sum_{i=0}^{r} \binom{m}{i}$.*

Démonstration. L'espace B_m^2 est de dimension 2^m donc $R(r, m)$ est de longueur 2^m. De plus, $R(r, m)$ est engendré par $\{x_1^{i_1} \ldots x_m^{i_m} : \forall 1 \leq j \leq m, i_j \in \{0, 1\}, \sum_{j=0}^{m} i_j \leq r\}$ donc sa dimension est $\sum_{i=0}^{r} \binom{m}{i}$. □

L'ensemble $\mathcal{P}(\mathbb{F}_2^m)$ des parties de $\mathbb{F}_2^m$, muni de la différence symétrique Δ et de l'intersection, est un anneau. On a alors la proposition suivante :

Proposition 1.2.8. *On a un isomorphisme d'anneaux entre $\mathcal{P}(\mathbb{F}_2^m)$ et B_m^2.*

Démonstration. L'application suivante est un morphisme d'anneaux :

$$\psi : \begin{array}{ccc} \mathcal{P}(\mathbb{F}_2^m) & \to & B_m^2 \\ A & \mapsto & 1_A \end{array}$$

où 1_A est la fonction caractéristique de A. L'inverse de ce morphisme est :

$$\varphi : \begin{array}{ccc} B_m^2 & \to & \mathcal{P}(\mathbb{F}_2^m) \\ f & \mapsto & A_f = \{x \in \mathbb{F}_2^m, f(x) \neq 0\} \end{array}.$$

□

Proposition 1.2.9. *Soit $f \in B_m^2$. Il y a équivalence entre les propositions suivantes :*

1. *Le degré de f est inférieur ou égal à r.*
2. *Le support de f appartient à l'ensemble des parties de $\mathbb{F}_2^m$ engendrées par les sous-espaces affines de codimension r.*

Démonstration. Commençons par montrer qu'une partie engendrée par les sous-espaces affines de codimension r est une fonction de degré au plus r. Pour cela, il suffit de prouver qu'un sous-espace affine de codimension r est une fonction de degré au plus r. Si A est un sous-espace affine de codimension r, alors il existe $f_1, \ldots, f_r \in B_m^2$ tels que pour tout $i \in [\![1, r]\!]$, $f_i(x) = \sum_{k=1}^{m} a_{i,k}x_k + b_i$ et $A = \{x \in \mathbb{F}_2^m : 1 \leq i \leq r, f_i(x) = 1\}$. On a alors $1_A = \prod_{i=1}^{r} f_i$ qui est de degré au plus r.
Réciproquement, il suffit de montrer que chaque monôme de degré au plus r est une partie engendrée par les sous-espaces affines de codimension r.
On commence par les monômes de degré r. Soit $f = x_{i_1} \ldots x_{i_r}$ un tel monôme. Alors $\{x \in \mathbb{F}_2^m : f(x) \neq 0\} = \{x \in \mathbb{F}_2^m : x_{i_1} = \ldots = x_{i_r} = 1\}$ qui est un sous-espace affine de codimension r. On considère maintenant un monôme de degré $k < r$: $f = x_{i_1} \ldots x_{i_k}$. Alors

$$\begin{aligned} f &= x_{i_1} \ldots x_{i_k} x_{i_{k+1}} + x_{i_1} \ldots x_{i_k}(x_{i_{k+1}} + 1) \\ &= \sum_{u \in \mathbb{F}_2^{r-k}} x_{i_1} \ldots x_{i_k}(x_{i_{k+1}} + u_1) \ldots (x_{i_r} + u_{r-k}) \\ &= \sum_{u \in \mathbb{F}_2^{r-k}} 1_{\mathrm{A_u}} \end{aligned}$$

où $A_u = \{x \in \mathbb{F}_2^m : x_{i_1} = \ldots = x_{i_k} = 1 = (x_{i_{k+1}} + u_1) = \ldots = (x_{i_r} + u_{r-k})\}$.

Or, pour tout $u \in \mathbb{F}_2^{r-k}$, A_u est un sous-espace affine de codimension r. □

On obtient donc une définition équivalente pour les codes de Reed-Muller :

Proposition 1.2.10. *Soit $0 \leq r \leq m$. Le code de Reed-Muller d'ordre r est l'ensemble des parties de $\mathcal{P}(\mathbb{F}_2^m)$ engendrées par les sous-espaces affines de codimension r.*

En utilisant l'identification de B_m^2 et $\mathbb{F}_2^{2^m}$, on peut donner une troisième définition des codes de Reed-Muller : pour $1 \leq r \leq m-1$ et $f \in R(r, m)$, on peut écrire

$$f(x_1, \ldots, x_m) = h(x_1, \ldots, x_{m-1}) + x_m g(x_1, \ldots, x_{m-1}),$$

avec $h \in R(r, m-1)$ et $g \in R(r-1, m-1)$. Autrement dit, tout élément de $R(r, m)$ peut s'écrire sous la forme $(x, x+y)$ où x et y sont des vecteurs de $\mathbb{F}_2^{2^{m-1}}$ tels que $x \in R(r, m-1)$ et $y \in R(r-1, m-1)$.

Définition 1.2.11. On a $R(0, m) = \{(0, \ldots, 0), (1, \ldots 1)\} \subset \mathbb{F}_2^{2^m}$, $R(m, m) = \mathbb{F}_2^{2^m}$ et pour $1 \leq r \leq m-1$, $R(r, m) = \{(x, x+y) : x \in R(r, m-1), y \in R(r-1, m-1)\}$.

Dans la suite, on redémontrera dans le cadre des codes de Reed-Muller généralisés certains théorèmes classiques des codes de Reed-Muller. On rappellera ainsi leur dimension, leur code dual, leur distance minimale ainsi que les mots de code qui atteignent cette distance et enfin leur groupe des automorphismes.

1.2.3 Codes de Reed-Muller généralisés

De manière analogue, nous allons maintenant définir les codes de Reed-Muller généralisés.

Définition 1.2.12. Soit r un entier tel que $0 \leq r \leq m(q-1)$. Le code de Reed-Muller généralisé d'ordre r de longueur q^m, noté $R_q(r,m)$, est le sous-espace des fonctions de B_m^q de degré au plus r. Autrement dit, c'est le sous-espace de B_m^q engendré par

$$\{x_1^{i_1} \dots x_m^{i_m} : \forall 1 \leq k \leq m, 0 \leq i_k \leq q-1, \sum_{k=1}^{m} i_k \leq r\}.$$

Remarque 1.2.13.
- Pour $q = 2$, on retrouve les codes de Reed-Muller.
- On a $R_q(0,m) \subset R_q(1,m) \subset \dots \subset R_q(m,m)$.
- Les codes de Reed-Muller généralisés sont stables sous l'action du groupe affine (proposition 1.2.4).

Théorème 1.2.14. *Soit $0 \leq r \leq m(q-1)$. Le code de Reed-Muller généralisé $R_q(r,m)$ est un code linéaire de longueur q^m et de dimension* $\displaystyle\sum_{i=0}^{r}\sum_{k=0}^{m}(-1)^k\binom{m}{k}\binom{i-kq+m-1}{i-kq}$.

Démonstration. Les codes de Reed-Muller généralisés sont des sous-espaces vectoriels de B_m^q qui est de dimension q^m.
Pour ce qui est de la dimension, on va commencer par calculer le nombre de monômes en m variables de degré global $i \in [\![0, m(q-1)]\!]$ et de degré au plus $q-1$ en chacune des variables. Autrement dit, on veut connaitre le nombre de façons de choisir i éléments parmi m avec répétition autorisée sachant que chaque élément ne peut pas être choisi plus de $q-1$ fois.
On note $S_{j,m}$ le nombre de façons de choisir j éléments parmi m avec répétition autorisée. On a, pour $x < 1$,

$$\frac{1}{(1-x)^m} = \left(\sum_{k=0}^{\infty} x^k\right)^m = \sum_{j=0}^{\infty} S_{j,m} x^j.$$

Par unicité du développement en série entière, on en déduit

$$S_{j,m} = \binom{j+m-1}{j}.$$

En utilisant le principe d'inclusion-exclusion pour les ensembles $A_k = \{x_1^{i_1} \dots x_m^{i_m}, i_k \geq q\}$, on obtient que le nombre de monômes de degré i en m variables et de degré au plus $q-1$ en chacune des variables est

$$\sum_{k=0}^{m}(-1)^k\binom{m}{k}\binom{i-kq+m-1}{i-kq}.$$

Comme on s'intéresse aux fonctions de degré inférieur ou égal à r, on a le résultat. □

Théorème 1.2.15. *Si $0 \leq r \leq (m(q-1)-1)$*

$$R_q(r,m)^\perp = R_q(m(q-1)-1-r, m).$$

Démonstration. Soit $f \in R_q(r,m)$ et $g \in R_q(m(q-1)-1-r)$ fg est alors de degré strictement plus petit que $m(q-1)$ et donc, par la proposition 1.2.3,

$$R_q(m(q-1)-1-r, m) \subset R_q(r,m)^\perp.$$

On considère maintenant l'involution qui à $x_1^{i_1} \dots x_m^{i_m}$ associe $x_1^{q-1-i_1} \dots x_m^{q-1-i_m}$. Alors il existe autant de monômes de degré strictement plus grand que $m(q-1)-1-r$ que de monômes de degré inférieur ou égal à r.
D'où $\dim(R_q(m(q-1)-1-r,m)) = q^m - \dim(R_q(r,m)) = \dim(R_q(r,m)^\perp)$. □

Pour $q-1 \leq r \leq (m-1)(q-1)$, si $f \in R_q(r,m)$, on a

$$f(x_1,\ldots,x_m) = \sum_{k=0}^{q-1} x_1^k g_k(x_2,\ldots,x_m).$$

On peut donc également donner une définition récursive des codes de Reed-Muller généralisés. Cependant, elle semble moins intéressante car il faut au préalable définir $R_q(r,m)$ pour $0 \leq r < (q-1)$ et $(m-1)(q-1) < r \leq m(q-1)$.
D'autre part, on n'a plus d'isomorphisme d'anneaux entre B_m^q et $\mathcal{P}(F_q^m)$ comme sur $\mathbb{F}_2$. En effet, une fonction de B_m^q peut prendre des valeurs différentes de 0 et 1. On a quand même le résultat suivant :
Pour A un ensemble, on définit la fonction 1_A sur $\mathbb{F}_q^m$ par $1_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{sinon} \end{cases}$.

Proposition 1.2.16. *Soit $0 \leq t \leq m$. Si $r \geq t(q-1)$, alors pour tout sous-espace affine A de codimension t, la fonction 1_A est dans $R_q(r,m)$.*

Démonstration. Si A est un sous-espace affine de codimension t, il est défini comme l'ensemble des points de $\mathbb{F}_q^m$ vérifiant les équations suivantes :

$$1 \leq i \leq t, \qquad f_i(x_1,\ldots,x_m) = \sum_{k=1}^{m} a_{i,k}x_k = w_i.$$

On considère maintenant le polynôme suivant :

$$p(x_1,\ldots,x_m) = \prod_{i=0}^{t}(1-(f_i(x_1,\ldots,x_m)-w_i)^{q-1}).$$

Le polynôme p est de degré $t(q-1)$ donc $p \in R_q(r,m)$ pour $r \geq t(q-1)$.
De plus, $p(x_1,\ldots,x_m)$ vaut 1 si $f_i(x_1,\ldots,x_m) = w_i$ pour tout $1 \leq i \leq t$ et 0 sinon. □

1.2.4 Codes de Reed-Muller généralisés et codes cycliques

Une autre façon de voir les codes de Reed-Muller généralisés est de les voir comme des codes cycliques étendus. Ce point de vue sur les codes de Reed-Muller généralisés est aussi appelé l'approche à une variable dans la littérature (voir [DGM70, PHB98] par exemple).

Définition 1.2.17. Soir $0 \leq r < m(q-1)$. Le code de Reed-Muller généralisé ponctué d'ordre r, noté $R_q(r,m)^*$ est le code linéaire de longueur q^m-1 obtenu à partir des mots de $R_q(r,m)$ en supprimant la coordonnée correspondant à 1_0.

Proposition 1.2.18. *Pour $0 \leq r \leq m(q-1)-1$, $R_q(r,m)^*$ est un code cyclique de longueur q^m-1 sur $\mathbb{F}_q$.*

Démonstration. Il existe un élément primitif de $\mathbb{F}_{q^m}$ tel que $\{\omega,\omega^q,\ldots,\omega^{q^{m-1}}\}$ soit une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ (voir [LN97]). On a un isomorphisme ϕ de $\mathbb{F}_q^m$ dans $\mathbb{F}_{q^m}$ qui a $(a_1,\ldots,a_m)$ associe $a_1\omega + a_2\omega^q + \ldots + a_m\omega^{q^{m-1}}$. On peut alors identifier $R_q(r,m)$ à $\{(p(0),p(\phi^{-1}(1)),\ldots,p(\phi^{-1}(\omega^{q^m-2}))) : p \in R_q(r,m)\}$ et donc $R_q(r,m)^*$ à $\{(p(\phi^{-1}(1)),\ldots,p(\phi^{-1}(\omega^{q^m-2}))) : p \in R_q(r,m)\}$. D'autre part, la multiplication par ω est une application linéaire et $\mathrm{GL}_m(\mathbb{F}_q)$ est le stabilisateur de 0 dans $\mathrm{GA}_m(\mathbb{F}_q)$ donc $\mathrm{GL}_m(\mathbb{F}_q)$ agit sur $R_q(r,m)^*$. D'où, $R_q(r,m)^*$ est cyclique. □

Corollaire 1.2.19. *Pour $0 \leq r \leq m(q-1)-1$, $R_q(r,m)$ est un code cyclique étendu.*

Démonstration. Soit $f \in R_q(r,m)$. Alors, si $r < m(q-1)$, on a $\sum_{x \in \mathbb{F}_q^m} f(x) = 0$ (proposition 1.2.3). Donc $R_q(r,m)$ est le code cyclique étendu du code de Reed-Muller généralisé ponctué correspondant. □

Définition 1.2.20. Si $0 \leq j \leq q^m - 1$ s'écrit $j = \sum_{k=0}^{m-1} j_k q^k$ avec $0 \leq j_k \leq q-1$, alors le q-poids de j est

$$wt_q(j) = \sum_{k=0}^{m-1} j_k.$$

Proposition 1.2.21. *Soit $0 \leq r < m(q-1)$, $R_q(r,m)^*$ est un code cyclique d'ensemble définissant $\{j : 0 < wt_q(j) < m(q-1) - r\}$.*

Démonstration. Soit ω un élément primitif de $\mathbb{F}_{q^m}$. Alors $\{1, \omega, \ldots, \omega^{m-1}\}$ est une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$. Il existe une unique base $\{\beta_1, \ldots, \beta_m\}$ de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ tel que

$$\forall i, j, \quad \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_i \omega^{j-1}) = \delta_{i,j}$$

où $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ désigne la trace de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ et $\delta_{i,j}$, le symbole de Kronecker (voir théorème 2.24 de [LN97]). On définit alors l'homomorphisme de $\mathbb{F}_q$-algèbres suivant :

$$\theta : \begin{array}{rcl} \mathbb{F}_q[x_1, \ldots, x_m] & \to & \mathbb{F}_{q^m}[z]/(z^{q^m} - z) \\ x_i & \mapsto & \beta_i z + (\beta_i z)^q + \ldots + (\beta_i z)^{q^{m-1}} = T(\beta_i z) \end{array}.$$

Or $\theta(x_i^q) = (T(\beta_i z))^q = T(\beta_i z) = \theta(x_i)$ donc θ induit un morphisme d'algèbres $\overline{\theta}$ de $\mathbb{F}_q[x_1, \ldots, x_m]/(x_1^q - x_1, \ldots, x_m^q - x_m)$ sur $\mathbb{F}_{q^m}[z]/(z^{q^m} - z)$.
Soit $P \in \mathbb{F}_q[x_1, \ldots, x_m]/(x_1^q - x_1, \ldots, x_m^q - x_m)$. On a

$$\mathbb{F}_q^m = \{(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_1 z), \ldots, \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_m z)) : z \in \mathbb{F}_{q^m}\}$$

et donc

$$\sum_{x \in \mathbb{F}_q^m} P(x) = \sum_{z \in \mathbb{F}_{q^m}} P(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_1 z), \ldots, \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_m z)) = \sum_{z \in \mathbb{F}_{q^m}} \overline{\theta}(P)(z).$$

Donc, par la proposition 1.2.3, $\deg(P) < m(q-1)$ si et seulement si $\deg(\overline{\theta}(P)) < q^m - 1$.
Soit $P \in \mathbb{F}_q[x_1, \ldots, x_m]/(x_1^q - x_1, \ldots, x_m^q - x_m)$ tel que $\deg(P) < m(q-1)$. Si

$$Q(z) = \sum_{j=0}^{q^m-2} c_j z^j$$

désigne son image par $\overline{\theta}$, alors on a $(Q(z))^q = Q(z)$ si et seulement si $\sum_{j=0}^{q^m-2} c_j^q z^{jq} = \sum_{j=0}^{q^m-2} c_j z^j$.
Or, si $j < q^m - 1$, l'application qui à j associe $[jq]$, son reste dans la division euclidienne par $q^m - 1$, est bijective. On obtient alors : $\sum_{j=0}^{q^m-2} c_j^q z^{jq} = \sum_{j=0}^{q^m-2} c_{[jq]} z^{jq}$.
De plus, pour $k \geq 1$, $(z^{q^m-1})^k = z^{q^m-1} \mod (z^{q^m} - z)$ donc l'image de $\overline{\theta}$ est incluse dans

$$L = \{Q(z) = \sum_{j=0}^{q^m-1} c_j z^j : c_{q^m-1} \in \mathbb{F}_q, \forall 0 \leq j \leq q^m - 2, c_j^q = c_{[jq]}\}.$$

Inversement, on considère le morphisme de $\mathbb{F}_q$-algèbres

$$\psi : \begin{array}{rcl} \mathbb{F}_{q^m}[z] & \to & \mathbb{F}_{q^m}[x_1,\ldots,x_m]/(x_1^q - x_1,\ldots,x_m^q - x_m) \\ z & \mapsto & \sum_{i=1}^{m} x_i\omega^{i-1} \end{array}.$$

Or $\left(\sum_{i=1}^{m} x_i\omega^{i-1}\right)^{q^m} = \sum_{i=1}^{m} x_i\omega^{i-1}$, donc ψ induit un morphisme d'algèbres $\overline{\psi}$ de $\mathbb{F}_{q^m}[z]/(z^{q^m} - z)$ dans $\mathbb{F}_{q^m}[x_1,\ldots,x_m]/(x_1^q - x_1,\ldots,x_m^q - x_m)$.
Soit $Q \in L$. Alors $Q(z)^q = Q(z)$ donc $\overline{\psi}(Q)^q = \overline{\psi}(Q)$, d'où

$$\overline{\psi}(Q) \in \mathbb{F}_q[x_1,\ldots,x_m]/(x_1^q - x_1,\ldots,x_m^q - x_m).$$

A partir de maintenant, on considère la restriction de $\overline{\psi}$ à L, que l'on notera encore $\overline{\psi}$.
Soit $1 \leq i \leq m$,

$$\begin{aligned} \overline{\psi} \circ \overline{\theta}(x_i) &= \sum_{k=0}^{m-1} \beta_i^{q^k} \sum_{j=1}^{m} x_j\omega^{(j-1)q^k} \\ &= \sum_{j=1}^{m} x_j \sum_{k=0}^{m-1} (\beta_i\omega^{j-1})^{q^k} \\ &= \sum_{j=1}^{m} x_j \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_i\omega^{j-1}) = x_i. \end{aligned}$$

Donc $\overline{\theta}$ est injective. De plus, tout élément de L de degré inférieur ou égal à $q^m - 2$ peut s'écrire sous la forme

$$Q(z) = \sum_{i=0}^{q^m-2} Q(\omega^i) g_i(z)$$

où $g_i(z) = -\omega^i \frac{z^{q^m-1}-1}{z-\omega^i}$. Comme $Q \in L$, pour tout i, $Q(\omega^i) \in \mathbb{F}_q$ et L est de dimension q^m sur $\mathbb{F}_q$. D'où $\overline{\theta}$ est un isomorphisme d'algèbres de $\mathbb{F}_q[x_1,\ldots,x_m]/(x_1^q - x_1,\ldots,x_m^q - x_m)$ dans L.
Soit $0 \leq j \leq q^m - 1$ s'écrivant $j = \sum_{k=0}^{m-1} j_k q^k$. Alors

$$\begin{aligned} \overline{\psi}(z^j) &= (\sum_{i=1}^{m} x_i\omega^{i-1})^j \\ &= \prod_{k=0}^{m-1} \left(\sum_{i=1}^{m} x_i\omega^{(i-1)q^k}\right)^{j_k} \end{aligned}$$

donc $\deg(\overline{\psi}(z^j)) \leq wt_q(j)$.
Inversement, soit $1 \leq i \leq m$, $0 \leq \alpha \leq q-1$

$$\begin{aligned} \overline{\theta}(x_i^\alpha) &= (\beta_i z + (\beta_i z)^q + \ldots + (\beta_i z)^{q^{m-1}})^\alpha \\ &= \sum_{\substack{l_1,\ldots,l_m \\ \sum l_k = \alpha}} \frac{\alpha!}{l_1!\ldots l_m!} \prod_{k=1}^{m} \beta_i^{l_k q^{k-1}} z^{\sum_{k=1}^{m} l_k q^{k-1}} \end{aligned}$$

donc $wt_q(\deg(\overline{\theta}(x_i^\alpha))) = \alpha$.
Finalement, pour $0 \leq r \leq m(q-1)-1$, $R_q(r,m)$ est isomorphe à

$$\{Q(z) = \sum_{i=0}^{q^m-2} c_j z^j \in L : c_j = 0 \text{ si } wt_q(j) > r\}.$$

On en déduit que $R_q(r,m)^*$ correspond à

$$C_r = \{(Q(1),\ldots,Q(\omega^{q^m-2})) : Q(z) = \sum_{i=0}^{q^m-2} c_j z^j \in L, c_j = 0 \text{ si } wt_q(j) > r\}.$$

D'autre part, on note $R = \{(Q(1),\ldots,Q(\omega^{q^m-2})) : Q(z) = \sum_{i=0}^{q^m-2} c_j z^j \in L\}$. On a l'isomorphisme de $\mathbb{F}_q$-espaces vectoriels

$$\alpha : \begin{array}{ccc} R & \to & \mathbb{F}_q[y]/(y^{q^m-1}-1) \\ (Q(1),\ldots,Q(\omega^{q^m-2})) & \mapsto & \sum_{i=0}^{q^m-2} Q(\omega^i)y^i \end{array},$$

d'inverse $\beta : f \mapsto (Q_f(1),\ldots,Q_f(\omega^{q^m-2}))$ où $Q_f(z) = \sum_{j=0}^{q^m-2} -f(\omega^{-j})z^j$.
Soit g un polynôme générateur d'un code cyclique C de longueur q^m-1. Alors un polynôme f est dans le code C si et seulement si pour tout $0 \leq j \leq q^m-2$ tel que $g(\omega^{-j}) = 0$, $f(\omega^{-j}) = 0$. Un code cyclique d'ensemble des zéros $\{\omega^{-j} : j \in T\}$ correspond donc par β à

$$\{(Q(1),\ldots,Q(\omega^{q^m-2}) : Q(z) = \sum_{i=0}^{q^m-2} c_j z^j \in L, c_j = 0 \text{ si } j \in T\}.$$

En appliquant ce résultat à $R_q(r,m)^*$, on obtient que l'ensemble des zéros de $R_q(r,m)^*$ est $\{\omega^{-j} : m(q-1) > wt_q(j) > r\} = \{\omega^j : 0 < wt_q(j) < m(q-1)-r\}$. □

Corollaire 1.2.22. *Pour $0 \leq r \leq m(q-1)-1$, on écrit $r = t(q-1)+s$, $0 \leq s \leq q-2$. Alors $R_q(r,m)^*$ est un sous-code d'un code BCH de distance assignée $(q-s)q^{m-t-1}-1$.*

Démonstration. Par le théorème précédent, on sait que le polynôme générateur de $R_q(r,m)^*$ a pour zéros $\{\omega^j : 0 < wt_q(j) < m(q-1)-r\}$ où ω est un élément primitif de $\mathbb{F}_{q^m}$. Le plus petit entier h vérifiant $wt_q(h) = m(q-1)-r$ est

$$h = \sum_{i=0}^{m-t-2} (q-1)q^i + (q-1-s)q^{m-t-1} = (q-s)q^{m-t-1}-1.$$

D'où, pour tout $0 < j < h$, ω^j annule le polynôme générateur de $R_q(r,m)^*$. □

1.3 Distance minimale

Dans cette section, on s'intéresse à la distance minimale des codes de Reed-Muller généralisés et aux mots de code qui atteignent cette distance.

1.3.1 Distance minimale des codes de Reed-Muller généralisés

On définit le poids d'un mot d'un code de Reed-Muller généralisé comme suit :

Définition 1.3.1. Soit $0 \leq r \leq m(q-1)$. Si f est un mot de $R_q(r,m)$ alors le poids de f est $|f| = \#\mathrm{Supp}(f)$.

Le théorème suivant donne la distance minimale des codes de Reed-Muller généralisés. On en trouve la preuve dans [MS77b] pour $q = 2$ et dans [KLP68] ou [PHB98] pour le cas $q \neq 2$.

Théorème 1.3.2. *Soit $0 \leq r \leq m(q-1)$, on écrit $r = t(q-1) + s$ avec $0 \leq s \leq q-2$. Alors la distance minimale du code de Reed-Muller généralisé $R_q(r,m)$ est $(q-s)q^{m-t-1}$.*

Remarque 1.3.3. Si $q = 2$, $s = 0$ et $t = r$, la distance minimale est 2^{m-r}.

Démonstration.

- Dans le cas où $q = 2$, il existe une preuve simple qui utilise la définition récursive des codes de Reed-Muller. On démontre le résultat par récurrence sur m.
  On a $R(0,m) = \{(0,\dots,0),(1,\dots,1)\}$ donc sa distance minimale est 2^m. En particulier, la distance minimale de $R(0,1)$ est 2. D'autre part, $R(m,m) = \mathbb{F}_q^m$ donc sa distance minimale est 1 pour tout m. Soit $m > 1$, on suppose que pour tout $1 \leq r \leq m-2$, la distance minimale de $R(r,m-1)$ est 2^{m-r-1}. Soit $1 \leq r \leq m-1$, on note $d_{r,m}$ la distance minimale de $R(r,m)$. On veut montrer qu'elle vaut 2^{m-r}. Pour $1 \leq r \leq m-1$, $R(r,m) = \{(c, c+c') : c \in R(r,m-1), c' \in R(r-1,m-1)\}$. On a $|(c,c+c')| = |c| + |c+c'|$ donc si $c' = 0$, $|(c,c+c')| \geq 2d_{r,m-1}$, avec égalité si c atteint la distance minimale de $R(r,m-1)$.
  Si $c' \neq 0$, $|c+c'| \geq |c'| - |c|$ donc $|(c,c+c')| \geq |c'| \geq d_{r-1,m-1}$ avec égalité si $c = 0$ et c' atteint la distance minimale de $R(r-1,m-1)$. Finalement,

$$d_{r,m} = \min(2d_{r,m-1}, d_{r-1,m-1}) = 2^{m-r}.$$

- Par le corollaire 1.2.22, le code de Reed-Muller généralisé ponctué $R_q(r,m)^*$ est un sous-code du code BCH de distance construite $(q-s)q^{m-t-1} - 1$ donc sa distance minimale est supérieure ou égale à $(q-s)q^{m-t-1} - 1$.
  Soit w'_j, $1 \leq j \leq s$, s éléments de $\mathbb{F}_q^*$. On définit le polynôme suivant :

$$P(x_1,\dots,x_m) = \prod_{i=1}^{t}(1 - x_i^{q-1}) \prod_{j=1}^{s}(x_{r+1} - w'_j).$$

  Alors P est de poids $(q-s)q^{m-t-1}$ et est non nul en 0 donc le mot de $R_q(r,m)^*$ correspondant est de poids $(q-s)q^{m-t-1} - 1$ et la distance minimale de $R_q(r,m)^*$ est $(q-s)q^{m-t-1} - 1$. Soit maintenant un mot de poids minimal dans $R_q(r,m)^*$. Supposons que le mot de $R_q(r,m)$ correspondant soit de poids $(q-s)q^{m-t-1}-1$, c'est-à-dire qu'il vaille 0 en 0. Comme $R_q(r,m)$ est invariant par translation (proposition 1.2.4), il existe un mot de $R_q(r,m)$ de poids $(q-s)q^{m-t-1} - 1$ différent de 0 en 0. Le mot de $R_q(r,m)^*$ correspondant est donc de poids $(q-s)q^{m-t-1} - 2$ ce qui est absurde donc la distance minimale de $R_q(r,m)$ est $(q-s)q^{m-t-1}$.

□

1.3.2 Mots qui atteignent la distance minimale pour $q = 2$

Le théorème suivant donne les mots de poids minimal des codes de Reed-Muller ([MS77a]). Bien que ce théorème soit un cas particulier du théorème 1.3.5 ci-dessous, on commence par prouver le résultat dans le cas particulier $q = 2$ car le preuve est plus simple et permet de mieux se rendre compte du type d'idée que l'on va utiliser par la suite.

Théorème 1.3.4. *Soit $1 \leq r \leq m$. Les mots de $R(r, m)$ de poids minimal sont exactement les sous-espaces affines de codimension r.*

Démonstration. On traite d'abord le cas $r = 0$. Si $f \in R(0, m)$ est de poids 2^m, alors son support est $\mathbb{F}_q^m$ qui est bien un sous-espace affine de codimension 0.
On traite les autres cas par récurrence descendante sur r.
Si $r = m$, soit f un mot de poids 1 de $R(r, m)$. Alors $f = 1_u$ et $\{u\}$ est bien un sous-espace affine de codimension m.
Soit $0 < r < m$, on suppose que les mots de poids minimal de $R(r + 1, m)$ sont les sous-espaces affines de codimension $r + 1$. Soit $f \in R(r, m)$ un mot de poids minimal. On écrit $f = 1_A$, $A \in \mathcal{P}(\mathbb{F}_2^m)$. Soit $a \in A$, on définit $F = \{\overrightarrow{ab} : b \in A\}$ et on veut montrer que F est un sous-espace vectoriel de $\mathbb{F}_2^m$ de codimension r. On a $\#F = 2^{m-r} \leq 2^{\mathrm{rg}(F)}$ où $\mathrm{rg}(F)$ est le rang de la famille F. Donc F contient au moins $m - r$ vecteurs indépendants, $\overrightarrow{v_1}$, $\overrightarrow{v_2} \ldots \overrightarrow{v_{m-r}}$. Soit $\overrightarrow{u} \notin \mathrm{Vect}(\overrightarrow{v_1}, \ldots, \overrightarrow{v_{m-r}})$ (c'est possible car $r \neq 0$). On considère alors un hyperplan affine H tel que $a + \overrightarrow{u} \notin H$ et $a, a + \overrightarrow{v_1}, \ldots, a + \overrightarrow{v_{m-r}} \in H$.
Supposons que $A \cap H \neq A$, alors $A \cap H^c \neq \emptyset$. Or H^c est un hyperplan affine donc $A \cap H$ et $A \cap H^c$ sont des mots de $R(r + 1, m)$ donc de poids supérieur ou égal à 2^{m-r-1}. Pour des raisons de cardinal, $A \cap H$ et $A \cap H^c$ sont en fait des mots de poids minimal de $R(r+1, m)$. Par hypothèse de récurrence, $A \cap H$ est donc un sous-espace affine de codimension $r+1$ or $A \cap H$ contient $a, a + \overrightarrow{v_1}, \ldots, a + \overrightarrow{v_{m-r}}$ ce qui est absurde. D'où $A = A \cap H$ et $a + \overrightarrow{u} \notin A$ et donc $F = \mathrm{Vect}(\overrightarrow{v_1}, \ldots, \overrightarrow{v_{m-r}})$. □

1.3.3 Mots qui atteignent la distance minimale pour $q \neq 2$

Le théorème suivant donne les mots de poids minimal des codes de Reed-Muller généralisés. Il a d'abord été prouvé dans [DGM70] mais comme le soulignent les auteurs, il serait souhaitable d'en trouver une preuve plus simple. C'est ce que nous faisons par la suite en utilisant des arguments similaires au cas $q = 2$ (voir aussi [Led10a]).

Théorème 1.3.5. *Soit $0 \leq r \leq m(q-1) - 1$, $r = t(q-1) + s$, $0 \leq s \leq q - 2$. Les mots de poids minimal de $R_q(r, m)$ sont les mots de $R_q(r, m)$ dont le support est l'union de $q - s$ sous-espaces affines de $\mathbb{F}_q^m$ parallèles de codimension $t + 1$ tous inclus dans un sous-espace affine de codimension t.*

Dans le cas $q \neq 2$, la difficulté est que le complémentaire d'un hyperplan n'est plus un hyperplan. Néanmoins, on montre le lemme suivant :

Lemme 1.3.6. *Soit $0 \leq r \leq m(q-1) - 1$, $r = t(q-1) + s$, $0 \leq s \leq q - 2$. Si f est un mot de poids minimal de $R_q(r, m)$, on note S son support. Alors, pour tout hyperplan affine H tel que $S \cap H \neq \emptyset$ et $S \cap H \neq S$,*

- *soit S rencontre tous les hyperplans parallèles à H,*
- *soit S rencontre $(q - s)$ hyperplans parallèles en q^{m-t-1} points.*

On commence par donner un résultat préliminaire (voir [DGM70]) :

Lemme 1.3.7. *Soit S un ensemble de $\mathbb{F}_q^m$, tel que $\#S = uq^n < q^m$, $0 < u < q$. Supposons que pour tout affine hyperplan de $\mathbb{F}_q^m$, soit $\#(S \cap H) = 0$ soit $\#(S \cap H) \geq uq^{n-1}$. Alors il existe un hyperplan affine de $\mathbb{F}_q^m$ qui ne rencontre pas S.*

Démonstration. Supposons que S rencontre tous les affines hyperplans. Alors on montre par récurrence sur k que pour $0 \leq k \leq m$, $\#(S \cap A_k) = uq^{n-k}$ où A_k est un sous-espace affine de codimension k.
C'est vrai pour $k = 0$. Si $k = 1$, soit H un hyperplan affine. Alors S rencontre tous les hyperplans parallèles à H en au moins uq^{n-1} points donc $\#(S \cap H) = uq^{n-1}$. Soit $k \geq 1$ et supposons que S rencontre tout sous-espace affine de codimension $k-1$ en uq^{n-k+1} points et tout sous-espace affine de codimension k en uq^{n-k} points. Soit A_{k+1} un sous-espace affine de codimension $k+1$ et A_{k-1} un sous-espace affine de codimension $k-1$ le contenant. Si on considère $A_k^{(1)}, \ldots, A_k^{(q+1)}$ les $q+1$ sous-espaces affines de codimension k inclus dans A_{k-1} et contenant A_{k+1} alors $\bigcup_{l=1}^{q+1} A_k^{(l)} = A_{k-1}$ et pour $i \neq j$ $A_k^{(i)} \cap A_k^{(j)} = A_{k+1}$ donc

$$uq^{n-k+1} = \#(S \cap A_{k+1}) + (q+1)(uq^{n-k} - \#(S \cap A_{k+1}))$$

et $\#(S \cap A_{k+1}) = uq^{n-k-1}$, ce qui montre qui montre que l'hypothèse de récurrence est vérifiée au rang $k+1$. Or, pour $k = n+1$, on obtient que $\#(S \cap A_{n+1}) = \frac{u}{q}$ ce qui est absurde car $0 < u < q$. □

On démontre maintenant le premier lemme.

Démonstration. Quitte à appliquer une transformation affine, on peut supposer que $x_1 = 0$ est une équation de H et I l'ensemble des $a \in \mathbb{F}_q$ tel que l'hyperplan parallèle à H d'équation $x_1 = a$ ne rencontre pas S. Soit k le cardinal de I ; supposons que $k \geq 1$. Comme $S \cap H \neq \emptyset$ et $S \cap H \neq S$, on a $k \leq q-2$. Pour tout c dans $\mathbb{F}_q$ tel que c n'est pas dans I, on définit :

$$\forall x = (x_1, \ldots, x_m \text{à} \in \mathbb{F}_q^m,\ f_c(x) = f(x) \prod_{\substack{\alpha \in \mathbb{F}_q \\ \alpha \neq c \\ \alpha \notin I}} (x_1 - \alpha).$$

Le degré de f_c est au plus $t(q-1) + s + q - 1 - k$. On a donc

$$\begin{aligned}(q-s)q^{m-t-1} = |f| &= \sum_{c \notin I} |f_c| \\ &\geq \begin{cases} (q-k)(k-s+1)q^{m-t-1} & \text{si } s-k < 0 \\ (q-k)(q-s+k)q^{m-t-2} & \text{si } s-k \geq 0 \end{cases}.\end{aligned}$$

On doit donc avoir

$$\begin{cases} (q-1-k)(k-s) \leq 0 & \text{si } s-k < 0 \\ k(s-k) \leq 0 & \text{si } s-k \geq 0 \end{cases}.$$

Ce qui n'est possible que si $s = k$. □

Maintenant, on peut prouver le théorème 1.3.5 :

Démonstration. On commence par prouver le théorème pour $t = 0$ et $t = m-1$.

- Supposons $t = 0$ et soit f un mot de poids minimal de $R_q(r, m)$.
  Si $s = 0$ alors $\deg(f) = 0$ et comme $f \neq 0$, on a $f = c$ avec $c \in \mathbb{F}_q^*$.
  Sinon, soit H un hyperplan affine de $\mathbb{F}_q^m$. Alors

  $$\#(\mathrm{Supp}(f) \cap H) = 0 \text{ ou } \#(\mathrm{Supp}(f) \cap H) \geq (q-s)q^{m-2}.$$

  Donc, par le lemme 1.3.7, il existe un hyperplan affine H_0 tel que

  $$\mathrm{Supp}(f) \cap H_0 = \emptyset.$$

  Cependant, $\mathbb{F}_q^m$ est l'union des q hyperplans parallèles à H_0 donc il existe H_1 parallèle à H_0 tel que $H_1 \cap \mathrm{Supp}(f) \neq \emptyset$. De plus, comme $|f| = (q-s)q^{m-1} \geq 2q^{m-1}$, $\mathrm{Supp}(f) \cap H_1 \neq \mathrm{Supp}(f)$. Donc par le lemme 1.3.6, puisque $\mathrm{Supp}(f) \cap H_0 = \emptyset$, $\mathrm{Supp}(f)$ rencontre $H_1, \ldots, H_{q-s}$, $(q-s)$ hyperplans parallèles à H_1 en q^{m-1} points, c'est-à-dire $\mathrm{Supp}(f) = \bigcup_{i=1}^{q-s} H_i$.

- Supposons $t = m-1$. Soit $f \in R_q((m-1)(q-1)+s, m)$, $0 \leq s \leq q-2$, tel que $|f| = q-s$. On pose $S = \mathrm{Supp}(f)$. Soit ω_1, $\omega_2 \in S$ et H un hyperplan tel que ω_1, $\omega_2 \in H$.
  Supposons que $S \cap H \neq S$ alors, par le lemme 1.3.6, soit S rencontre tous les hyperplans parallèles à H (ce qui est possible seulement si $s = 0$) soit S rencontre $(q-s)$ hyperplans parallèles à H en un point. Dans les deux cas on obtient une contradiction puisque S rencontre chaque hyperplan en exactement un point et ω_1, $\omega_2 \in H$.
  Donc S est inclus dans tous les hyperplans H tels que ω_1, $\omega_2 \in H$, ce qui signifie que S est inclus dans la droite passant par ω_1 et ω_2.

  Maintenant on prouve le théorème par récurrence descendante sur t.

- Supposons que pour un t fixé, $1 \leq t \leq m-2$ et pour tout s, $0 \leq s \leq q-2$, le support d'un mot de $R_q((t+1)(q-1)+s, m)$ de poids minimal est l'union de $q-s$ sous-espaces affines de $\mathbb{F}_q^m$, parallèles, de codimension $t+2$ et tous inclus dans un sous-espace affine de codimension $t+1$.

  Soit $f \in R_q(t(q-1)+s, m)$ tel que $|f| = (q-s)q^{m-t-1}$.
  On pose $S = \mathrm{Supp}(f)$. Soit $a \in S$ et $F = \{\overrightarrow{ab} : b \in S\}$. On a :

  $$\#F = (q-s)q^{m-t-1} \leq q^{rg(F)}.$$

  Donc, puisque $0 \leq s \leq q-2$, $rg(F) \geq m-t$. Soit $\overrightarrow{v_1}, \ldots, \overrightarrow{v_{m-t}}$, $m-t$ vecteurs indépendants de F et $\overrightarrow{u} \in \mathbb{F}_q^m$ tel que $\overrightarrow{u} \notin \mathrm{Vect}(\overrightarrow{v_1}, \ldots, \overrightarrow{v_{m-t}})$. Puisque $t \geq 1$, il existe un hyperplan affine H tel que $a, a+\overrightarrow{v_1}, \ldots, a+\overrightarrow{v_{m-t}} \in H$ et $a+\overrightarrow{u} \notin H$.
  Supposons que $S \cap H \neq S$. Alors par le lemme 1.3.6, soit S rencontre tous les hyperplans parallèles à H soit S rencontre $(q-s)$ hyperplans parallèles à H en q^{m-t-1} points. Soit $z = 0$ une équation de H et I l'ensemble des $a \in \mathbb{F}_q$ tels que S rencontre l'hyperplan H_a d'équation $z = a$.

  - *1er cas* : $\#I = q-s$.
    Considérons $P = \prod_{a \in I \setminus \{0\}} (z-a)f(x)$. Alors $\deg(P) \leq (t+1)(q-1)$ et

    $$|P| = \#(S \cap H) = q^{m-t-1}.$$

Donc P est un mot de $R_q((t+1)(q-1), m)$ de poids minimal et par hypothèse de récurrence, son support $\mathrm{Supp}(P) = S \cap H$ est un sous-espace affine de codimension $t+1$.

– *2ème cas* : $\#I = q$.
Pour tout $a \in \mathbb{F}_q$, $f_a = (1-(z-a)^{q-1})f \in R_q((t+1)(q-1)+s, m)$ et $f_a \neq 0$. Donc si on note S_{f_a} le support de f_a, $\#S_{f_a} \geq (q-s)q^{m-t-2}$. Puisque $\#S = (q-s)q^{m-t-1}$ et $S_{f_a} = S \cap H_a$, $\#(S_{f_a}) = (q-s)q^{m-t-2}$. Par hypothèse de récurrence, $S_{f_0} = S \cap H$ est inclus dans un sous-espace affine de codimension $t+1$.

Dans les deux cas, $S \cap H$ est inclus dans un sous-espace affine de codimension $t+1$ ce qui est impossible puisque $a, a+\overrightarrow{v_1}, \ldots, a+\overrightarrow{v_{m-t}} \in S \cap H$. Donc $S \cap H = S$ et $a + \overrightarrow{u} \notin S$, ce qui signifie que $\overrightarrow{u} \notin F$. D'où $F \subset \mathrm{Vect}(\overrightarrow{v_1}, \ldots, \overrightarrow{v_{m-t}})$, *i.e* S est inclus dans un sous-espace affine de codimension t, notons-le A.

Quitte à appliquer une transformation affine, on peut supposer que

$$A = \{x : x_1 = 0, \ldots, x_t = 0\}.$$

Le polynôme réduit

$$f(x) - (1-x_1^{q-1}) \ldots (1-x_t^{q-1}) f(0, \ldots, 0, x_{t+1}, \ldots, x_m)$$

est nul sur $\mathbb{F}_q^m$ donc identiquement nul. D'où

$$P = f(0, \ldots, 0, x_{t+1}, \ldots, x_m) \in R_q(s, m-t).$$

De plus, $|P| = |f| = (q-s)q^{m-t-1}$, donc par le cas $t = 0$, le support de P est l'union de $q-s$ hyperplans de A. Ce qui donne le résultat.

□

1.3.4 Les codes de Reed-Muller généralisés sur $\mathbb{F}_p$ sont engendrés par les mots de poids minimal

Dans le cas $q = 2$, on a montré que les mots de poids minimal engendrent les codes de Reed-Muller (proposition 1.2.9). Ici, on se propose de démontrer que ce résultat est vrai pour q premier.

Théorème 1.3.8. *Pour $q = p$, pour tout $m \geq 1$ et $1 \leq r \leq m(p-1)$, $R_p(r, m)$ est engendré comme $\mathbb{F}_p$-espace vectoriel par ses mots de poids minimal.*

Démonstration. Soit $m \geq 1$, on démontre ce résultat par récurrence sur r. Pour $r = 0$, tous les mots non nuls sont de poids minimal donc on a le résultat. Soit $1 \leq r \leq m(p-1)$ et on suppose que $R_p(r-1, m)$ est engendré par ses mots de poids minimal. On écrit r sous la forme $r = t(p-1)+s$, $0 \leq s \leq p-2$. Les mots de poids minimal de $R_p(r, m)$ sont de la forme $\prod_{i=1}^{t}((f_i(x)+a_i)^{p-1}-1)\prod_{j=1}^{s}(f_{t+1}(x)+b_j)$ où les f_i sont des formes linéaires linéairement indépendantes, $a_i \in \mathbb{F}_p$, $b_j \in \mathbb{F}_p$.

Si $s \geq 1$, comme $s \leq p-2$, il existe $\beta \neq b_1, \ldots, b_s$. Alors

$$\begin{aligned}\prod_{i=1}^{t}((f_i(x)+a_i)^{p-1}-1)\prod_{j=1}^{s}(f_{t+1}(x)+b_j)\\ -\prod_{i=1}^{t}((f_i(x)+a_i)^{p-1}-1)\prod_{j=1}^{s-1}(f_{t+1}(x)+b_j)(f_{t+1}(x)+\beta)\\ =(b_s-\beta)\prod_{i=1}^{t}((f_i(x)+a_i)^{p-1}-1)\prod_{j=1}^{s-1}(f_{t+1}(x)+b_j).\end{aligned}$$

Si $s=0$, $(f_t(x)+a_t)^{p-1}-1=\prod_{\alpha\in\mathbb{F}_p\setminus\{a_t\}}(f_t(x)+\alpha)$. Soit $a \neq a_t$. alors

$$\begin{aligned}\prod_{i=1}^{t}((f_i(x)+a_i)^{p-1}-1)-\prod_{i=1}^{t-1}((f_i(x)+a_i)^{p-1}-1)((f_t(x)+a)^{p-1}-1)\\ =(a_t-a)\prod_{i=1}^{t-1}((f_i(x)+a_i)^{p-1}-1)\prod_{\alpha\in\mathbb{F}_p\setminus\{a_t,a\}}(f_t(x)+\alpha).\end{aligned}$$

On peut donc écrire les mots de poids minimal de $R_p(r-1,m)$ comme combinaisons linéaires de mots de poids minimal de $R_p(r,m)$. Par hypothèse de récurrence, on peut écrire tous les mots de $R_p(r-1,m)$ comme combinaison linéaire de mots de poids minimal de $R_p(r,m)$. Il reste à prouver que l'on peut écrire tous les monômes de degré r comme combinaison linéaire de mots de poids minimal de $R_p(r,m)$ pour avoir le résultat. Supposons que le monôme $x_1^{k_1}\ldots x_m^{k_m}$ avec $0 \leq k_i \leq p-1$ et $\sum_{i=1}^{m} k_i = r$ soit combinaison linéaire de mots de poids minimal. Soit $1 \leq i \leq m$ tel que $k_i \geq 1$ et $j \neq i$. Alors pour tout $a \in \mathbb{F}_p$, $x_1^{k_1}\ldots x_{i-1}^{k_{i-1}}(x_i+ax_j)^{k_i}x_{i+1}^{k_{i+1}}\ldots x_m^{k_m}$ est aussi combinaison linéaire de mots de poids minimal de $R_p(r,m)$. En effet, il suffit de changer les formes linéaires indépendantes $f_1,\ldots,f_{t+1}$ intervenant dans chaque mot de poids minimal en $f'_k(x)=f_k(x_1,\ldots,x_{i-1},x_i+ax_j,x_{i+1}\ldots,x_m)$ et les f'_k sont encore linéairement indépendantes.
D'autre part, pour tout $a \in \mathbb{F}_q^*$,

$$x_1^{k_1}\ldots(x_i+ax_j)^{k_i}\ldots x_m^{k_m}=\sum_{l=0}^{k_i}\binom{k_i}{l}x_i^{k_i-l}a^l x_j^{k_j+l}\prod_{u\neq i,j}x_u^{k_u}.$$

Comme les monômes de degré inférieur ou égal à $r-1$ et $x_1^{k_1}\ldots x_m^{k_m}$ sont combinaisons linéaires de mots de poids minimal,

$$\sum_{l=1}^{\min(k_i,p-1-k_j)}\binom{k_i}{l}x_i^{k_i-l}a^l x_j^{k_j+l}\prod_{u\neq i,j}x_u^{k_u}$$

est combinaison linéaire de mots de poids minimal. On pose $n=\min(k_i,p-1-k_j)\leq p-1$. Soit $a_1,\ldots,a_n$ n éléments de $\mathbb{F}_q^*$ distincts. On a

$$\begin{pmatrix}M_1\\ \vdots\\ M_n\end{pmatrix}=\begin{pmatrix}a_1 & \ldots & a_1^n\\ \vdots & & \vdots\\ a_n & \ldots & a_n^n\end{pmatrix}\begin{pmatrix}\binom{k_i}{1}x_i^{k_i-1}x_j^{k_j+1}\prod_{u\neq i,j}x_u^{k_u}\\ \vdots\\ \binom{k_i}{n}x_i^{k_i-n}x_j^{k_j+n}\prod_{u\neq i,j}x_u^{k_u}\end{pmatrix}$$

où les M_i sont des combinaisons linéaires de mots de $R_p(r,m)$ de poids minimal. Comme les a_i sont tous distincts et non nuls, la matrice de Vandermonde est inversible. Comme de plus tous les coefficients binomiaux $\binom{k_i}{l}$ sont non nuls puisque $k_i \leq p-1$, on peut exprimer tous les monômes du type $x_i^{k_i-l}x_j^{k_j+l}\prod_{u\neq i,j} x_u^{k_u}$ comme combinaison linéaire de mots de poids minimal.
En prenant $f_i(x) = x_i$, on obtient que $x_1^{p-1}\dots x_t^{p-1}x_{t+1}^s$ est combinaison linéaire de mots de poids minimal. Ensuite, en appliquant plusieurs fois le procédé ci-dessus, on obtient que tous les monômes de degré r sont combinaisons linéaires de mots de poids minimal. □

Ce résultat devient faux en général dès que q n'est pas premier. Par exemple pour $q = p^e$, $e \geq 2$, $R_q(p,m)$ n'est pas engendré par ses mots de poids minimal. En effet, comme $q \neq p$, $p \leq q-2$ et donc les mots de poids minimal sont de la forme

$$\prod_{i=1}^{p}(\sum_{k=1}^{m} a_k x_k + b_i) = \sum_{k=1}^{m} a_k^p x_k^p + g$$

où g est un polynôme de degré inférieur ou égal à $p-1$. Donc tous les monômes de degré p de type $x_{i_1}\dots x_{i_p}$ avec au moins deux i_j distincts n'apparaissent dans aucun mot de poids minimal et ne peuvent donc pas s'écrire comme combinaison linéaire de mots de poids minimal.

En fait, Ding et Key démontrent le résultat plus précis suivant dans [DK00] :

Théorème 1.3.9. *Soit $m \geq 1$, $0 \leq r \leq m(q-1)$. Le code de Reed-Muller généralisé $R_q(r,m)$ est engendré par ses mots de poids minimal si $m = 1$ ou $q = p$ ou $r < p$ ou $r > (m-1)(q-1) + p^{e-1} - 2$ ($q = p^e$).*

1.4 Groupe des automorphismes

On a démontré dans la première partie de ce chapitre que le groupe des automorphismes des codes de Reed-Muller généralisés contenait le groupe affine (proposition 1.2.4). On a de plus le résultat plus fort suivant :

Théorème 1.4.1. *Soit $0 \leq r \leq m(q-1)$.*

- *Si $r = 0$, $r = m(q-1)$ ou $r = m(q-1)-1$, on a $\mathrm{Aut}(R_q(r,m)) = \mathcal{S}_{q^m}$.*
- *Si $1 \leq r \leq m(q-1)-2$, $\mathrm{Aut}(R_q(r,m)) = \mathrm{GA}_m(\mathbb{F}_q)$.*

Encore une fois, on va prouver le théorème en deux temps : le cas $q = 2$ (voir [MS77b]) puis le cas $q \neq 2$ (voir [BC93]). Dans les deux cas, on montre que σ, un automorphisme des codes de Reed-Muller généralisés est une bijection qui conserve les sous-espaces affines. Cependant dans le cas $q = 2$, on en déduit immédiatement que σ est une application affine alors que dans le cas $q \neq 2$, on obtient seulement que σ est semi-affine et il faut un travail supplémentaire pour obtenir le théorème.

1.4.1 Preuve du théorème 1.4.1 dans le cas $q = 2$

- Si $r = 0$, $r = m$ ou $r = m-1$, $R(0,m) = \{(1,\dots,1),(0,\dots,0)\}$, $R(m,m) = \mathbb{F}_2^{2^m}$ et $R(m-1,m)$ est l'ensemble des mots de poids pair donc ces codes sont inchangés par permutation de coordonnées.

- Si $1 \leq r \leq m-2$. On a déjà montré que $\mathrm{GA}_m(\mathbb{F}_q) \subset \mathrm{Aut}(R(r,m))$ (proposition 1.2.4). On commence par montrer le cas $r = m-2$. Un mot de poids minimal de $R(m-2,m)$ est envoyé sur un mot de poids minimal. Or on a vu dans le théorème 1.3.5 que les mots de poids minimal de $R(m-2,m)$ sont des plans affines donc les éléments de $\mathrm{Aut}(R(m-2,m))$ sont des bijections qui envoient un plan sur un plan. Soit f une bijection de $\mathbb{F}_2^m$ dans $\mathbb{F}_2^m$ qui envoie un plan affine sur un plan affine. Soit O un point de $\mathbb{F}_2^m$, soit $\overrightarrow{a}$, $\overrightarrow{b}$ deux vecteurs de $\mathbb{F}_2^m$. On note $\overrightarrow{c} = \overrightarrow{a} + \overrightarrow{b}$. Alors $\{O, O+\overrightarrow{a}, O+\overrightarrow{b}, O+\overrightarrow{c}\}$ est un plan affine. Comme f est une bijection qui envoie un plan affine sur un plan affine, $\{f(O), f(O+\overrightarrow{a}), f(O+\overrightarrow{b}), f(O+\overrightarrow{c})\}$ est aussi un plan affine et donc $\overrightarrow{f(O)f(O+\overrightarrow{c})} = \overrightarrow{f(O)f(O+\overrightarrow{a})} + \overrightarrow{f(O)f(O+\overrightarrow{b})}$. Donc f est une application affine.
  Si $r < m-2$, tous les automorphismes de $R(r,m)$ envoient un mot de poids minimal sur un mot de poids minimal donc un sous-espace affine de codimension r sur un sous espace-affine de codimension r. Comme tout plan affine peut s'écrire comme intersection de sous-espaces affines de codimension r par le cas $r = m-2$, on a le résultat.

1.4.2 Preuve du théorème 1.4.1 dans le cas $q \neq 2$

Si $r = 0$, $r = m(q-1)$ ou $r = m(q-1)-1$ alors $R_q(0,m) = \{(\alpha,\ldots,\alpha) : \alpha \in \mathbb{F}_q\}$, $R_q(m(q-1),m) = \mathbb{F}_q^m$ et par la proposition 1.2.3, $R_q(m(q-1)-1,m)$ est l'ensemble des mots f tels que $\sum_{x\in\mathbb{F}_q^m} f(x) = 0$. Ces trois ensembles sont donc invariants par permutation de coordonnées.

Soit $1 \leq r \leq m(q-1)-2$. On note $G_{q,r}$ le groupe de Galois de $\mathbb{F}_{q^r}$ sur $\mathbb{F}_q$. On rappelle que $G_{q,r} = \{\varphi_q^i : 1 \leq i \leq r\}$ où φ_q est l'automorphisme de Frobenius défini par $\varphi_q(x) = x^q$.

Définition 1.4.2. Soit V et V' deux espaces vectoriels sur $\mathbb{F}_q$. Une application $f : V \to V'$ est semi-linéaire s'il existe $\sigma \in G_{p,e}$ $(q = p^e)$ tel que pour tout x, $y \in V$ et pour tout λ, $\nu \in \mathbb{F}_q$ on ait :

$$f(\lambda x + \nu y) = \sigma(\lambda)f(x) + \sigma(\nu)f(y).$$

Définition 1.4.3. Soit A et A' deux espaces affines sur $\mathbb{F}_q$. On dit qu'une application $f : A \to A'$ est semi-affine s'il existe $a \in A$ tel que l'application suivante soit semi-linéaire

$$\overrightarrow{f} : \begin{array}{ccc} A_a := \{\overrightarrow{ax} : x \in A\} & \to & A'_{f(a)} \\ \overrightarrow{ax} & \mapsto & \overrightarrow{f(a)f(x)} \end{array}.$$

Le théorème suivant est démontré dans [Ber77] :

Théorème 1.4.4. *Soit A et A' deux espaces affines sur $\mathbb{F}_q$, $q \neq 2$ de même dimension $d \geq 2$. Soit $F : A \to A'$ une bijection qui envoie trois points alignés de A sur trois points alignés de A'. Alors f est semi-affine.*

Si on arrive à démontrer qu'un automorphisme σ de $R_q(r,m)$ conserve les droites affines alors par le théorème de Berger, on aura montré que σ est semi-affine. La proposition et le lemme suivants permettent de démontrer que σ est en fait affine.

L'automorphisme de Frobenius φ_p est un automorphisme de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_p$. En identifiant $\mathbb{F}_q^m$ et $\mathbb{F}_{q^m}$, φ_p réalise une permutation de coordonnées sur $R_q(r,m)$. Étudions plus en

détail l'action de φ_p sur $\mathbb{F}_q^m$. Soit ω un élément primitif de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$. Alors l'application suivante est un isomorphisme :

$$\begin{array}{ccc} \mathbb{F}_q^m & \to & \mathbb{F}_{q^m} \\ (x_1,\ldots,x_m) & \mapsto & x_1+x_2\omega+\ldots+x_m\omega^{m-1} \end{array}.$$

Donc $\varphi_p^i(x_1,\ldots,x_m) = x_1^{p^i} + x_2^{p^i}\omega^{p^i} + \ldots + x_m^{p^i}\omega^{(m-1)p^i}$. Or $(\omega^{p^i l})_{0\leq l\leq m-1}$ est aussi une base de $\mathbb{F}_q^m$ sur $\mathbb{F}_q$ donc il existe $A_i = (a_{l,k}^{(i)}) \in \mathrm{GL}_m(\mathbb{F}_q)$ qui envoie $(\omega^l)_{0\leq l\leq m-1}$ sur $(\omega^{p^i l})_{0\leq l\leq m-1}$. On en déduit que $\varphi_p^i(x_1,\ldots,x_m) = \sum_{k=1}^{m}\omega^{k-1}(\sum_{l=1}^{m} a_{l,k}^{(i)}x_l^{p^i}) = ((x_1,\ldots,x_m)A_i^*)^{p^i}$ où les coefficients de la matrice A_i^* sont les coefficients de A_i élevés à la puissance p^{e-i}. D'où, pour $f \in R_q(r,m)$, $\varphi_p^i.f = (A_i^*.f^{(i)})^{p^i}$ où $f^{(i)}$ est l'élément de $R_q(r,m)$ dont les coefficients sont les coefficients de f à la puissance p^{e-i}.

Proposition 1.4.5. *Le groupe des applications semi-affines bijectives sur le $\mathbb{F}_q$-espace affine $\mathbb{F}_q^m$ est*

$$\mathrm{GSA}_m(\mathbb{F}_q) = \{\varphi_p^i \circ h + b : 1 \leq i \leq e, h \in \mathrm{GL}_m(\mathbb{F}_q), b \in \mathbb{F}_q^m\}.$$

Démonstration. Si h est une application linéaire bijective alors $\varphi_p^i \circ h$ est une application semi-linéaire bijective d'automorphisme associé φ_p^i.
Réciproquement soit f une application semi-linéaire d'automorphisme associé φ_p^i. Alors $\varphi_p^{-i} \circ f$ est une application linéaire. □

Lemme 1.4.6. *Pour $1 \leq r \leq m(q-1)-2$, on a*

$$\mathrm{Aut}(R_q(r,m)) \cap G_{p,e} = \{\mathrm{Id}\}.$$

Démonstration. Par la proposition 1.1.17 et le théorème 1.2.15, on a

$$\mathrm{Aut}(R_q(r,m)) = \mathrm{Aut}(R_q(m-1-r,m)).$$

Il suffit donc de considérer le cas où $r \leq \frac{m(q-1)-1}{2}$. Supposons que pour $1 \leq i \leq \lfloor \frac{e}{2} \rfloor$, $\varphi_p^i \notin \mathrm{Aut}(R_q(r,m))$. Soit $\lfloor \frac{e}{2} \rfloor < j \leq e-1$. Alors $1 \leq e-j \leq \lfloor \frac{e}{2} \rfloor$ et

$$\varphi_p^j = (\varphi_p^{e-j})^{-1} \notin \mathrm{Aut}(R_q(r,m)).$$

Il suffit donc de montrer que pour tout $1 \leq i \leq \lfloor \frac{e}{2} \rfloor$, $\varphi_p^i \notin \mathrm{Aut}(R_q(r,m))$. On montre ce résultat par récurrence sur r.
Soit $f \in R_q(1,m)$. Comme $\mathrm{GA}_m(\mathbb{F}_q) \subset \mathrm{Aut}(R_q(1,m))$, $g_i = A_i^*.f^{(i)} \in R_q(1,m)$. On a donc pour tout $1 \leq i \leq \lfloor \frac{e}{2} \rfloor$,

$$\varphi_p^i.f = g_i^{p^i} \notin R_q(1,m).$$

Soit $2 \leq r \leq \frac{m(q-1)-1}{2}$. Supposons que pour tout $1 \leq i \leq \lfloor \frac{e}{2} \rfloor$, $\varphi_p^i \notin \mathrm{Aut}(R_q(r-1,m))$. Soit $1 \leq i \leq \lfloor \frac{e}{2} \rfloor$. Il existe $f \in R_q(r-1,m)$ tel que $\varphi_p^i.f \notin R_q(r-1,m)$. Si $\varphi_p^i.f \notin R_q(r,m)$, on a le résultat. Supposons que $\varphi_p^i.f \in R_q(r,m) \setminus R_q(r-1,m)$. Comme $\mathrm{GA}_m(\mathbb{F}_q) \subset R_q(r,m)$, $g_i = A_i^*.f^{(i)} \in R_q(r-1,m)$. On écrit $g_i(x) = \sum_{\substack{\alpha\in\{0,\ldots,q-1\}^m \\ \alpha_1+\ldots+\alpha_m\leq r-1}} a_\alpha x^\alpha$. Soit $\beta \in \{0,\ldots,q-1\}^m$

tel que la forme réduite de $x^{\beta p^i}$ soit de degré r et $a_\beta \neq 0$. Il existe alors $1 \leq k \leq m$ tel que le degré en x_k de la forme réduite de $x^{\beta p^i}$ soit strictement plus petit que $q - p^i$. En effet, on aurait sinon $\frac{m(q-1)}{2} > r \geq m(q-p^i)$ et donc $2p^i - q - 1 > 0$ ce qui est impossible puisque $i \leq \lfloor \frac{e}{2} \rfloor$. On considère $f' \in R_q(r,m)$ tel que

$$A_i^*.f'^{(i)} = g_i'(x) = \sum_{\substack{\alpha \in \{0,\dots,q-1\}^m \\ \alpha_1+\dots+\alpha_m \leq r-1 \\ \alpha \neq \beta}} a_\alpha x^\alpha + a_\beta x_1^{\beta_1} \dots x_{k-1}^{\beta_{k-1}} x_k^{\beta_k+1} x_{k+1}^{\beta_{k+1}} \dots x_m^{\beta_m} \in R_q(r,m).$$

On a $\deg(\varphi_p^i.f') = r + p^i$ donc $\varphi_p^i.f' \notin R_q(r,m)$. □

Comme le groupe affine est inclus dans le groupe des automorphismes de $R_q(r,m)$, on en déduit que

$$\mathrm{Aut}(R_q(r,m)) \cap \mathrm{GSA}_m(\mathbb{F}_q) = \mathrm{GA}_m(\mathbb{F}_q).$$

Il ne reste donc plus qu'à prouver que tout élément du groupe des automorphismes conserve les droites.

Soit σ un automorphisme de $R_q(r,m)$. On écrit $r = t(q-1) + s$ avec $0 \leq s \leq q-2$. Si $s = q-2$, $0 \leq t \leq m-2$, alors $m(q-1) - r - 1 = (m-t-1)(q-1)$ et si $1 \leq s \leq q-3$, $t = 0$ alors $m(q-1) - r - 1 = (m-1)(q-1) + q - 2 - s$. Donc par la proposition 1.1.17 et le théorème 1.2.15, il suffit de considérer les deux cas suivants :

- Cas 1 : $s = 0$, $1 \leq t \leq m-1$.
  Un mot de poids minimal de $R_q(r,m)$ est envoyé par σ sur un mot de poids minimal. Or les mots de poids minimal de $R_q(r,m)$ sont les mots dont le support est un sous-espace affine de $\mathbb{F}_q^m$ de codimension t. Comme toute droite peut s'écrire comme intersection de sous-espaces de codimension t, on a le résultat.

- Cas 2 : $1 \leq s \leq q-3$, $1 \leq t \leq m-1$.
  Les mots de poids minimal de $R_q(r,m)$ sont les mots dont le support est l'union de $(q-s)$ sous-espaces affines parallèles de codimension $t+1$ inclus dans un sous-espace affine de codimension t. Comme $s \leq q-3$, il existe deux mots distincts c, c' de $R_q(r,m)$ de poids minimal tels que

  $$\#(\mathrm{Supp}(c) \cap \mathrm{Supp}(c')) \geq 2q^{m-t-1}.$$

  Comme σ conserve les mots de poids minimal, $\sigma.c$ et $\sigma.c'$ sont aussi des mots de poids minimal de $R_q(r,m)$. Soit alors W et W' les deux sous-espaces affines de codimension t contenant respectivement les supports de $\sigma.c$ et $\sigma.c'$. On a

  $$\begin{aligned} q^{m-t} &\geq \#(W \cap W') \\ &\geq \#(\sigma(\mathrm{Supp}(c)) \cap \sigma(\mathrm{Supp}(c')) \\ &= \#(\sigma(\mathrm{Supp}(c) \cap \mathrm{Supp}(c'))) \\ &= \#(\mathrm{Supp}(c) \cap \mathrm{Supp}(c')) \geq 2q^{m-1-t}. \end{aligned}$$

  Donc $W = W'$.
  Soit A un sous-espace affine de codimension t de $\mathbb{F}_q^m$. On considère une suite $(c_k)_{1 \leq k \leq b}$ de mots de $R_q(r,m)$ de poids minimal tels que :

  1. $\bigcup_{k=1}^{b} \mathrm{Supp}(c_k) = A$,

2. pour tout $2 \leq k \leq b$, $\#(\mathrm{Supp}(c_{k-1}) \cap \mathrm{Supp}(c_k)) \geq 2q^{m-t-1}$.

Comme $\sigma.c_k$ est aussi un mot de poids minimal, $\sigma(\mathrm{Supp}(c_k))$ est inclus dans un sous-espace affine W_k de $\mathbb{F}_q^m$ de codimension t. Alors, par la propriété (2) de la suite (c_k) et ce qui précède on a $W_1 = \ldots = W_b = W$. D'où, par la propriété (1), $\sigma(A) = W$ et σ conserve les sous-espaces affines de codimension t donc les droites affines.

Ce chapitre contient surtout des rappels sur les codes de Reed-Muller généralisés. Cependant, nous donnons une nouvelle preuve d'un théorème de Delsarte, Goethals et Mac Williams [DGM70] sur les mots de poids minimal des codes de Reed-Muller généralisés que nous espérons plus simple.

Chapitre 2

Rayon de recouvrement

Dans ce chapitre, on étend des résultats sur le rayon de recouvrement des codes de Reed-Muller d'ordre 1 au rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1. On connait sa valeur exacte pour les codes en un nombre pair de variables et pour $1, 3, 5, 7$ variables. Pour un nombre impair de variables $m \geq 9$, on en connait seulement un encadrement (voir [HKM78]). Ici, on se propose de donner un encadrement pour le rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1. On en déduit le rayon de recouvrement pour un nombre pair de variables. De plus, pour $q = 3$, on donne les valeurs de $\rho(1, 3)$ et $\rho(1, 5)$ (voir [Led11]).

2.1 Notations

Pour tout q, on note $\rho(1, m)$ le rayon de recouvrement du code de Reed-Muller généralisé en m variables d'ordre 1.

Dans la suite on va aussi s'intéresser aux rayons de recouvrement partiels des codes de Reed-Muller généralisés d'ordre 1, c'est-à-dire au rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1 dans les codes de Reed-Muller généralisés d'ordre r :

$$\rho_r(1, m) := \max_{x \in R_q(r,m)} \min_{c \in R_q(1,m)} |x - c|.$$

2.2 Rappels sur les formes quadratiques en toute caractéristique

On trouve les résultats de cette section dans [Hir98].

2.2.1 Définitions

On trouve les définitions suivantes dans [Die71].

Définition 2.2.1. On dit qu'une application de $\mathbb{F}_q^n$ dans $\mathbb{F}_q$ est une forme quadratique si

1. pour $a \in \mathbb{F}_q$ et $x \in \mathbb{F}_q^n$, $Q(ax) = a^2 Q(x)$,
2. l'application $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ tel que $\phi(x, y) = Q(x + y) - Q(x) - Q(y)$ est une forme bilinéaire.

ϕ est appelée la forme bilinéaire associée à Q.

Définition 2.2.2. On appelle rang d'une forme bilinéaire ϕ sur $\mathbb{F}_q^n \times \mathbb{F}_q^n$, le rang de l'application suivante :

$$\psi_\phi : \begin{array}{ccc} \mathbb{F}_q^n & \to & \mathbb{F}_q^{n*} \\ x & \mapsto & (y \mapsto \phi(x,y)) \end{array}.$$

Soit Q une forme quadratique sur $\mathbb{F}_q^n$ et ϕ la forme bilinéaire associée. On définit l'espace vectoriel

$$V := \{x \in \mathrm{Ker}(\psi_\phi) : Q(x) = 0\}.$$

Si $v = \dim(V) \leq n - \mathrm{Rg}(\phi)$, alors le rang de Q est $\mathrm{Rg}(Q) := n - v$. On dit que Q est non dégénérée si $v = 0$.

Remarque 2.2.3. Si q est impair, $v = n - \mathrm{Rg}(\phi)$ et $\mathrm{Rg}(\phi) = \mathrm{Rg}(Q)$.

Remarque 2.2.4. La définition de forme quadratique non dégénérée en caractéristique 2 dépend des auteurs. Par exemple, en utilisant la définition de [Bou07], la forme quadratique sur $\mathbb{F}_2$ $x \mapsto x^2$ est dégénérée, ce qui n'est pas la cas avec la définition que nous avons prise.

2.2.2 Un théorème de réduction

Théorème 2.2.5. *Soit Q une forme quadratique de rang R sur $\mathbb{F}_q^n$. Il existe une base $(e_i)_{1\leq i\leq n}$ de $\mathbb{F}_q^n$ telle que :*

- *Si $R = 2s+1$, $Q(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{s} x_{2i-1}x_{2i} + ax_{2s+1}^2$ (1)*
- *Si $R = 2s$, $Q(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{s} x_{2i-1}x_{2i}$ (2)*
  ou $Q(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{s-1} x_{2i-1}x_{2i} + ax_{2s-1}^2 + bx_{2s}^2 + cx_{2s-1}x_{2s}$ où ax^2+cx+b est irréductible sur $\mathbb{F}_q$ (3).

Démonstration. Soit ϕ la forme bilinéaire associée à Q. On note

$$N = \{x : \forall y \in \mathbb{F}_q^n, \phi(x,y) = 0\}.$$

Soit S un sous-espace supplémentaire de N dans $\mathbb{F}_q^n$. On définit alors

$$V_0 = \{x \in N : Q(x) = 0\}.$$

Soit V_1 un sous espace supplémentaire à V_0 dans N. Alors la restriction de Q à $V_1 \oplus S$ est non dégénérée et il existe une base $(\varepsilon_i)_{1\leq i\leq R}$ que l'on complète en une base $(\varepsilon_i)_{1\leq i\leq n}$ de $\mathbb{F}_q^n$ telle que $Q(\sum_{i=1}^{n} x_i\varepsilon_i) = \sum_{1\leq i\leq j\leq R} a_{i,j}x_ix_j$.
Si $R = 1$, on peut ramener Q à ax_1^2.

Si $R = 2$, on peut écrire Q sous la forme $ax_1^2 + bx_2^2 + cx_1x_2$. Si $ax^2 + cx + b$ est irréductible, on a le résultat. Sinon, si α et β sont les racines de $ax^2 + cx + b$ alors $ax_1^2 + bx_2^2 + cx_1x_2 = a(x_1 - \beta x_2)(x_1 - \alpha x_2)$ et on a aussi le résultat.

Si $R \geq 3$,

- 1er cas : q est pair.
  Si quelque soit i, j tels que $i \neq j$, $a_{i,j} = 0$ alors

$$Q = (\sqrt{a_{1,1}}x_1 + \ldots + \sqrt{a_{R,R}}x_R)^2$$

  ce qui est impossible car $R \geq 3$. Quitte à réordonner, on peut supposer que $a_{2,3} \neq 0$. On veut se ramener au cas où $a_{1,1} = 0$. Supposons que $a_{1,1} \neq 0$ et supposons de plus que $a_{2,2} \neq 0$. Sinon en posant $y_1 = x_2$, $y_2 = x_1$ et $y_i = x_i$ pour $i \geq 3$, on se ramène au cas où $a_{1,1} = 0$. On a alors

$$Q = a_{2,2}x_2^2 + x_2(a_{1,2}x_1 + a_{2,3}x_3 + \ldots + a_{2,R}x_R) + G(x_1, x_3, \ldots, x_R).$$

  On pose $y_3 = a_{1,2}x_1 + a_{2,3}x_3 + \ldots + a_{2,R}x_R$ et $y_i = x_i$ pour $i \neq 3$ et on a

$$Q = a_{2,2}y_2^2 + y_2y_3 + G_1(y_1, y_3, \ldots, y_R).$$

  Soit $t \in \mathbb{F}_q$ et $\beta = G_1(1, 0, \ldots, 0)$, on pose $z_2 = y_2 + ty_1$ et $z_i = y_i$, pour $i \neq 2$. En remplaçant dans Q, on obtient que le coefficient de z_1^2 dans Q est $a_{2,2}t^2 + \beta$. En choisissant t tel que $a_{2,2}t^2 + \beta = 0$, on est bien ramené au cas où $a_{1,1} = 0$.
  Comme Q est de rang R, il existe $1 \leq j \leq R$ tel que $a_{1,j} \neq 0$. Quitte à faire une permutation, on peut supposer $a_{1,2} \neq 0$. On pose $y_2 = a_{1,2}x_2 + \ldots + a_{1,R}x_R$ et $y_i = x_i$ pour $i \neq 2$ et alors $Q = y_1y_2 + \sum_{2 \leq i \leq j \leq R} b_{i,j}y_iy_j$.
  Soit maintenant $z_1 = y_1 + b_{2,2}y_2 + b_{2,3}y_3 + \ldots + b_{2,R}y_R$ et $z_i = y_i$ pour $i \neq 1$. On a $Q = z_1z_2 + \sum_{3 \leq i \leq j \leq R} b_{i,j}z_iz_j$. En itérant, on a $Q = x_1x_2 + \ldots + x_{2s-1}x_{2s} + ax_{2s+1}^2$ si $R = 2s + 1$ ou $Q = x_1x_2 + \ldots + x_{2s-3}x_{2s-2} + f(x_{2s-1}, x_{2s})$ si $R = 2s$. Comme f est une forme quadratique de rang 2, si elle se factorise, $Q = x_1x_2 + \ldots + x_{2s-1}x_{2s}$. Sinon $Q = x_1x_2 + \ldots + x_{2s-3}x_{2s-2} + ax_{2s-1}^2 + bx_{2s}^2 + cx_{2s-1}x_{2s}$ avec $ax^2 + cx + b$ irréductible.

- 2ème cas : q est impair.
  Par Gauss, on peut écrire $Q = a_1x_1^2 + \ldots + a_Rx_R^2$. Quitte à changer l'ordre, on peut supposer que $a_1, \ldots a_t$ sont des carrés dans $\mathbb{F}_q$ et que $a_{t+1}, \ldots a_R$ ne le sont pas. On peut alors écrire $Q = x_1^2 + \ldots x_t^2 + \mu(x_{t+1}^2 + \ldots + x_R^2)$ où μ n'est pas carré dans $\mathbb{F}_q$. Comme μ n'est pas carré, il existe c, d dans $\mathbb{F}_q$ tel que $\mu = c^2 + d^2$. Si $R - t \geq 2$, on pose $y_{t+1} = cx_{t+1} - dx_{t+2}$ et $y_{t+2} = dx_{t+1} + cx_{t+2}$, alors

$$y_{t+1}^2 + y_{t+2}^2 = (c^2 + d^2)(x_{t+1}^2 + x_{t+2}^2).$$

  En itérant, on obtient que $Q = x_1^2 + \ldots + x_R^2$ ou $Q = x_1^2 + \ldots x_{R-1}^2 + \mu x_R^2$.
  Supposons que Q peut s'écrire sous la forme $x_1^2 + \ldots + x_R^2$. Il existe c, d dans $\mathbb{F}_q$ tel que $-1 = c^2 + d^2$. On pose alors $y_{2i-2} = cy_{2i-2} + dy_{2i}$, $x_{2i} = dy_{2i-2} - cy_{2i}$ et $x_{2i+1} = y_{2i+1}$ et on obtient $x_{2i-2}^2 + x_{2i}^2 = (c^2 + d^2)(y_{2i-2}^2 + y_{2i}^2) = -y_{2i-2}^2 - y_{2i}^2$. Alors, si R est impair,

$$\begin{aligned} Q &= y_1^2 - y_2^2 + \ldots + y_{R-2}^2 - y_{R-1}^2 + y_R^2 \\ &= (y_1 + y_2)(y_1 - y_2) + \ldots + (y_{R-2} + y_{R-1})(y_{R-2} - y_{R-1}) + y_R^2. \end{aligned}$$

  Si R est pair, on a

$$Q = y_1^2 - y_2^2 + \ldots + y_{R-1}^2 - y_R^2 = (y_1 + y_2)(y_1 - y_2) + \ldots + (y_{R-1} + y_R)(y_{R-1} - y_R).$$

Si Q peut s'écrire sous la forme $x_1^2+\ldots x_{R-1}^2+\mu x_R^2$ alors, en utilisant le cas précédent, si R est impair, on peut écrire $Q = x_1x_2 + \ldots + x_{R-2}x_{R-1} + \mu x_R^2$, ce qui démontre le théorème dans ce cas.
Si R est pair, on peut écrire $Q = x_1x_2 + \ldots + x_{R-3}x_{R-2} + x_{R-1}^2 + \mu x_R^2$. Si -1 n'est pas carré dans $\mathbb{F}_q$, $-\mu$ est un carré dans $\mathbb{F}_q$ et on a

$$Q = x_1x_2 + \ldots + x_{R-3}x_{R-2} + (x_{R-1} + \sqrt{-\mu}x_R)(x_{R-1} - \sqrt{-\mu}x_R).$$

Si -1 est un carré alors $-\mu$ n'est pas carré et alors $x^2 + \mu$ est irréductible.

□

2.2.3 Zéros d'une forme quadratique

Théorème 2.2.6. *Soit Q une forme quadratique sur $\mathbb{F}_q$ en n variables de rang R, alors le nombre de zéros de Q est*

$$N(Q) = q^{n-1} + (\omega - 1)(q-1)q^{n-\frac{R}{2}-1}$$

où

$$\omega = \begin{cases} 1 & \textit{si } R \textit{ est impair} \\ 0 & \textit{si } R \textit{ est pair et si } Q(Px) = x_1x_2 + \ldots + x_{R-3}x_{R-2} + ax_{R-1}^2 + bx_R^2 + cx_{R-1}x_R \\ & \textit{avec } ax^2 + cx + b \textit{ irréductible} \\ 2 & \textit{si } R \textit{ est pair et si } Q(Px) = x_1x_2 + \ldots + x_{R-1}x_R \end{cases}$$

Démonstration.

- Si $R = 0$, il y a q^n zéros et on a bien le résultat.
- Si $R = 1$, Q peut s'écrire sous la forme ax_1^2 ; on a donc q^{n-1} zéros.
- Si $R = 2$, Q peut s'écrire sous la forme $ax_1^2+bx_2^2+cx_1x_2$. Si ax^2+cx+b est irréductible, on est dans le cas (2) du théorème 2.2.5 et on a $q^{n-2} = q^{n-1} - (q-1)q^{n-\frac{2}{2}-1}$ zéros. Sinon, on peut factoriser Q, on est alors dans le cas (3) et le nombre s de zéros est $(2q-1)q^{n-2} = q^{n-1} + (q-1)q^{n-\frac{2}{2}-1}$.
- Si $R \geq 3$, par le théorème 2.2.5, Q peut se ramener à une forme quadratique de la forme $x_1x_2 + Q^{(1)}(x_3, \ldots, x_n)$ où $Q^{(1)}$ est une forme quadratique de rang $R-2$. Si $Q^{(1)}(a_3, \ldots, a_n) = 0$, on a $(2q-1)$ couples (x_1, x_2) tels que $Q(x_1, x_2, a_3, \ldots, a_n) = 0$. Sinon, on a $(q-1)$ couples (x_1, x_2) tels que $Q(x_1, x_2, a_3, \ldots, a_n) = 0$. D'où

  $$N(Q) = (2q-1)N(Q^{(1)}) + (q-1)(q^{n-2} - N(Q^{(1)})) = qN(Q^{(1)}) + (q-1)q^{n-2}.$$

  En itérant, on a pour r tel que $R - 2r \geq 1$,

  $$\begin{aligned} N(Q) &= q^rN(Q^{(r)}) + (q-1)(q^{n-2} + q^{n-3} + \ldots + q^{n-(r+1)}) \\ &= q^rN(Q^{(r)}) + q^{n-1} - q^{n-(r+1)} \end{aligned}$$

  où $Q^{(r)}$ est une forme quadratique en $x_{2r+1}, \ldots, x_n$ de rang $R - 2r$.
  Si R est impair, on pose $R = 2s + 1$. En appliquant ce qui précède avec $r = s$, on a $Q^{(s)}$ qui est une forme quadratique en $n - 2s$ variables de rang 1 et donc $N(Q) = q^sq^{n-2s-1} + q^{n-1} - q^{n-s-1} = q^{n-1}$ ce qui démontre le théorème quand R est impair.
  Si R est pair, $R = 2s$ et on prend $r = s - 1$. Alors $Q^{(s-1)}$ est une forme quadratique

en $n-2s+2$ variables de rang 2. Si Q est de type (2), $Q^{(s-1)}$ ne se factorise pas et a q^{n-2s} zéros. On obtient $N(Q) = q^{s-1}q^{n-2s} + q^{n-1} - q^{n-s} = q^{n-1} - (q-1)q^{n-s-1}$. Si Q est de type (3), $Q^{(s-1)}$ se factorise et a $(2q-1)q^{n-2s}$ zéros. On obtient

$$N(Q) = q^{s-1}(2q-1)q^{n-2s} + q^{n-1} - q^{n-s} = q^{n-1} + (q-1)q^{n-s-1}$$

ce qui donne le résultat pour R pair.

□

2.3 Rayon de recouvrement des codes de Reed-Muller d'ordre 1

On commence par s'intéresser au rayon de recouvrement des codes de Reed-Muller d'ordre 1 (c'est-à-dire pour $q = 2$). On considère ce cas à part car même si les méthodes de démonstration utilisées pour les codes de Reed-Muller généralisés restent valables (voir [HKM78]), il existe dans ce cas d'autres méthodes basées sur la transformée de Hadamard (voir [CH10, Lan91b, Hou93]).

Définition 2.3.1. Soit $f \in B_m^2$. On définit la transformée de Hadamard de f comme suit :

$$\forall a \in \mathbb{F}_2^m, \quad \widehat{f}(a) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)+<a,x>}$$

où $< a, x >= \sum_{i=1}^{m} a_i x_i$.

Remarque 2.3.2. Pour $f \in B_m^2$, $\widehat{f}$ est la transformée de Fourier de $(-1)^f$.

Soit $f \in B_m^2$ et $\alpha \in R(1,m)$. On écrit α sous la forme $\alpha(x) =< a, x > +b$ où $a \in \mathbb{F}_2^m$ et $b \in \mathbb{F}_2$. On peut interpréter le poids de $f + \alpha$ à l'aide de la transformée de Hadamard :

$$|f+\alpha| = 2^{m-1} - \frac{1}{2} \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)+<a,x>+b} = 2^{m-1} - \frac{1}{2}(-1)^b \widehat{f}(a).$$

On en déduit :

$$d(f, R(1,m)) = 2^{m-1} - \frac{1}{2} \sup_{a \in \mathbb{F}_2^m} |\widehat{f}(a)|.$$

En utilisant la formule de Parseval (Plancherel), on peut maintenant donner un majorant du rayon de recouvrement :

Théorème 2.3.3. *Pour tout m, $\rho(1,m) \leq 2^{m-1} - 2^{\frac{m}{2}-1}$.*

Démonstration. Par la formule de Plancherel,

$$2^{2m} = 2^m \sum_{x \in \mathbb{F}_2^m} (-1)^{2f(x)} = \sum_{a \in \mathbb{F}_2^m} (\widehat{f}(a))^2.$$

Donc $\sup_{a \in \mathbb{F}_2^m} |\widehat{f}(a)| \geq 2^{\frac{m}{2}}$ d'où pour tout $f \in B_m^2$

$$d(f, R(1,m)) \leq 2^{m-1} - 2^{\frac{m}{2}-1}$$

ce qui donne le résultat. □

On va maintenant calculer $\rho_2(1,m)$.

Théorème 2.3.4. *Pour tout m, $\rho_2(1,m) = 2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1}$.*

Pour démontrer ce théorème, on calcule la transformée de Fourier d'une forme quadratique. Voici une idée de la preuve.

Démonstration. Soit Q une forme quadratique sur $\mathbb{F}_2^m$ dont on note B la forme bilinéaire associée et $N = \{x \in \mathbb{F}_2^m : \forall y \in \mathbb{F}_{2^m}, B(x,y) = 0\}$. On note k la dimension de N. On démontre à l'aide des relations d'orthogonalité des caractères le résultat suivant (voir [Lan91a]) :

- Si $Q(x) = 0$ pour tout $x \in N$, alors

$$\widehat{Q}(a) = \begin{cases} \pm 2^{\frac{m+k}{2}} & \text{si } < a, x >= 0 \text{ pour tout } x \in N \\ 0 & \text{sinon} \end{cases}.$$

- S'il existe $d \in N$ tel que $Q(d) = 1$, alors

$$\widehat{q}(a) = \begin{cases} \pm 2^{\frac{m+k}{2}} & \text{si } < a, x >= 0 \text{ pour tout } x \in N \text{ et } < a, d > \neq 0 \\ 0 & \text{sinon} \end{cases}.$$

On a donc $d(Q, R(1,m)) = 2^{m-1} - 2^{\frac{m+k}{2}-1}$.
Soit $l = \lfloor \frac{m}{2} \rfloor$. On considère $Q = x_1x_2 + x_3x_4 + \ldots + x_{2l-1}x_{2l}$.

- Si m est pair, le rang de B est $2l$ et la dimension de N est 0 donc

$$\rho_2(1,m) = 2^{m-1} - 2^{\frac{m}{2}-1}.$$

- Si m est impair, la dimension de N est 1. De plus, comme m est impair, on a pour toute forme quadratique $\dim(N) \geq 1$. D'où

$$\rho_2(1,m) = 2^{m-1} - 2^{\frac{m+1}{2}-1}.$$

□

On en déduit une minoration du rayon de recouvrement des codes de Reed-Muller d'ordre 1.

Théorème 2.3.5. *Pour tout m, $\rho(1,m) \geq 2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1}$.*

Démonstration. Puisque $\rho(1,m) \geq \rho_2(1,m)$, c'est une conséquence du théorème 2.3.4. □

Corollaire 2.3.6. *Si m est pair, $\rho(1,m) = 2^{m-1} - 2^{\frac{m}{2}-1}$.*

Démonstration. Par le théorème 2.3.3, $\rho(1,m) \leq 2^{m-1} - 2^{\frac{m}{2}-1}$. Par le théorème 2.3.5, $\rho(1,m) \geq 2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1} = 2^{m-1} - 2^{\frac{m}{2}-1}$. □

On a de plus les résultats suivants :

Théorème 2.3.7. *On a :*

1. $\rho(1,3) = 2$
2. $\rho(1,5) = 12$

3. $\rho(1,7) = 56$

On trouve la preuve du point 3 dans [Myk80] ou [Hou96], celle du point 2 se trouve dans [BW72] mais on peut aussi démontrer ce résultat en utilisant les mêmes méthodes que dans [Hou96]. Enfin, le point 1 peut se calculer directement à l'aide d'un ordinateur.

D'après ce théorème, on peut se demander si le rayon de recouvrement $\rho(1,m)$ est toujours égal à $\rho_2(1,m)$. Ceci est faux :

Théorème 2.3.8. *On a :*

1. $\rho(1,9) \geq 242$
2. $\rho(1,11) \geq 996$
3. $\rho(1,13) \geq 4040$
4. *Pour* $m \geq 15$ *impair,* $\rho(1,m) \geq 2^{m-1} - \frac{27}{32}2^{\frac{m-1}{2}}$

On peut trouver la preuve des trois premier points dans [KDY10]. Ils procèdent par recherche exhaustive parmi les fonctions booléennes à symétrie rotationnelle. L'idée de la preuve du dernier point est de montrer que $\rho(1,15) \geq 2^{14} - 27.4$ ([PW83, PW90]) puis d'utiliser la relation de récurrence suivante pour généraliser à tout m :

$$\forall m, \quad \rho(1,m+2) \geq 2\rho(1,m) + 2^m.$$

Cette relation est démontrée dans [HKM78] pour $q = 2$; on généralise cette relation dans la section 2.6 à tout q.

2.4 Une borne supérieure pour $\rho(1,m)$ pour les codes de Reed-Muller généralisés

2.4.1 Un théorème général

Avant de donner une majoration du rayon de recouvrement d'un code linéaire auto-complémentaire de force 2, on étend la définition de code auto-complémentaire (voir [HKM78]) à la caractéristique impaire et on rappelle la définition de force d'un code (voir [Bos61]).

Définition 2.4.1. Un code C sur $\mathbb{F}_q$ est dit auto-complémentaire si

$$\forall c \in C, \forall \omega \in \mathbb{F}_q \qquad \overline{c}^{\omega} = (\omega, \ldots, \omega) + c \in C.$$

Définition 2.4.2. Un code C sur $\mathbb{F}_q$ est dit de force s si pour tout sous-ensemble de s coordonnées du code $\{i_1, \ldots, i_s\}$ le cardinal de l'image réciproque d'un élément de $\mathbb{F}_q^s$ par l'application

$$\begin{array}{ccc} C & \to & \mathbb{F}_q^s \\ c & \mapsto & (c_{i_1}, \ldots, c_{i_s}) \end{array}$$

est constant et ne dépend pas de l'ensemble de coordonnées choisi.

Théorème 2.4.3. *Soit C un code sur $\mathbb{F}_q$ de longueur n auto-complémentaire et de force 2 alors*

$$\rho(C) \leq \frac{(q-1)}{q}n - \frac{\sqrt{n}}{q}.$$

Pour démontrer ce résultat, on a besoin du lemme suivant :

Lemme 2.4.4. *Soit C un code sur $\mathbb{F}_q$ de longueur n et de force 2 alors*

$$\forall v \in \mathbb{F}_q^n, \qquad \sum_{u \in v+C} |u|^2 = n\left(\frac{q-1}{q}\right)\left((n-1)\left(\frac{q-1}{q}\right)+1\right)\#C.$$

Démonstration. Le code C est de force 2 si et seulement si le code $v+C$ est de force 2. En effet, ajouter v revient à faire une permutation des $(x_i, x_j)_{x_i,x_j \in \mathbb{F}_q}$ et $(p-1)v+v+C = C$. De plus $\#(v+C) = \#C$, on est donc ramené au cas où $v = 0$. Alors

$$\begin{aligned}\sum_{u \in C} |u|^2 &= \sum_{u \in C} \sum_{i, u_i \neq 0} \sum_{j, u_j \neq 0} 1 \\ &= \sum_{u \in C} \sum_{i, u_i \neq 0} \sum_{j \neq i, u_j \neq 0} 1 + \sum_{u \in C} \sum_{i, u_i \neq 0} 1 \\ &= \sum_{i=1}^{n} \sum_{j \neq i} \sum_{u \in C, u_i u_j \neq 0} 1 + \sum_{i=1}^{n} \sum_{u \in C, u_i \neq 0} 1.\end{aligned}$$

Comme C est de force 2,

$$\sum_{u \in C, u_i u_j \neq 0} 1 = \left(\frac{q-1}{q}\right)^2 \#C \text{ et } \sum_{u \in C, u_i \neq 0} 1 = \left(\frac{q-1}{q}\right)\#C$$

et donc $\displaystyle\sum_{u \in C} |u|^2 = n(n-1)\left(\frac{q-1}{q}\right)^2 \#C + n\left(\frac{q-1}{q}\right)\#C.$ □

On peut maintenant démontrer le théorème.

Démonstration. Soit $v \in \mathbb{F}_q^n$ et soit r tel que $\forall u \in v+C$, $|u| \geq r$. Comme le code est auto-complémentaire, $\forall \omega \in \mathbb{F}_q, \forall u \in v+C$, $|\overline{u}^\omega| \geq r$. Alors

$$\sum_{\omega \in \mathbb{F}_q} |\overline{u}^\omega| = \sum_{\omega \in \mathbb{F}_q} |u| - n_{-\omega} + n_0 = q(|u| + n_0) - \sum_{\omega \in \mathbb{F}_q} n_{-\omega} = (q-1)n$$

où $n_\omega = \#\{i : u_i = \omega\}$. Supposons $r > \frac{q-1}{q}n$. Alors

$$(q-1)n < qr \leq \sum_{\omega \in \mathbb{F}_q} |\overline{u}^\omega| = n(q-1)$$

Ce qui est absurde donc $r = \frac{q-1}{q}n - \rho$ avec $\rho \geq 0$. On a alors

$$\begin{aligned}\sum_{\omega \in \mathbb{F}_q} |\overline{u}^\omega|^2 &= \sum_{\omega \in \mathbb{F}_q^*} |\overline{u}^\omega|^2 + |u|^2 \\ &= \sum_{\omega \in \mathbb{F}_q^*} |\overline{u}^\omega|^2 + \left((q-1)n - \sum_{\omega \in \mathbb{F}_q^*} |\overline{u}^\omega|\right)^2\end{aligned}$$

Or,

$$L = \sum_{\omega \in \mathbb{F}_q^*} |\overline{u}^\omega|^2 + \left((q-1)n - \sum_{\omega \in \mathbb{F}_q^*} |\overline{u}^\omega|\right)^2 \leq (q-1)r^2 + (q-1)^2(n-r)^2 = R.$$

En effet :

$$\begin{aligned}
L-R &= \sum_{\omega\in\mathbb{F}_q^*}(|\overline{u}^\omega|-r^2)+\left(\left((q-1)n-\sum_{\omega\in\mathbb{F}_q^*}|\overline{u}^\omega|\right)^2-(q-1)^2(n-r)^2\right)\\
&= \sum_{\omega\in\mathbb{F}_q^*}(|\overline{u}^\omega|-r)(|\overline{u}^\omega|+r)+\left((q-1)n-\sum_{\omega\in\mathbb{F}_q^*}|\overline{u}^\omega|-(q-1)n+(q-1)r\right)\\
&\qquad\qquad\times\left(2(q-1)n-\sum_{\omega\in\mathbb{F}_q^*}|\overline{u}^\omega|-(q-1)r\right)\\
&= \sum_{\omega\in\mathbb{F}_q^*}(|\overline{u}^\omega|-r)\left(|\overline{u}^\omega|+r-2(q-1)n+\sum_{\zeta\in\mathbb{F}_q^*}|\overline{u}^\zeta|+(q-1)r\right)\\
&= \sum_{\omega\in\mathbb{F}_q^*}(|\overline{u}^\omega|-r)\left(|\overline{u}^\omega|-(q-1)(n-r)+r-|u|\right)\leq 0\\
&\text{car } \sum_{\omega\in\mathbb{F}_q}|\overline{u}^\omega|=(q-1)n \text{ donc } |\overline{u}^\omega|=n(q-1)-\sum_{\zeta\neq\omega}|\overline{u}^\zeta|\leq(q-1)(n-r).
\end{aligned}$$

Donc

$$\begin{aligned}
\sum_{\omega\in\mathbb{F}_q}|\overline{u}^\omega|^2 &\leq (q-1)r^2+(q-1)^2(n-r)^2\\
&= (q-1)\left(\frac{q-1}{q}n-\rho\right)^2+(q-1)^2\left(\frac{n}{q}+\rho\right)^2\\
&= q\left(n^2\frac{(q-1)^2}{q^2}+(q-1)\rho^2\right)
\end{aligned}$$

d'où

$$\sum_{u\in v+C}|u|^2\leq q\left(n^2\frac{(q-1)^2}{q^2}+(q-1)\rho^2\right)\frac{\#C}{q}=\left(n^2\frac{(q-1)^2}{q^2}+(q-1)\rho^2\right)\#C.$$

Or, par le lemme 2.4.4, $\displaystyle\sum_{u\in v+C}|u|^2=n\left(\frac{q-1}{q}\right)\left((n-1)\left(\frac{q-1}{q}\right)+1\right)\#C$ donc

$$n^2\frac{(q-1)^2}{q^2}+n\frac{(q-1)}{q^2}\leq\left(n^2\frac{(q-1)^2}{q^2}+(q-1)\rho^2\right).$$

On obtient alors $\frac{n}{q^2}\leq\rho^2$ et comme $\rho\geq 0$ on a $\rho\geq\frac{\sqrt{n}}{q}$. On en déduit $r\leq\frac{(q-1)}{q}n-\frac{\sqrt{n}}{q}$ d'où le résultat. □

2.4.2 Application aux codes de Reed-Muller généralisés

On veut appliquer le théorème général aux codes de Reed-Muller d'ordre 1. Comme $R_q(0,m)\subset R_q(1,m)$, on a déjà que $R_q(1,m)$ est auto-complémentaire. Pour appliquer le théorème 2.4.3, il faut vérifier que $R_q(1,m)$ est de force 2.

Lemme 2.4.5. *Pour tout q et pour tout $m\geq 1$, $R_q(1,m)$ est de force 2.*

Démonstration. Soit $y = (y_1, \ldots, y_m)$ et $z = (z_1, \ldots, z_m)$ deux coordonnées fixées distinctes. On définit la relation d'équivalence suivante sur $R_q(1, m)$:

$$f \sim g \Leftrightarrow f(y) = g(y) \quad et \quad f(z) = g(z).$$

On va calculer le cardinal d'une classe d'équivalence. Soit $f(x) = a_1x_1 + \ldots + a_mx_m + b$ et $g = \alpha_1x_1 + \ldots + \alpha_mx_m + \beta$ tel que $f \sim g$. Alors

$$\begin{cases} \alpha_1y_1 + \ldots + \alpha_my_m + \beta = a_1y_1 + \ldots + a_my_m + b \\ \alpha_1z_1 + \ldots + \alpha_mz_m + \beta = a_1z_1 + \ldots + a_mz_m + b \end{cases}$$

$$\Leftrightarrow \begin{pmatrix} y_1 & \ldots & y_m & 1 \\ z_1 & \ldots & z_m & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \\ \beta \end{pmatrix} = \begin{pmatrix} a_1y_1 + \ldots + a_my_m + b \\ a_1z_1 + \ldots + a_mz_m + b \end{pmatrix}.$$

Comme $z \neq y$, le système est de rang 2, il y a donc q^{m-1} solutions et chaque classe d'équivalence a q^{m-1} éléments. Or, $\#R_q(1, m) = q^{m+1}$ donc le nombre de classes d'équivalence est $\frac{q^{m+1}}{q^{m-1}} = q^2 = \#\mathbb{F}_q^2$ et donc $R_q(1, m)$ est de force 2. □

On déduit donc du théorème 2.4.3 et du lemme 2.4.5 le théorème suivant :

Théorème 2.4.6. *Pour tout q et pour tout $m \geq 1$, $\rho(1, m) \leq (q-1)q^{m-1} - q^{\frac{m}{2}-1}$.*

2.5 Une borne inférieure pour $\rho(1, m)$

Comme dans le cas $q = 2$, on calcule le rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1 dans les codes de Reed-Muller généralisés d'ordre 2. Pour cela on utilise le résultat sur les zéros d'une forme quadratique ci-dessus.

2.5.1 Rayon de recouvrement de $R_q(1, m)$ dans $R_q(2, m)$

Théorème 2.5.1. *Pour tout m et tout q, $\rho_2(1, m) = (q-1)q^{m-1} - q^{\lceil \frac{m}{2} \rceil - 1}$.*

Démonstration. Soit $q_0 = \sum_{1 \leq i \leq j \leq m} a_{i,j}x_ix_j$. On cherche à calculer le poids de

$$q_0 + \alpha_1x_1 + \ldots + \alpha_mx_m + \beta.$$

Soit $Q = q_0 + \alpha_1x_1z + \ldots + \alpha_mx_mz + \beta z^2$. On note N_q^∞ le nombre de zéros de q_0 et N_q le nombre de zéros de Q.
Par le théorème 2.2.6, on a :

$$N_q^\infty = q^{m-1} + q^{m-\frac{r}{2}-1}(q-1)(\omega_{q_0} - 1)$$

où $r = \mathrm{rg}(q_0)$ et

$$\omega_{q_0} = \begin{cases} 1 & \text{si } r \text{ est impair} \\ 0 & \text{si } r \text{ est pair et si } q_0(Px) = x_1x_2 + \ldots + x_{r-3}x_{r-2} + ax_{r-1}^2 + bx_r^2 + cx_{r-1}x_r \\ & \text{avec } ax^2 + cx + b \text{ irréductible} \\ 2 & \text{si } r \text{ est pair et si } q_0(Px) = x_1x_2 + \ldots + x_{r-1}x_r \end{cases}$$

et

$$N_q = q^m + q^{m-\frac{R}{2}}(q-1)(\omega_Q - 1)$$

où $R = \mathrm{rg}(Q)$ et

$$\omega_Q = \begin{cases} 1 & \text{si } R \text{ est impair} \\ 0 & \text{si } R \text{ est pair et si } Q(Px) = x_1x_2 + \ldots + x_{R-3}x_{R-2} + ax_{R-1}^2 + bx_R^2 + cx_{R-1}x_R \\ & \text{avec } ax^2 + cx + b \text{ irréductible} \\ 2 & \text{si } R \text{ est pair et si } Q(Px) = x_1x_2 + \ldots + x_{R-1}x_R \end{cases}$$

Alors le nombre de zéros de $q_0 + \alpha_1x_1 + \ldots + \alpha_mx_m + \beta$ est

$$N = q^{m-1} - (\omega_{q_0} - 1)q^{m-\frac{r}{2}-1} + (\omega_Q - 1)q^{m-\frac{R}{2}}$$

et donc $|q_0 + \alpha_1x_1 + \ldots + \alpha_mx_m + \beta| = (q-1)q^{m-1} + (\omega_{q_0} - 1)q^{m-\frac{r}{2}-1} - (\omega_Q - 1)q^{m-\frac{R}{2}}$.

On cherche maintenant à calculer $d(q_0, R_q(1,m))$.

- Si r est impair.
  Alors $\omega_{q_0} = 1$ et $|q_0 + \alpha_1x_1 + \ldots + \alpha_mx_m + \beta| = (q-1)q^{m-1} - (\omega_Q - 1)q^{m-\frac{R}{2}}$. Quitte à appliquer un changement de variables linéaire, ce qui ne change pas le poids, on peut supposer que $q_0 = x_1x_2 + \ldots + x_{r-2}x_{r-1} + ax_r^2$. Alors

$$\begin{aligned} Q &= x_1x_2 + \ldots + x_{r-2}x_{r-1} + ax_r^2 + \alpha_1x_1z + \ldots + \alpha_mx_mz + \beta z^2 \\ &= (x_1 + \alpha_2z)(x_2 + \alpha_1z) + \ldots + (x_{r-2} + \alpha_{r-1}z)(x_{r-1} + \alpha_{r-2}z) + ax_r^2 \\ &\qquad + z(\alpha_rx_r + \ldots + \alpha_mx_m) + \underbrace{(\beta - \alpha_1\alpha_2 - \ldots - \alpha_{r-2}\alpha_{r-1})}_{\theta} z^2 \\ &= (x_1 + \alpha_2z)(x_2 + \alpha_1z) + \ldots + (x_{r-2} + \alpha_{r-1}z)(x_{r-1} + \alpha_{r-2}z) + ax_r^2 \\ &\qquad + z(\alpha_rx_r + \ldots + \alpha_mx_m + \theta z). \end{aligned}$$

  S'il existe $i > r$ tel que $\alpha_i \neq 0$ alors $R = r+2$ et $\omega_Q = 1$. Supposons que pour tout $i > r$, $\alpha_i = 0$. Si $\theta \neq 0$, $R = r+1$ et $\omega_Q = \begin{cases} 0 & \text{si } ax^2 + \alpha_rx + \theta \text{ est irréductible} \\ 2 & \text{sinon} \end{cases}$.
  Si $\theta = 0$ alors, si $\alpha_r = 0$, on a $R = r$ et $\omega_Q = 1$. Sinon, on a $R = r+1$ et $\omega_Q = 2$. Donc $d(q_0, R_q(1,m)) = (q-1)q^{m-1} - q^{m-\frac{r+1}{2}}$.

- Si r est pair et $\omega_{q_0} = 2$.
  Alors $|q_0 + \alpha_1x_1 + \ldots + \alpha_mx_m + \beta| = (q-1)q^{m-1} + q^{m-\frac{r}{2}-1} - (\omega_Q - 1)q^{m-\frac{R}{2}}$. Quitte à appliquer un changement de variables linéaire, on peut supposer que

$$q_0 = x_1x_2 + \ldots + x_{r-1}x_r.$$

  Alors

$$\begin{aligned} Q &= x_1x_2 + \ldots + x_{r-1}x_r + \alpha_1x_1z + \ldots + \alpha_mx_mz + \beta z^2 \\ &= (x_1 + \alpha_2z)(x_2 + \alpha_1z) + \ldots + (x_{r-1} + \alpha_rz)(x_r + \alpha_{r-1}z) \\ &\qquad + z(\alpha_{r+1}x_{r+1} + \ldots + \alpha_mx_m) + \underbrace{(\beta - \alpha_1\alpha_2 - \ldots - \alpha_{r-1}\alpha_r)}_{\theta} z^2. \end{aligned}$$

  S'il existe $i > r$ tel que $\alpha_i \neq 0$ alors $R = R+2$ et $\omega_Q = 2$. Supposons que pour tout $i > r$, $\alpha_i = 0$. Si de plus $\theta = 0$, $R = r$ et $\omega_Q = 2$. Sinon $R = r+1$ et $\omega_Q = 1$. Donc $d(q_0, R_q(1,m)) = (q-1)q^{m-1} + q^{m-\frac{r}{2}-1} - q^{m-\frac{r}{2}}$.

- Si r est pair et $\omega_{q_0} = 0$.
  On a alors $|q_0 + \alpha_1 x_1 + \ldots + \alpha_m x_m + \beta| = (q-1)q^{m-1} - q^{m-\frac{r}{2}-1} - (\omega_Q - 1)q^{m-\frac{R}{2}}$.
  Quitte à appliquer un changement de variables linéaire, on peut supposer que

$$q_0 = x_1x_2 + \ldots + x_{r-3}x_{r-2} + ax_{r-1}^2 + bx_r^2 + cx_{r-1}x_r$$

avec $ax^2 + cx + b$ irréductible. Alors

$$\begin{aligned} Q &= x_1x_2 + \ldots + x_{r-3}x_{r-2} + ax_{r-1}^2 + bx_r^2 + cx_{r-1}x_r + \alpha_1 x_1 z + \ldots + \alpha_m x_m z + \beta z^2 \\ &= (x_1 + \alpha_2 z)(x_2 + \alpha_1 z) + \ldots + (x_{r-3} + \alpha_{r-2}z)(x_{r-2} + \alpha_{r-3}z) + ax_{r-1}^2 + bx_r^2 \\ &\quad + cx_{r-1}x_r + z(\alpha_{r-1}x_{r-1} + \ldots + \alpha_m x_m) + \underbrace{(\beta - \alpha_1\alpha_2 - \ldots - \alpha_{r-3}\alpha_{r-2})}_{\theta} z^2. \end{aligned}$$

S'il existe $i > r$ tel que $\alpha_i \neq 0$ alors $R = r+2$ et $\omega_Q = 0$. Supposons que pour tout $i > r$, $\alpha_i = 0$. On différentie le cas où q est pair et le cas où q est impair.
Si q est impair, comme $ax^2 + cx + b$ est irréductible, $a \neq 0$ et $b - \frac{c^2}{4a} = \delta \neq 0$. Alors

$$\begin{aligned} Q &= (x_1 + \alpha_2 z)(x_2 + \alpha_1 z) + \ldots + (x_{r-3} + \alpha_{r-2}z)(x_{r-2} + \alpha_{r-3}z) \\ &\quad + a(x_{r-1} + \frac{c}{2a}x_r + \frac{\alpha_{r-1}}{2a}z)^2 + \delta x_r^2 + (\alpha_r - \frac{c\alpha_{r-1}}{2a})x_r z + (\theta - \frac{\alpha_{r-1}^2}{4a})z^2 \\ &= (x_1 + \alpha_2 z)(x_2 + \alpha_1 z) + \ldots + (x_{r-3} + \alpha_{r-2}z)(x_{r-2} + \alpha_{r-3}z) \\ &\quad + a(x_{r-1} + \frac{c}{2a}x_r + \frac{\alpha_{r-1}}{2a}z)^2 + \delta(x_r + \frac{2a\alpha_r - c\alpha_{r-1}}{4a\delta}z)^2 \\ &\quad + (\theta - \frac{\alpha_{r-1}^2}{4a} - \frac{(2a\alpha_r - c\alpha_{r-1})^2}{16a^2\delta})z^2. \end{aligned}$$

Si $\theta \neq \frac{\alpha_{r-1}^2}{4a} + \frac{(2a\alpha_r - c\alpha_{r-1})^2}{16a^2\delta}$, $R = r+1$ et $\omega_Q = 1$. Sinon $R = r$ et $\omega_Q = 0$ car $ax^2 + cx + b$ est irréductible.
Si q est pair, $c \neq 0$ car $ax^2 + b + cx$ est irréductible. On a donc

$$\begin{aligned} Q &= (x_1 + \alpha_2 z)(x_2 + \alpha_1 z) + \ldots + (x_{r-3} + \alpha_{r-2}z)(x_{r-2} + \alpha_{r-3}z) \\ &\quad + c(x_{r-1} + \frac{\alpha_r}{c}z)(x_r + \frac{\alpha_{r-1}}{c}z) + \left(\sqrt{a}x_{r-1} + \sqrt{b}x_r + \sqrt{\theta - \frac{\alpha_{r-1}\alpha_r}{c}}z\right)^2. \end{aligned}$$

Si $c^2\theta \neq a\alpha_r^2 + b\alpha_{r-1}^2 + c\alpha_{r-1}\alpha_r$, $R = r+1$ et $\omega_Q = 1$. Sinon

$$\begin{aligned} Q &= (x_1 + \alpha_2 z)(x_2 + \alpha_1 z) + \ldots + (x_{r-3} + \alpha_{r-2}z)(x_{r-2} + \alpha_{r-3}z) \\ &\quad + c(x_{r-1} + \frac{\alpha_r}{c}z)(x_r + \frac{\alpha_{r-1}}{c}z) + \left(\sqrt{a}x_{r-1} + \sqrt{b}x_r + (\frac{\sqrt{a}}{c}\alpha_r + \frac{\sqrt{b}}{c}\alpha_{r-1})z\right)^2 \\ &= (x_1 + \alpha_2 z)(x_2 + \alpha_1 z) + \ldots + (x_{r-3} + \alpha_{r-2}z)(x_{r-2} + \alpha_{r-3}z) \\ &\quad + c(x_{r-1} + \frac{\alpha_r}{c}z)(x_r + \frac{\alpha_{r-1}}{c}z) + a(x_{r-1} + \frac{\alpha_r}{c}z)^2 + b(x_r + \frac{\alpha_{r-1}}{c}z)^2 \end{aligned}$$

donc $R = r$ et $\omega_Q = 0$. D'où $d(q_0, R_q(1,m)) = (q-1)q^{m-1} - q^{m-\frac{r}{2}-1}$.

□

2.5.2 Une borne inférieure pour $\rho(1, m)$

Comme dans le cas $q = 2$, on déduit de $\rho_2(1, m)$ une borne inférieure pour le rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1.

Théorème 2.5.2. *Pour tout q et tout m, $\rho(1, m) \geq (q-1)q^{m-1} - q^{\lceil \frac{m}{2} \rceil - 1}$.*

Démonstration. Comme $\rho(1, m) \geq \rho_2(1, m)$, on a le résultat par le théorème 2.5.1. □

Corollaire 2.5.3. *Pour tout q et pour tout m pair, $\rho(1, m) = (q-1)q^{m-1} - q^{\frac{m}{2}-1}$.*

Démonstration. Pour m pair, $(q-1)q^{m-1} - q^{\lceil \frac{m}{2} \rceil - 1} = (q-1)q^{m-1} - q^{\frac{m}{2}-1}$. Le résultat découle des théorèmes 2.5.2 et 2.4.6. □

On a de plus montré au cours de la preuve du théorème 2.5.1 que le rayon de recouvrement était atteint pour

$$f(x) = x_1x_2 + \ldots + x_{m-3}x_{m-2} + ax_{m-1}^2 + bx_m^2 + cx_{m-1}x_m$$

avec $ax^2 + cx + b$ irréductible sur $\mathbb{F}_q$.

2.6 Le cas $q = 3$

Dans cette section, on utilise Magma pour calculer le rayon de recouvrement de $R_3(1, 3)$. On en déduit une meilleure minoration du rayon de recouvrement de $R_3(1, m)$ pour tout m.

2.6.1 Calcul du rayon de recouvrement pour $m = 3$

Théorème 2.6.1. *Pour $q = 3$, $\rho(1, 3) = 16$.*

Démonstration. Par les théorèmes 2.5.2 et 2.4.6, $15 \leq \rho(1, 3) \leq 16$. De plus, si $\rho(1, 3) = 16$, alors il existe $f \in B_m^q$ tel que $d(f, R_3(1, 3)) = 16$. Comme $\rho_2(1, 3) = 15$ par le théorème 2.5.1, nécessairement le degré de f est plus grand que 3. En utilisant tous ces résultats, on calcule le rayon de recouvrement avec Magma.

Algorithme 1

```
K:=GF(3);
P<x,y,z>:=PolynomialRing(K,3);
R1:=[a*x+b*y+c*z+d : a in K, b in K, c in K, d in K];
M:=15;
L:=[0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0];

ad:=function(L); i:=1; r:=true;
while i le #L and r do
if L[i]+1 eq 3 then i:=i+1; L[i-1]:=0;
   else r:=false; L[i]:=L[i]+1; end if; end while;
   return L;
 end function;

while M eq 15  and L[23] le 1 do
pol:=L[1]*z^2+L[2]*y*z+L[3]*y^2+L[4]*x*z+L[5]*x*y+L[6]*x^2
```

```
 +L[7]*y*z^2+L[8]*y^2*z+L[9]*x*z^2+L[10]*x*y*z+L[11]*x*y^2
 +L[12]*x^2*z+L[13]*x^2*y+L[14]*y^2*z^2+L[15]*x*y*z^2
 +L[16]*x*y^2*z+L[17]*x^2*z^2+L[18]*x^2*y*z+L[19]*x^2*y^2
 +L[20]*x*y^2*z^2+L[21]*x^2*y*z^2+L[22]*x^2*y^2*z
 +L[23]*x^2*y^2*z^2;
k:=1; m:=16;
while k le #R1 and m eq 16 do
if Evaluate(R1[k],<0,0,0>) ne 0 then r:=1; else; r:=0; end if;
p:=<1,0,0>;
while r lt 16 and p ne <0,0,0>  do
if Evaluate(pol+R1[k],p) ne 0 then r:=r+1; p:=ad(p);
   else p:=ad(p); end if; end while;
if r lt m then m:=r; end if;
k:=k+1; end while;
if m gt M then M:=m; else L:=ad(L); end if; end while;

print(M);
print(L);
```

On obtient que $d(y^2 + xy + y^2z + xyz + y^2z^2 + x^2z^2, R_3(1,3)) = 16$. □

2.6.2 Mots qui atteignent le rayon de recouvrement

On cherche maintenant les mots qui atteignent le rayon de recouvrement de $R_3(1,3)$.

Proposition 2.6.2. *Il n'y a pas de $f \in R_3(6,4) \setminus R_3(4,3)$ tel que $d(f, R_3(1,3)) = 16$.*

Pour prouver ce résultat, on a besoin des lemmes suivants :

Lemme 2.6.3. *Pour $q \geq 3$, si $f \in R_q(m(q-1), m) \setminus R_q(m(q-1)-1, m)$, il existe $\sigma \in \mathrm{GA}_m(\mathbb{F}_q)$, $a \in \mathbb{F}_q^*$ et $r \in R_q(m(q-1)-2, m)$ tels que*

$$\sigma.f = a \prod_{i=1}^{m} x_i^{q-1} + r.$$

Démonstration. On écrit f sous la forme

$$f(x) = a \prod_{i=1}^{m} x_i^{q-1} + \sum_{i=1}^{m} a_i \prod_{k \neq i} x_k^{q-1} x_i^{q-2} + s$$

où a, $a_i \in \mathbb{F}_q$, $a \neq 0$ et $s \in R_q(m(q-1)-2, m)$.

Soit $\omega \in \mathbb{F}_q^m$ alors

$$\begin{aligned}
1_\omega &= \prod_{i=1}^{m} (1 - (x_i - \omega_i)^{q-1}) \\
&= \prod_{i=1}^{m} \left(1 - \sum_{k=1}^{q-1} \binom{q-1}{k} x_i^k (-\omega_i)^{q-1-k} \right) \\
&= (-1)^m \prod_{i=1}^{m} x_i^{q-1} + (-1)^m \sum_{i=1}^{m} -\omega_i \prod_{k \neq i} x_k^{q-1} x_i^{q-2} + t, \qquad t \in R_q(m(q-1)-2, m).
\end{aligned}$$

D'où
$$f = (-1)^m a 1_{(-a^{-1}a_i)} + r', \qquad r' \in R_q(m(q-1)-2, m).$$
Soit $\sigma \in \mathrm{GA}_m(\mathbb{F}_q)$,
$$\sigma.f = (-1)^m a 1_{\sigma^{-1}((-a^{-1}a_i))} + \sigma.r', \qquad r' \in R_q(m(q-1)-2, m).$$
On choisit σ tel que $\sigma^{-1}((-a^{-1}a_i)) = 0$.

$$1_0 = \prod_{i=1}^{m}(1 - x_i^{q-1}) = (-1)^m \prod_{i=1}^{m} x_i^{q-1} + u,$$
$$u \in R_q((m-1)(q-1), m) \subset R_q(m(q-1)-2, m) \quad \text{puisque } q \geq 3.$$

Finalement, puisque $\mathrm{Aut}(R_q(m(q-1)-2, m)) = \mathrm{GA}_m(\mathbb{F}_q)$, on a
$$\sigma.f = a \prod_{i=1}^{m} x_i^{q-1} + r, \qquad r \in R_q(m(q-1)-2, m).$$

□

Lemme 2.6.4. *Si $f \in R_q(m(q-1)-1, m) \backslash R_q(m(q-1)-2, m)$, alors il existe $\sigma \in \mathrm{GL}_m(\mathbb{F}_q)$ et $r \in R_q(m(q-1)-2, m)$ tels que*
$$\sigma.f = \prod_{i=1}^{m-1} x_i^{q-1} x_m^{q-2} + r.$$

Démonstration. On écrit $f(x) = \sum_{i=1}^{m} \alpha_i \prod_{k \neq i} x_k^{q-1} x_i^{q-2} + t$, $t \in R_q(m(q-1)-2, m)$.

Soit $b \in \mathbb{F}_q^m$,
$$\begin{aligned} 1_0 - 1_b &= \prod_{i=1}^{m}(1 - x_i^{q-1}) - \prod_{i=1}^{m}(1 - (x_i - b_i)^{q-1}) \\ &= \prod_{i=1}^{m}(1 - x_i^{q-1}) - \prod_{i=1}^{m}(1 - \sum_{k=1}^{q-1} \binom{q-1}{k} x_i^k (-b_i)^{q-1-k}) \\ &= (-1)^m \sum_{i=1}^{m} b_i \prod_{k \neq i} x_k^{q-1} x_i^{q-2} + s, \qquad s \in R_q(m(q-1)-2, m). \end{aligned}$$

D'où $f = 1_0 - 1_{((-1)^m \alpha_i)} + r'$, $r' \in R_q(m(q-1)-2, m)$.

Soit $\sigma \in \mathrm{GL}_m(\mathbb{F}_q)$. On a
$$\sigma.f = 1_{\sigma^{-1}(0)} - 1_{\sigma^{-1}(((-1)^m \alpha_i))} + \sigma.r' = 1_0 - 1_{\sigma^{-1}(((-1)^m \alpha_i))} + \sigma.r'.$$

Comme $f \in R_q(m(q-1)-1, m) \setminus R_q(m(q-1)-2, m)$, $((-1)^m \alpha_i) \neq 0$. Il existe donc $\sigma \in \mathrm{GL}_m(\mathbb{F}_q)$ tel que
$$\sigma^{-1}(((-1)^m \alpha_i)) = \begin{pmatrix} (-1)^m \\ 0 \\ \vdots \\ 0 \end{pmatrix} = c$$

et

$$\sigma.f = 1_0 - 1_c + \sigma.r' = \prod_{i=1}^{m-1} x_i^{q-1} x_m^{q-1} + r$$

avec $r \in R_q(m(q-1)-2, m)$ puisque $\mathrm{Aut}(R_q(m(q-1)-2, m)) = \mathrm{GA}_m(\mathbb{F}_q)$. □

On peut maintenant prouver la proposition :

Démonstration. Par les lemmes 2.6.3 et 2.6.4, les algorithmes suivants donnent le résultat.

Algorithme 2 (degré 6)

```
K:=GF(3);
P<x,y,z>:=PolynomialRing(K,3);
R1:=[a*x+b*y+c*z+d : a in K, b in K, c in K, d in K];

ad:=function(L); i:=1; r:=true;
while i le #L and r do
   if L[i]+1 eq 3 then i:=i+1; L[i-1]:=0;
      else r:=false; L[i]:=L[i]+1; end if; end while;
return L;
end function;

L:=[1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0];
while L ne [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0] do
pol:=L[1]*z^2+L[2]*y*z+L[3]*y^2+L[4]*x*z+L[5]*x*y+L[6]*x^2
     +L[7]*y*z^2+L[8]*y^2*z+L[9]*x*z^2+L[10]*x*y*z+L[11]*x*y^2
     +L[12]*x^2*z+L[13]*x^2*y+L[14]*y^2*z^2+L[15]*x*y*z^2
     +L[16]*x*y^2*z+L[17]*x^2*z^2+L[18]*x^2*y*z
     +L[19]*x^2*y^2+x^2*y^2*z^2;
k:=1; m:=16;
while k le #R1 and m eq 16 do
if Evaluate(R1[k],<0,0,0>) ne 0 then r:=1; else; r:=0; end if;
p:=<1,0,0>;
while r lt 16 and p ne <0,0,0>  do
  if Evaluate(pol+R1[k],p) ne 0 then r:=r+1; p:=ad(p);
   else p:=ad(p); end if; end while;
if r lt m then m:=r; end if;
k:=k+1; end while;
if m gt 15 then print(pol); L:=ad(L);  else L:=ad(L); end if;  end while;
```

Algorithme 3 (degré 5)

```
K:=GF(3);
P<x,y,z>:=PolynomialRing(K,3);
R1:=[a*x+b*y+c*z+d : a in K, b in K, c in K, d in K];

ad:=function(L); i:=1; r:=true;
while i le #L and r do
```

```
 if L[i]+1 eq 3 then i:=i+1; L[i-1]:=0;
   else r:=false; L[i]:=L[i]+1; end if; end while;
 return L;
 end function;

L:=[1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0];
while L ne [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0] do
pol:=L[1]*z^2+L[2]*y*z+L[3]*y^2+L[4]*x*z+L[5]*x*y+L[6]*x^2
     +L[7]*y*z^2+L[8]*y^2*z+L[9]*x*z^2+L[10]*x*y*z+L[11]*x*y^2
     +L[12]*x^2*z+L[13]*x^2*y+L[14]*y^2*z^2+L[15]*x*y*z^2
     +L[16]*x*y^2*z+L[17]*x^2*z^2+L[18]*x^2*y*z+L[19]*x^2*y^2+x^2*y^2*z;
k:=1; m:=16;
while k le #R1 and m eq 16 do
if Evaluate(R1[k],<0,0,0>) ne 0 then r:=1; else; r:=0; end if;
p:=<1,0,0>;
while r lt 16 and p ne <0,0,0>  do
 if Evaluate(pol+R1[k],p) ne 0 then r:=r+1; p:=ad(p);
   else p:=ad(p); end if; end while;
if r lt m then m:=r; end if;
k:=k+1; end while;
if m gt 15 then print(pol); L:=ad(L);  else L:=ad(L); end if; end while;
```

Les deux algorithmes ne donnent aucun f tel que $d(f, R_3(1,3)) = 16$. □

En utilisant des algorithmes similaires, on peut prouver la proposition suivante :

Proposition 2.6.5. *Tous les f dans $R_3(4,3)$ tels que $d(f, R_3(1,3)) = 16$ sont équivalents sous l'action de $\mathrm{GA}_3(\mathbb{F}_3)$ et $R_3(1,3)$ à*

$$2x^2z^2 + 2yz + x^2z^2 + xyz + 2x^2yz.$$

2.6.3 Amélioration de la borne inférieure

On utilise le théorème 2.6.1 pour améliorer, pour $q = 3$, la borne inférieure du rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1 donnée dans le théorème 2.5.2.

Théorème 2.6.6. *Pour $q = 3$ et m un entier impair,*

$$\rho(1,m) \geq (q-1)q^{m-1} - \frac{2}{3}q^{\lceil \frac{m}{2} \rceil - 1}.$$

On a besoin de la relation de récurrence suivante pour prouver ce résultat.

Lemme 2.6.7. *Pour tout q et tout m,*

$$\rho(1,m+2) \geq (q-1)^2 q^m + q\rho(1,m).$$

Démonstration. Soit $f \in R_q(1,m+2)$. On écrit

$$f(x_1,\ldots,x_{m+2}) = g(x_1,\ldots,x_m) + \alpha x_{m+1} + \beta x_{m+2}$$

où $g \in R_q(1,m)$ et α, $\beta \in \mathbb{F}_q$. On note ω_0, $\omega_1, \ldots, \omega_{q-1}$ les éléments de $\mathbb{F}_q$. On peut supposer que $\omega_0 = 0$. Alors

$$R_q(1,m+2) = \{M(c,\alpha,\beta) : c \in R_q(1,m), \alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q\}$$

où $M(c,\alpha,\beta) = (c, \overline{c}^{\alpha\omega_1}, \ldots, \overline{c}^{\alpha\omega_{q-1}}, \overline{c}^{\beta\omega_1}, \overline{c}^{\alpha\omega_1+\beta\omega_1}, \ldots, \overline{c}^{\beta\omega_1+\alpha\omega_{q-1}}, \ldots, \overline{c}^{\alpha\omega_{q-1}+\beta\omega_{q-1}})$.

Si v_0 est tel que $d(v_0, R_q(1,m)) = \rho(1,m)$, alors pour tout $c \in R_q(1,m)$, $|v_0 + c| \geq \rho(1,m)$.
Soit $u = (\overline{v_0}^{\omega_0\omega_0}, \ldots, \overline{v_0}^{\omega_0\omega_{q-1}}, \overline{v_0}^{\omega_1\omega_0}, \ldots, \overline{v_0}^{\omega_1\omega_{q-1}}, \ldots, \overline{v_0}^{\omega_{q-1}\omega_{q-1}}) \in B^q_{m+2}$.
Si α, $\beta \in \mathbb{F}_q$ et $c \in R_q(1,m)$, alors

$$\begin{aligned}
|u + M(c,\alpha,\beta)| &= \sum_{i=0}^{q-1}\sum_{j=0}^{q-1} |\overline{v_0}^{\omega_i\omega_j} + \overline{c}^{\alpha\omega_i+\beta\omega_j}| \\
&= \sum_{i=0}^{q-1}\sum_{j=0}^{q-1} |\overline{v_0}^{(\beta+\omega_i)\omega_j} + \overline{c}^{\alpha\omega_i}| \\
&= q|\overline{c}^{\alpha(-\beta)} + v_0| + \sum_{\omega_i \neq -\beta}\sum_{j=0}^{q-1} |\overline{v_0}^{(\beta+\omega_i)\omega_j} + \overline{c}^{\alpha\omega_i}| \\
&\geq q\rho(1,m) + (q-1)^2 q^m
\end{aligned}$$

ce qui donne le résultat. □

On prouve maintenant le théorème 2.6.6.

Démonstration. On écrit $m = 2k+1$. On prouve par récurrence sur u que pour $u \leq k$,

$$\rho(1,m) \geq (q-1)(q^{m-1} - q^{m-1-u}) + q^u \rho(1, m-2u).$$

Cette inegalité est vraie pour $u = 0$ et $u = 1$ par lemme 2.6.7. Supposons qu'elle soit vraie pour un $u < k$. Alors

$$\begin{aligned}
\rho(1,m) &\geq (q-1)(q^{m-1} - q^{m-1-u}) + q^u \rho(1, m-2u) \\
&\geq (q-1)(q^{m-1} - q^{m-1-u}) + q^u \left((q-1)^2 q^{m-2u-2} + q\rho(1, m-2u-2)\right) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(par le lemme 2.6.7)} \\
&\geq (q-1)q^{m-1} - (q-1)(q-(q-1))q^{m-u-2} + q^{u+1}\rho(1, m-2(u+1)) \\
&\geq (q-1)(q^{m-1} - q^{m-(u+1)-1}) + q^{u+1}\rho(1, m-2(u+1)).
\end{aligned}$$

D'où, pour $q = 3$ et $u = k-1$, on a :

$$\begin{aligned}
\rho(1,m) &\geq (q-1)(q^{m-1} - q^{k+1}) + q^{k-1}\rho(1,3) \\
&\geq (q-1)q^{m-1} - 2q^{k-1} = (q-1)q^{m-1} - \frac{2}{3}q^{\lceil \frac{m}{2} \rceil - 1}.
\end{aligned}$$

□

Corollaire 2.6.8. *Pour $q = 3$, $\rho(1,5) = 156$.*

Démonstration. Par le théorème 2.6.6, $\rho(1,5) \geq 2.3^4 - \frac{2}{3}.9 = 156$. et par le théorème 2.4.6, $\rho(1,5) \leq [2.3^4 - 3\sqrt{3}] = 156$. □

Dans ce chapitre, nous généralisons des résultats sur le rayon de recouvrement des codes binaires. Nous donnons notamment un encadrement pour le rayon de recouvrement des codes de Reed-Muller généralisés. Ce résultat repose sur un théorème qui donne une majoration du rayon de recouvrement des codes en général et sur l'étude du rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1 dans les codes de Reed-Muller généralisés d'ordre 2. Cet encadrement permet d'obtenir le rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1 pour un nombre pair de variables. Dans le cas d'un nombre impair de variables, le calcul de $\rho(1,3)$ pour $q = 3$ à l'aide du logiciel Magma nous permet d'obtenir une meilleure minoration pour le rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1 sur $\mathbb{F}_3$. Cependant le rayon de recouvrement des codes de Reed-Muller généralisés d'ordre 1 sur $\mathbb{F}_q$ reste inconnu pour un nombre impair de variables $m \geq 3$ si $q \geq 5$ et pour $m \geq 7$ si $q = 3$.

Chapitre 3

Fonctions presque parfaitement non linéaires et parfaitement non linéaires

Dans ce chapitre, on s'intéresse aux fonctions presque parfaitement non linéaires et parfaitement non linéaires. La notion de fonctions presque parfaitement non linéaires a surtout été étudiée en caractéristique paire et plus particulièrement dans le cas des fonctions puissances. Après quelques rappels, on se propose de démontrer deux conjectures de Dobbertin, Mills, Müller, Pott et Willems (voir [DMM+03]) sur des familles de fonctions puissances en caractéristique impaire. On donnera ensuite de nouvelles familles de fonctions puissances toujours en caractéristique impaire (voir [Led10b]).

3.1 Résultats préliminaires

On trouve la preuve du théorème suivant dans [LN97, p. 225].

Théorème 3.1.1 (Borne de Weil)**.** *Soit ψ un caractère multiplicatif de $\mathbb{F}_q$ d'ordre $n > 1$ et $f \in \mathbb{F}_q[x]$ unitaire de degré d qui n'est pas une puissance n-ième d'un polynôme. Alors*

$$|\sum_{x\in\mathbb{F}_q} \psi(f(x))| \leq (d-1)\sqrt{q}.$$

Lemme 3.1.2. *Soit e un entier impair et $Q = \{x^2 : x \in \mathbb{F}_{3^e}\}$. Pour $b \in \mathbb{F}_{3^e}$, on note*

$$M_b = \{(x+b)^N + (-1)^N x^N : x, x+b \in Q\}$$

où $N = 3^{\frac{e+1}{2}} + 1$, $N = 4$ ou $N = \frac{3^k+1}{2}$, $k \in \mathbb{N}$.
Alors, pour tout $b \in \mathbb{F}_{3^e}^*$, $M_b \cap (-M_b) = \emptyset$.

Démonstration. 1. Si $N = 3^{\frac{e+1}{2}} + 1$.

Comme N est pair, $M_b = M_{-b}$. Comme de plus, e est impair, -1 n'est pas un carré dans $\mathbb{F}_3^e$ et on peut supposer que b est un carré. Alors, comme

$$(x+b)^N + x^N = b^N((\frac{x}{b}+1)^N + (\frac{x}{b})^N)$$

et $\frac{x}{b}$ et $\frac{x}{b}+1$ sont des carrés, on peut supposer que $b = 1$. Supposons qu'il existe x, $y \in Q$ tels que $x+1$ et $y+1 \in Q$ et

$$x^N + (x+1)^N = -y^N - (y+1)^N.$$

On pose $m = \frac{e+1}{2}$. Alors,

$$2x^N + x^{3^m} + x + 1 = -(2y^N + y^{3^m} + y + 1).$$

On élève cette équation à la puissance 3^m :

$$2x^3x^{3^m} + x^3 + x^{3^m} + 1 = -(2y^3y^{3^m} + y^3 + y^{3^m} + 1).$$

En soustrayant la première équation à la deuxième on a :

$$(x^{3^m} - 1)(x^3 - x) = -(y^{3^m} - 1)(y^3 - y).$$

Or $(x^{3^m} - 1)(x^3 - x) = 0$ et $(y^{3^m} - 1)(y^3 - y) = 0$ si et seulement si x, $y \in \mathbb{F}_3$. Puisque $M_1 \cap -M_1 \cap \mathbb{F}_3 = \emptyset$, on peut supposer que $(x^{3^m} - 1)(x^3 - x) \neq 0$ et $(y^{3^m} - 1)(y^3 - y) \neq 0$. On a alors :

$$-1 = \frac{(x^{3^m} - 1)(x^3 - x)}{(y^{3^m} - 1)(y^3 - y)} = \frac{x(x+1)}{y(y+1)}\left(\frac{x-1}{y-1}\right)^N.$$

Comme x, $x+1$, y et $y+1$ sont des carrés et que N est pair, c'est impossible.

2. Si $N = 4$
Comme dans le cas précédent, on peut supposer que $b = 1$. Supposons qu'il existe x, $y \in Q$ tels que $x+1$ et $y+1 \in Q$ et

$$x^N + (x+1)^N = -y^N - (y+1)^N.$$

Alors,

$$2x^4 + x^3 + x + 1 + 2y^4 + y^3 + y + 1 = 0$$

c'est-à-dire

$$(y^2 + y + x^2 + x + 1)^2 = -y(y+1)x(x+1)$$

ce qui est absurde puisque x, $x+1$, y et $y+1$ sont des carrés.

3. Si $N = \frac{3^k+1}{2}$, $k \in \mathbb{N}$.
Supposons qu'il existe x, $y \in \mathbb{F}_{3^e}$ tels que x, $x+b$, y, $y+b \in Q$ et

$$(x+b)^N + (-1)^N x^N = -(y+b)^N - (-1)^N y^N.$$

On a

$$(\frac{x}{b} + 1)^N + (-1)^N(\frac{x}{b})^N + (\frac{y}{b} + 1)^N + (-1)^N(\frac{y}{b})^N = 0.$$

Soit α, $\beta \in \mathbb{F}_{3^{2e}}$ tels que $\alpha^2 - (\frac{x}{b} - 1)\alpha + 1 = 0$ et $\beta^2 - (\frac{y}{b} - 1)\beta + 1 = 0$ alors $\delta_x = (\frac{x}{b} - 1)^2 - 4 = \frac{1}{b^2}x(x+b)$ et $\delta_y = (\frac{y}{b} - 1)^2 - 4 = \frac{1}{b^2}y(y+b)$ sont des carrés et α et $\beta \in \mathbb{F}_{3^e}$. On a

$$\frac{(\alpha+1)^{2N} + (-1)^N(\alpha-1)^{2N}}{\alpha^N} + \frac{(\beta+1)^{2N} + (-1)^N(\beta-1)^{2N}}{\beta^N} = 0$$

ce qui donne

$$\alpha^{2K}\beta^K + \beta^K + \beta^{2K} + \alpha^K = 0$$

où $K = \begin{cases} N & \text{si } N \text{ est pair} \\ N-1 & \text{si } N \text{ est impair} \end{cases}$.
Autrement dit

$$(\alpha^K \beta^K + 1)(\alpha^K + \beta^K) = 0$$

On a donc $\alpha^K = -\beta^K$ ou $\alpha^K = -\beta^{-K}$, ce qui est impossible car K est pair et -1 n'est pas un carré dans $\mathbb{F}_{3^e}$

□

On rappelle ensuite le critère d'Hermite et Dickson (voir par exemple [LN97, p. 349]) qui donne une condition nécessaire et suffisante pour qu'une fonction polynomiale de $\mathbb{F}_q$ dans $\mathbb{F}_q$ soit un polynôme de permutation.

Lemme 3.1.3. *Les propositions suivantes sont équivalentes :*

1. *$f(x) \in \mathbb{F}_q[x]$ est un polynôme de permutation de $\mathbb{F}_q$*
2. *$f(x)$ a exactement une racine dans $\mathbb{F}_q$ et*
   $\forall t,\ 1 \leq t \leq q-2,\ t \not\equiv 0 \mod p$, la réduction $(f(x))^t \mod x^q - x$ est de degré strictement plus petit que $q-1$.

Pour démontrer ce lemme, on montre d'abord le résultat suivant :

Lemme 3.1.4. *Soit $a_0, \ldots, a_{q-1}$, q éléments de $\mathbb{F}_q$. On a alors équivalence entre les propositions suivantes :*

1. *$a_0, \ldots, a_{q-1}$ sont distincts.*
2. $\displaystyle\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{si } 0 \leq t \leq q-2 \\ -1 & \text{si } t = q-1 \end{cases}$

Démonstration. On considère les polynômes suivants :

$$g_i(x) = 1 - \sum_{t=0}^{q-1} a_i^t x^{q-1-t}.$$

Alors $g_i(a_i) = 1$ et pour tout $b \in \mathbb{F}_q$, $b \neq a_i$, $g_i(b) = 0$. On définit maintenant le polynôme suivant :

$$g(x) = \sum_{i=0}^{q-1} g_i(x) = \sum_{t=0}^{q-1} \left(-\sum_{i=0}^{q-1} a_i^t \right) x^{q-1-t}$$

Les a_i sont tous distincts si et seulement si $\forall x \in \mathbb{F}_q$, $g(x) = 1$. Comme $\deg(g) \leq q-1$, les a_i sont tous distincts si et seulement si $g = 1$. En identifiant les coefficients, on a le résultat. □

On prouve maintenant le lemme 3.1.3 :

Démonstration. Soit $1 \leq t \leq q-2$. On a pour tout $x \in \mathbb{F}_q$

$$f(x)^t = \sum_{c \in \mathbb{F}_q} f(c)^t (1 - (x-c)^{q-1})$$

donc

$$f(x)^t \equiv \sum_{c \in \mathbb{F}_q} f(c)^t (1 - (x-c)^{q-1}) \mod (x^q - x).$$

D'où le terme de degré $q-1$ de $f(x)^t \mod (x^q - x)$ est $-\sum_{c\in\mathbb{F}_q} f(c)^t$. Supposons d'abord que f est un polynôme de permutation. Il a donc une unique racine dans $\mathbb{F}_q$. Comme f est une bijection, $-\sum_{c\in\mathbb{F}_q} f(c)^t = -\sum_{c\in\mathbb{F}_q} c^t$. Donc, par le lemme 3.1.4, le degré de $f(x)^t \mod (x^q - x)$ est strictement plus petit que $q-1$.
Réciproquement, supposons que f n'ait qu'une racine dans $\mathbb{F}_q$ et que $\forall t$, $1 \leq t \leq q-2$, $t \not\equiv 0 \mod p$, la réduction $(f(x))^t \mod x^q - x$ soit de degré strictement plus petit que $q-1$. Alors, $\sum_{c\in\mathbb{F}_q} f(c)^{q-1} = q-1 = -1$ et pour $1 \leq t \leq q-2$, $t \not\equiv 0 \mod p$, $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$. Comme pour tout j, $(\sum_{c\in\mathbb{F}_q} f(c)^t)^{p^j} = \sum_{c\in\mathbb{F}_q} f(c)^{tp^j}$, on a en fait que $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$ pour tout $0 \leq t \leq q-2$. Par le lemme 3.1.4, les $f(c)$, $c \in \mathbb{F}_q$, sont tous distincts et donc f est un polynôme de permutation sur $\mathbb{F}_q$. □

On rappelle maintenant un résultat de Lucas (voir [Luc78]) :

Lemme 3.1.5. *Soit p un nombre premier, n et r des entiers. On considère les décompositions p-adiques de n et r :*
$n = n_0 + n_1 p + \ldots + n_k p^k$ *avec* $0 \leq n_i \leq p-1$,
$r = r_0 + r_1 p + \ldots + r_k p^k$ *avec* $0 \leq r_i \leq p-1$.
Alors

$$\binom{n}{r} \equiv \prod_{i=0}^{k} \binom{n_i}{r_i} \mod p.$$

Démonstration. On considère le polynôme de $\mathbb{F}_p[x]$ suivant :

$$(x+1)^n = \sum_{r=0}^{n} \binom{n}{r} x^r.$$

D'autre part, $(x+1)^n = \prod_{i=0}^{k} (x^{p^i}+1)^{n_i} = \prod_{i=0}^{k} \sum_{r_i=0}^{n_i} \binom{n_i}{r_i} x^{p^i r_i}$.
Par unicité de la décomposition p-adique et en identifiant les coefficients, on a le résultat. □

3.2 Définitions et premières propriétés

3.2.1 Définitions

Soit f une fonction de $\mathbb{F}_q$ dans $\mathbb{F}_q$. Pour tout a, $b \in \mathbb{F}_q$, on s'intéresse au nombre de solutions de l'équation suivante :

$$f(x+a) - f(x) = b. \tag{3.1}$$

On note $N_f(a,b)$ le nombre de solutions de cette équation. Plus particulièrement, on étudie les fonctions qui satisfont

$$\Delta_f := \max\{N_f(a,b) : a, b, \in \mathbb{F}_q, a \neq 0\} \leq 2.$$

Définition 3.2.1. On dit qu'une fonction $f : \mathbb{F}_q \to \mathbb{F}_q$ est presque parfaitement non linéaire si elle vérifie $\Delta_f = 2$.

Définition 3.2.2. Si p est impair, on dit qu'une fonction $f : \mathbb{F}_q \to \mathbb{F}_q$ est parfaitement non linéaire si elle vérifie $\Delta_f = 1$.

Remarque 3.2.3. En caractéristique paire, les fonctions parfaitement non linéaires n'existent pas. En effet, si x est solution de l'équation (3.1), $x + a$ est aussi solution de (3.1).

3.2.2 Propriétés

On commence par faire quelques remarques :

- Si $a = 0$, alors
$$N_f(0, b) = \begin{cases} 0 & \text{si } b \neq 0 \\ q & \text{si } b = 0 \end{cases}.$$
- Sinon, $\displaystyle\sum_{a,b \in \mathbb{F}_q, a \neq 0} N_f(a, b) = q^2 - q$.

Pour les fonctions puissances, on a quelques propriétés supplémentaires. Soit $f : x \mapsto x^d$ une fonction puissance sur $\mathbb{F}_q$. On note $\Delta_d = \Delta_f$.

Lemme 3.2.4. *On a* $\Delta_d = \max\{N(1, b) : b \in \mathbb{F}_q\}$.

Démonstration. Soit a, $b \in \mathbb{F}_q$, $a \neq 0$. On s'intéresse au nombre de solutions de l'équation $(x + a)^d - x^d = b$. En factorisant par a^d, on obtient

$$a^d \left(\left(\frac{x}{a} + 1 \right)^d - \left(\frac{x}{a} \right)^d \right) = b$$

et finalement, en posant $y = \frac{x}{a}$,

$$(y + 1)^d - y^d = ba^{-d}.$$

On a donc $N_f(1, ba^{-d}) = N_f(a, b)$ pour tout a, $b \in \mathbb{F}_q$, $a \neq 0$. □

Lemme 3.2.5. *Si* $\operatorname{pgcd}(d, q - 1) = 1$, *alors* $\Delta_d = \Delta_{d^{-1}}$ *où* d^{-1} *est l'inverse de* d *modulo* $q - 1$.

Démonstration. Soit a, $b \in \mathbb{F}_q$. On s'intéresse au nombre de solutions de l'équation

$$(x + a)^d - x^d = b.$$

En élevant à la puissance d^{-1}, on obtient

$$x + a = (x^d + b)^{d^{-1}}$$

et finalement, en posant $y = x^d$,

$$a = (y + b)^{d^{-1}} - y^{d^{-1}}.$$

Donc pour tout a, $b \in \mathbb{F}_q$ $N_d(a, b) = N_{d^{-1}}(b, a)$. □

3.2.3 Équivalence

Ici, on introduit deux notions d'équivalence qui sont intéressantes dans notre cadre puisqu'elles stabilisent les fonctions presque parfaitement non linéaires et les fonctions parfaitement non linéaires (voir [CCZ98, KP08]).

Dans cette section, on munit $\mathbb{F}_{p^e}$ de sa structure canonique de $\mathbb{F}_p$-espace affine.

Définition 3.2.6. Soit f et g deux fonctions de $\mathbb{F}_{p^e}$ dans $\mathbb{F}_{p^e}$. On dit que f et g sont affine étendu équivalentes s'il existe A_1 et $A_2 \in \mathrm{GA}_e(\mathbb{F}_p)$ et A une application affine de $\mathbb{F}_{p^e}$ telles que pour tout $x \in \mathbb{F}_{p^e}$ on ait

$$g(x) = A_1 \circ f \circ A_2(x) + A(x).$$

Définition 3.2.7. On dit que deux fonctions sur $\mathbb{F}_{p^e}$ f et g sont CCZ (Carlet-Charpin-Zinoviev) équivalentes si leurs graphes sont affine-équivalents. Autrement dit, si on note $G_f = \{(x, f(x)) : x \in \mathbb{F}_{p^e}\}$ et $G_g = \{(x, g(x)) : x \in \mathbb{F}_{p^e}\}$ les graphes de f et g, alors il existe $A \in \mathrm{GA}_{2e}(\mathbb{F}_p)$ tel que

$$A(G_f) = G_g.$$

Proposition 3.2.8. *Si deux fonctions f et g de $\mathbb{F}_{p^e}$ sont affine étendu équivalentes, alors elles sont CCZ-équivalentes.*

Démonstration. Comme f et g sont affine étendu équivalentes, il existe A_1, $A_2 \in \mathrm{GA}_e(\mathbb{F}_p)$ et A une application affine telles que pour tout $x \in \mathbb{F}_{p^e}$,

$$g(x) = A_2 \circ f \circ A_1(x) + A(x).$$

On écrit $A_1(x) = L_1(x) + c_1$, $A_2(x) = L_2(x) + c_2$ et $A(x) = L(x) + c$ où L_1, $L_2 \in \mathrm{GL}_e(\mathbb{F}_p)$, L est une application linéaire sur $\mathbb{F}_{p^e}$ et c_1 c_2, $c \in \mathbb{F}_{p^e}$.
On pose $y = A_1(x)$ alors $x = L_1^{-1}(y) - L_1^{-1}(c_1)$ et

$$\begin{aligned}\begin{pmatrix} x \\ g(x) \end{pmatrix} &= \begin{pmatrix} L_1^{-1}(y) - L_1^{-1}(c_1) \\ L \circ L_1^{-1}(y) - L \circ L_1^{-1}(c_1) + c + c_2 + L_2 \circ f(y) \end{pmatrix} \\ &= \begin{pmatrix} L_1^{-1} & 0 \\ L \circ L_1^{-1} & L_2 \end{pmatrix} \begin{pmatrix} y \\ f(y) \end{pmatrix} + \begin{pmatrix} -L_1^{-1}(c_1) \\ -L \circ L_1^{-1}(c_1) + c + c_2 \end{pmatrix}.\end{aligned}$$

D'où f et g sont CCZ-équivalentes. □

Proposition 3.2.9. *Les fonctions presque parfaitement non linéaires et parfaitement non linéaires sont stables par CCZ-équivalence.*

Démonstration. Soit f une fonction presque parfaitement non linéaire (resp. parfaitement non linéaire) et g une fonction CCZ-équivalente à f. Alors il existe $A \in \mathrm{GA}_{2e}(\mathbb{F}_p)$ tel que $A(G_f) = G_g$ où G_f et G_g sont les graphes respectifs de f et g. On écrit $A = (A_1, A_2)$ où A_1 et A_2 sont des applications affines de $\mathbb{F}_{p^e} \times \mathbb{F}_{p^e}$ dans $\mathbb{F}_{p^e}$. Pour tout $x \in \mathbb{F}_{p^e}$, on définit $F_1(x) = A_1(x, f(x))$ et $F_2(x) = A_2(x, f(x))$. Comme $A(G_f) = G_g$, F_1 est bijective sur $\mathbb{F}_{p^e}$ et pour tout $y \in \mathbb{F}_{p^e}$ $g(y) = F_2 \circ F_1^{-1}(y)$.
Soit a, $b \in \mathbb{F}_{p^e}$, $a \neq 0$. Pour tout $y \in \mathbb{F}_{p^e}$,

$$g(y + a) - g(y) = b \Leftrightarrow F_2 \circ F_1^{-1}(y + a) - F_2 \circ F_1^{-1}(y) = b.$$

Soit $x = F_1^{-1}(y)$ et $x_a = F_1^{-1}(y+a)$. Alors $F_1(x_a) - F_1(x) = a$ et $F_2(x_a) - F_2(x) = b$. On en déduit que

$$g(y+a) - g(y) = b \Leftrightarrow A((x_a, f(x_a))) - A((x, f(x))) = (a, b).$$

Si on écrit $A(x) = L(x) + c$ où $L \in \mathrm{GL}_{2e}(\mathbb{F}_p)$ et $c \in \mathbb{F}_{p^e}^2$ alors

$$g(y+a) - g(y) = b \Leftrightarrow (x_a, f(x_a)) - (x, f(x)) = L^{-1}(a, b) = (a'b').$$

D'où finalement

$$g(y+a) - g(y) = b \Leftrightarrow f(x+a') - f(x) = b'.$$

Ce qui donne le résultat. □

Corollaire 3.2.10. *Les fonctions presque parfaitement non linéaires et parfaitement non linéaires sont stables par équivalence affine étendue.*

Démonstration. C'est immédiat en utilisant les propositions 3.2.8 et 3.2.9. □

Proposition 3.2.11. *Si f est parfaitement non linéaire, alors*

$$f \text{ et } g \text{ sont affine étendu équivalentes} \Leftrightarrow f \text{ et } g \text{ sont CCZ-équivalentes}$$

Démonstration. La proposition 3.2.8 donne l'implication directe. Supposons que f et g soient CCZ-équivalentes. Il existe $A \in \mathrm{GA}_{2e}(\mathbb{F}_p)$ tel que $A(G_f) = G_g$ où G_f et G_g sont les graphes respectifs de f et g. On écrit A sous la forme

$$A\begin{pmatrix} x \\ y \end{pmatrix} = L\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} L_1 & L_2 \\ L_3 & L_4 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

où $L \in \mathrm{GL}_{2e}(\mathbb{F}_p)$, les L_i sont des applications linéaires de $\mathbb{F}_{p^e}$ et $c_i \in \mathbb{F}_{p^e}$. On a

$$L\begin{pmatrix} x \\ f(x) \end{pmatrix} = \begin{pmatrix} y - c_1 \\ g(y) - c_2 \end{pmatrix} = \begin{pmatrix} y' \\ g(y' + c_1) - c_2 \end{pmatrix}.$$

On définit alors $\widetilde{g} : y \mapsto g(y + c_1) - c_2$. Soit a, $b \in \mathbb{F}_{p^e}$, $a \neq 0$. Comme f est parfaitement non linéaire, il existe $x \in \mathbb{F}_{p^e}$ tel que $f(x+a) - f(x) = b$. Alors

$$L\begin{pmatrix} a \\ b \end{pmatrix} = L\begin{pmatrix} x + a - x \\ f(x+a) - f(x) \end{pmatrix} = L\begin{pmatrix} x + a \\ f(x+a) \end{pmatrix} - L\begin{pmatrix} x \\ f(x) \end{pmatrix} = \begin{pmatrix} y_a \\ \widetilde{g}(y_a) \end{pmatrix} - \begin{pmatrix} y \\ \widetilde{g}(y) \end{pmatrix}.$$

Comme $\begin{pmatrix} a \\ b \end{pmatrix} \neq 0$, $y_a \neq y$ et donc, comme L est bijective,

$$L\left(\left\{\begin{pmatrix} 0 \\ c \end{pmatrix} : c \in \mathbb{F}_{p^e}\right\}\right) = \left\{\begin{pmatrix} 0 \\ c \end{pmatrix} : c \in \mathbb{F}_{p^e}\right\}.$$

Pour tout $c \in \mathbb{F}_{p^e}$, $L\begin{pmatrix} 0 \\ c \end{pmatrix} = \begin{pmatrix} L_2(c) \\ L_4(c) \end{pmatrix} = \begin{pmatrix} 0 \\ d \end{pmatrix}$ donc $L_2 = 0$. On a donc L_1 et $L_4 \in \mathrm{GL}_e(\mathbb{F}_p)$ et

$$A\begin{pmatrix} x \\ f(x) \end{pmatrix} = \begin{pmatrix} L_1(x) + c_1 \\ L_3(x) + L_4(f(x)) + c_2 \end{pmatrix}.$$

On note $A_1(x) = L_1(x) + c_1$, $A_1 \in \mathrm{GA}_e(\mathbb{F}_p)$ et $g(y) = L_3 \circ A_1^{-1}(y) + c_2 + L_4 \circ f \circ A_1^{-1}(y)$. □

3.3 Exemples de fonctions presque parfaitement non linéaires et parfaitement non linéaires

Dans cette section, on donne les fonctions presque parfaitement non linéaires et parfaitement non linéaires connues à ce jour.

3.3.1 Fonctions puissances parfaitement non linéaires

Dans cette sous-section p est impair.

Aujourd'hui, les seules fonctions puissances parfaitement non linéaires connues sont celles données dans le théorème suivant :

Théorème 3.3.1. *Soit $f : x \mapsto x^d$ une fonction puissance. Alors f est parfaitement non linéaire sur $\mathbb{F}_{p^e}$ pour*

1. $d = 2$
2. $d = p^k + 1$ *où k est un entier tel que* $\frac{e}{\mathrm{pgcd}(e,k)}$ *soit impair [CM97, DO68].*
3. $d = \frac{3^k+1}{2}$ *où $p = 3$ et k est un entier impair tel que* $\mathrm{pgcd}(e, k) = 1$ *[CM97].*

Pour démontrer ce théorème, on prouve d'abord la proposition suivante :

Proposition 3.3.2. *Soit p un nombre premier impair. Pour $d = \frac{p^k+1}{2}$, la fonction $x \mapsto x^d$ définie sur $\mathbb{F}_{p^e}$ vérifie*

$$\Delta_d \leq \mathrm{pgcd}(\frac{p^k - 1}{2}, p^{2e} - 1).$$

Démonstration. Par le lemme 3.2.4, il suffit de montrer que pour tout $b \in \mathbb{F}_{p^e}$, l'équation $(x + 1)^d - x^d = b$ a au plus $T = \mathrm{pgcd}(\frac{p^k-1}{2}, p^{2e} - 1)$ solutions.
On pose $u = \begin{cases} \frac{p-1}{4} & \text{si } p \equiv 1 \mod 4 \\ -\frac{p+1}{4} & \text{si } p \equiv 3 \mod 4 \end{cases}$ et $t = u^2$. Soit $\alpha \in \mathbb{F}_{p^{2e}}$ tel que

$$\alpha^2 - (x + \frac{p-1}{2})\alpha + t = 0.$$

L'équation devient alors

$$\frac{(\alpha - u)^{2d} - (\alpha + u)^{2d}}{\alpha^d} = b.$$

En simplifiant, on a

$$\alpha^{d-1} + \alpha^{-(d-1)} = 2b. \tag{3.2}$$

Soit α_1 et α_2 deux solutions de cette équation, on a

$$(\alpha_1^{d-1}\alpha_2^{d-1} - 1)(\alpha_2^{d-1} - \alpha_1^{d-1}) = 0.$$

Donc, soit $\alpha_2 = \gamma\alpha_1$, soit $\alpha_2 = \gamma\alpha_1^{-1}$ où γ est une racine Tème de 1. D'où, si α est une solution de l'équation (3.2), toutes les solutions de cette équation sont de la forme $\gamma\alpha$ ou $\gamma\alpha^{-1}$ avec γ racine Tème de 1. Chacune de ces solutions donne une solution

$$x = \alpha + t\alpha^{-1} - \frac{p-1}{2}.$$

Soit α_1 et α_2 deux solutions telles que $\alpha_1 + t\alpha_1^{-1} = \alpha_2 + t\alpha_2^{-1}$ alors soit $\alpha_1 = \alpha_2$ soit $\alpha_1\alpha_2 = t$. Puisque $t^T = 1$, l'équation $(x + 1)^d - x^d = b$ a au plus T solutions. □

On peut maintenant démontrer le théorème.

Démonstration. Comme on considère des fonctions puissances, par le lemme 3.2.4, il suffit de montrer que pour tout $b \in \mathbb{F}_q$, l'équation $(x+1)^d - x^d = b$ a une unique solution. Autrement dit, il faut montrer que l'application $\phi : x \mapsto (x+1)^d - x^d$ est une bijection sur $\mathbb{F}_q$.

1. On a $(x+1)^2 - x^2 = 2x+1$. Donc ϕ est bien une bijection sur $\mathbb{F}_q$.

2. On a $(x+1)^{p^k+1} - x^{p^k+1} = x^{p^k} + x + 1$. L'application $x \mapsto x^{p^k} + x$ est linéaire sur $\mathbb{F}_q$. De plus, $x^{p^k} + x = 0$ si et seulement si $x = 0$ ou $x^{p^k-1} = -1$. Comme $\frac{e}{\mathrm{pgcd}(e,k)}$ est impair, -1 n'est pas une puissance (p^k-1)ème. D'où $x \mapsto x^{p^k} + x$ est injective, ce qui donne le résultat.

3. Par la proposition 3.3.2, comme k est impair et $\mathrm{pgcd}(k,e) = 1$,

$$\Delta_d \leq \mathrm{pgcd}(\frac{3^k-1}{2}, 3^{2e}-1) = 1.$$

□

3.3.2 Fonctions puissances presque parfaitement non linéaires

En caractéristique 2, on conjecture que la liste des fonctions puissance presque parfaitement non linéaires donnée dans le théorème suivant est complète à équivalence près.

Théorème 3.3.3. *Soit $f : x \mapsto x^d$ une fonction puissance. Alors f est presque parfaitement non linéaire sur $\mathbb{F}_{2^e}$ pour*

1. *$d = 2^k + 1$ où k est un entier tel que $\mathrm{pgcd}(e,k) = 1$ (Gold, [Nyb94]).*

2. *$d = 2^{2k} - 2^k + 1$ où k est un entier tel que $\mathrm{pgcd}(k,e) = 1$ (Kasami, [JW93, Dob99c, Dob99b]).*

3. *$d = 2^e - 2$ si e est impair (Kloostermann, [Nyb94]).*

4. *$d = 2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1$ si $e = 5k$ (Dobbertin, [Dob01]).*

5. *$d = 2^k + 3$ si $e = 2k+1$ est impair (Welch, [Dob99b]).*

6. *$d = 2^{2k} + 2^k - 1$ où k est un entier tel que $4k + 1 \equiv 0 \mod e$ (Niho, [Dob99a]).*

Démonstration. D'après le lemme 3.2.4 et la remarque 3.2.3, il suffit de montrer que l'équation $(x+1)^d - x^d = b$ a au plus deux solutions pour tout $b \in \mathbb{F}_{2^e}$.

1. Soit $b \in \mathbb{F}_{2^e}$. On cherche le nombre de $x \in \mathbb{F}_{2^e}$ tels que

$$(x+1)^d + x^d = b;$$

autrement dit tels que

$$x^{2^k} + x = b - 1.$$

Or, $x \mapsto x^{2^k} + x$ est une application linéaire sur $\mathbb{F}_{2^e}$, il faut donc montrer que son noyau a au plus deux éléments. On a $x^{2^k} + x = 0$ si et seulement si $x = 0$ ou $x^{2^k-1} = 1$. Comme $\mathrm{pgcd}(e,k) = 1$, $x^{2^k-1} = 1$ si et seulement si $x = 1$.

2. Pour prouver ce résultat, on utilise la transformée de Walsh d'une fonction de $\mathbb{F}_{2^e}$ dans $\mathbb{F}_2$: soit $f : F_{2^e} \to \mathbb{F}_2$, $a \in \mathbb{F}_{2^e}$,

$$W(f)(a) = \sum_{x \in \mathbb{F}_{2^e}} (-1)^{f(x)+\mathrm{tr}(ax)}$$

où $\mathrm{tr} = \mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}$.
En particulier, la transformée de Walsh de la fonction $tr^{(d)} : x \mapsto \mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(x^d)$ est telle que :

$$\sum_{a \in \mathbb{F}_{2^e}} (W(tr^{(d)})(a))^4 = 2^e \sum_{y,z \in \mathbb{F}_{2^e}} \sum_{v \in \mathbb{F}_{2^e}} (-1)^{\mathrm{tr}(v((y+1)^d+y^d+(z+1)^d+z^d))}.$$

Or,

$$\sum_{v \in \mathbb{F}_{2^e}} (-1)^{\mathrm{tr}(v((y+1)^d+y^d+(z+1)^d+z^d))} = \begin{cases} 2^e & \text{si } (y+1)^d + y^d = (z+1)^d + z^d \\ 0 & \text{sinon} \end{cases}$$

donc

$$\sum_{a \in \mathbb{F}_{2^e}} (W(tr^{(d)})(a))^4 = 2^{2e} \#\{(y,z) \in \mathbb{F}_{2^e}^2 : (y+1)^d + y^d = (z+1)^d + z^d\}.$$

Par [Dob99c], on obtient

$$2^{3e+1} = 2^{2e} \#\{(y,z) \in \mathbb{F}_{2^e}^2 : (y+1)^d + y^d = (z+1)^d + z^d\}$$

ce qui donne le résultat.

3. On commence par remarquer que $x = 1$ et $x = 0$ sont solutions de l'équation pour $b = 1$. Supposons maintenant que $x \neq 0$ et $x \neq 1$. L'équation devient

$$(x+1)^{-1} + x^{-1} = b$$

c'est-à-dire

$$bx^2 + bx + 1 = 0.$$

On a donc bien au plus deux solutions si $b \neq 1$. Supposons que $b = 1$ alors l'équation devient $x^2 + x + 1 = 0$ qui est irréductible sur $\mathbb{F}_{2^e}$ pour e impair.

4. Voir [Dob01].

5. Il est démontré dans [Dob99b] que $P(x) = x^{2^{k+1}+1} + x^3 + x$ est un polynôme de permutation sur $\mathbb{F}_{2^e}$. Or $(x+1)^d + x^d = P(x^{2^k} + x) + 1$ ce qui donne le résultat.

6. Il est démontré dans [Dob99a] que

$$P(x) = x^{2^{2k+1}+2^{k+1}+1} + x^{2^{2k+1}+2^{k+1}-1} + x^{2^{2k+1}+1} + x^{2^{2k+1}-1} + x$$

est un polynôme de permutation sur $\mathbb{F}_{2^e}$. Pour $x = 0$ ou $x = 1$, $(x+1)^d + x^d = 1$. Pour $x \neq 0$ et $x \neq 1$, $(x+1)^d + x^d = (P((x^{2^k} + x)^{2^k-1} + 1))^{2^e-2} + 1$. Si x, $y \in \mathbb{F}_{2^e}$,

$$(x^{2^k} + x)^{2^k-1} + 1 = (y^{2^k} + y)^{2^k-1} + 1 \Leftrightarrow y = x \text{ ou } y = x + 1$$

puisque $\gcd(k,e)=1$. Comme de plus $x \mapsto (P(x))^{2^e-2}+1$ est une bijection, pour $b \neq 1$, l'équation $(x+1)^d + x^d = b$ a au plus deux solutions. Si $b=1$,

$$(P((x^{2^k}+x)^{2^k-1}+1))^{2^e-2}+1=1$$

et on obtient

$$x^{2^k}+x+1=0.$$

Comme $x^{2^k}+x+1$ est irréductible sur $\mathbb{F}_{2^e}$ pour e impair, on a le résultat.

□

En caractéristique impaire, Helleseth, Rong et Sandberg ont recherché par ordinateur des fonctions puissances qui sont presque parfaitement non linéaires sur des petits corps, i.e pour $p^e \in \{2^2, 2^3, \ldots, 2^{11}, 3^2, \ldots, 3^7, 5^2, \ldots, 5^5, 7^2, 7^3, 7^4, 11^2, 11^3\}$. Dans [HRS99], ils donnent un certain nombre de familles infinies contenant les exposants qu'ils ont trouvés. On regroupe ces familles dans le théorème suivant :

Théorème 3.3.4. *Soit $f : x \mapsto x^d$ une fonction puissance. Alors f est presque parfaitement non linéaire sur $\mathbb{F}_{p^e}$ pour*

1. $d = p^e - 2$ *si* $p^e \equiv 2 \mod 3$ *[HRS99].*
2. $d = \frac{p^e-1}{2} - 1$ *si* $p \equiv 3, 7 \mod 20$, $p^e > 7$, $p^e \neq 27$ *et e est impair [HS97].*
3. $d = 3$ *si* $p \neq 3$ *[HRS99].*
4. $d = \begin{cases} \frac{p^e+1}{4} + \frac{p^e-1}{2} & \text{si } p^e \equiv 3 \mod 8 \\ \frac{p^e+1}{4} & \text{si } p^e \equiv 7 \mod 8 \end{cases}$ *si* $p^e > 7$ *[HRS99].*
5. $d = \frac{2p^e-1}{3}$ *si* $p^e \equiv 2 \mod 3$ *[HRS99].*
6. $d = p^e - 3$ *si* $p = 3$ *et* $e > 1$ *est impair [HRS99].*
7. $d = p^{\frac{e}{2}} + 2$, $p > 3$, *e pair et* $p^{\frac{e}{2}} \equiv 1 \mod 3$ *[HRS99].*
8. $d = p^{\frac{e+1}{2}} - 1$ *si* $p = 3$ *et e est impair [HRS99].*
9. $d = \frac{5^k+1}{2}$ *si* $p = 5$ *et k est un entier tel que* $\mathrm{pgcd}(2e, k) = 1$ *[HRS99].*

Démonstration. D'après le lemme 3.2.4, il suffit de regarder le nombre de solutions de l'équation $(x+1)^d - x^d = b$ pour tout $b \in \mathbb{F}_{p^e}$.

1. Si $x = 0$ ou $x = -1$ alors $(x+1)^d - x^d = 1$. Supposons que $x \neq 0$ et $x \neq -1$. Alors l'équation devient

$$(x+1)^{-1} - x^{-1} = b$$

autrement dit

$$bx^2 + x + 1 = 0.$$

Donc, pour $b \neq 1$, l'équation $(x+1)^d - x^d = b$ a au plus deux solutions. Si $b = 1$, on obtient l'equation du second degré x^2+x+1 de discriminant $\delta = -3$. Donc la fonction est presque parfaitement non linéaire si et seulement si -3 n'est pas une carré dans $\mathbb{F}_{p^e}$. Or, $p^e \equiv 2 \mod 3$ et 2 n'est pas un carré dans $\mathbb{F}_3$ donc nécessairement e est impair et $p \equiv 2 \mod 3$. Donc la fonction est presque parfaitement non linéaire si et seulement si (-3) est un carré dans $\mathbb{F}_p$. Or, la loi de réciprocité quadratique nous donne $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$. Comme $p \equiv 2 \mod 3$, $\left(\frac{-3}{p}\right) = -1$ et -3 n'est pas un carré dans $\mathbb{F}_{p^e}$.

2. Pour $x \neq 0$ et $x \neq -1$, l'équation devient $\chi(x+1)\frac{1}{x+1} - \chi(x)\frac{1}{x} = b$ où χ est le caractère quadratique. On étudie le nombre de solutions dans les deux cas suivants : $\chi(x) = \chi(x+1)$ et $\chi(x) = -\chi(x+1)$ et on trouve que $\Delta_d \leq 2$. De plus, $\Delta_d = 2$ si et seulement s'il existe $b \in \mathbb{F}_{p^e}$ tel que $\chi(b) = 1$, $\chi(1+4b) = 1$ et $\chi(1+4b^2) = 1$. Soit
$$A = \sum_{\substack{c \in \mathbb{F}_{p^e} \setminus \{-1,0,1\} \\ \chi(1+4c^2)=1}} (1 + \chi(1+4c^4)).$$
Alors
$$\begin{aligned} A + 2 &= \sum_{c \in \mathbb{F}_{p^e}} (\chi(1+4c^2)+1)(\chi(1+4c^4)+1) \\ &= \sum_{c \in \mathbb{F}_{p^e}} (\chi((1+4c^2)(1+4c^4)) + \chi(1+4c^4) + \chi(1+4c^2) + 1. \end{aligned}$$
Donc, par le théorème 3.1.1, on a
$$|A + 2 - p^e| \leq 9\sqrt{p^e}.$$
Donc, pour $p^e \geq 85$, $A > 0$ et on a le résultat. Il reste à traiter les cas $p^e = 23$, 27, 43, 47, 49, 67, 81, 83. Pour cela, on utilise un ordinateur.

3. On a $(x+1)^3 - x^3 = b \Leftrightarrow 3x^2 + 3x + 1 - b = 0$. On a donc au plus deux solutions pour chaque b si $p \neq 3$. De plus pour $b = 1$, $x = 0$ et $x = -1$ sont solutions.

4. On a $2d \equiv 1 + \frac{p^e-1}{2} \mod p^e - 1$ alors, si on on note $u_x = x^d$, en élevant l'équation $u_{x+1} = u_x + b$ au carré, on obtient l'équation suivante :
$$\chi(x+1)(x+1) - \chi(x)x = 2bu_x + b^2.$$
On étudie le nombre de solutions de cette équation dans les cas où $\chi(x) = \chi(x+1)$ et $\chi(x+1) = -\chi(x)$ et on trouve que $\Delta_d \leq 2$. De plus, $\sum_{b \in \mathbb{F}_{p^e}} N(1,b) = p^e$ donc $\Delta_d = 2$ s'il existe $b \in \mathbb{F}_{p^e}$ tel que $N(1,b) = 0$. Si $b \in \mathbb{F}_{p^e}$ vérifie $\chi(1-b^2) = -\chi(2)$ et $\chi(1+b^2) = \chi(2)$ alors $N(1,b) = 0$. On prouve qu'un tel b existe à l'aide du théorème 3.1.1.

5. On a $3d \equiv 1 \mod p^e - 1$. Si on note $u_x = x^d$, on a $u_{x+1} = u_x + b$. En élevant cette équation à la puissance 3, on obtient
$$3bu_x^2 + 3b^2u_x + b^3 - 1 = 0.$$
On a donc au plus deux valeurs possibles pour u_x. Comme $\mathrm{pgcd}(d, p^e - 1) = 1$, on a au plus deux possibilités pour x. De plus, comme $\mathrm{pgcd}(p^e - 1, d) = 1$, l'équation $(x+1)^d - x^d = 0$ n'a pas de solution. Puisque $\sum_{b \in \mathbb{F}_{p^e}} N(1,b) = p^e$, on a le résultat.

6. Si $x \neq 0$ et $x \neq -1$, l'équation devient
$$(x+1)^{-2} - x^{-2} = b$$
c'est-à-dire
$$bx^4 + 2bx^3 + bx^2 + 2x + 1 = 0$$
et pour $p = 3$, $e > 1$ impair et $b \neq 0, 1, -1$, cette équation a au plus deux solutions. Elle a au plus une solution si $b = -1, 0, 1$.

7. Voir [HRS99].

8. 0 est solution de $(x+1)^d - x^d = 1$ et -1 est solution de $(x+1)^d - x^d = -1$. Supposons que $x \neq 0$ et $x \neq -1$. L'équation devient alors

$$-x^{p^{\frac{e+1}{2}}} = bx^2 + (b-1)x.$$

En élevant cette équation à la puissance $p^{\frac{e+1}{2}}$, on obtient :

$$x^p + b^{p^{\frac{e+1}{2}}}(x^{p^{\frac{e+1}{2}}})^2 + (b-1)^{p^{\frac{e+1}{2}}} x^{p^{\frac{e+1}{2}}} = 0.$$

En remplaçant $x^{p^{\frac{e+1}{2}}}$, on a

$$b^{p^{\frac{e+1}{2}}+2}x^4 + (1 + 2b(b-1)b^{p^{\frac{e+1}{2}}})x^3 + (b^{p^{\frac{e+1}{2}}+2} + b^{p^{\frac{e+1}{2}}} + b)x^2 - (b-1)^{p^{\frac{e+1}{2}}+1}x = 0$$

soit en factorisant

$$x(x+1)(b^{p^{\frac{e+1}{2}}+2}x^2 + (1 + b^{p^{\frac{e+1}{2}}+2} + b^{p^{\frac{e+1}{2}}+1})x - (b-1)^{p^{\frac{e+1}{2}}+1}) = 0.$$

Le discriminant du terme de degré 2 est $\delta = (b^{p^{\frac{e+1}{2}}} + 2)^{p^{\frac{e+1}{2}}+1}$ donc si $b^{p^{\frac{e+1}{2}}} \neq 1$, on a deux solutions distinctes. De plus, si $b = 1$, l'équation devient $x^3(x+1) = 0$. Si $b = -1$, l'équation devient $x(x+1)^3 = 0$.

9. Par la proposition 3.3.2, on a $\Delta_d \leq 2$. Comme d est impair, 0 et -1 sont solutions de $(x+1)^d - x^d = 1$.

□

Les seuls exposants trouvés par Helleseth, Sandberg et Rong lors de leur étude sur les petits corps qui ne sont pas inclus dans une famille infinie sont récapitulés dans le tableau 3.1

Table 3.1 – Exposants pour lesquels [HRS99] ne donne pas de famille infinie

	p^e	d	dp^i
I	3^5	134	(134,160,238,230,206)
II	3^5	152	(152,214,158,232,212)
III	3^7	40	(40,120,360,1080,1054,976,742)
IV	3^7	224	(224,672,2016,1676,656,1968,1532)
V	3^7	274	(274,822,280,840,334,1002,820)
VI	5^3	14	(14,70,102)
VII	5^5	843	(843,1091,2331,2283,2043)

Dans [ZW10], Wang et Zha démontrent les deux théorèmes suivants. Ils ne donnent pas de familles explicites de fonctions puissances mais ils expliquent certains cas du tableau 3.1. Voici d'abord un premier théorème qui concerne la caractéristique 3.

Théorème 3.3.5. *Sur $\mathbb{F}_{3^e}$, la fonction $f : x \mapsto x^d$ vérifie $\Delta_d \leq 2$ pour d pair tel que $(3^k+1)d - 2 = u(3^e - 1)$ où u est impair et $\gcd(e,k) = 1$. De plus, f est presque parfaitement non linéaire si $2k < e$.*

Démonstration. Puisque d est pair, on a nécessairement u et e impair. Par le lemme 3.2.4, on veut montrer que l'équation $(x+1)^d - x^d = b$ a au plus deux solutions pour tout $b \in \mathbb{F}_{3^e}$. Si $b = 0$, puisque $\text{pgcd}(d, 3^e - 1) = 2$, cette équation a une solution. A partir de maintenant, on suppose que $b \neq 0$. Si on note $N = \frac{3^k+1}{2}$, alors

$$Nd \equiv 1 + \frac{3^e - 1}{2} \mod 3^e - 1.$$

On note $u_x = x^d$, alors $u_{x+1} = u_x + b$ et pour tout $x \in \mathbb{F}_{3^e}$, $u_x^N = \chi(x)x$. Donc

$$(u_x + b)^N - u_x^N = \chi(x+1)(x+1) - \chi(x)x.$$

- Cas A : $\chi(x) = \chi(x+1)$, $x = 0$ ou $x = -1$.
  Si $x = 0$, $(u_x + b)^N - u_x^N = 1$.
  Si $x = -1$, $(u_x + b)^N - u_x^N = -1$.
  Si $\chi(x) = \chi(x+1)$, $(u_x + b)^N - u_x^N = \chi(x)$.
  Dans tous les cas, on cherche à résoudre une des équations suivantes :

  $$(u_x + b)^N - u_x^N = \varepsilon, \qquad \text{avec } \varepsilon \in \{-1, 1\} \tag{3.3}$$

  On veut résoudre cette équation avec les mêmes méthodes que dans la proposition 3.3.2 : soit $\alpha \in \mathbb{F}_{3^{2e}}$ tel que $\alpha^2 - (\frac{u_x}{b} - 1)\alpha + 1 = 0$. Cependant, le discriminant de cette équation est

  $$\delta = (\frac{u_x}{b} - 1)^2 - 4 = \frac{1}{b^2} u_x u_{x+1}.$$

  Puisque d est pair, δ est un carré et donc $\alpha \in \mathbb{F}_{3^e}$. On a au plus $\text{pgcd}(N-1, 3^e-1)$ solutions à l'équation (3.3).
  Si k est impair, $\text{pgcd}(N-1, 3^e-1) = 1$ et N est pair. Les deux équations

  $$(u_x + b)^N - u_x^N = 1 \text{ et } (u_x + b)^N - u_x^N = -1$$

  ont chacune au plus une solution. Supposons qu'elles aient chacune une solution, c'est-à -dire qu'il existe $x \in \mathbb{F}_{3^e}$ tel que $\chi(x) = 1$ ou $x = 0$ et $(u_x + b)^N - u_x^N = 1$ d'une part et $y \in \mathbb{F}_{3^e}$ tel que $\chi(y) = -1$ et $(u_y + b)^N - u_y^N = -1$ d'autre part. On a alors $(-(u_x + b) + b)^N - (-(u_x + b))^N = u_x^N - (u_x + b)^N = -1$ et par unicité, on a $u_y = -(u_x + b) = -u_{x+1}$ ce qui est absurde car u_y et u_{x+1} sont des carrés dans $\mathbb{F}_{3^e}$ mais pas -1.
  Si k est pair, alors $\text{pgcd}(N-1, 3^e-1) = 2$ et N est impair. Par le lemme 3.1.2, au plus une des deux équations a une solution. De plus, si une de ces équations a des solutions, elle en a au plus 2. Ces deux solutions donnent les couples (u_x, u_{x+1}) suivants :

  $$\begin{array}{l} u_x = b(\alpha + \alpha^{-1}) + b \\ u_{x+1} = b(\alpha + \alpha^{-1}) - b \end{array} \quad \text{ou} \quad \begin{array}{l} u_x = -b(\alpha + \alpha^{-1}) + b \\ u_{x+1} = -b(\alpha + \alpha^{-1}) - b \end{array}$$

  où α est solution de l'équation $\alpha^{N-1} + \alpha^{-N+1} = 2\varepsilon b^{-N}$. Or u_x et u_{x+1} sont tous les deux des carrés mais pas -1 donc au plus une de ces solutions est possible.

- Cas B : $\chi(x) = -\chi(x+1)$.
  Alors $(u_x + b)^N - u_x^N = \chi(x)x - \chi(x) = u_x^N - \chi(x)$. On cherche donc à résoudre une des deux équations suivantes :

  $$(u_x + b)^N + u_x^N = \varepsilon, \qquad \text{avec } \varepsilon \in \{-1, 1\} \tag{3.4}$$

Comme dans le cas A, les deux équations (3.4) ont au plus $\mathrm{pgcd}(N, 3^e - 1)$ solutions. Si k est impair, alors $\mathrm{pgcd}(N, 3^e - 1) = 2$ et N est pair. Par le lemme 3.1.2, au plus une des deux équations de (3.4) a une solution. De plus, si une de ces équations a des solutions, elle en a au plus 2. Ces deux solutions donnent les couples (u_x, u_{x+1}) suivants :

$$\begin{array}{l} u_x = b(\alpha + \alpha^{-1}) + b \\ u_{x+1} = b(\alpha + \alpha^{-1}) - b \end{array} \quad \text{ou} \quad \begin{array}{l} u_x = -b(\alpha + \alpha^{-1}) + b \\ u_{x+1} = -b(\alpha + \alpha^{-1}) - b \end{array}$$

où α est solution de l'équation $\alpha^N + \alpha^{-N} = 2\varepsilon b^{-N}$. Or, u_x et u_{x+1} sont tous les deux des carrés mais pas -1 donc au plus une de ces solutions est possible.
Si k est pair alors $\mathrm{pgcd}(N, 3^e - 1) = 1$ et N est impair. Pour les mêmes raisons que dans le cas A, k impair, on a au plus une solution.

Il reste à montrer que si $2k < e$, il existe un b dans $\mathbb{F}_{3^e}$ tel que $N(1, b) = 2$. Or

$$\sum_{b \in \mathbb{F}_q} N(1, b) = 3^e$$

donc il suffit de prouver qu'il existe b tel que $N(1, b) = 0$. Dans tous les cas, il y a une solution à l'équation $(x + 1)^d - x^d = b$ si l'équation $\alpha^K + \alpha^{-K} = 2\varepsilon b^{-N}$ avec $K = N$ ou $K = N - 1$ a au moins une solution dans $\mathbb{F}_{3^e}$. Ceci n'est possible que si

$$\delta = (2\varepsilon b^{-N})^2 - 4 = 4b^{-2N}(1 - b^{2N})$$

est un carré. On montre que si $2k < e$, il existe $b \in \mathbb{F}_{3^e}^*$ tel que $\chi(1 - b^{3^k+1}) = -1$. On note $L = \sum_{b \in \mathbb{F}_{3^n}} 1 - \chi(1 - b^{3^k+1})$. Alors, par le théorème 3.1.1, on a $|L - 3^e| \leq 3^k.3^{\frac{e}{2}}$ d'où $L > 0$ si $e > 2k$. □

On rappelle maintenant un second théorème de Wang et Zha qui concerne la caractéristique 5.

Théorème 3.3.6. *La fonction $x \mapsto x^d$ est presque parfaitement non linéaire sur $\mathbb{F}_{5^e}$ pour d tel que $(5^k + 1)d - 2 = u(5^e - 1)$ où $\mathrm{pgcd}(e, k) = 1$, u est impair et k est pair.*

Démonstration. On commence par remarquer que nécessairement d est impair, alors -1 et 0 sont solutions de $(x + 1)^d - x^d = 1$ et donc $\Delta_d \geq 2$. On montre maintenant que $\Delta_d \leq 2$. Par le lemme 3.2.4, il suffit de montrer que l'équation $(x + 1)^d - x^d = b$ a au plus deux solutions pour tout $b \in \mathbb{F}_{5^e}$. Si $b = 0$, puisque $\mathrm{pgcd}(d, 5^e - 1) = 2$, cette équation a une solution. A partir de maintenant, on suppose $b \neq 0$. On note $N = \frac{5^k+1}{2}$. Puisque u est impair, on a

$$Nd \equiv 1 + \frac{5^e - 1}{2} \mod 5^e - 1.$$

On note $u_x = x^d$ et on a $u_{x+1} = u_x + b$ et

$$(u_x + b)^N - u_x^N = \chi(x + 1)(x + 1) - \chi(x)x.$$

- Cas A : : $\chi(x) = \chi(x + 1)$, $x = 0$ ou $x = -1$.
  Si $x = 0$, $(u_x + b)^N - u_x^N = 1$.
  Si $x = -1$, $(u_x + b)^N - u_x^N = 1$.
  Si $\chi(x) = \chi(x+1)$, $(u_x + b)^N - u_x^N = \chi(x)$. On obtient alors les équations suivantes :

$$(u_x + b)^N - u_x^N = \varepsilon, \qquad \text{avec } \varepsilon \in \{-1, 1\}. \tag{3.5}$$

Soit α tel que $\alpha^2-(\frac{u_x}{b}-2)\alpha+1=0$. Alors $\delta=(\frac{u_x}{b}-2)^2-4=\frac{1}{b^2}u_xu_{x+1}$ est un carré car $\chi(x)=\chi(x+1)$ et donc $\alpha\in\mathbb{F}_{5^e}$. Comme dans la proposition 3.3.2, chacune des équations (3.5) a au plus $\mathrm{pgcd}(\frac{5^k-1}{2},5^e-1)=2$ solutions et ces solutions donnent les couples de solutions (u_x,u_{x+1}) suivants :

$$\begin{array}{l} u_x=b(\alpha+\alpha^{-1})+b \\ u_{x+1}=b(\alpha+\alpha^{-1})-b \end{array} \quad \text{ou} \quad \begin{array}{l} u_x=-b(\alpha+\alpha^{-1})+2b \\ u_{x+1}=-b(\alpha+\alpha^{-1})-2b \end{array}$$

où α est solution de l'équation $\alpha^{N-1}+\alpha^{-N+1}=2\varepsilon b^{-N}$. Or,

$$b(\alpha+\alpha^{-1})+2b=b\alpha^{-1}(\alpha+1)^2 \text{ et } b(\alpha+\alpha^{-1})-2b=b\alpha^{-1}(\alpha-1)^2$$

donc u_x et u_{x+1} sont des carrés dans $\mathbb{F}_{5^e}$. D'où, comme d est impair, seule l'équation avec $\varepsilon=1$ a des solutions. On a donc au plus deux solutions dans ce cas.

- Cas B : $\chi(x)=-\chi(x+1)$. On obtient alors les équations suivantes :

$$(u_x+b)^N+u_x^N=\varepsilon, \qquad \text{avec } \varepsilon\in\{-1,1\}.$$

Soit α tel que $\alpha^2-(\frac{u_x}{b}-2)\alpha+1=0$. Comme dans la proposition 3.3.2, on obtient au plus $\mathrm{pgcd}(\frac{5^k+1}{2},5^{2e}-1)=1$ solution pour chaque équation. Alors

$$u_x=b(\alpha+\alpha^{-1})+2b \text{ et } u_{x+1}=b(\alpha+\alpha^{-1})-2b$$

où α est solutions de $\alpha^N+\alpha^{-N}=2\varepsilon b^{-N}$. On a alors

$$u_xu_{x+1}=b^2(\alpha+\alpha^{-1})^2-4b^2=b^2(\alpha-\alpha^{-1})^2$$

ce qui est absurde puisque d est impair et $\chi(x)=-\chi(x+1)$. On n'a donc pas de solution dans ce cas.

□

3.3.3 Exemples de fonctions qui ne sont pas des fonctions puissances

Dans la suite, on donne une liste de fonctions parfaitement non linéaires et presque parfaitement non linéaires qui ne sont pas des fonctions puissances, c'est-à-dire qu'elles ne sont pas équivalentes à une fonction puissance.

Théorème 3.3.7. *Les fonctions suivantes sont des fonctions parfaitement non linéaires :*

1. $f(x)=x^{10}+x^6-x^2$ *sur* $\mathbb{F}_{3^e}$, $e\geq 5$, e *impair [CM97, DY06].*
2. $f(x)=x^{10}-x^6-x^2$ *sur* $\mathbb{F}_{3^e}$, $e\geq 5$, e *impair [DY06].*
3. $f(x)=x^{p^s+1}-u^{p^k-1}x^{p^k+p^{2k+s}}$ *sur* $\mathbb{F}_{p^{3k}}$ *où* $\mathrm{pgcd}(3,k)=1$, $k-s\equiv 0 \mod 3$, $s\neq k$, $\frac{k}{\mathrm{pgcd}(k,s)}$ *est impair et* u *est un élément primitif de* $\mathbb{F}_{p^{3k}}$ *[ZKW09].*
4. $f(x)=x^{p^m+1}+\omega\mathrm{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_{p^m}}(\alpha x^{p^i(p^r+1)})$ *sur* $\mathbb{F}_{p^e}$ *où* $e=2m$, $p^m-1=2^sk$, $r\geq 1$, $p^r-1=2^tl$, k *et* l *impair,* $\omega\in\mathbb{F}_{p^e}\setminus\mathbb{F}_{p^m}$, α *n'est pas une puissance* p^r+1*ème et* $s\leq t$ *[BK10].*

Par la proposition 3.2.11, il suffit de vérifier que ces fonctions ne sont pas affine-étendu équivalentes à une fonction puissance.
Il est en fait démontré dans [DY06] que pour e impair et pour tout $u \in \mathbb{F}_{3^e}$, la fonction $x \mapsto x^{10} - ux^6 - u^2x^2$ est parfaitement non linéaire sur $\mathbb{F}_{3^e}$. On conserve seulement les cas $u = \pm 1$ pour des raisons d'équivalence. En effet, comme -1 n'est pas un carré, tout $u \in \mathbb{F}_{3^e}^*$ peut s'écrire $u = \varepsilon b^4$ où $\varepsilon \in \{-1, 1\}$ et $b \in \mathbb{F}_{3^e}^*$. Alors

$$x^{10} - ux^6 - u^2x^2 = b^{10}\left(\left(\frac{x}{b}\right)^{10} - \varepsilon\left(\frac{x}{b}\right)^6 - \left(\frac{x}{b}\right)^2\right).$$

Définition 3.3.8. On dit qu'un polynôme f de $\mathbb{F}_{p^e}[x]$ est un polynôme de Dembowski-Ostrom s'il a la forme réduite suivante :

$$\sum_{k,l=0}^{e-1} a_{k,l}x^{p^k+p^l}, \text{ où } a_{k,l} \in \mathbb{F}_{p^e}.$$

Les applications linéaires sur $\mathbb{F}_{p^e}$ sont de la forme $L(x) = \sum_{k=0}^{e-1} b_k x^{p^k}$ où $b_k \in \mathbb{F}_p$ (voir [Rom06]). La composée à droite ou à gauche d'un polynôme de Dembowski-Ostrom avec une application linéaire est encore un polynôme de Dembowski-Ostrom. Toutes les fonctions données dans le théorème ci-dessus sont des polynômes de Dembowski-Ostrom. Comme $x^{\frac{3^k+1}{2}}$ n'est pas un polynôme de Dembowski-Ostrom, aucune des fonctions du théorème ci-dessus n'est équivalente à $x^{\frac{3^k+1}{2}}$.
On voudrait donc qu'aucune de ces fonctions ne soit équivalente à x^{p^s+1}, pour $s \geq 0$. On commence par traiter le cas des deux premières fonctions. Soit $L_1(x) = \sum_{k=0}^{e-1} b_k x^{p^k}$ et $L_2(x) = \sum_{k=0}^{e-1} c_k x^{p^k}$ des applications linéaires inversibles, L une application linéaire et c, $d \in \mathbb{F}_{p^e}$ tels que $L_1(x^{10} - \varepsilon x^6 - x^2) = (L_2(x) + c)^{p^s+1} + L(x) + d$. Dans la suite, on considère les indices des coefficients modulo e.
Supposons dans un premier temps que $s = 0$. On obtient les équations suivantes :

$$\begin{cases} c_k c_l = 0 & \text{si } l - k \neq 0, 2, -2 \\ b_k = 2c_k c_{k+2} & \\ c_k^2 = -b_k - \varepsilon b_{k-1} & \end{cases}.$$

Comme L_2 est inversible, il existe k_0 tel que $c_{k_0} \neq 0$. Alors, pour tout $l \neq k_0, k_0+2, k_0-2$, $c_l = 0$. Comme de plus $c_{k_0-2}c_{k_0+2} = 0$, quitte à prendre $k_0 - 2$ au lieu de k_0, pour tout $l \neq k_0, k_0+2$, $c_l = 0$. En utilisant la deuxième équation, on obtient que pour tout $l \neq k_0$, $b_l = 0$. Finalement, en utilisant la troisième équation pour $k = k_0 + 1$, on obtient que $b_l = 0$ pour tout l, ce qui est absurde puisque L_1 est inversible.
Supposons maintenant que $s \neq 0$. On obtient les équations suivantes :

$$\begin{cases} c_k^{p^s} c_l + c_{l-s}^{p^s} c_{k+s} = 0 & \text{si } k + s - l \neq 0, 2, -2 \\ b_{k+s} = c_k^{3^s} c_{k+s+2} + c_{k+2}^{3^s} c_{k+s} & \\ c_k c_{k+s} = -b_{k+s} - \varepsilon b_{k+s-1} & \end{cases} \tag{3.6}$$

Supposons qu'il existe k_0 tel que $c_{k_0} = 0$ alors pour tout $l \neq k_0 + s, k_0 + s + 2, k_0 + s - 2$ $c_{l-s}^{3^s} c_{k_0+s} = 0$. Si $c_{k_0+s} \neq 0$, pour tout $l \neq k_0 - 2, k_0 + 2$, $c_l = 0$. Pour $s \not\equiv \pm 2 \mod e$,

on obtient $b_k = 0$ pour tout k, ce qui est absurde. Si $s \equiv \pm 2 \mod e$, alors pour tout $l \neq k_0, k_0-2, k_0+2$, $b_l = 0$. Si $s \equiv -2 \mod e$, $0 = b_{k_0-4} = c_{k_0-2}^{3^s+1}$ et on a une contradiction. Sinon, en utilisant la troisième équation, on obtient $b_{k_0+2} = 0$. En remplaçant dans la deuxième équation, on a $c_{k_0+2} = 0$ ce qui est absurde. On en déduit que pour tout k, la suite $(c_{k+us})_u$ est soit identiquement nulle, soit tous ses termes sont non nuls.
Comme L_2 est inversible, il existe $c_{k_0} \neq 0$. Si $\mathrm{pgcd}(e,s) = 1$, alors par ce qui précède, $c_k \neq 0$ pour tout k. Comme pour tout u, v,

$$c_{k+sv}^{3^s} c_{k+su+1} + c_{k+s(u-1)+1}^{3^s} c_{k+2(v+1)} = 0,$$

on a

$$-\left(\frac{c_{k+1+s(u-1)}}{c_{k+sv}}\right)^{3^s} = \frac{c_{k+1+su}}{c_{k+s(v+1)}}.$$

En itérant le procédé e fois, on a -$\frac{c_{k+1+su}}{c_{k+s(v+1)}} = \frac{c_{k+1+su}}{c_{k+s(v+1)}}$, ce qui est absurde.
Si $\mathrm{pgcd}(e,s) > 1$, en particulier $s \neq \pm 2$ et on peut prendre $l = k$ dans la première équation du système (3.6). On obtient $c_k^{3^s+1} + c_{k-s}^{3^s} c_{k+s} = 0$. On considère alors la suite $(c_{k_0+us})_u$, tous ses termes sont non nuls par ce qui précède et de plus pour tout u on a $\chi(c_{k_0+us}) = -\chi(c_{k_0+(u+2)s})$. On en déduit que $\chi(c_{k_0}) = -\chi(c_{k_0})$, ce qui est absurde.
Dans le cas de la troisième fonction, la non équivalence est démontrée dans [ZKW09] en utilisant les mêmes méthodes.
Enfin, pour la quatrième fonction, la non équivalence est démontrée dans [ZW09] dans le cas particulier où $i = r$, $\alpha = c^l$, $\omega = \frac{1}{c^l b}$ où c est un élément d'ordre k premier avec $p^m - 1$ tel que si l est l'inverse de $p^m - 1$ modulo k alors c^l n'est pas un puissance $p^i + 1$ème et b est un élément de $\mathbb{F}_{p^e}$ tel que $c^l b \notin \mathbb{F}_{p^m}$.

Théorème 3.3.9. *Les fonctions suivantes sont presque parfaitement non linéaires :*

1. $f(x) = x^{2^s+1} + \alpha x^{2^{ik}+2^{mk+s}}$ *sur* $\mathbb{F}_{2^{3k}}$ *avec* $\mathrm{pgcd}(3,k) = \mathrm{pgcd}(s,3k) = 1$, $k \geq 3$, $i \equiv sk \mod 3$, $m \equiv -i \mod 3$ *et* $\alpha = t^{2^k-1}$, t *un élément primitif de* $\mathbb{F}_{2^{3k}}$ *[BCFL06].*

2. $f(x) = x^{2^s+1} + \alpha x^{2^{ik}+2^{mk+s}}$ *sur* $\mathbb{F}_{2^{4k}}$ *avec* $\mathrm{pgcd}(2,k) = \mathrm{pgcd}(s,2k) = 1$, $k \geq 3$, $i \equiv sk \mod 4$, $m = 4 - i$ *et* $\alpha = t^{2^k-1}$, t *un élément primitif de* $\mathbb{F}_{2^{3k}}$ *[BCP07].*

3. $f(x) = \alpha x^{2^s+1} + \alpha^{2^k} x^{2^{k+s}+2^k} + \beta x^{2^k+1} + \sum_{i=1}^{k-1} \gamma_i x^{2^{k+i}+2^i}$ *sur* $\mathbb{F}_{2^{2k}}$, α *pas un cube,* $\beta \notin \mathbb{F}_{2^k}$, $\gamma_i \in \mathbb{F}_{2^k}$ *pour tout* i, $\mathrm{pgcd}(k,s) = 1$, k *impair et* s *impair [BBMM08].*

4. $f(x) = x^{2^{2s}+2^s} + bx^{2^k+1} + cx^{2^k(2^{2s}+2^s)}$ *sur* $\mathbb{F}_{2^{2k}}$, $\mathrm{pgcd}(s,k) = 1$, $\mathrm{pgcd}(2^s+1, 2^k+1) > 1$, $c^{2^k+1} = 1$, $cb^{2^k} \neq b$ *et* $c \notin \{\gamma^{(2^s+1)(2^k-1)} : \gamma \in \mathbb{F}_{2^{2k}}\}$ *[BC08].*

5. $f(x) = \theta x^{2^{s+k}+1} + \theta^{2^k} x^{2^k+2^s} + x^{2^s+1} + x^{2^k(2^s+1)} + x^{2^k+1} + \pi x^{2^{s+k}+2^s}$ *sur* $\mathbb{F}_{2^{2k}}$ *avec* $\mathrm{pgcd}(s,k) = 1$, $\pi \notin \mathbb{F}_{2^k}$ *et l'équation* $x^{2^s+1} + \theta x^{2^s} + \theta^{2^k} x + 1 = 0$ *n'as pas de solution* x *tel que* $x^{2^k+1} = 1$ *[BC08].*

6. $f(x) = x^3 + \mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(x^9)$ *sur* $\mathbb{F}_{2^e}$ *[BCL09].*

7. $f(x) = ux^{2^{-k}+2^{k+s}} + u^{2^k} x^{2^s+1} + vx^{2^{k+s}+2^s}$ *sur* $\mathbb{F}_{2^{3k}}$, u *élément primitif,* $v \in \mathbb{F}_{2^k}$, $\mathrm{pgcd}(s,3k) = 1$, $\mathrm{pgcd}(3,k) = 1$ *et* $k + s \equiv 0 \mod 3$ *[BBMM08].*

8. $f(x) = u^{2^k} x^{2^{-k}+2^{k+s}} + ux^{2^s+1} + vx^{2^{-k}+1} + wu^{2^k+1} x^{2^{k+S}+2^s}$ *sur* $\mathbb{F}_{2^{3k}}$, u *élément primitif,* v, $w \in \mathbb{F}_{2^k}$ $vw \neq 1$, $\mathrm{pgcd}(s,3k) = 1$, $\mathrm{pgcd}(3,k) = 1$ *et* $k + s \equiv 0 \mod 3$ *[BBMM11].*

9. *$f(x) = ux^{d_1} + x^{d_2}$, sur $\mathbb{F}_{3^e}$ avec $e \geq 3$ impair, $d_1 = \frac{3^e-1}{2} - 1$, $d_2 = 3^e - 2$ et $u \in \mathbb{F}_{3^e}$ tel que $\chi(u) = \chi(u+1) = \chi(u-1)$ [NH07].*

La deuxième fonction n'est pas CCZ-équivalente à une fonction puissance. Dans les autres cas, on a seulement des résultats partiels plus ou moins complets. Les fonctions 3, 4 et 5 ne sont pas CCZ-équivalentes aux fonctions puissances de Kloosterman, Niho et Welch car elles sont presque parfaitement non linéaires sur des extensions de degré pair de $\mathbb{F}_2$ au contraire de ces fonctions puissances. Les fonctions 1 et 6 ne sont affine étendu équivalentes à aucune fonction puissance et ne sont pas CCZ-équivalentes à la fonction puissance de Gold. De plus, la fonction 6 n'est pas CCZ-équivalente aux fonctions puissances de Dobbertin et Kloosterman. Dans le cas de la fonction 7, pour $v \neq 0$ et $n = 6$ la fonction n'est pas CCZ-équivalente aux fonctions puissances. Pour $v = 0$, on retrouve la fonction 1. Pour la famille 8, la non équivalence a été étudiée pour $n = 6$ et $n = 12$. Enfin, la non équivalence de la famille 9 n'a pas été étudiée.

3.4 Nouvelles familles en caractéristique 3

Dans cette section, $p = 3$.

3.4.1 Deux conjectures de Dobbertin, Mills, Müller, Pott et Willems

Dans [DMM+03], Dobbertin, Mills, Müller, Pott et Willems démontrent les théorèmes suivants :

Théorème 3.4.1. *Soit e un entier impair. Dans $\mathbb{F}_{3^e}$, la fonction $x \mapsto x^d$ vérifie $\Delta_d \leq 2$ pour*

$$d = \begin{cases} \frac{3^{\frac{e+1}{2}}-1}{2} & \text{si } e \equiv 3 \mod 4 \\ \frac{3^{\frac{e+1}{2}}-1}{2} + \frac{3^e-1}{2} & \text{si } e \equiv 1 \mod 4 \end{cases}.$$

Théorème 3.4.2. *Soit e un entier impair. Dans $\mathbb{F}_{3^e}$, la fonction $x \mapsto x^d$ vérifie $\Delta_d \leq 2$ pour*

$$d = \begin{cases} \frac{3^{e+1}-1}{8} & \text{si } e \equiv 3 \mod 4 \\ \frac{3^{e+1}-1}{8} + \frac{3^e-1}{2} & \text{si } e \equiv 1 \mod 4 \end{cases}.$$

On prouve ces deux théorèmes de la même façon :

Démonstration. Par le lemme 3.2.4, il suffit de prouver que l'équation $(x+1)^d - x^d = b$ a au plus deux solutions pour tout $b \in \mathbb{F}_{3^e}$. Si $b = 0$, puisque $\mathrm{pgcd}(d, 3^e - 1) = 2$, cette équation a une solution. A partir de maintenant, on suppose $b \neq 0$.
Dans un premier temps, supposons que $e \equiv 3 \mod 4$. On pose

$$m = \begin{cases} \frac{e+1}{2} & \text{dans le cas du théorème 3.4.1} \\ 1 & \text{dans le cas du théorème 3.4.2} \end{cases}$$

et $u_x = x^d$. On a $u_{x+1} = u_x + b$ alors en élevant cette équation à la puissance $3^m + 1$ et puisque

$$(3^m + 1)d \equiv 1 + \frac{3^e - 1}{2} \mod 3^e - 1,$$

on obtient l'équation suivante :

$$bu_x^{3^m} + b^{3^m} u_x + b^{3^m+1} = \chi(x+1)(x+1) - \chi(x)x.$$

- Cas A : $\chi(x) = \chi(x+1)$ ou $x = 0$ ou $x = -1$.
  On obtient alors les équations suivantes :
  $$bu_x^{3^m} + b^{3^m} u_x = -b^{3^m+1} + \varepsilon, \qquad \text{avec } \varepsilon \in \{-1, 1\}. \tag{3.7}$$
  L'application $z \mapsto bz^{3^m} + b^{3^m} z$ est linéaire. De plus $bz^{3^m} + b^{3^m} z = 0$ si et seulement si $z = 0$ ou $z^{3^m-1} = -b^{3^m-1}$. Comme -1 n'est pas un carré, cette application est bijective et donc chaque équation (3.7) a au plus une solution. Supposons qu'elles aient chacune une solution, c'est-à -dire qu'il existe $x \in \mathbb{F}_{3^e}$ tel que $\chi(x) = 1$ ou $x = 0$ et $bu_x^{3^m} + b^{3^m} u_x + b^{3^m+1} = 1$ d'une part et $y \in \mathbb{F}_{3^e}$ tel que $\chi(y) = -1$ et $bu_x^{3^m} + b^{3^m} u_x + b^{3^m+1} = -1$ d'autre part. Alors, en additionnant ces deux équations, on a
  $$b(u_x + u_y)^{3^m} + b^{3^m}(u_x + u_y) + 2b^{3^m+1} = 0.$$
  On a déjà vu que l'application $z \mapsto bz^{3^m} + b^{3^m} z$ est bijective donc la seule possibilité est que $u_x + u_y = 2b$ ce qui signifie que $u_y = -u_{x+1}$. Ceci est impossible puisque u_y et u_{x+1} sont des carrés mais pas -1.

- Cas B : $\chi(x) = -\chi(x+1)$
  On obtient alors les équations suivantes puisque $\chi(x)x = u_x^{3^m+1}$
  $$-u_x^{3^m+1} + bu_x^{3^m} + b^{3^m} u_x = -b^{3^m+1} + \varepsilon, \qquad \text{avec } \varepsilon \in \{-1, 1\}.$$
  On remplace u_x par $u + b$ dans cette équation et on obtient
  $$u^{3^m+1} = -b^{3^m+1} - \varepsilon.$$
  Comme $\text{pgcd}(3^m + 1, 3^e - 1) = 2$, cette équation a au plus deux solutions $\pm\alpha$ dans $\mathbb{F}_{3^e}$. On obtient alors les couples (u_x, u_{x+1}) suivants :
  $$(\alpha + b, \alpha - b) \text{ et } (-\alpha + b, -\alpha - b).$$
  Comme u_x et u_{x+1} sont des carrés mais pas -1, au plus un de ces couples est possible. Supposons que les deux équations aient des solutions, c'est-à-dire qu'il y ait une solution x telle que $\chi(x) = 1 = -\chi(x+1)$ et une solution y telle que $\chi(y) = -1 = -\chi(y+1)$. Alors $-1 = u_x^{3^m+1} + u_{x+1}^{3^m+1}$ et $1 = u_y^{3^m+1} + u_{y+1}^{3^m+1}$. Comme u_x, $u_{x+1} = u_x + b$, u_y et $u_{y+1} = u_y + b$ sont des carrés par le lemme 3.1.2, ceci est impossible.

On a donc prouvé les théorèmes pour $e \equiv 3 \mod 4$. Supposons que $e \equiv 1 \mod 4$. Alors $3e \equiv 3 \mod 4$ et

$$d' = \begin{cases} \frac{3^{\frac{3e+1}{2}}-1}{2} \equiv \frac{3^{\frac{e+1}{2}}-1}{2} + \frac{3^e-1}{2} \mod 3^e - 1 & \text{dans le cas du théorème 3.4.1} \\ \frac{3^{3e+1}-1}{8} \equiv \frac{3^{e+1}-1}{8} + \frac{3^e-1}{2} \mod 3^e - 1 & \text{dans le cas du théorème 3.4.2} \end{cases}.$$

Comme les théorèmes sont vrais pour $e \equiv 3 \mod 4$, l'équation $(x+1)^d - x^d = b$ a au plus deux solutions dans $\mathbb{F}_{3^{3e}}$ donc dans $\mathbb{F}_{3^e}$ pour tout $b \in \mathbb{F}_{3^e}$. □

Ils font alors les deux conjectures suivantes :

Conjecture 3.4.3. *Pour $e \geq 5$ impair, la fonction $x \mapsto x^d$ est presque parfaitement non linéaire sur $\mathbb{F}_{3^e}$ pour*

$$d = \begin{cases} \frac{3^{\frac{e+1}{2}}-1}{2} & \text{si } e \equiv 3 \mod 4 \\ \frac{3^{\frac{e+1}{2}}-1}{2} + \frac{3^e-1}{2} & \text{si } e \equiv 1 \mod 4 \end{cases}.$$

Conjecture 3.4.4. *Pour $e \geq 5$ impair, la fonction $x \mapsto x^d$ est presque parfaitement non linéaire sur $\mathbb{F}_{3^e}$ pour*

$$d = \begin{cases} \frac{3^{e+1}-1}{8} & si\ e \equiv 3 \mod 4 \\ \frac{3^{e+1}-1}{8} + \frac{3^e-1}{2} & si\ e \equiv 1 \mod 4 \end{cases}.$$

Remarque 3.4.5.

1. On prend $e \geq 5$ dans les conjectures car pour $e = 1$ ou $e = 3$, par le théorème 3.3.1, $x \mapsto x^d$ est parfaitement non linéaire.
2. La conjecture 3.4.3 donne une famille infinie pour les cas I et III du tableau 3.1 et la conjecture 3.4.4 pour les cas II et V.

Par les théorèmes 3.4.1 et 3.4.2, il suffit de prouver que $\Delta_d \neq 1$. Autrement dit, par le lemme 3.2.4, il suffit de prouver que la fonction $f : x \mapsto (x+1)^d - x^d$ n'est pas une bijection sur $\mathbb{F}_{3^e}$. On prouve les conjectures 3.4.3 et 3.4.4 à l'aide du critère d'Hermite et Dickson (lemme 3.1.3). Dans les deux cas, $\text{pgcd}(d, 3^e - 1) = 2$ donc f a exactement une racine. Il faut donc trouver un t, $1 \leq t \leq q-2$, $t \not\equiv 1 \mod p$ tel que $f(x)^t$ soit de degré $q-1$ modulo $x^q - x$.

Soit $1 \leq t \leq q-2$, $t \not\equiv 1 \mod p$. On a

$$\begin{aligned}
\left((x+1)^d - x^d\right)^t &= \sum_{k=0}^{t} \binom{t}{k} (x+1)^{dk} (-1)^{t-k} x^{d(t-k)} \\
&= \sum_{k=0}^{t} \binom{t}{k} (-1)^{t-k} \left(\sum_{j=0}^{dk} \binom{dk}{j} x^{dk-j} \right) x^{d(t-k)} \\
&= \sum_{k=0}^{t} \binom{t}{k} (-1)^{t-k} \sum_{j=0}^{dk} \binom{dk}{j} x^{dt-j} \\
&= \sum_{j=0}^{dt} x^{dt-j} \sum_{k=\lceil \frac{j}{d} \rceil}^{t} (-1)^{t-k} \binom{t}{k} \binom{dk}{j}.
\end{aligned}$$

Le degré de la réduction modulo $x^q - x$ de x^k est $q-1$ si et seulement si $k \equiv 0 \mod q-1$ et $k \neq 0$. Le coefficient de degré $q-1$ de la réduction modulo $x^q - x$ de $\left((x+1)^d - x^d\right)^t$ est donc

$$C = \sum_{i=1}^{\lfloor \frac{dt}{q-1} \rfloor} \sum_{k=\lceil \frac{dt-i(q-1)}{d} \rceil}^{t} (-1)^{t-k} \binom{t}{k} \binom{dk}{dt-i(q-1)}.$$

A partir de maintenant, on différentie les cas. Le but est de trouver un t tel que $C \neq 0$ et alors, par le critère d'Hermite et Dickson, on obtient le résultat.

Cas de la conjecture 3.4.3, $e \equiv 1 \mod 4$

On a $d = \frac{3^{\frac{e+1}{2}}-1}{2} + \frac{3^e-1}{2}$. On choisit $t = 2$ alors $\lfloor \frac{dt}{q-1} \rfloor = 1$ et $\lceil \frac{dt-(q-1)}{d} \rceil = 1$ car $e \neq 1$. D'où

$$C = \binom{3^e + 3^{\frac{e+1}{2}} - 2}{3^{\frac{e+1}{2}} - 1} + \binom{\frac{3^e-1}{2} + \frac{3^{\frac{e+1}{2}}-1}{2}}{3^{\frac{e+1}{2}} - 1}.$$

Or, d'une part, $3^e + 3^{\frac{e+1}{2}} - 2 = 3^e + \sum_{k=1}^{\frac{e-1}{2}} 2 \times 3^k + 1$ et $3^{\frac{e+1}{2}} - 1 = \sum_{k=0}^{\frac{e-1}{2}} 2 \times 3^k$ donc par le théorème de Lucas, $\binom{3^e + 3^{\frac{e+1}{2}} - 2}{3^{\frac{e+1}{2}} - 1} \equiv 0 \mod 3$.

D'autre part, $\frac{3^e-1}{2} + \frac{3^{\frac{e+1}{2}}-1}{2} = \sum_{k=0}^{e-1} 3^k + \sum_{k=0}^{\frac{e-1}{2}} 3^k = \sum_{k=\frac{e+1}{2}}^{e-1} 3^k + \sum_{k=0}^{\frac{e-1}{2}} 2 \times 3^k$. On a donc $\binom{\frac{3^e-1}{2} + \frac{3^{\frac{e+1}{2}}-1}{2}}{3^{\frac{e+1}{2}} - 1} \equiv 1 \mod 3$.

Cas de la conjecture 3.4.3, $e \equiv 3 \mod 4$

On a $d = \frac{3^{\frac{e+1}{2}}-1}{2}$. Soit $s = 2 \times (3^{\frac{e+1}{2}-1} + 1)$ et on choisit $t = 2s + 4$ (pour $e > 3$, on a bien $0 < t < q - 1$ et $t \not\equiv 0 \mod 3$). De plus, $\lfloor \frac{dt}{q-1} \rfloor = 2$, $\lceil \frac{dt-(q-1)}{d} \rceil = s + 6$ et $\lceil \frac{dt-2(q-1)}{d} \rceil = 7$. D'où

$$C = \sum_{k=s+6}^{t} (-1)^k \binom{t}{k} \binom{dk}{dt-(q-1)} + \sum_{k=7}^{t} (-1)^k \binom{t}{k} \binom{dk}{dt-2(q-1)}. \tag{3.8}$$

On a $t = 4 \times 3^{\frac{e+1}{2}-1} + 8 = 3^{\frac{e+1}{2}} + 3^{\frac{e+1}{2}-1} + 2 \times 3 + 2$.
D'où, par le théorème de Lucas, $\binom{t}{k} \not\equiv 0 \mod 3$ si et seulement si k est de la forme $a3^{\frac{e+1}{2}} + b3^{\frac{e-1}{2}} + c3 + d$ avec a, $b \in \{0, 1\}$ et c, $d \in \{0, 1, 2\}$. Alors

$$dk = a3^e + (a + b) \sum_{j=\frac{e+1}{2}+1}^{e-1} 3^j + (a + b + c)3^{\frac{e+1}{2}} + (b + c + d)3^{\frac{e-1}{2}} + (c + d) \sum_{j=1}^{\frac{e+1}{2}-2} 3^j + d.$$

D'autre part,

$$dt - 2(q - 1) = 3^{\frac{e+1}{2}+1} + \sum_{j=1}^{\frac{e+1}{2}-2} 2 \times 3^j + 1$$

et

$$dt - (q - 1) = 3^e + 3^{\frac{e+1}{2}+1} + \sum_{j=1}^{\frac{e+1}{2}-2} 2 \times 3^j.$$

Donc $\binom{dk}{dt-(q-1)} \not\equiv 0 \mod 3$ si $a = 1$ et $c + d = 2$. Supposons de plus que $b = 1$, alors $b + c + d = 3$ et donc $5 \geq a + b + c + 1 \geq 3$. Le coefficient de $3^{\frac{e+1}{2}+1}$ dans la décomposition 3-adique de dk est alors 0, ce qui implique $\binom{dk}{dt-2(q-1)} \equiv 0 \mod 3$. Les k restants dans la première somme de (3.8) sont donc $3^{\frac{e+1}{2}} + 2 \times 3$, $3^{\frac{e+1}{2}} + 3 + 1$, $3^{\frac{e+1}{2}} + 2$.
Considérons maintenant la deuxième somme : $\binom{dk}{dt-2(q-1)} \not\equiv 0 \mod 3$ si $d \in \{1, 2\}$ et $c + d = 2$, c'est-à -dire si $c = 1$ et $d = 1$ ou si $c = 0$ et $d = 2$. De plus, comme on veut $k \geq 7$, a et b ne peuvent pas être nuls tous les deux. Supposons $a = b = 1$ alors $b+c+d = 3$ et donc $4 \geq a + c + b + 1 \geq 3$. Le coefficient de $3^{\frac{e+1}{2}+1}$ dans la décomposition 3-adique de dk est alors 0, ce qui implique $\binom{dk}{dt-2(q-1)} \equiv 0 \mod 3$. Les k restants dans cette somme sont donc $3^{\frac{e+1}{2}} + 3 + 1$, $3^{\frac{e+1}{2}} + 2$, $3^{\frac{e+1}{2}-1} + 3 + 1$, $3^{\frac{e+1}{2}-1} + 2$.

Finalement,

$$\begin{aligned}C = &-\binom{t}{3^{\frac{e+1}{2}}+2\times 3}\binom{d(3^{\frac{e+1}{2}}+2\times 3)}{dt-(q-1)} - \binom{t}{3^{\frac{e+1}{2}}+3+1}\binom{d(3^{\frac{e+1}{2}}+3+1)}{dt-(q-1)}\\ &-\binom{t}{3^{\frac{e+1}{2}}+2}\binom{d(3^{\frac{e+1}{2}}+2)}{dt-(q-1)} - \binom{t}{3^{\frac{e+1}{2}}+3+1}\binom{d(3^{\frac{e+1}{2}}+3+1)}{dt-2(q-1)}\\ &-\binom{t}{3^{\frac{e+1}{2}}+2}\binom{d(3^{\frac{e+1}{2}}+2)}{dt-2(q-1)} - \binom{t}{3^{\frac{e-1}{2}}+3+1}\binom{d(3^{\frac{e-1}{2}}+3+1)}{dt-2(q-1)}\\ &-\binom{t}{3^{\frac{e-1}{2}}+2}\binom{d(3^{\frac{e-1}{2}}+2)}{dt-2(q-1)}.\end{aligned}$$

D'une part, $t = 3^{\frac{e+1}{2}} + 3^{\frac{e-1}{2}} + 2\times 3 + 2$, alors $\binom{t}{3^{\frac{e+1}{2}}+2\times 3} \equiv 1 \mod 3$ par le théorème de Lucas. D'autre part,

$$d(3^{\frac{e+1}{2}}+2\times 3) = 3^e + \sum_{j=\frac{e+1}{2}+2}^{e-1} 3^j + 2\times 3^{\frac{e+1}{2}+1} + 2\times 3^{\frac{e-1}{2}} + 2\sum_{j=1}^{\frac{e+1}{2}-2} 3^j$$

et

$$dt-(q-1) = 3^e + 3^{\frac{e+1}{2}+1} + \sum_{j=1}^{\frac{e+1}{2}-2} 2\times 3^j$$

donc $\binom{d(3^{\frac{e+1}{2}}+2\times 3)}{dt-(q-1)} \equiv 2 \mod 3$. En procédant de même pour chacun des autres coefficients binomiaux, on a $C \equiv 1 \mod 3$.

Cas de la conjecture 3.4.4, $e \equiv 1 \mod 4$

On a $d = \frac{3^{e+1}-1}{8} + \frac{3^e-1}{2}$. On choisit $t = 2$ alors $\lfloor \frac{dt}{q-1} \rfloor = 1$ et $\lceil \frac{dt-(q-1)}{d} \rceil = 1$. D'où

$$C = \binom{\frac{3^{e+1}-1}{4}+3^e-1}{\frac{3^{e+1}-1}{4}} + \binom{\frac{3^e-1}{2}+\frac{3^{e+1}-1}{8}}{\frac{3^{e+1}-1}{4}}.$$

Or, $\frac{3^{e+1}-1}{4} + 3^e - 1 = \sum_{k=1}^{\frac{e-1}{2}} 2\times 3^{2k} + 3^e + 1$ et $\frac{3^{e+1}-1}{4} = 2\sum_{k=0}^{\frac{e-1}{2}} 3^{2k}$. Alors, par le théorème de Lucas, $\binom{\frac{3^{e+1}-1}{4}+3^e-1}{\frac{3^{e+1}-1}{4}} \equiv 0 \mod 3$.

D'autre part, $\frac{3^e-1}{2} + \frac{3^{e+1}-1}{8} = \sum_{k=0}^{\frac{e-1}{2}} 2\times 3^{2k} + \sum_{k=0}^{\frac{e-1}{2}-1} 3^{2k+1}$. D'où $\binom{\frac{3^e-1}{2}+\frac{3^{e+1}-1}{8}}{\frac{3^{e+1}-1}{4}} \equiv 1 \mod 3$.

Cas de la conjecture 3.4.4, $e \equiv 3 \mod 4$

On a $d = \frac{3^{e+1}-1}{8}$. On choisit $t = 26$. Pour $e \geq 5$, on a bien $1 \leq t \leq q-2$ et $t \not\equiv 0 \mod 3$. De plus,

$$\frac{dt}{q-1} = \frac{13}{4}(2\frac{3^e}{3^e-1}+1).$$

Or, pour $e \geq 5$, $\frac{243}{242} \geq \frac{3^e}{3^e-1} \geq 1$. D'où $\lfloor \frac{dt}{q-1} \rfloor = 9$.
On a $t = 2 + 2 \times 3 + 2 \times 9$ donc par le théorème de Lucas, $\binom{t}{k} \not\equiv 0 \mod 3$ si et seulement si $k = a + 3b + 9c$, a, b, $c \in \{0, 1, 2\}$.

De plus, $d = \sum_{k=0}^{\frac{e-1}{2}} 3^{2k}$ donc $dk = a + \sum_{k=1}^{\frac{e-1}{2}} (a+c)3^{2k} + \sum_{k=0}^{\frac{e-1}{2}} b3^{2k+1} + c3^{e+1}$ et d'autre part, $dt - (q-1) = \sum_{k=1}^{\frac{e-1}{2}} 2 \times 3^{2k} + 2 \times 3^e + 2 \times 3^{e+1}$ donc, si on écrit $j = \alpha + 3\beta$, α, $\beta \in \{0, 1, 2\}$, $dt - (j+1)(q-1) = \alpha + \beta 3 + \sum_{k=1}^{\frac{e-1}{2}} 2 \times 3^{2k} + (2-\alpha)3^e + (2-\beta)3^{e+1}$. D'où, par le théorème de Lucas, $\binom{dk}{dt-(j+1)(q-1)} \not\equiv 0 \mod 3$ si et seulement si $a \geq \alpha$, $b \geq \beta$, $b \geq 2 - \alpha$, $c \geq 2 - \beta$ et $a + c = 2$.
Finalement,

$$\begin{aligned} C &\equiv \binom{26}{24} + 2\binom{26}{16} + \binom{26}{24} + 2\binom{26}{13} + \binom{26}{16} + \binom{26}{8} + \binom{26}{16} \\ &\qquad + \binom{26}{24} + 2\binom{26}{16} + \binom{26}{8} + \binom{26}{8} \mod 3 \\ &\equiv 1 \mod 3. \end{aligned}$$

Dans tous les cas, on a trouvé un t tel que $((x+1)^d - x^d)^t \mod x^q - x$ soit de degré $q-1$ ce qui prouve les deux conjectures.

3.4.2 Une nouvelle famille déduite du théorème 3.3.5

Soit l un entier plus grand que 2 et e un entier tel que $e \equiv -1 \mod 2^l$. Alors, en prenant $u = 3$ et $k = \frac{e+1}{2^l}$ dans le théorème 3.3.5, on a immédiatement :

Proposition 3.4.6. *Soit $l \geq 2$ et e un entier tel que $e \equiv -1 \mod 2^l$. Alors la fonction $x \mapsto x^d$ est presque parfaitement non linéaire sur $\mathbb{F}_{3^e}$ pour*

$$d = \frac{3^{e+1} - 1}{3^{\frac{e+1}{2^l}} + 1}.$$

Remarque 3.4.7. Cette famille contient 656 pour $l = 2$, ce qui correspond au cas IV du tableau 3.1.

3.5 Nouvelles familles en caractéristique 5

3.5.1 Une conjecture de Dobbertin, Mills, Müller, Pott et Willems

Dans [DMM+03], Dobbertin, Mills, Müller, Pott et Willems donnent la conjecture suivante pour expliquer le cas VII du tableau 3.1.

Conjecture 3.5.1. *Soit e un entier impair. La fonction $x \mapsto x^d$ est presque parfaitement non linéaire sur $\mathbb{F}_{5^e}$ pour*

$$d = \frac{5^e - 1}{4} + \frac{5^{\frac{e+1}{2}} - 1}{2}.$$

Wang et Zha démontrent cette conjecture dans [ZW10, théorème 4.5], notamment en utilisant le théorème 3.3.6 pour démontrer le cas où $e \equiv 3 \mod 4$. Dans cette section, nous donnons une nouvelle preuve de ce cas.

On commence par rappeler la démonstration du cas $e \equiv 1 \mod 4$:

$$\frac{5^{\frac{e+1}{2}}+1}{2}d = \frac{5^{\frac{e+1}{2}}+1}{2}\frac{5^e-1}{4} + \frac{5^{e+1}-1}{4} = 5^e + \frac{5^{\frac{e+1}{2}}+3}{2}\frac{5^e-1}{4}.$$

Or $e \equiv 1 \mod 4$ donc $5^{\frac{e+1}{2}}+3 \equiv 0 \mod 8$ d'où

$$\frac{5^{\frac{e+1}{2}}+1}{2}d \equiv 1 \mod (5^e-1).$$

Alors d est inversible modulo 5^e-1, d'inverse $d^{-1} = \frac{5^{\frac{e+1}{2}}+1}{2}$. Or, puisque $e \equiv 1 \mod 4$, $\mathrm{pgcd}(2e, \frac{e+1}{2}) = 1$ donc par le lemme 3.2.5 et le (9) du théorème 3.3.4, on a le résultat pour $e \equiv 1 \mod 4$.
On considère maintenant le cas $e \equiv 3 \mod 4$ alors $3e \equiv 1 \mod 4$ et

$$\begin{aligned} d' = \frac{5^{3e}-1}{4} + \frac{5^{\frac{3e+1}{2}}-1}{2} &= \frac{5^{2e}(5^e-1)+(5^{2e}-1)}{4} + \frac{5^e(5^{\frac{e+1}{2}}-1)+(5^e-1)}{2} \\ &= (5^e)^2\frac{5^e-1}{4} + \frac{5^e+3}{4}(5^e-1) + 5^e\frac{5^{\frac{e+1}{2}}-1}{2} \\ &\equiv \frac{5^e-1}{4} + \frac{5^{\frac{e+1}{2}}-1}{2} \mod (5^e-1). \end{aligned}$$

Or, par le cas $e \equiv 1 \mod 4$, $x \mapsto x^{d'}$ est presque parfaitement non linéaire sur $\mathbb{F}_{5^{3e}}$, on en déduit que $\Delta_d \leq 2$ pour $e \equiv 3 \mod 4$. De plus, comme d est impair,

$$(0+1)^d - 0^d = 1 = (-1+1)^d - (-1)^d,$$

et donc $\Delta_d = 2$.

3.5.2 Une nouvelle famille

En poussant la recherche de Helleseth, Rong et Sandberg sur $\mathbb{F}_{5^7}$, on peut ajouter un nouvel exposant qui n'est pas dans les familles infinies précédemment connues :

	p^e	d	dp^i
VIII	5^7	27043	(27043,57091,51083,21043,27091,57331,52283)

Le théorème suivant donne une famille infinie qui contient ce cas pour $l = 2$.

Théorème 3.5.2. *Soit $l \geq 2$ et e un entier tel que $e \equiv -1 \mod 2^l$. Alors la fonction $x \mapsto x^d$ est presque parfaitement non linéaire sur $\mathbb{F}_{5^e}$ pour*

$$d = \frac{1}{2}\frac{5^{e+1}-1}{5^{\frac{e+1}{2^l}}+1} + \frac{5^e-1}{4}.$$

Remarque 3.5.3. Le théorème 3.3.6 prouve le cas $e \equiv -1 \mod 2^{l+1}$. Cependant, nous donnons une preuve qui n'utilise pas ce théorème.

Démonstration. On considère d'abord le cas où $e \equiv 2^l - 1 \mod 2^{l+1}$. Alors

$$\begin{aligned}\frac{5^{\frac{e+1}{2^l}}+1}{2}d &= \frac{5^{e+1}-1}{4} + \frac{5^{\frac{e+1}{2^l}}+1}{2}\frac{5^e-1}{4}\\ &= 5^e + \frac{5^e-1}{4}\frac{5^{\frac{e+1}{2^l}}+3}{2}.\end{aligned}$$

Or, si $e \equiv 2^l - 1 \mod 2^{l+1}$, $5^{\frac{e+1}{2^l}} + 3 \equiv 0 \mod 8$ donc

$$\frac{5^{\frac{e+1}{2^l}}+1}{2}d \equiv 1 \mod 5^e - 1.$$

Comme $e \equiv 2^l - 1 \mod 2^{l+1}$, $\mathrm{pgcd}(2e, \frac{e+1}{2^l}) = 1$ d'où par le lemme 3.2.5 et le (9) du théorème 3.3.4, $\Delta_d = 2$ pour $e \equiv 2^l - 1 \mod 2^{l+1}$.
Supposons maintenant que $e \equiv -1 \mod 2^{l+1}$. On a alors $(2^l+1)e \equiv 2^l - 1 \mod 2^{l+1}$ et

$$\begin{aligned}d' &= \frac{1}{2}\frac{5^{(2^l+1)e+1}-1}{5^{\frac{(2^l+1)e+1}{2^l}}+1} + \frac{5^{(2^l+1)e}-1}{4}\\ &= \frac{1}{2}\sum_{k=0}^{2^l-1}(-1)^{k+1}(5^{\frac{(2^l+1)e+1}{2^l}})^k + \frac{5^{(2^l+1)e}-1}{4}\\ &= \frac{1}{2}\sum_{k=0}^{2^l-1}(-1)^{k+1}5^{ek}(5^{\frac{e+1}{2^l}})^k + 5^e\frac{5^{2^le}-1}{4} + \frac{5^e-1}{4}\\ &= 5^e(5^e-1)\frac{1}{4}\sum_{j=0}^{2^l-1}5^{ej} + \frac{5^e-1}{4} + (5^e-1)\frac{1}{2}\sum_{k=1}^{2^l-1}\sum_{j=0}^{k-1}5^{ej}(5^{\frac{e+1}{2^l}})^k\\ &\quad + \frac{1}{2}\sum_{k=0}^{2^l-1}(-1)^{k+1}(5^{\frac{e+1}{2^l}})^k.\end{aligned}$$

Puisque $\sum_{k=0}^{2^l-1}5^{ej} \equiv 0 \mod 4$ et $\sum_{k=1}^{2^l-1}(-1)^{k+1}\sum_{j=0}^{k-1}5^{ej}(5^{\frac{e+1}{2^l}})^k \equiv 0 \mod 2$ pour $l \geq 2$,

$$d' \equiv \frac{1}{2}\frac{5^{e+1}-1}{5^{\frac{e+1}{2^l}}+1} + \frac{5^e-1}{4} \mod 5^e - 1.$$

Comme $x \mapsto x^{d'}$ est presque parfaitement non linéaire sur $\mathbb{F}_{5^{(2^l+1)e}}$ par le cas $e \equiv 2^l - 1 \mod 2^{l+1}$, $\Delta_d \leq 2$. De plus, comme e est impair, $\frac{5^e-1}{4} \equiv 1 \mod 2$. On a $\frac{1}{2}\frac{5^{e+1}-1}{5^{\frac{e+1}{2^l}}+1} \equiv 0 \mod 4$ donc d est impair et 0 et -1 sont solutions de $(x+1)^d - x^d = 1$. D'où $\Delta_d = 2$. □

Notre principale contribution dans ce chapitre est de démontrer les deux conjectures de Dobbertin, Mills, Müller, Pott et Willems [DMM+03] pour la caractéristique 3 et de donner une nouvelle famille de fonctions puissances presque parfaitement linéaires en caractéristique 5. De plus, nous donnons une nouvelle preuve de la conjecture de Dobbertin, Mills, Müller, Pott et Willems pour la caractéristique 5 et, dans le cadre du théorème de Zha et Wang [ZW10] en caractéristique 3, nous donnons une famille explicite de fonctions presque parfaitement non linéaires.

Chapitre 4

Nombres exceptionnels

Dans le chapitre précédent, on constate que les seules fonctions puissances connues presque parfaitement non linéaires sur une infinité d'extensions de $\mathbb{F}_2$ sont $x \mapsto x^{2^l+1}$ et $x \mapsto x^{2^{2l}-2^l+1}$. De même, les seules fonctions puissances connues parfaitement non linéaires sur un infinité d'extensions de $\mathbb{F}_p$ sont $x \mapsto x^{p^l+1}$ et, si $p = 3$, $x \mapsto x^{\frac{3^l+1}{2}}$. Dans [Jed07] et [HM09], Jedlicka, Hernando et McGuire ont démontré que les exposants de Gold et de Kasami sont les seuls qui donnent une fonction puissance presque parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_2$. Pour cela, ils utilisent le fait qu'une fonction puissance $x \mapsto x^d$ est presque parfaitement non linéaire sur $\mathbb{F}_{2^e}$ si et seulement si les seuls points rationnels sur $\mathbb{F}_{2^e}$ de $f(x,y) = (x+1)^d + x^d + (y+1)^d + y^d = 0$ sont tels que $x = y$ ou $x = y+1$. Ils cherchent alors à déterminer les d tels que pour une infinité d'extensions de $\mathbb{F}_2$, tous les points rationnels de $f(x,y)$ vérifient $x = y$ ou $x = y+1$. Ceci ne peut se produire que si la courbe $\frac{f(x,y)}{(x+y)(x+y+1)}$ n'a pas de facteur absolument irréductible sur $\mathbb{F}_2$. En caractéristique impaire, contrairement à la caractéristique 2, pour ϕ presque parfaitement non linéaire, on ne connait pas la relation entre les deux solutions éventuelles (il peut n'y en avoir qu'une) de $\phi(x+a) - \phi(x) = b$. Il ne semble donc pas possible d'adapter cette démonstration aux fonctions presque parfaitement non linéaires. Le bon cadre semble être les fonctions parfaitement non linéaires. Dans ce chapitre, on se propose de démontrer que les seuls exposants congrus à 1 modulo p qui donnent une fonction puissance parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_p$ sont de la forme $d = p^l + 1$ (voir [Led10c]).

4.1 Préliminaires

Dans cette section on rappelle certains outils qui nous seront utiles par la suite, notamment le théorème de Bézout pour les courbes. Une référence pour les résultats qui vont suivre est [Ful89].

4.1.1 Un lemme préliminaire

Lemme 4.1.1. *Soit $n \geq 2$ et $N \in \mathbb{N}$. Les $x_1, \ldots, x_n$ réels tels que $x_1 + \ldots + x_n = N$ qui maximisent*

$$Q_n(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n} x_i x_j$$

vérifient $x_1 = \ldots = x_n = \frac{N}{n}$.

Démonstration. On a

$$N^2 = (\sum_{i=1}^{n} x_i)^2 = \sum_{i=1}^{n} x_i^2 + 2 \sum_{1 \leq i < j \leq n} x_i x_j.$$

Donc trouver le maximum de $\sum_{1 \leq i < j \leq n} x_i x_j$ revient à minimiser

$$g(x_1, \ldots, x_{n-1}) = \sum_{i=1}^{n-1} x_i^2 + (\sum_{i=1}^{n-1} x_i - N)^2.$$

Ce minimum existe car g est continue, positive et tend vers l'infini avec les x_i. Ce minimum est atteint en $(x_1, \ldots, x_{n-1})$ si et seulement si

$$\forall 1 \leq k \leq n-1,\ 0 = \frac{\partial g}{\partial x_k}(x_1, \ldots, x_{n-1}) = 2x_k + 2(\sum_{i=1}^{n-1} x_i - N)$$

Donc si et seulement si $x_1 = \ldots = x_n = \frac{N}{n}$. □

4.1.2 Rappels sur les courbes algébriques

Définition 4.1.2. Soit $F \in \mathbb{F}_q[x_1, \ldots, x_m]$. On dit que F est absolument irréductible sur $\mathbb{F}_q$ s'il est irréductible sur toutes les extensions finies de $\mathbb{F}_q$, c'est-à dire sur une clôture algébrique de $\mathbb{F}_q$.

Lemme 4.1.3 ([Sor91])**.** *Soit $P \in \mathbb{F}_q[x_1, \ldots, x_n]$ irréductible sur $\mathbb{F}_q$ de degré d. Alors il existe r divisant d tel que P ait r facteurs absolument irréductibles de degré $\frac{d}{r}$.*

Démonstration. Si P est absolument irréductible, on a le résultat. Maintenant on suppose que P n'est pas absolument irréductible. Soit h un facteur absolument irréductible de P. Quitte à diviser par une constante, on peut supposer qu'un des coefficients de h est dans $\mathbb{F}_q$. Soit r le plus petit entier tel que les coefficients de h soient dans $\mathbb{F}_{q^r}$. Comme P n'est pas absolument irréductible, $r > 1$. Soit $\sigma \in G_{q,r}$, on considère l'application suivante :

$$\phi_\sigma : \begin{array}{ccc} \mathbb{F}_{q^r}[x_1, \ldots, x_n] & \to & \mathbb{F}_{q^r}[x_1, \ldots, x_n] \\ \sum_\alpha a_\alpha x^\alpha & \mapsto & \sum_\alpha \sigma(a_\alpha) x^\alpha \end{array}$$

Pour tout $\sigma \in G_{q,r}$, $\phi_\sigma(h)$ divise $\phi_\sigma(P) = P$. De plus, si $\sigma \neq \mathrm{Id}$ alors $\mathrm{pgcd}(\phi_\sigma(h), h) = 1$. En effet, sinon, comme h est absolument irréductible, il existe une constante λ dans $\mathbb{F}_{q^r}$ tel que $\phi_\sigma(h) = \lambda h$. Donc pour tous a, b coefficients non nuls de h on a $\sigma(\frac{a}{b}) = \frac{a}{b}$. Comme on a supposé qu'un des coefficients de h était dans $\mathbb{F}_q$, on en déduit que tous les coefficients de h sont fixés par les éléments de $G_{q,r}$. Ce qui est absurde par définition de r.
Finalement, $\prod_{\sigma \in G_{q,r}} \phi_\sigma(h)$ divise P. Comme $\prod_{\sigma \in G_{q,r}} \phi_\sigma(h) \in \mathbb{F}_q[x_1, \ldots, x_n]$ et que P est irréductible sur $\mathbb{F}_q$, on a le résultat. □

Dans ce qui suit, deux élément F et G de $\mathbb{F}_q[x, y]$ sont dits équivalents s'il existe $\lambda \in \mathbb{F}_q^*$ tel que $F = \lambda G$. On appelle courbe affine sur $\mathbb{F}_q$ une classe d'équivalence de cette relation. On appelle degré d'une courbe affine le degré d'un polynôme qui la définit.

Définition 4.1.4. Soit $F \in \mathbb{F}_q[x,y]$ et $t = (a,b) \in \mathbb{F}_q^2$. On écrit

$$F(x+a, y+b) = F_0 + F_1 + \dots$$

où F_i est un polynôme homogène de $\mathbb{F}_q[x,y]$ de degré i. Le plus petit i tel que F_i soit non nul s'appelle la multiplicité de F en t, on la note $m_t(F)$. Comme $F_{m_t(F)}$ est un polynôme homogène en deux variables, il se factorise en produit de polynômes homogènes de degré 1 sur un corps algébriquement clos. Ces facteurs s'appellent les tangentes de F en t. On dit que les tangentes de F sont simples si $F_{m_t(F)}$ n'a que des facteurs simples.

On dit que t est un point de la courbe F si $m_t(F) \geq 1$. Dans ce cas, t est un point simple de F si $m_t(F) = 1$. Sinon, t est un point singulier de F.

Lemme 4.1.5. *Soit $F \in \mathbb{F}_q[x,y]$, $t = (a,b)$ un point. Alors t est un point singulier de F si et seulement si*

$$\begin{cases} F(a,b) = 0 \\ F_x(a,b) := \frac{\partial F}{\partial x}(a,b) = 0 \\ F_y(a,b) := \frac{\partial F}{\partial y}(a,b) = 0 \end{cases}$$

Démonstration. On a $G(x,y) = F(x+a, y+b) = \alpha + \beta x + \gamma y + F_2 + F_3 + \dots$ où les F_i sont des polynômes homogènes de degré i. Alors, $F(a,b) = G(0,0) = \alpha$, $F_x(a,b) = G_x(0,0) = \beta$ et $F_y(a,b) = G_y(0,0) = \gamma$. Si t est un point de F de multiplicité au moins deux alors $\alpha = \beta = \gamma = 0$. □

Si $F = \prod_{i=1}^{r} F_i^{e_i}$ où les F_i sont irréductibles sur $\mathbb{F}_q[x,y]$, $e_i \geq 1$. Les F_i s'appellent les composantes de F et pour tout point $t = (a,b)$, on a

$$m_t(F) = \sum_{i=1}^{r} e_i m_P(F_i). \tag{4.1}$$

En effet, on a $F(x+a, y+b) = \prod_{i=1}^{r} (F_i(x+a, y+b))^{e_i} = \prod_{i=1}^{r} (F_{i,m_t(F_i)} + F_{i,m_t(F_i)+1} + \dots)^{e_i}$.

Le polynôme homogène de plus bas degré du membre de droite est $\prod_{i=1}^{r} (F_{i,m_t(F_i)})^{e_i}$ qui est de degré $\sum_{i=1}^{r} e_i m_t(F_i)$.

Si F est irréductible sur $\mathbb{F}_q$, on note $\Gamma(F)$ l'anneau intègre $\mathbb{F}_q[x,y]/(F)$. Pour t un point de F, on définit l'anneau local $O_t(F) = \{\frac{a}{b} : a, b \in \Gamma(F), b(t) \neq 0\}$.

Les théorèmes suivants sont prouvés dans [Ful89] :

Théorème 4.1.6. *Soit t un point sur une courbe irréductible F. Alors la multiplicité de F en t ne dépend que de l'anneau local $O_t(F)$.*

Théorème 4.1.7. *Soit t un point d'une courbe irréductible F ; t est un point simple de F si et seulement si l'anneau local $O_t(F)$ est un anneau de valuation discrète. De plus tout polynôme L de degré 1 tel que $L(t) = 0$ et L ne soit pas une tangente de F en P est une uniformisante de $O_t(F)$.*

On veut maintenant étendre la notion de multiplicité aux courbes projectives.

On définit une relation d'équivalence sur les polynômes homogènes de $\mathbb{F}_q[x,y,z]$ comme suit : deux polynômes F et G homogènes non nuls sont équivalents s'il existe $\lambda \in \mathbb{F}_q^*$ tel que $F = \lambda G$. Une courbe projective est une classe de cette relation d'équivalence. Comme précédemment, le degré d'une courbe projective est le degré d'un polynôme la définissant.

Pour $v \in \{x,y,z\}$, on note $U_v = \{(x:y:z) \in \mathbb{P}(\mathbb{F}_q^3) : v \neq 0\}$. On peut alors identifier U_v et $\mathbb{F}_q^2$. On note aussi $\widetilde{F}^v$ la deshomogénéisée de F en v.

Exemple 4.1.8. Si F est un polynôme homogène de $\mathbb{F}_q[x,y,z]$, $\widetilde{F}^z(x,y) = F(x,y,1)$.

On peut maintenant définir la multiplicité en un point t d'une courbe projective F : si $t \in U_v$, $v \in \{x,y,z\}$, $m_t(F) = m_t(\widetilde{F}^v)$.

La multiplicité ne dépend pas du choix de U_v. En effet, quitte à appliquer la relation (4.1), on peut supposer F irréductible. Alors la multiplicité de $\widetilde{F}^v$ ne dépend que de $O_t(\widetilde{F}^v)$. Or, l'application suivante est un isomorphisme

$$\begin{array}{ccc} O_t(F) & \to & O_t(\widetilde{F}^v) \\ \frac{a}{b} & \mapsto & \frac{\widetilde{a}^v}{\widetilde{b}^v} \end{array}.$$

Définition 4.1.9. On dit que deux courbes F et G s'intersectent proprement en un point t si F et G n'ont pas de composante commune qui contient t.

Le théorème suivant est démontré dans [Ful89].

Théorème 4.1.10. *Il existe une unique application qui a tout couple (F,G) de polynômes de $\mathbb{F}_q[x,y]$ et à tout point t associe l'élément $I_t(F,G)$ de $\mathbb{N} \cup \{+\infty\}$ vérifiant les propriétés ci-dessous :*

1. *Si F et G s'intersectent proprement en t alors $I_t(F,G) \in \mathbb{N}$, sinon $I_t(F,G) = \infty$.*
2. *On a $I_t(F,G) = 0$ si et seulement si $m_t(F) = 0$ ou $m_t(G) = 0$; $I_t(F,G)$ ne dépend que des composantes de F et G qui passent par P.*
3. *Si $T \in \mathrm{GA}_2(\mathbb{F}_q)$ et $T(s) = t$, $I_s(F \circ T, G \circ T) = I_t(F,T)$.*
4. *$I_t(F,G) = I_t(G,F)$.*
5. *$I_t(F,G) \geq m_t(F)m_t(G)$ avec égalité si et seulement si F et G n'ont pas de tangente commune en t.*
6. *Si $F = \prod_{i=1}^{r} F_i^{e_i}$ et $G = \prod_{i=1}^{s} G_j^{f_j}$ alors $I_t(F,G) = \sum_{i,j} e_i f_j I_t(F_i, G_j)$*
7. *Pour tout polynôme $A \in \mathbb{F}_q[x,y]$, $I_t(F,G) = I_t(F, G + AF)$.*

On appelle $I_t(F,G)$ la multiplicité d'intersection de F et G au point t.

Remarque 4.1.11. La multiplicité d'intersection est en fait la dimension du $\mathbb{F}_q$-espace vectoriel $O_t(0)/(F,G)$ (voir [Ful89, théorème 3 p. 75]).

On peut étendre cette définition aux courbes projectives, il faut cependant prendre un changement de variable projectif dans le point 3 et le polynôme A du point 7 doit être un polynôme homogène tel que $\deg(A) = \deg(G) - \deg(F)$.

Dans la suite, on a besoin de quelques propriétés supplémentaires sur les multiplicités d'intersection. On donne un premier résultat démontré dans [Ful89].

Proposition 4.1.12. *Si t est un point simple sur une courbe irréductible F alors*

$$I_t(F, G) = \mathrm{ord}_t^F(G)$$

où ord_t^F est une valuation sur l'anneau de valuation discrète $O_t(F)$.

On démontre de plus le résultat suivant :

Proposition 4.1.13. *Soit F une courbe sur $\mathbb{F}_q$ telle que $F = UV$. Soit $t = (a, b)$ un point de F de multiplicité m. On écrit $F(x + a, y + b) = F_m + F_{m+1} + \dots$. Supposons de plus que $\mathrm{pgcd}(F_m, F_{m+1}) = 1$. Alors $I_t(U, V) = m_t(U)m_t(V)$.*
Si de plus F n'a qu'une tangente en t, alors $I_t(U, V) = 0$.

Démonstration. On écrit

$$U(x + a, y + b) = U_r + U_{r+1} + \dots \text{ et } V(x + a, y + b) = V_s + V_{s+1} + \dots \text{ avec } r,\ s \geq 0.$$

Alors $F_m = U_r V_s$ et $F_{m+1} = U_r V_{s+1} + V_s U_{r+1}$ et $\mathrm{pgcd}(U_r, V_s)$ divise $\mathrm{pgcd}(F_m, F_{m+1}) = 1$. On déduit de la propriété (5) des multiplicités d'intersection que

$$I_t(U, V) = m_t(U)m_t(V) = rs.$$

Si F n'a qu'une tangente en t, comme $F_m = U_r V_s$ et que $\mathrm{pgcd}(U_r, V_s) = 1$, nécessairement $r = 0$ ou $s = 0$. □

Le théorème suivant est démontré dans [Ful89].

Théorème 4.1.14. *Soit F et G deux courbes projectives de degrés respectifs m et n. Alors, si F et G n'ont pas de composante commune sur une clôture algébrique de $\mathbb{F}_q$,*

$$\sum_t I_t(F, G) = mn$$

On en déduit les résultats suivants qui nous seront utiles par la suite.

Lemme 4.1.15. *Si h n'a pas de facteur absolument irréductible sur $\mathbb{F}_p$, alors il existe une factorisation de $h = uv$ telle que*

$$\sum_t I_t(u, v) \geq 2\frac{\deg(h)^2}{9}.$$

Autrement dit , si I_{tot} est un majorant de la multiplicité d'intersection globale $\sum_t I_t(u, v)$,

$$\alpha = \frac{I_{tot}}{\frac{\deg(h)^2}{4}} \geq \frac{8}{9}.$$

Démonstration. Supposons que h se factorise sur $\mathbb{F}_p$. Comme $h = e_1 \dots e_r$, où chaque e_i est irréductible sur $\mathbb{F}_p$ mais pas absolument irréductible, chaque e_i se factorise en $c_i \geq 2$ facteurs sur une clôture algébrique de $\mathbb{F}_p$ et chacun de ces facteurs est de degré $\frac{\deg(e_i)}{c_i}$ (lemme 4.1.3). On factorise maintenant chaque facteur e_i en 2 polynômes u_i, v_i tels que $\deg(u_i) = \deg(v_i)$ si c_i est pair et $\deg(u_i) = \deg(v_i) + \frac{\deg(e_i)}{c_i}$ si c_i est impair (donc $c_i \geq 3$). On pose $u = \prod_{i=1}^{r} u_i$ et $v = \prod_{i=1}^{r} v_i$. On a alors $\deg(u) - \deg(v) \leq \frac{\deg(h)}{3}$. Comme de plus $\deg(u) + \deg(v) = \deg(h)$,

$$\deg(u)\deg(v) \geq \frac{8}{9}\frac{\deg(h)^2}{4}.$$

Soit I_{tot} un majorant de la multiplicité d'intersection globale pour tout u, v. Alors, par le théorème de Bézout, on a

$$I_{tot} \geq \sum_t I_t(u,v) = \deg(u)\deg(v) \geq \frac{8}{9}\frac{\deg(h)^2}{4} = 2\frac{\deg(h)^2}{9}.$$

□

Lemme 4.1.16. *Soit F une courbe et un point t tels que F n'ait que des tangentes simples en t. Si on décompose $F = f_1 \dots f_r$ en facteurs irréductibles sur $\mathbb{F}_q$ et chaque $f_k = f_{k,1} \dots f_{k,n_k}$ en facteurs absolument irréductibles sur $\mathbb{F}_q$, on a les résultats suivants :*

1. $\deg(f_k)^2 \leq \sum_{t \in Sing(F)} m_t(f_k)^2$ *où $Sing(F)$ est l'ensemble des points singuliers de F.*

2. $\sum_{1 \leq i < j \leq n_k} m_t(f_{k,i})m_t(f_{k,j}) \leq m_t(f_k)^2 \frac{n_k - 1}{2n_k}$.

Démonstration. Comme $m_t(f_k) = \sum_{i=1}^{n_k} m_t(f_{k,i})$, par le lemme 4.1.1, on a la deuxième inégalité :

$$\sum_{1 \leq i < j \leq n_k} m_t(f_{k,i})m_t(f_{k,j}) \leq m_t(f_k)^2 \frac{n_k - 1}{2n_k}.$$

En appliquant Bézout à $f_{k,i}$ et $f_{k,j}$ pour tout $1 \leq i < j \leq n_k$, on a

$$\sum_{1 \leq i < j \leq n_k} \sum_{t \in Sing(f_k)} I_t(f_{k,i}, f_{k,j}) = \sum_{1 \leq i < j \leq n_k} \deg(f_{k,i})\deg(f_{k,j}).$$

Or, par le lemme 4.1.3, pour tout i, $\deg(f_{k,i}) = \frac{\deg(f_k)}{n_k}$ d'où

$$\sum_{1 \leq i < j \leq n_k} \deg(f_{k,i})\deg(f_{k,j}) = \deg(f_k)^2 \frac{n_k - 1}{2n_k}.$$

De plus, comme les tangentes de F sont simples, par la propriété (5) des multiplicités d'intersection, on a $I_t(f_{k,i}, f_{k,j}) = m_t(f_{k,i})m_t(f_{k,j})$. En remplaçant et en utilisant la deuxième inégalité, on a le résultat. □

4.2 Définitions

Dans cette section, on rappelle la définition des nombres exceptionnels en caractéristique paire et on étend cette définition à la caractéristique impaire. On donne ensuite leur lien avec les fonctions presque parfaitement non linéaires et parfaitement non linéaires.

Si d est un entier tel que $d \equiv 0 \mod p$ alors x^d est équivalent à $x^{\frac{d}{p}}$ donc dans toute la suite de ce chapitre, on suppose $d \not\equiv 0 \mod p$. On note $f(x,y) = (x+1)^d - x^d - (y+1)^d + y^d$.

4.2.1 En caractéristique paire

Définition 4.2.1. Un entier $d \geq 3$ est dit exceptionnel si le polynôme de $\mathbb{F}_{2^e}[x,y]$

$$g(x,y) = \frac{(x+1)^d + x^d + (y+1)^d + y^d}{(x+y)(x+y+1)}$$

n'a pas de facteur absolument irréductible.

Par ailleurs, on dispose de la caractérisation suivante d'une fonction presque parfaitement non linéaire.

Proposition 4.2.2. *Une fonction ϕ est presque parfaitement non linéaire sur $\mathbb{F}_{2^e}$ si et seulement si pour tout $\alpha \in \mathbb{F}_{2^e}$ tous les points rationnels sur $\mathbb{F}_{2^e}$ de*

$$\varphi_\alpha(x,y) = \phi(x+\alpha) + \phi(x) + \phi(y+\alpha) + \phi(y)$$

sont tels que $x = y$ ou $x = y + \alpha$.

Remarque 4.2.3. Par le lemme 3.2.4, si ϕ est une fonction puissance, il suffit de considérer $\alpha = 1$.

Proposition 4.2.4. *Soit d un entier tel que $x \mapsto x^d$ soit presque parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_2$, alors d est un nombre exceptionnel.*

Démonstration. Soit d impair tel que $x \mapsto x^d$ soit presque parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_2$. Supposons que g ait un facteur absolument irréductible que l'on note j.
Si $j = c(x+y)$, $c \in \mathbb{F}_{2^e}^*$, alors $(x+1)^d + x^d + (y+1)^d + y^d = (y+x)^2(y+x+1)\widetilde{j}(x,y)$, $\widetilde{j} \in \mathbb{F}_{2^e}[x,y]$. On dérive cette expression par rapport à y :

$$d(y+1)^{d-1} + dy^{d-1} = (y+x)^2(y+x+1)\frac{\partial \widetilde{j}}{\partial y}(x,y) + (y+x)^2\widetilde{j}(x,y).$$

On obtient donc que pour tout $x \in \mathbb{F}_{2^e}$, $d(x+1)^{d-1} + dx^{d-1} = 0$. C'est impossible car d est impair. De la même façon, on prouve que $j \neq c(x+y+1)$, $c \in \mathbb{F}_{2^e}^*$.
Soit n le degré de j. Comme $j \neq c(x+y)$ et $j \neq c(x+y+1)$, $j(x,x)$ et $j(x,x+1)$ sont différents du polynôme nul. Il y a donc au plus $2n$ points rationnels de j tels que $x = y$ ou $x = y+1$.
D'autre part, puisqu'on voudrait estimer le nombre de points rationnels affines de j sur $\mathbb{F}_{2^e}$, on ne peut pas utiliser l'inégalité de Weil (voir [Wei48]). Cependant, si on note n_P le nombre total de points rationnels de j sur $\mathbb{F}_{2^e}$, par [LN97, p. 331], on a :

$$|n_P - 2^e| \leq (n-1)(n-2)\sqrt{2^e} + n^2.$$

Donc pour e assez grand, j a un point rationnel tel que $x \neq y$ et $x \neq y+1$, ce qui est absurde car $x \mapsto x^d$ est parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_2$. $\square$

4.2.2 En caractéristique impaire

Définition 4.2.5. Un entier $d \geq 3$ est dit exceptionnel si le polynôme de $\mathbb{F}_q[x, y]$

$$h(x, y) = \frac{(x+1)^d - x^d - (y+1)^d + y^d}{x - y}$$

n'a pas de facteur absolument irréductible.

On donne maintenant une caractérisation d'une fonction parfaitement non linéaire.

Proposition 4.2.6. *Une fonction ϕ est parfaitement non linéaire sur $\mathbb{F}_{p^e}$ si et seulement si pour tout $\alpha \in \mathbb{F}_{p^e}$ tous les points rationnels sur $\mathbb{F}_{p^e}$ de*

$$\varphi_\alpha(x, y) = \phi(x + \alpha) - \phi(x) - \phi(y + \alpha) + \phi(y)$$

sont tels que $x = y$.

Remarque 4.2.7. Par le lemme 3.2.4, si ϕ est une fonction puissance, il suffit de considérer $\alpha = 1$.

Proposition 4.2.8. *Soit d un entier tel que $x \mapsto x^d$ soit parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_p$; alors d est un nombre exceptionnel.*

Démonstration. Soit $d \not\equiv 0 \mod p$ tel que $x \mapsto x^d$ soit parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_p$. Supposons que h ait un facteur absolument irréductible que l'on note j. Comme dans le cas de la caractéristique paire, on démontre que $j \neq c(x - y)$, $c \in \mathbb{F}_{p^e}$.
Soit n le degré de j. Comme $j \neq c(x - y)$, $j(x, x)$ n'est pas le polynôme nul. Il y a donc au plus n points rationnels de j tels que $x = y$.
D'autre part, si on note n_P le nombre total de points rationnels de j sur $\mathbb{F}_{p^e}$, par [LN97, p. 331], on a :

$$|n_P - p^e| \leq (n-1)(n-2)\sqrt{p^e} + n^2.$$

Donc pour e assez grand, j a un point rationnel tel que $x \neq y$, ce qui est absurde car $x \mapsto x^d$ est parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_p$. □

4.3 Nombres exceptionnels en caractéristique paire

Dans cette section, on rappelle des résultats prouvés par Jedlicka dans [Jed07] et Hernando et McGuire dans [HM09]. Ils démontrent qu'en caractéristique 2, les seuls nombres exceptionnels sont les exposants de Gold et Kasami. Les méthodes que nous utilisons par la suite pour la caractéristique impaire étant analogues aux méthodes utilisées par ces auteurs, on ne rappelle pas les démonstrations des résultats. On note l le plus grand entier tel que 2^l divise $d - 1$, et $n = \text{pgcd}(d - 1, 2^l - 1) = \text{pgcd}\left(\frac{d-1}{2^l}, 2^l - 1\right)$.

Théorème 4.3.1. *Les singularités de g avec leur multiplicité et leur multiplicité d'intersection sont données dans le tableau 4.1.*

Théorème 4.3.2. *Si $d \neq 2^l + 1$ et $d \neq 2^{2l} - 2^l + 1$, h un facteur absolument irréductible.*

La preuve de ce théorème découle des théorèmes 3 et 4 de [Jed07] et du théorème 16 de [HM09].

Table 4.1 – Singularités de g

Type	Description	$m_t(h)$	max de I_t	nombre de points max
Ia	Affine $x_0 = y_0$ ou $x_0 = y_0 + 1$, x_0, $y_0 \in \mathbb{F}_{2^l}^*$	2^l	$(2^{l-1})^2$	$2(n-1)$
Ib	Affine $x_0 = y_0$ ou $x_0 = y_0 + 1$, x_0, $y_0 \notin \mathbb{F}_{2^l}^*$	$2^l - 1$	0	$\frac{d-1}{2^{l-1}} - 2$
IIa	Affine $x_0 \neq y_0$ et $x_0 \neq y_0 + 1$, x_0, $y_0 \in \mathbb{F}_{2^l}^*$	$2^l + 1$	$2^{l-1}(2^{l-1} + 1)$	$(n-1)(n-3)$
IIb	Affine $x_0 \neq y_0$ et $x_0 \neq y_0 + 1$, x_0 ou $y_0 \notin \mathbb{F}_{2^l}^*$	2^l	0	sans importance
IIc	Affine $x_0 \neq y_0$ et $x_0 \neq y_0 + 1$, x_0 et $y_0 \notin \mathbb{F}_{2^l}^*$	2^l	2^l si $l > 1$, 0 sinon	N [a]
IIIa	$(1:1:0)$	$2^l - 2$	$\left(\frac{2^l-2}{2}\right)^2$	1
IIIb	$(\omega:1:0)$, $\omega^n = 1$ et $\omega \neq 1$	2^l	$(2^{l-1})^2$	$n-1$
IIIc	$(\omega:1:0)$, $\omega^n \neq 1$	$2^l - 1$	0	sans importance

a. $N = \begin{cases} \left(\frac{d-1}{2^l} - 1\right)\left(\frac{d-1}{2^{l-1}} - 2^{i_b - l + 1} - 2\right) - (n-1)(n-3) & \text{si } l > 1 \text{ et } d = \sum_{j=1}^{b} 2^{i_j},\ i_j > i_{j-1} \\ \text{ou } ((2^l-2)(2^l+1)-1)(\frac{d-1}{2^l} - 1) & \text{si } l = 1 \end{cases}$

4.4 Les nombres exceptionnels congrus à 1 modulo p en caractéristique impaire

Dans cette partie, on suppose $d \equiv 1 \mod p$. On note l le plus grand entier tel que p^l divise $d-1$, et $n = \text{pgcd}(d-1, p^l - 1) = \text{pgcd}\left(\frac{d-1}{p^l}, p^l - 1\right)$.

Le théorème suivant donne les nombres exceptionnels congrus à 1 modulo p.

Théorème 4.4.1. *Soit $d \geq 3$, $d \neq p^l + 1$. Supposons de plus que $\frac{d-1}{p^l} \neq p^l - 1$, alors h a un facteur absolument irréductible sur $\mathbb{F}_p$.*

On en déduit le résultat suivant sur les exposants congrus à 1 modulo p qui donnent une fonction puissance parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_p$:

Corollaire 4.4.2. *Les seuls $d \equiv 1 \mod p$ tels que $x \mapsto x^d$ soit parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_p$ sont de la forme $d = 1 + p^l$.*

Démonstration. Par le théorème 4.4.1 et la proposition 4.2.8, on a tous les cas sauf le cas où $n = \frac{d-1}{p^l} = p^l - 1$. Dans ce dernier cas, on a $d = p^l(p^l - 1) + 1$, il est donc impair et -1 et 0 sont solutions de l'équation $(x+1)^d - x^d = 1$. D'où $x \mapsto x^{p^l(p^l-1)+1}$ n'est pas parfaitement non linéaire $\mathbb{F}_{p^e}$ pour tout e. □

Proposition 4.4.3. *Les singularités de h sont décrites dans le tableau 4.2.*

La preuve de cette proposition découle des lemmes 4.4.4 à 4.4.18 et de leurs corollaires.

TABLE 4.2 – Singularités de h pour $d \equiv 1 \mod p$

Type	Description	$m_t(h)$	max de I_t	nombre de points max
Ia	Affine $x_0 = y_0$ x_0, $y_0 \in \mathbb{F}_{p^l}^*$	p^l	$\frac{p^{2l}-1}{4}$	$n-1$
Ib	Affine $x_0 = y_0$, x_0, $y_0 \notin \mathbb{F}_{p^l}^*$	$p^l - 1$	0	$\frac{d-1}{p^l} - n$
IIa	Affine $x_0 \neq y_0$, x_0, $y_0 \in \mathbb{F}_{p^l}^*$	$p^l + 1$	$\left(\frac{p^l+1}{2}\right)^2$	$(n-1)(n-2)$
IIb	Affine $x_0 \neq y_0$, x_0 ou $y_0 \notin \mathbb{F}_{p^l}^*$	p^l	0	N_1 [a]
IIc	Affine $x_0 \neq y_0$, x_0 et $y_0 \notin \mathbb{F}_{p^l}^*$	p^l	p^l [b]	N_2 [c]
IIIa	$(1:1:0)$	$p^l - 1$	$\left(\frac{p^l-1}{2}\right)^2$	1
IIIb	$(\omega:1:0)$, $\omega^n = 1$ et $\omega \neq 1$	p^l	$\frac{p^{2l}-1}{4}$	$n-1$
IIIc	$(\omega:1:0)$, $\omega^n \neq 1$	$p^l - 1$	0	$\frac{d-1}{p^l}$

a. $N_1 = \left(\frac{d-1}{p^l} - 1\right)\left(2\frac{d-1}{p^l} - (d_b+1)p^{i_b - l} - 1\right) - (n-1)(n-2)$ où $d = \sum_{j=0}^{b} d_j p^{i_j}$ avec $1 \leq d_j \leq q-1$ et $i_j > i_{j-1}$

b. $I_t(u,v) = 0$ si $y_0(x_0+1)^{p^l}(y_0^{p^l-1}-1)^{p^l+1} \neq x_0(y_0+1)^{p^l}(x_0^{p^l-1}-1)^{p^l+1}$

c. $N_2 = \begin{cases} \left(\frac{d-1}{p^l} - 1\right)\left(2\frac{d-1}{p^l} - (d_b+1)p^{i_b - l} - 1\right) - (n-1)(n-2) \\ \text{ou } ((p^l-2)(p^l+1)-1)(\frac{d-1}{p^l} - 1) \\ \qquad \text{si } y_0(x_0+1)^{p^l}(y_0^{p^l-1}-1)^{p^l+1} = x_0(y_0+1)^{p^l}(x_0^{p^l-1}-1)^{p^l+1} \end{cases}$

4.4.1 Points singuliers et multiplicités

Singularités à l'infini

On note $\overline{f}$ (resp. $\overline{h}$) l'homogénéisée de f (resp. h). On note $\widetilde{f}$ (resp. $\widetilde{h}$) la forme deshomogénéisée de $\overline{f}$ (resp. $\overline{h}$) par rapport à y.

Soit $F(x,y,z) = (x+z)^d - x^d - (y+z)^d + y^d = z\overline{f}$. On a

$$\begin{cases} F_x &= d(x+z)^{d-1} - dx^{d-1} \\ F_y &= -d(y+z)^{d-1} + dy^{d-1} \\ F_z &= d(x+z)^{d-1} - d(y+z)^{d-1} \end{cases}.$$

A l'infini ($z = 0$), on a $F_x = F_y = 0$ et $F_z = d(x^{d-1} - y^{d-1})$ donc $(x_0, y_0, 0)$ est un point singulier de F si et seulement si $x_0^{d-1} = y_0^{d-1}$. Si $y_0 = 0$ alors $x_0 = 0$. Par conséquent, $y_0 \neq 0$ et on est ramené à étudier les solutions de

$$x_0^{d-1} = 1 \tag{4.2}$$

L'équation (4.2) est équivalente à $x_0^{\frac{d-1}{p^l}} = 1$. Or, pgcd $\left(\frac{d-1}{p^l}, p\right) = 1$ donc (4.2) a au plus $\frac{d-1}{p^l}$ solutions. De plus, $x_0 = 1$ est la seule solution telle que $x_0 = y_0$.

On étudie maintenant la multiplicité de ces singularités :

$$\begin{aligned} \widetilde{F}(x+x_0, z) &= (x+x_0+z)^d - (x+x_0)^d - (z+1)^d + 1 \\ &= \sum_{k=2}^{d} \binom{d}{k} (x+z)^k x_0^{d-k} - \sum_{k=2}^{d} \binom{d}{k} x^k x_0^{d-k} - \sum_{k=2}^{d} \binom{d}{k} z^k. \end{aligned}$$

Puisque $d-1 \equiv 0 \mod p^l$, pour tout $1 < k < p^l$, $\binom{d}{k} = 0$. Calculons le terme de degré $p^l - 1$ de $\overline{f}$:

$$\frac{1}{z}\binom{d}{p^l}(x_0^{d-p^l}(x+z)^{p^l} - x_0^{d-p^l}x^{p^l} - z^{p^l}) = \binom{d}{p^l}(x_0^{d-p^l} - 1)z^{p^l-1}$$

donc on a un point singulier de $\overline{f}$ de multiplicité strictement plus grande que $p^l - 1$ si et seulement si

$$x_0^{d-p^l} = 1;$$

autrement dit si et seulement si

$$x_0^n = 1.$$

Regardons maintenant le terme de degré p^l de $\widetilde{f}$:

$$\begin{aligned}\frac{1}{z}\binom{d}{p^l+1}&(x_0^{d-p^l-1}(x+z)^{p^l+1} - x_0^{d-p^l-1}x^{p^l+1} - z^{p^l+1})\\ &= \binom{d}{p^l+1}(x_0^{d-p^l-1}x^{p^l} + x_0^{d-p^l-1}xz^{p^l-1} + (x_0^{d-p^l-1} - 1)z^{p^l}).\end{aligned}$$

Or, $x_0^{d-p^l-1} \neq 0$ donc les points singuliers de $\overline{f}$ de multiplicité strictement supérieure à $p^l - 1$ sont de multiplicité p^l.

On a donc démontré le lemme suivant :

Lemme 4.4.4. *Soit ω tel que $\omega^{\frac{d-1}{p^l}} = 1$. Le point $(\omega : 1 : 0)$ est un point singulier de $\overline{h}$ de multiplicité :*

$$\begin{cases} p^l & \text{si } \omega^n = 1,\ \omega \neq 1 \\ p^l - 1 & \text{sinon} \end{cases}.$$

Il y a donc $\frac{d-1}{p^l}$ points singuliers à l'infini.

Singularités affines

On a

$$\begin{cases} f_x &= d(x+1)^{d-1} - dx^{d-1} \\ f_y &= -d(y+1)^{d-1} + dy^{d-1} \end{cases}.$$

Donc, puisque $d \not\equiv 0 \mod p$,

$$\begin{aligned}(x_0, y_0) \text{ point singulier de } f &\Leftrightarrow \begin{cases} f(x_0, y_0) = 0 \\ (x_0+1)^{d-1} = x_0^{d-1} \\ (y_0+1)^{d-1} = y_0^{d-1} \end{cases}\\ &\Leftrightarrow \begin{cases} x_0^{d-1}(x_0+1) - x_0^d - y_0^{d-1}(y_0+1) + y_0^d = 0 \\ (x_0+1)^{d-1} = x_0^{d-1} \\ (y_0+1)^{d-1} = y_0^{d-1} \end{cases}\\ &\Leftrightarrow \begin{cases} x_0^{d-1} = y_0^{d-1} \\ (x_0+1)^{d-1} = x_0^{d-1} \\ (y_0+1)^{d-1} = y_0^{d-1} \end{cases}.\end{aligned}$$

Lemme 4.4.5. *Les points singuliers affines de f sont les points vérifiant :*

$$(x_0+1)^{d-1} = x_0^{d-1} = y_0^{d-1} = (y_0+1)^{d-1}.$$

Du lemme 4.4.5, on déduit que x_0, $y_0 \neq 0, -1$. Comme $d \equiv 1 \mod p^l$,

$$(x_0, y_0) \text{ point singulier de } f \Leftrightarrow \begin{cases} x_0^{\frac{d-1}{p^l}} = y_0^{\frac{d-1}{p^l}} \\ (x_0+1)^{\frac{d-1}{p^l}} = x_0^{\frac{d-1}{p^l}} \\ (y_0+1)^{\frac{d-1}{p^l}} = y_0^{\frac{d-1}{p^l}} \end{cases} \tag{4.3}$$

Il y a au plus $\frac{d-1}{p^l} - 1$ solutions à la deuxième équation du système (4.3). Soit x_0 une telle solution. On cherche à déterminer le nombre de y_0 tels que (x_0, y_0) soit un point singulier de f.

On écrit $d = 1 + \sum_{j=1}^{b} d_j p^{i_j}$ avec $1 \leq d_j \leq p-1$, $i_j > i_{j-1}$, $i_1 = l$. On a alors :

$$(y_0+1)^{\frac{d-1}{p^l}} = y_0^{\frac{d-1}{p^l}}.$$

Soit en développant

$$\prod_{j=1}^{b} (y_0+1)^{d_j p^{i_j - l}} = y_0^{\frac{d-1}{p^l}}$$

puis

$$\sum_{0 \leq k_j \leq d_j}^{*} \left(\prod_{j=1}^{b} \binom{d_j}{k_j} \right) y_0^{\sum_{j=1}^{b} k_j p^{i_j - l}} = 0$$

où la somme * est la somme privée de l'indice $(d_1, \ldots, d_b)$.

On multiplie par $y_0^{\frac{d-1}{p^l} - d_b p^{i_b - l}}$ et on pose $\alpha = y_0^{\frac{d-1}{p^l}}$:

$$\sum_{\substack{0 \leq k_j \leq d_j \\ j \neq b}}^{*} \left(\prod_{j=1}^{b-1} \binom{d_j}{k_j} \right) \alpha y_0^{\sum_{j=1}^{b-1} k_j p^{i_j - l}}$$

$$+ \sum_{k_b=0}^{d_b-1} \sum_{\substack{0 \leq k_j \leq d_j \\ j \neq b}} \left(\prod_{j=1}^{b} \binom{d_j}{k_j} \right) y_0^{\frac{d-1}{p^l} - (d_b - k_b) p^{i_b - l} + \sum_{j=1}^{b-1} k_j p^{i_j - l}} = 0.$$

Le degré de ce polynôme en y_0 est $\frac{d-1}{p^l} - p^{i_b - l} + \sum_{j=1}^{b-1} d_j p^{i_j - l} = 2\frac{d-1}{p^l} - (d_b+1)p^{i_b - l}$.

Lemme 4.4.6. *Le nombre de singularités affines de h est au plus*

$$\left(\frac{d-1}{p^l} - 1 \right) \left(2\frac{d-1}{p^l} - (d_b+1)p^{i_b - l} \right)$$

où $d = 1 + \sum_{j=1}^{b} d_j p^{i_j}$ *avec* $1 \leq d_j \leq p-1$, $i_j > i_{j-1}$, $i_1 = l$.

On étudie la multiplicité de ces singularités :

$$\begin{aligned} f(x+x_0, y+y_0) &= (x+x_0+1)^d - (x+x_0)^d - (y+y_0+1)^d + (y+y_0)^d \\ &= \sum_{k=2}^{d} \binom{d}{k} x^k (x_0+1)^{d-k} - \sum_{k=2}^{d} x^k x_0^{d-k} \\ &\qquad - \sum_{k=2}^{d} \binom{d}{k} y^k (y_0+1)^{d-k} + \sum_{k=2}^{d} y^k y_0^{d-k}. \end{aligned}$$

Comme $d-1 \equiv 0 \mod p^l$, pour tout $2 \leq k < p^l$, $\binom{d}{k} = 0$ et (x_0, y_0) est une singularité de multiplicité au moins p^l. Regardons maintenant le terme de degré p^l+1 :

$$\binom{d}{p^l+1}(((x_0+1)^{d-p^l-1} - x_0^{d-p^l-1})x^{p^l+1} - ((y_0+1)^{d-p^l-1} - y_0^{d-p^l-1})y^{p^l+1}).$$

Or, (x_0, y_0) est un point singulier de f donc $(x_0+1)^{d-1} = x_0^{d-1}$ et $x_0 \neq -1, 0$ donc $(x_0+1)^{d-p^l-1} - x_0^{d-p^l-1} = 0$ si et seulement si $(x_0+1)^{p^l}((x_0+1)^{d-p^l-1} - x_0^{d-p^l-1}) = 0$. Autrement dit si et seulement si $-x_0^{d-p^l-1} = 0$ ce qui est absurde puisque $x_0 \neq 0$. Les singularités sont donc de multiplicité au plus p^l+1.

Considérons maintenant le terme de degré p^l :

$$\binom{d}{p^l}(((x_0+1)^{d-p^l} - x_0^{d-p^l})x^{p^l} - ((y_0+1)^{d-p^l} - y_0^{d-p^l})y^{p^l}).$$

Or,

$$(x_0+1)^{d-p^l} - x_0^{d-p^l} = 0$$

si et seulement si

$$(x_0+1)^{p^l}((x_0+1)^{d-p^l} - x_0^{d-p^l}) = 0$$

autrement dit si et seulement si

$$(x_0+1)^{d-1}(x_0+1) - x_0^d - x_0^{d-p^l} = 0$$

c'est-à-dire si et seulement si

$$x_0^{d-p^l}(x_0^{p^l-1} - 1) = 0$$

ce qui est équivalent puisque $x_0 \neq 0$ à $x_0 \in \mathbb{F}_{p^l}^*$. On peut procéder de même pour y_0.

Lemme 4.4.7. *Il y a au plus :*

- $n-1$ *singularités affines de* h *(resp.* f*) telles que* $x_0 = y_0 \in \mathbb{F}_{p^l}^*$*. Elles sont de multiplicité* p^l *(resp.* p^l+1*).*
- $\frac{d-1}{p^l} - n$ *singularités affines de* h *(resp.* f*) telles que* $x_0 = y_0 \notin \mathbb{F}_{p^l}^*$*. Elles sont de multiplicité* $p^l - 1$ *(resp.* p^l*).*
- $(n-1)(n-2)$ *singularités affines de* h *(et de* f*) telles que* $x_0 \neq y_0$ *et* x_0*,* $y_0 \in \mathbb{F}_{p^l}^*$*. Elles sont de multiplicité* p^l+1*.*
- $\left(\frac{d-1}{p^l} - 1\right)\left(2\frac{d-1}{p^l} - (d_b+1)p^{i_b-l} - 1\right) - (n-1)(n-2)$ *singularités affines de* h *(et de* f*) telles que* $x_0 \neq y_0$ *et* x_0 *ou* $y_0 \notin \mathbb{F}_{p^l}^*$*. Elles sont de multiplicité* p^l*.*

4.4.2 Multiplicités d'intersection

On écrit $h = uv$; on cherche à majorer la multiplicité d'intersection $I_t(u, v)$ où t est une singularité de h.

Points singuliers à l'infini

Soit $t = (\omega : 1 : 0)$ un point singulier de h à l'infini, $\omega^{\frac{d-1}{p^l}} = 1$. On écrit

$$\widetilde{h}(x + \omega, z) = \widetilde{H}_{m_t} + \widetilde{H}_{m_t+1} + \dots$$

où m_t est la multiplicité de t et $\widetilde{H}_i$ est le polynôme homogène de degré i composé des termes de degré i de $\widetilde{h}(x + \omega, z)$. On a

$$\begin{aligned}\widetilde{f}(x + \omega, z) &= \widetilde{h}(x + \omega, z)(x + \omega - 1)\\ &= (R + \widetilde{H}_{m_t+1} + \widetilde{H}_{m_t})(x + \omega - 1)\\ &\qquad \text{où } R \text{ est un polynôme de degré supérieur ou égal à } m_t + 2\\ &= xR + (\omega - 1)R + x\widetilde{H}_{m_t} + (\omega - 1)\widetilde{H}_{m_t+1} + (\omega - 1)\widetilde{H}_{m_t}\end{aligned}$$

donc

- si $\omega \neq 1$, on a $\widetilde{F}_{m_t} = (\omega - 1)\widetilde{H}_{m_t}$ et $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t} + (\omega - 1)\widetilde{H}_{m_t+1}$,
- si $\omega = 1$, $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t}$.

Lemme 4.4.8. *Si $\omega^{\frac{d-1}{p^l}} = 1$ et $t = (\omega : 1 : 0)$ est un point singulier à l'infini de h de multiplicité m_t, alors*

- *si $\omega \neq 1$, $\widetilde{F}_{m_t} = (\omega - 1)\widetilde{H}_{m_t}$ et $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t} + (\omega - 1)\widetilde{H}_{m_t+1}$.*
- *si $\omega = 1$, $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t}$.*

Corollaire 4.4.9. *Si $t = (1 : 1 : 0)$, alors*

$$I_t(u, v) \leq \left(\frac{p^l - 1}{2}\right)^2.$$

Démonstration. Si $t = (1 : 1 : 0)$, alors il est de multiplicité $p^l - 1$. Par le lemme 4.4.8, $\widetilde{H}_{m_t} = a(x^{p^l-1} + z^{p^l-1})$. Tous ses facteurs sont différents donc $I_t(u, v) = m_t(u)m_t(v)$. De plus, $m_t(u) + m_t(v) = p^l - 1$ d'où le résultat par le lemme 4.1.1. □

Corollaire 4.4.10. *Si $t = (\omega : 1 : 0)$ tel que $\omega^n = 1$, $\omega \neq 1$ alors*

$$I_t(u, v) \leq \frac{p^{2l} - 1}{4}.$$

Démonstration. La multiplicité de t est p^l. Par le lemme 4.4.8, on a

$$(\omega - 1)\widetilde{H}_{p^l} = \widetilde{F}_{p^l} = x^{p^l}\omega^{d-p^l-1} + xz^{p^l-1}\omega^{d-p^l-1} + (\omega^{d-p^l-1} - 1)z^{p^l}.$$

Donc $\widetilde{H}_{p^l}$ n'a que des facteurs simples et $I_t(u, v) = m_t(u)m_t(v)$. On a le résultat puisque $m_t(u) + m_t(v) = p^l$. □

Corollaire 4.4.11. *Si $t = (\omega : 1 : 0)$ avec $\omega^{\frac{d-1}{p^l}}$, $\omega^n \neq 1$, on a*

$$I_t(u, v) = 0.$$

Démonstration. La multiplicité de t est $p^l - 1$. Par le lemme 4.4.8,

$$(\omega - 1)\widetilde{H}_{p^l-1} = \widetilde{F}_{p^l-1} = \alpha z^{p^l-1}$$

et

$$x\widetilde{H}_{p^l-1} + (\omega - 1)\widetilde{H}_{p^l} = \widetilde{F}_{p^l} = x^{p^l}\omega^{d-p^l-1} + xz^{p^l-1}\omega^{d-p^l-1} + z^{p^l}(\omega^{d-1-p^l} - 1).$$

Donc $\mathrm{pgcd}(\widetilde{H}_{p^l}, \widetilde{H}_{p^l-1}) = \mathrm{pgcd}(\widetilde{F}_{p^l}, \widetilde{F}_{p^l-1}) = 1$ et $I_t(u, v) = 0$ par la proposition 4.1.13. □

Points singuliers affines

Soit $t = (x_0, y_0)$ un point singulier affine de h de multiplicité m_t. On écrit

$$h(x + x_0, y + y_0) = H_{m_t} + H_{m_t+1} + \dots$$

où m_t est la multiplicité de t et H_i est le polynôme homogène de degré i composé des termes de degré i de $h(x + x_0, y + y_0)$.

Supposons que $x_0 = y_0$. Alors

$$\begin{aligned} f(x + x_0, y + y_0) &= h(x + x_0, y + y_0)(x + x_0 - y - y_0) \\ &= (R + H_{m_t+1} + H_{m_t})(x - y) \\ &\quad \text{où } R \text{ est un polynôme de degré supérieur ou égal à } m_t + 2 \\ &= (x - y)R + (x - y)H_{m_t+1} + (x - y)H_{m_t} \\ &= F_{m_t+1} + F_{m_t+2} + \dots \end{aligned}$$

On a donc $F_{m_t+2} = (x - y)H_{m_t+1}$ et $F_{m_t+1} = (x - y)H_{m_t}$ et F_{m_t+1} est de la forme $a(x^{m_t+1} - y^{m_t+1})$ (*cf.* preuve du lemme 4.4.7).

Lemme 4.4.12. *Pour $t = (x_0, y_0)$ point singulier affine de h de multiplicité m_t tel que $x_0 = y_0$, $F_{m_t+2} = (x - y)H_{m_t+1}$ et $F_{m_t+1} = (x - y)H_{m_t}$.*
De plus, les tangentes à h en t sont les facteurs de $\frac{x^{m_t+1} - y^{m_t+1}}{x-y}$.

Corollaire 4.4.13. *Les singularités affines de h, $t = (x_0, y_0)$ telles que $x_0 = y_0 \in \mathbb{F}_{p^l}^*$ vérifient*

$$I_t(u, v) \leq \frac{p^{2l} - 1}{4}.$$

Démonstration. La multiplicité de t pour h est p^l. Les facteurs de $\frac{x^{p^l+1} - y^{p^l+1}}{x-y}$ étant tous distincts, $I_t(u, v) = m_t(u)m_t(v)$. On a de plus $m_t(u) + m_t(v) = p^l$ d'où $m_t(u)m_t(v) \leq \frac{p^{2l}-1}{4}$, ce qui donne le résultat. □

Corollaire 4.4.14. *Les singularités affines de h, $t = (x_0, y_0)$, $x_0 = y_0 \notin \mathbb{F}_{p^l}^*$ vérifient*

$$I_t(u, v) = 0.$$

Démonstration. La multiplicité de t est $p^l - 1$. Par le lemme 4.4.12, on a

$$H_{p^l-1} = a(x-y)^{p^l-1} \text{ et } H_{p^l} = \frac{b(x^{p^l+1} - y^{p^l+1})}{x-y}$$

d'où $\operatorname{pgcd}(H_{p^l-1}, H_{p^l}) = 1$. Par la proposition 4.1.13, on a donc $I_t(u,v) = 0$. □

Supposons que $x_0 \neq y_0$. Alors

$$\begin{aligned} f(x+x_0, y+y_0) &= h(x+x_0, y+y_0)(x+x_0-y-y_0) \\ &= (R + H_{m_t+1} + H_{m_t})(x+x_0-y-y_0) \\ &\quad \text{où } R \text{ est un polynôme de degré supérieur ou égal à } m_t+2 \\ &= (x_0-y_0)H_{m_t} + ((x-y)H_{m_t} + (x_0-y_0)H_{m_t+1}) \\ &\qquad + ((x-y+x_0-y_0)R + (x-y)H_{m_t+1}) \\ &= F_{m_t} + F_{m_t+1} + R' \\ &\quad \text{où } R' \text{ est un polynôme de degré supérieur ou égal à } m_t+2. \end{aligned}$$

On a donc $F_{m_t} = (x_0-y_0)H_{m_t}$ et $F_{m_t+1} = (x_0-y_0)H_{m_t+1} + (x-y)H_{m_t}$.

Lemme 4.4.15. *Si $t = (x_0, y_0)$ est un point singulier affine de h de multiplicité m_t tel que $x_0 \neq y_0$ alors*

$$F_{m_t} = (x_0-y_0)H_{m_t} \text{ et } F_{m_t+1} = (x-y)H_{m_t} + (x_0-y_0)H_{m_t+1}.$$

Corollaire 4.4.16. *Si $t = (x_0, y_0)$ est un point singulier affine de h tel que $x_0 \neq y_0$, x_0, $y_0 \in \mathbb{F}_{p^l}^*$ alors*

$$I_t(u,v) \leq \left(\frac{p^l+1}{2}\right)^2.$$

Démonstration. La multiplicité de t est $p^l + 1$. Par le lemme 4.4.15,

$$(x_0-y_0)H_{m_t} = F_{m_t} = c_1 x^{p^l+1} - c_2 y^{p^l+1}, \text{ avec } c_1,\, c_2 \neq 0.$$

On en déduit que H_{m_t} n'a que des facteurs simples, puis que $I_t(u,v) = m_t(u)m_t(v)$. Comme $m_t(u) + m_t(v) = p^l + 1$, on a le résultat. □

Corollaire 4.4.17. *Si $t = (x_0, y_0)$ est un point singulier affine de h tel que $x_0 \neq y_0$. Supposons de plus que soit $x_0 \in \mathbb{F}_{p^l}^*$ et $y_0 \notin \mathbb{F}_{p^l}^*$ soit $x_0 \notin \mathbb{F}_{p^l}^*$ et $y_0 \in \mathbb{F}_{p^l}^*$. Alors*

$$I_t(u,v) = 0.$$

Démonstration. La multiplicité de t est p^l. On a par le lemme 4.4.15

$$(x_0-y_0)H_{p^l} = F_{p^l} = \begin{cases} c_1 x^{p^l} & \text{si } y_0 \in \mathbb{F}_{p^l}^*,\ c_1 \neq 0 \\ c_2 y^{p^l} & \text{si } x_0 \in \mathbb{F}_{p^l}^*,\ c_2 \neq 0 \end{cases}$$

et

$$(x-y)H_{p^l} + (x_0-y_0)H_{p^l+1} = F_{p^l+1} = c_1' x^{p^l+1} - c_2' y^{p^l+1},\ c_1',\, c_2' \neq 0$$

donc $1 = \operatorname{pgcd}(F_{p^l}, F_{p^l+1}) = \operatorname{pgcd}(H_{p^l}, H_{p^l+1})$. Par la proposition 4.1.13, $I_t(u,v) = 0$. □

Supposons que $x_0 \neq y_0$ et que x_0 et $y_0 \notin \mathbb{F}_{p^l}$. Alors t est de multiplicité p^l et

$$F_{p^l} = c_1 x^{p^l} - c_2 y^{p^l} = (c_3 x - c_4 y)^{p^l}$$

où $c_1 = (x_0+1)^{d-p^l} - x_0^{p^l} \neq 0$, $c_2 = (y_0+1)^{d-p^l} - y_0^{d-p^l} \neq 0$ car x_0, $y_0 \notin \mathbb{F}_{p^l}^*$.
Par le lemme 4.4.15, on a $F_{p^l} = (x_0 - y_0)H_{p^l}$ et $F_{p^l+1} = (x_0-y_0)H_{p^l+1} + (x-y)H_{p^l}$ donc H_{p^l} n'a qu'un facteur et $\mathrm{pgcd}(F_{p^l}, F_{p^l+1}) = \mathrm{pgcd}(H_{p^l}, H_{p^l+1})$. On a $F_{p^l+1} = d_1 x^{p^l+1} - d_2 y^{p^l+1}$ avec $d_1 = (x_0+1)^{d-p^l-1} - x_0^{d-p^l-1} \neq 0$ et $d_2 = (y_0+1)^{d-p^l-1} - y_0^{d-p^l-1} \neq 0$. Les polynômes F_{p^l} et F_{p^l+1} ont donc un facteur commun si et seulement si $c_3 x - c_4 y$ divise F_{p^l+1}, c'est-à-dire si et seulement si

$$\left(\frac{c_1}{c_2}\right)^{p^l+1} = \left(\frac{d_1}{d_2}\right)^{p^l}.$$

Si (x_0, y_0) est un point singulier, on a

$$\begin{cases} x_0^{d-1} = y_0^{d-1} \\ (x_0+1)^{d-1} = x_0^{d-1} \\ (y_0+1)^{d-1} = y_0^{d-1} \end{cases}.$$

Alors

$$\begin{aligned} d_1 = (x_0+1)^{d-p^l-1} - x_0^{d-p^l-1} &= \frac{(x_0+1)^{d-1} - x_0^{d-p^l-1}(x_0+1)^{p^l}}{(x_0+1)^{p^l}} \\ &= \frac{x_0^{d-1} - x_0^{d-1} - x_0^{d-p^l-1}}{(x_0+1)^{p^l}} \\ &= \frac{-x_0^{d-p^l-1}}{(x_0+1)^{p^l}}. \end{aligned}$$

De même, $d_2 = \frac{-y_0^{d-p^l-1}}{(y_0+1)^{p^l}}$.
D'où $\frac{d_1}{d_2} = \frac{x_0^{d-p^l-1}(y_0+1)^{p^l}}{y_0^{d-p^l-1}(x_0+1)^{p^l}} = \frac{x_0^{d-1} y_0^{p^l}(y_0+1)^{p^l}}{y_0^{d-1} x_0^{p^l}(x_0+1)^{p^l}} = \frac{y_0^{p^l}(y_0+1)^{p^l}}{x_0^{p^l}(x_0+1)^{p^l}}$.

D'autre part,

$$\begin{aligned} c_1 = (x_0+1)^{d-p^l} - x_0^{d-p^l} &= \frac{(x_0+1)(x_0+1)^{d-1} - x_0^{d-p^l}(x_0+1)^{p^l}}{(x_0+1)^{p^l}} \\ &= \frac{x_0^d + x_0^{d-1} - x_0^d - x_0^{d-p^l}}{(x_0+1)^{p^l}} \\ &= \frac{x_0^{d-p^l}(x_0^{p^l-1} - 1)}{(x_0+1)^{p^l}}. \end{aligned}$$

De même, $c_2 = \frac{y_0^{d-p^l}(y_0^{p^l-1}-1)}{(y_0+1)^{p^l}}$.
D'où $\frac{c_1}{c_2} = \frac{x_0^{d-p^l}(x_0^{p^l-1}-1)(y_0+1)^{p^l}}{y_0^{d-p^l}(y_0^{p^l-1}-1)(x_0+1)^{p^l}} = \frac{y_0^{p^l}(y_0+1)^{p^l}(x_0^{p^l-1}-1)}{x_0^{p^l}(x_0+1)^{p^l}(y_0^{p^l-1}-1)}$.

Après simplification, on obtient que F_{p^l} et F_{p^l+1} ont un facteur commun si et seulement si

$$y_0(x_0+1)^{p^l}(y_0^{p^l-1} - 1)^{p^l+1} = x_0(y_0+1)^{p^l}(x_0^{p^l-1} - 1)^{p^l+1} \tag{4.4}$$

Si (x_0, y_0) n'est pas solution de (4.4), alors $\mathrm{pgcd}(H_{p^l}, H_{p^l+1}) = 1$ et par la proposition 4.1.13, $I_t(u, v) = 0$.

Sinon, on écrit $u(x+x_0, y+y_0) = U_r + U_{r+1} + \dots$ et $v(x+x_0, y+y_0) = V_s + V_{s+1} + \dots$ avec $U_r \neq 0$ et $V_s \neq 0$. Si $r = 0$ ou $s = 0$, alors u ou v ne contient pas t et $I_t(u, v) = 0$. Supposons $r, s > 0$. Comme (x_0, y_0) vérifie (4.4), F_{p^l} et F_{p^l+1}ont un facteur commun que l'on notera j. On a $H_{p^l} = U_r V_s = j^{p^l}$ et $H_{p^l+1} = U_r V_{s+1} + U_{r+1} V_s$. On a de plus $\mathrm{pgcd}(F_{p^l}, F_{p^l+1}) = j$ et donc $\mathrm{pgcd}(H_{p^l}, H_{p^l+1}) = j$. Comme $r \geq 1$ et $s \geq 1$, j divise U_r et V_s et donc $\mathrm{pgcd}(U_r, V_s)$. Si $\mathrm{pgcd}(U_r, V_s) = j^k$, j^k divise $\mathrm{pgcd}(H_{p^l}, H_{p^l+1})$ donc $\mathrm{pgcd}(U_r, V_s) = j$.
On peut supposer, sans perte de généralité, que $U_r = j^{p^l-1}$ et $V_s = j$; t est un point simple de v donc par la proposition 4.1.12, $I_t(u, v) = \mathrm{ord}_t^v(u)$; j^2 ne divisant pas H_{p^l+1}, j ne divise pas U_{p^l}, on peut donc écrire U_{p^l} comme produit de p^l facteurs linéaires différents de j. Chaque facteur linéaire n'est pas tangent à v donc l'ordre de chaque facteur est 1 et l'ordre de U_{p^l} est p^l. On a donc $\mathrm{ord}_t^v(u) \leq p^l$.

Lemme 4.4.18. *Si $t = (x_0, y_0)$ est un point singulier affine de h tel que $x_0 \neq y_0$ et x_0 et $y_0 \notin \mathbb{F}_{p^l}^*$ alors*

- *si $y_0(x_0+1)^{p^l}(y_0^{p^l-1} - 1)^{p^l+1} \neq x_0(y_0+1)^{p^l}(x_0^{p^l-1} - 1)^{p^l+1}$, $I_t(u, v) = 0$*
- *sinon, $I_t(u, v) \leq p^l$ et il y a au plus $((p^l-2)(p^l+1)-1)(\frac{d-1}{p^l}-1)$ tels points singuliers.*

4.4.3 Preuve du théorème 4.4.1

Les théorèmes suivants permettent de démontrer le théorème 4.4.1. On suppose jusqu'à la fin que $d \neq 1 + p^l$.

Théorème 4.4.19. *Si $n = 1$, h a un facteur absolument irréductible sur $\mathbb{F}_p$.*

Démonstration. Supposons que h n'ait pas de facteur absolument irréductible. Alors, par le lemme 4.1.15, on doit avoir $\alpha = \frac{I_{tot}}{\frac{(d-2)^2}{4}} \geq \frac{8}{9}$ où I_{tot} est un majorant de la multiplicité d'intersection globale.
Comme $n = 1$, il n'existe que des singularités de type Ib, IIc, IIIa et IIIc (*cf.* tableau 4.2). On a donc

$$\sum_t I_t(u, v) \leq p^l \left(\frac{d-1}{p^l} - 1\right)\left(2\frac{d-1}{p^l} - (d_b+1)p^{i_b-l} - 1\right) + \left(\frac{p^l-1}{2}\right)^2. \tag{4.5}$$

Or, $d = 1 + p^l k$ et $d \neq 1 + p^l$ donc $k \geq 2$, alors $\frac{d-3}{4} = \frac{p^l k - 2}{4} \geq \frac{p^l-1}{2}$ d'où

$$\begin{aligned}\alpha &\leq \frac{1}{\frac{(d-2)^2}{4}}\left(\frac{(d-3)^2}{16} + p^l\left(\frac{d-1}{p^l} - 1\right)^2\right)\\ &\leq \frac{1}{4} + \frac{4}{p^l}\end{aligned}$$

donc pour $p^l \neq 3$ ou 5, on a $\alpha < \frac{8}{9}$ ce qui est absurde.

Regardons d'abord le cas où $p^l = 3$. Comme $1 = n = \mathrm{pgcd}(2, k)$, k est impair et non

divisible par 3 par définition de l. D'où $k \geq 5$ et on a alors

$$\begin{aligned}\alpha &\leq \frac{p^l((p^l-2)(p^l+1)-1)(\frac{d-1}{p^l}-1)+\left(\frac{p^l-1}{2}\right)^2}{\frac{(d-2)^2}{4}} = \frac{9(k-1)+1}{\frac{(3k-1)^2}{4}} \\ &\leq \frac{4}{k-\frac{1}{3}} + \frac{4}{(3k-1)^2} \\ &\leq \frac{12}{14} + \frac{1}{49} < \frac{8}{9}\end{aligned}$$

ce qui est absurde.

Si $p^l = 5$, $1 = n = \mathrm{pgcd}(4, k)$ et k est impair, d'où $k = 3$ ou $k \geq 7$. Comme pour le cas $p^l = 3$, on a

$$\alpha \leq \frac{68}{5}\frac{k-1}{(k-\frac{1}{5})^2} + \frac{16}{(5k-1)^2}.$$

Or, $\frac{68}{5}\frac{k-1}{(k-\frac{1}{5})^2} + \frac{16}{(5k-1)^2}$ est une fonction décroissante de k, donc pour $k \geq 17$, on a $\alpha < \frac{8}{9}$ ce qui est absurde. Il reste à traiter les cas où $k = 3, 7, 9, 11, 13$. En reprenant l'équation (4.5), on a

k	3	7	9	11	13
d	16	36	46	56	66
I_{tot}	24	124	324	354	664
α	$\frac{24}{7^2}$	$\frac{124}{17^2}$	$\frac{324}{22^2}$	$\frac{354}{27^2}$	$\frac{664}{32^2}$

Dans tous les cas, on a $\alpha < \frac{8}{9}$ ce qui est absurde. □

Théorème 4.4.20. *Si $1 < n < \frac{d-1}{p^l}$, h a un facteur absolument irréductible sur $\mathbb{F}_p$.*

Démonstration. Supposons que h n'ait pas de facteur absolument irréductible. Alors, par le lemme 4.1.15, on doit avoir $\alpha = \frac{I_{tot}}{\frac{(d-2)^2}{4}} \geq \frac{8}{9}$, où I_{tot} est un majorant de la multiplicité d'intersection globale. On a alors

$$\begin{aligned}\sum_t I(u,v) &\leq \frac{p^{2l}-1}{4}(n-1) + \left(\frac{p^l-1}{2}\right)^2 \\ &\quad + p^l\left((\frac{d-1}{p^l}-1)(2\frac{d-1}{p^l}-(d_b+1)p^{i_b-l}-1)-(n-1)(n-2)\right) \\ &\qquad + \left(\frac{p^l+1}{2}\right)^2(n-1)(n-2) + (n-1)\frac{p^{2l}-1}{4} \\ &\leq \frac{p^{2l}-1}{2}(n-1) + \left(\frac{p^l-1}{2}\right)^2(n-1)(n-2) \\ &\qquad + p^l\left(\frac{d-1}{p^l}-1\right)^2 + \left(\frac{p^l-1}{2}\right)^2.\end{aligned}$$

Or, $d = 1 + kp^l$ avec $k \neq 1$ car $d \neq 1 + p^l$ et $k \not\equiv 0 \mod p$ par définition de l. De plus, n

divise $k = \frac{d-1}{p^l}$ et $n < k$ donc $n \leq \frac{d-1}{2p^l}$ d'où

$$\begin{aligned}
\alpha &\leq \frac{2(p^{2l}-1)(\frac{k}{2}-1)+(p^l-1)^2(\frac{k}{2}-1)(\frac{k}{2}-2)+4p^l(k-1)^2+(p^l-1)^2}{(p^lk-1)^2} \\
&\leq \frac{1}{\left(k-\frac{1}{p^l}\right)^2}\Big((1-\frac{1}{p^{2l}})(k-2)+\frac{1}{4}(1-\frac{1}{p^l})^2(k-2)(k-4) \\
&\qquad\qquad + \frac{4}{p^l}(k-1)^2+(1-\frac{1}{p^l})^2\Big) \\
\alpha &\leq \frac{1}{k-\frac{1}{p^l}}+\frac{1}{4}+\frac{4}{p^l}+\frac{1}{\left(k-\frac{1}{p^l}\right)^2}.
\end{aligned}$$

Comme on doit avoir $\alpha \geq \frac{8}{9}$, $1 < n < k$ et $\mathrm{pgcd}(k,p) = 1$, les seules possibilités restantes sont :

k	4	6	8	9	10	12	14	15	≥ 16
p^l	$3, 7, 11$	5	$3, 5, 7$	7	$3, 7$	$5, 7$	$3, 5$	7	$3, 5$

.

On a d'une part

$$\begin{aligned}
\alpha \leq \frac{2(p^{2l}-1)(n-1)+(p^l+1)^2(n-1)(n-2)}{(p^lk-1)^2} \\
+\frac{4p^l(k-1)\left((p^l-2)(p^l+1)-1\right)+(p^l-1)^2}{(p^lk-1)^2}
\end{aligned} \tag{4.6}$$

et d'autre part

$$\begin{aligned}
\alpha \leq \frac{2(p^{2l}-1)(n-1)+(p^l-1)^2(n-1)(n-2)}{(p^lk-1)^2} \\
+\frac{4p^l(k-1)(2k-(d_b+1)p^{i_b-l}-1)+(p^l-1)^2}{(p^lk-1)^2}.
\end{aligned} \tag{4.7}$$

Considérons d'abord le cas $k \geq 16$. Dans l'inéquation (4.6), α est majoré par une fonction décroissante de k. On ne va donc considérer que le cas $k = 16$. Si $p^l = 3$ ou $p^l = 5$, on obtient alors $\alpha < \frac{8}{9}$, ce qui mène à une contradiction.
Ensuite, en utilisant soit l'inégalité (4.6), soit l'inégalité (4.7), on a dans tous les autres cas du tableau $\alpha < \frac{8}{9}$, ce qui est absurde. □

Théorème 4.4.21. *Si $n = \frac{d-1}{p^l} \neq p^l - 1$, alors h a un facteur absolument irréductible sur $\mathbb{F}_p$.*

Démonstration. On remarque d'abord que, comme $n = \frac{d-1}{p^l}$, il n'existe que des singularités de type Ia, IIa, IIa, IIIb (*cf.* tableau 4.2). Dans tous les cas, h n'a que des tangentes simples et donc quelque soit la factorisation $h = uv$, on a $I_t(u,v) = m_t(u)m_t(v)$. Comme $\frac{d-1}{p^l} \neq p^l - 1$, $\frac{d-1}{p^l} \leq \frac{p^l-1}{2}$.
Supposons maintenant que h n'ait pas de facteur absolument irréductible sur $\mathbb{F}_p$. On écrit alors $h = h_1 \dots h_r$ où chaque h_i se décompose en $c_i \geq 2$ facteurs de degré $\frac{\deg(h_i)}{c_i}$ sur une

clôture algébrique de $\mathbb{F}_p$ (lemme 4.1.3). On écrit $h_i = h_{i,1} \dots h_{i,c_i}$.

$$\begin{aligned} A &= \sum_{k=1}^{r} \sum_{1 \le i < j \le c_k} \sum_t I_t(h_{k,i}, h_{k,j}) + \sum_{1 \le k < l \le r} \sum_{\substack{1 \le i \le c_k \\ 1 \le j \le c_l}} \sum_t I_t(h_{k,i}, h_{l,j}) \\ &= \sum_{k=1}^{r} \sum_{1 \le i < j \le c_k} \sum_t m_t(h_{k,i}) m_t(h_{k,j}) + \sum_{1 \le k < l \le r} \sum_{\substack{1 \le i \le c_k \\ 1 \le j \le c_l}} \sum_t m_t(h_{k,i}) m_t(h_{l,j}). \end{aligned}$$

Or,

$$\begin{aligned} (m_t(h))^2 &= \left(\sum_{k=1}^{r} m_t(h_k) \right)^2 \\ &= \sum_{k=1}^{r} m_t(h_k)^2 + 2 \sum_{1 \le k < l \le r} m_t(h_k) m_t(h_l) \\ &= \sum_{k=1}^{r} m_t(h_k)^2 + 2 \sum_{1 \le k < l \le r} \sum_{\substack{1 \le i \le c_k \\ 1 \le j \le c_l}} m_t(h_{k,i}) m_t(h_{l,j}) \end{aligned}$$

d'où, en utilisant le lemme 4.1.16,

$$A \le \sum_t \left(\sum_{k=1}^{r} m_t(h_k)^2 \frac{c_k - 1}{2c_k} + \frac{1}{2} (m_t(h)^2 - \sum_{k=1}^{r} m_t(h_k)^2) \right)$$

et donc

$$A \le \frac{1}{2} \sum_t \left(m_t(h)^2 - \sum_{k=1}^{r} \frac{m_t(h_k)^2}{c_k} \right)$$

D'autre part, par le théorème de Bézout, on a aussi

$$\begin{aligned} A &= \sum_{k=1}^{r} \sum_{1 \le i < j \le c_k} \deg(h_{k,i}) \deg(h_{k,j}) + \sum_{1 \le k < l \le r} \sum_{\substack{1 \le i \le c_k \\ 1 \le j \le c_l}} \deg(h_{k,i}) \deg(h_{l,j}) \\ &= \sum_{k=1}^{r} \frac{\deg(h_k)^2}{c_k^2} \frac{c_k(c_k - 1)}{2} + \sum_{1 \le k < l \le r} \deg(h_k) \deg(h_l) \\ &= \sum_{k=1}^{r} \deg(h_k)^2 \frac{c_k - 1}{2c_k} + \frac{1}{2} \left(\deg(h)^2 - \sum_{k=1}^{r} \deg(h_k)^2 \right) \\ &= \frac{1}{2} \left(\deg(h)^2 - \sum_{k=1}^{r} \frac{\deg(h_k)^2}{c_k} \right). \end{aligned}$$

On en déduit que

$$\deg(h)^2 - \sum_{k=1}^{r} \frac{\deg(h_k)^2}{c_k} \le \sum_t \left(m_t(h)^2 - \sum_{k=1}^{r} \frac{m_t(h_k)^2}{c_k} \right).$$

Puis en utilisant le lemme 4.1.16,

$$\deg(h)^2 - \sum_t m_t(h)^2 \le \sum_{k=1}^{r} \frac{1}{c_k} \left(\deg(h_k)^2 - \sum_t m_t(h_k)^2 \right) \le 0.$$

Si on note $k = \frac{d-1}{p^l}$, en remplaçant $\deg(h)$ et $m_t(h)$ par leur valeur dans

$$\deg(h)^2 \leq \sum_t m_t(h)^2,$$

on obtient

$$(d-2)^2 \leq 2(k-1)p^{2l} + (k-1)(k-2)(1+p^l)^2 + (p^l-1)^2$$

autrement dit

$$(2p^l+1)k^2 + (p^{2l}+4p^l+3)k - (p^{2l}+2p^l+2) \leq 0.$$

Comme c'est une équation du second degré en k, on a $k \leq 1$ ou $k \geq \frac{p^{2l}+2p^l+2}{2p^l+1}$. Or, par hypothèse, on a $k \geq 2$ ($d \neq 1+p^l$) et $k \leq \frac{p^l-1}{2} < \frac{p^{2l}+2p^l+2}{2p^l+1}$, ce qui est absurde. □

4.5 Les nombres exceptionnels non congrus à 1 modulo p en caractéristique impaire

Dans cette partie on suppose $d \not\equiv 0 \mod p$ et $d \not\equiv 1 \mod p$.

L'étude des singularités dans ce cas donne le résultat suivant :

Lemme 4.5.1. *Le polynôme h n'a pas de singularité à l'infini. Les singularités affines de h sont les solutions de $(x_0+1)^{d-1} = (y_0+1)^{d-1} = x_0^{d-1} = y_0^{d-1}$ telles que $x_0 \neq y_0$. Elles sont toutes de multiplicité 2.*

La méthode de démonstration de ce lemme est la même que pour les lemmes 4.4.4, 4.4.5 et 4.4.7. En utilisant le même raisonnement que pour le théorème 4.4.21, on obtient que si h n'a pas de facteur absolument irréductible alors

$$(d-2)^2 \leq 4N \text{ où } N \text{ est le nombre de points singuliers de } h.$$

On ne sait pas trouver une bonne majoration de N pour éliminer certains d. Cependant on peut montrer le résultat suivant :

Proposition 4.5.2. *Si* $\operatorname{pgcd}(d-1, p-1) > 1$, *alors h a un facteur absolument irréductible.*

Démonstration. On écrit $h = ag_1 \dots g_r$ où les g_i sont unitaires en x et absolument irréductibles sur une extension E de $\mathbb{F}_p$. Soit h_i le terme homogène de plus haut degré de g_i. On a alors

$$\frac{x^{d-1}-y^{d-1}}{x-y} = h_1 \dots h_r.$$

D'autre part, comme $d \not\equiv 1 \mod p$,

$$\frac{x^{d-1}-y^{d-1}}{x-y} = \prod_\zeta (x-\zeta y)$$

où le produit porte sur les racines $(d-1)$ème de l'unité différentes de 1. Chaque $(x-\zeta y)$ divise un seul des h_i.

On considère maintenant l'application

$$\sigma : \begin{array}{ccc} E[x,y] & \to & E[x,y] \\ \sum_{i,j} a_{i,j} x^i y^j & \mapsto & \sum_{i,j} a_{i,j}^p x^i y^j \end{array}.$$

Alors $h = \sigma(h) = a\sigma(g_1)\dots\sigma(g_r)$. Par unicité de la factorisation, pour tout $1 \leq i \leq r$, il existe un j tel que $\sigma(g_i) = g_j$ et donc $\sigma(h_i) = h_j$. Or, comme $\mathrm{pgcd}(d-1, p-1) > 1$, il existe ζ_0 racine de l'unité différente de 1 telle que $\zeta_0 \in \mathbb{F}_p$ et donc $\sigma(x - \zeta_0 y) = x - \zeta_0 y$. Supposons par exemple que $x - \zeta_0 y$ divise h_1. Alors, $\sigma(h_1) = h_1$ puisque $x - \zeta_0 y$ divise un seul des h_i. Par conséquent, $\sigma(g_1) = g_1$ ce qui signifie que $g_1 \in \mathbb{F}_p[x, y]$ et donc h a un facteur absolument irréductible sur $\mathbb{F}_p$. $\square$

A l'aide de Magma, pour $p = 3$, 5 ou 7, on peut montrer qu'il n'y a pas de d tel que $3 \leq d \leq 200$, $d \not\equiv 1 \mod p$, $d \not\equiv 0 \mod p$, $\mathrm{pgcd}(d-1, p-1) = 1$ et $4N \geq (d-2)^2$ en dehors de $d = 14$ et $d = 122$ pour $p = 3$. Or, $14 = \frac{3^3+1}{2}$ et $122 = \frac{3^5+1}{2}$ correspondent à des nombres exceptionnels connus (voir théorème 3.3.1).

Dans ce chapitre, nous démontrons que les seuls entiers d congrus à 1 modulo un nombre premier p qui donnent une fonction puissance $x \mapsto x^d$ parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_p$ sont ceux de la forme $d = 1 + p^l$. Les mêmes méthodes ne semblent pas s'appliquer pour les entiers non congrus à 1 modulo p. Dans ce cas, nous disposons seulement du résultat suivant : si $\mathrm{pgcd}(d-1, p-1) > 1$ alors $x \mapsto x^d$ n'est pas parfaitement non linéaire sur une infinité d'extensions de $\mathbb{F}_p$. D'autre part, dans le cas de la caractéristique paire, Aubry, McGuire et Rodier dans [AMR10] ont démontré que les fonctions polynomiales de degré impair qui ne sont pas de degré 2^l+1 ou $2^{2l}-2^l+1$ ne sont pas presque parfaitement non linéaires sur une infinité d'extensions de $\mathbb{F}_2$. Ils ont aussi obtenu des résultats sur les fonctions polynomiales de degré pair. On peut se demander si on peut étendre ces résultats à la caractéristique impaire et aux fonctions polynomiales parfaitement non linéaires.

Annexe A

Encodage et décodage des codes de Reed-Muller généralisés

Dans cette partie, on appellera produit scalaire de deux éléments a, b de $\mathbb{F}_q^n$, $n \in \mathbb{N}$ la quantité suivante $a.b := \sum_{i=1}^{n} a_i b_i \in \mathbb{F}_q$.

A.1 Encodage des codes de Reed-Muller généralisés

Soit $0 \leq r \leq m(q-1)$. On note $M_{q,r} = \{x_1^{k_1} \dots x_m^{k_m} : 0 \leq k_i \leq q-1, \sum_{i=1}^{m} k_i \leq r\}$ l'ensemble des monômes qui engendrent $R_q(r,m)$. La matrice

$$G_q(r,m) = (v(w))_{\substack{v \in M_{q,r} \\ w \in \mathbb{F}_q^m}}$$

est alors une matrice génératrice de $R_q(r,m)$. En effet, si $f = \sum_{v \in M_{q,r}} a_v v \in R_q(r,m)$, alors $(a_v)_{v \in M_{q,r}} G_q(r,m) = (f(w))_{w \in \mathbb{F}_q^m}$.

Exemple A.1.1. La matrice génératrice de $R_3(2,3)$ est

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}
\begin{matrix}
1 \\ x_1 \\ x_2 \\ x_3 \\ x_1^2 \\ x_1x_2 \\ x_1x_3 \\ x_2^2 \\ x_2x_3 \\ x_3^2
\end{matrix}$$

A.2 Décodage des codes de Reed-Muller

Dans cette section, on rappelle des méthodes de décodage pour les codes de Reed-Muller usuels : d'abord une méthode basée sur la transformée de Fourier rapide pour les code de Reed-Muller d'ordre 1 ; puis une méthode par vote majoritaire que l'on étendra par la suite aux codes de Reed-Muller généralisés. Une référence pour cette section est [MS77b].

A.2.1 Utilisation de la transformée de Hadamard pour les codes de Reed-Muller d'ordre 1

Supposons qu'on envoie un mot $\alpha_0 \in R(1,m)$ et qu'on reçoive $f \in B_m^q$. On a vu au chapitre 2 que pour tout $\alpha \in R(1,m)$,

$$d(f,\alpha) = 2^{m-1} - \frac{1}{2}(-1)^b \widehat{f}(a).$$

Cette distance est donc minimale lorsque $|\widehat{f}(a)|$ est maximal. La méthode de décodage est donc la suivante :

- Trouver a_0 tel que $|\widehat{f}(a_0)|$ soit maximal.
- Si $\widehat{f}(a_0) \geq 0$, on décode f en $< a_0, x >$. Sinon, on décode f en $< a_0, x > +1$.

En utilisant la transformée de Fourier rapide pour calculer les transformées de Fourier, on obtient un algorithme de complexité $O(m2^m)$.

Cet algorithme a été étendu dans [AL96] par Ashikhmin et Litsyn aux codes de Reed-Muller généralisés d'ordre 1. Leur algorithme a une complexité en $O(mq^m)$.

A.2.2 Décodage par vote majoritaire

On commence par expliquer le principe sur un exemple très simple :
si $C = \{(0,\dots,0),(1,\dots,1)\}$ est un code à deux éléments de longueur n et d'alphabet $\mathbb{F}_2$ et s'il y a strictement moins de $\frac{n}{2}$ erreurs, le mot envoyé est $(0,\dots,0)$ si il y a une majorité de 0 dans le mot reçu. Sinon, le mot envoyé est $(1,\dots,1)$. Le décodage par vote majoritaire est une extension de ce principe.

Soit $(m_v)_{v\in M_{2,r}}$ le mot à coder, $M_c = \sum_{v\in M_{2,r}} m_v v$ le mot codé et M_r le mot reçu. On note $\overline{x_i}$ le polynôme $x_i + 1$.

Définition A.2.1. On appelle vecteur caractéristique d'un monôme $x_{i_1}\dots x_{i_d} \in M_{2,r}$ tout polynôme de la forme

$$x_{j_1}\dots x_{j_a}\overline{x_{k_1}}\dots\overline{x_{k_b}}$$

où $a+b = m-d$ et $\{j_1,\dots,j_a,k_1,\dots,k_b\} = \{1,\dots,m\}\setminus\{i_1,\dots,i_d\}$.

Pour un monôme v de degré r, il y a 2^{m-r} vecteurs caractéristiques. On les note v_i, $1 \leq i \leq 2^{m-r}$. Soit alors U_i le support de v_i.

Théorème A.2.2. *S'il n'y a pas d'erreur, on a*

$$\forall i \in \{1,\dots,2^{m-r}\}, m_v = \sum_{P\in U_i} M_{r,P}.$$

On peut corriger au moins $2^{m-r-1}-1$ erreurs avec cette méthode.

Démonstration. S'il n'y a pas d'erreurs $M_r = \sum_{v\in M_{2,r}} m_v v$ et $\sum_{P\in U_i} M_{r,P} = M_r.v_i$ alors par la proposition 1.2.3, $\sum_{P\in U_i} M_{r,P} = m_v$.
De plus, les U_i étant disjoints, chaque $M_{r,P}$ apparait dans au plus une des 2^{m-r} équations obtenues. S'il y a strictement moins de 2^{m-r-1} erreurs, moins de la moitié des équations sont affectées par ses erreurs et donc la valeur majoritaire est bien celle voulue. □

Pour déterminer chaque coefficient, on doit faire $O(2^m)$ additions et déterminer la valeur majoritaire parmi 2^{m-r} valeurs (complexité en $O(2^{m-r})$) donc la complexité de cet algorithme est $O(k_r 2^m)$ où k_r est la dimension de $R(r,m)$.

Remarque A.2.3. Pour $r = 1$, $k_1 = m+1$ et on retrouve la même complexité que l'algorithme précédent.

Dans [Gru90], Grushko étend ce résultat pour les codes de Reed-Muller généralisés d'ordre 1 valable uniquement sur les corps finis de cardinal premier et qui n'assure pas un décodage jusqu'à $\frac{(q-1)q^{m-1}}{2}$ erreurs. La complexité de cet algorithme est $O(mp^m)$. Dans la suite nous proposons un décodage des codes de Reed-Muller généralisés pour tout degré et tout corps. Cependant nous ne pouvons assurer non plus un décodage jusqu'à $\frac{d_{min}}{2}$ erreurs.

A.3 Décodage des codes de Reed-Muller généralisés

Définition A.3.1. Soit $v = x_1^{k_1} \dots x_m^{k_m} \in M_{q,r}$. On appelle vecteur caractéristique de v tout polynôme de la forme

$$v_b(x) = \prod_{i=1}^{m} \prod_{j=1}^{q-1-k_i} (x_i - b_{i,j}), \text{ avec } b_{i,j} \in \mathbb{F}_q \text{ et } \forall i,\ b_{i,j} \neq b_{i,k} \text{ si } i \neq k.$$

Exemple A.3.2. Les vecteurs caractéristiques de $x_1x_2 \in R_3(2,3)$ sont :

$$\begin{aligned}
&x_1x_2x_3(x_3-1), x_1x_2x_3(x_3-2), x_1x_2(x_3-1)(x_3-2), x_1(x_2-1)x_3(x_3-1),\\
&x_1(x_2-1)x_3(x_3-2), x_1(x_2-1)(x_3-1)(x_3-2), x_1(x_2-2)x_3(x_3-1),\\
&x_1(x_2-2)x_3(x_3-2), x_1(x_2-2)(x_3-1)(x_3-2), (x_1-1)x_2x_3(x_3-1),\\
&(x_1-1)x_2x_3(x_3-2), (x_1-1)x_2(x_3-1)(x_3-2), (x_1-1)(x_2-1)x_3(x_3-1),\\
&(x_1-1)(x_2-1)x_3(x_3-2), (x_1-1)(x_2-1)(x_3-1)(x_3-2), (x_1-1)(x_2-2)x_3(x_3-1),\\
&(x_1-1)(x_2-2)x_3(x_3-2), (x_1-1)(x_2-2)(x_3-1)(x_3-2), (x_1-2)x_2x_3(x_3-1),\\
&(x_1-2)x_2x_3(x_3-2), (x_1-2)x_2(x_3-1)(x_3-2), (x_1-2)(x_2-1)x_3(x_3-1),\\
&(x_1-2)(x_2-1)x_3(x_3-2), (x_1-2)(x_2-1)(x_3-1)(x_3-2), (x_1-2)(x_2-2)x_3(x_3-1),\\
&(x_1-2)(x_2-2)x_3(x_3-2), (x_1-2)(x_2-2)(x_3-1)(x_3-2)
\end{aligned}$$

On commence par remarquer que pour tout $v' \in M_{q,r} \setminus \{v\}$ tel que $\deg(v') \leq \deg(v)$, tous les vecteurs caractéristiques de v sont orthogonaux à v' au sens où pour tout b, puisque le représentant de plus petit degré de $v'v_b$ dans $\mathbb{F}_q[x_1,\dots,x_m]/(x_1^q - x_1, \dots, x_m^q - x_m)$ est de degré strictement plus petit que $m(q-1)$, $\sum_{x \in \mathbb{F}_q^m} v'(x)v_b(x) = 0$.

A.3.1 Correction d'effacements

Soit $(m_v)_{v \in M_{q,r}}$ le mot à coder et $M_c = \sum_{v \in M_{q,r}} m_v v$ le mot codé. Supposons qu'il y ait eu des effacements aux coordonnées $F = \{\alpha_1, \dots, \alpha_u\} \subset \mathbb{F}_q^m$. On note M_r le mot reçu.
Pour chaque monôme v de $M_{q,r}$ différent de 1 et en partant du plus haut degré, on procède comme suit :

1. Trouver un vecteur caractéristique v_b associé à v tel que pour tout $\alpha \in F$, $v_b(\alpha) = 0$. On calcule le produit scalaire de M_r avec ce vecteur caractéristique (vu comme un vecteur de $\mathbb{F}_q^{q^m}$ en l'évaluant en chacun des éléments de $\mathbb{F}_q^m$), on note β la valeur obtenue et on prend $m_v = (-1)^m \beta$.

2. On fait $M_r \leftarrow M_r - m_v v$.

Une fois ce processus appliqué à tous les monômes différents de 1, il reste à déterminer m_1. On prend la valeur qui apparait dans tous les coefficients non effacés du dernier M_r obtenu.

Théorème A.3.3. *Soit* $0 \leq r \leq m(q-1)-1$ *et*

$$N = \max(\prod_{i=1}^{m}(k_i+1) : 0 \leq k_i \leq q-1, \sum_{i=1}^{m} k_i = r).$$

L'algorithme précédent permet de retrouver jusqu'à $\lceil \frac{q^m}{N} - 1 \rceil$ *effacements sur le code de Reed-Muller généralisé* $R_q(r,m)$.

Démonstration. On commence par prouver que si pour chaque monôme, on peut trouver un vecteur caractéristique qui est nul sur F, alors on obtient bien le mot encodé. Soit v_0 un des monômes de plus grand degré à traiter et soit v_b un vecteur caractéristique associé à v_0 qui est nul sur F. Alors

$$v_b.M_r = v_b.\sum_{v \in M_{q,r}} m_v v = (-1)^m m_{v_0}.$$

En procédant par degré décroissant sur les monômes, on arrive à obtenir ainsi tous les coefficients sauf le terme constant. Le M_r final correspond justement au terme constant donc tous les coefficients non effacés ont la même valeur.
Il reste donc à prouver que si $u \leq \lceil \frac{q^m}{N} - 1 \rceil$, on peut trouver pour chaque monôme un vecteur caractéristique qui est nul sur F. Soit $v = x_1^{k_1} \dots x_m^{k_m}$ un monôme. Il a $\prod_{i=1}^{m} \binom{q}{k_i+1}$ vecteurs caractéristiques. Le nombre de vecteurs caractéristiques qui ne sont pas identiquement nuls sur F est plus petit que

$$u \prod_{i=1}^{m} \binom{q-1}{k_i} = u \frac{\prod_{i=1}^{m}(k_i+1)}{q^m} \prod_{i=1}^{m} \binom{q}{k_i+1}.$$

Comme $u < \frac{q^m}{N}$, $u \prod_{i=1}^{m} \binom{q-1}{k_i} < \prod_{i=1}^{m} \binom{q}{k_i+1}$ et donc il existe un vecteur caractéristique qui est nul sur F. □

Exemple A.3.4. Décodage de $R_3(1,3)$
Comme $N = 2$, par le théorème A.3.3, on peut retrouver jusqu'à 13 effacements. On veut coder le message suivant $(1,0,1,1)$ après encodage et transmission on obtient le mot suivant $M_r = (1,e,e,2,e,2,0,0,e,2,2,2,e,e,0,e,1,1,e,e,0,1,1,e,2,2,2)$ avec des effacements aux coordonnées suivantes

$$F = \left\{ \begin{array}{c} (1,0,0),(1,1,0),(2,0,0),(2,2,0),(2,1,2),(1,1,0),(1,1,1), \\ (1,0,2),(0,2,1),(0,0,2),(2,0,0),(2,2,0),(0,1,1) \end{array} \right\}.$$

On commence par traiter le cas du monôme x_3. Le vecteur caractéristique de x_3 $v_b = x_1(x_1-1)x_2(x_2-1)x_3$ est nul sur F. Le produit scalaire $v_b.M_r = 2$ donc, comme m est impair, $m_{x_3} = 1$. De la même façon $m_{x_2} = 1$ et $m_{x_1} = 0$. De plus, le dernier M_r obtenu étant $(1,e,e,1,2+e,1,1,1,1+e,1,1,1,1+e,1+e,1,e,1,1,1+e,1+e,1,1,1,e,1,1,1)$, $m_1 = 1$.

L'étude sur plusieurs exemples nous permet de faire la conjecture suivante :

Conjecture A.3.5. *Soit* $0 \leq r \leq m(q-1)-1$, $r = t(q-1)+s$ *avec* $0 \leq s \leq q-2$. *L'algorithme ci-dessus permet de corriger jusqu'à* $(q-s)q^{m-t-1}-1 = d-1$ *effacements sur le code de Reed-Muller généralisé* $R_q(r,m)$.

A.3.2 Correction d'erreurs par vote majoritaire

Soit $(m_v)_{v \in M_{q,r}}$ le mot à coder, $M_c = \sum_{v \in M_{q,r}} m_v v$ le mot codé et M_r le mot reçu.
Pour chaque monôme v de $M_{q,r}$ sauf 1 et en partant du plus grand degré, on procède comme suit :

1. Soit E_v l'ensemble des vecteurs caractéristiques associés au monôme v que l'on considère. On calcule le produit scalaire de chaque vecteur caractéristique (vu comme vecteur de $\mathbb{F}_q^{q^m}$) avec M_r, on note α la valeur majoritairement obtenue et on prend $m_v = (-1)^m \alpha$.
2. On fait $M_r \leftarrow M_r - m_v v$.

Une fois ce processus appliqué à chaque monôme sauf 1, il reste à déterminer le coefficient associé au monôme 1. On prend pour m_1 la valeur majoritaire dans les coefficients du dernier M_r obtenu.

Théorème A.3.6. *Soit* $0 \leq r \leq m(q-1)-1$,

$$N = \max(\prod_{i=1}^{m}(k_i+1) : 0 \leq k_i \leq q-1, \sum_{i=1}^{m} k_i = r).$$

L'algorithme précédent permet de corriger jusqu'à $\lceil \frac{1}{2}\frac{q^m}{N} - 1 \rceil$ *erreurs sur le code de Reed-Muller généralisé* $R_q(r,m)$.

Démonstration. On commence par vérifier que s'il n'y a pas d'erreur, on obtient bien par cet algorithme le mot qu'on a codé. Soit v_0 un des monômes de plus grand degré à traiter et soit v_b un vecteur caractéristique associé à v_0. Alors, comme pour tout $v' \neq v$ tel que $\deg(v') \leq \deg(v)$, v_b est orthogonal à v', on a

$$v_b . \sum m_v v = (-1)^m m_{v_0}.$$

En procédant par degré décroissant sur les monômes, on arrive à obtenir ainsi tous les coefficients sauf le terme constant. Le terme final est justement le terme constant.
Maintenant, on écrit $e = \sum_{x \in \mathbb{F}_q^m} e_x 1_x$ où au plus $\lceil \frac{1}{2}\frac{q^m}{N} - 1 \rceil$ coefficients e_x sont non nuls. Soit $v = x_1^{k_1} \dots x_m^{k_m}$ un monôme. En faisant les produits scalaires de M_r avec les polynômes caractéristiques de v on obtient les $\prod_{i=1}^{m} \binom{q}{k_i+1}$ équations suivantes

$$\sum_{x \in \mathbb{F}_q^m} M_r(x) v_b(x) = (-1)^m m_v + \sum_{x \in \mathbb{F}_q^m} e_x v_b(x). \tag{A.1}$$

Soit $\alpha \in \mathbb{F}_q^m$, $\#\{b : v_b(\alpha) \neq 0\} = \prod_{i=1}^{m} \binom{q-1}{k_i}$ donc e_α apparait dans au plus $\prod_{i=1}^{m} \binom{q-1}{k_i}$ équations (A.1). Il y a donc au plus $|e| \prod_{i=1}^{m} \binom{q-1}{k_i}$ équations (A.1) affectées par les erreurs.

Comme $|e| < \frac{1}{2}\frac{q^m}{N}$,

$$|e|\prod_{i=1}^{m}\binom{q-1}{k_i} < \frac{1}{2}\frac{q^m}{N}\prod_{i=1}^{m}\binom{q-1}{k_i} \leq \frac{1}{2}\frac{q^m}{\prod_{i=1}^{m}(k_i+1)}\prod_{i=1}^{m}\binom{q-1}{k_i} = \frac{1}{2}\prod_{i=1}^{m}\binom{q}{k_i+1}.$$

D'où il y a strictement moins de la moitié des équations affectées par les erreurs. □

Exemple A.3.7. Décodage de $R_3(1,3)$
Comme $N = 2$, par le théorème A.3.6, on peut corriger jusqu'à 6 erreurs. On veut coder le mot $(1,0,1,1)$. Après encodage et transmission, on obtient le message suivant

$$M_r = (0,0,1,0,2,2,1,1,2,2,2,2,0,0,0,1,1,1,0,0,0,1,1,1,2,2,2)$$

comportant au plus 6 erreurs.
On commence par traiter le cas du monôme x_3. Les vecteurs caractéristiques ainsi que leurs produits scalaires avec M_r sont donnés dans le tableau A.1.

TABLE A.1 – Calcul de m_{x_3}.

v_b	$M_r.v_b$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2)$	2
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0)$	2
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0)$	2
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0)$	2
$(0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0$	2
$(0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,0)$	2
$(0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,0,0)$	2
$(0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,0,0,0)$	2
$(0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0)$	2
$(0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0)$	1
$(0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1)$	0
$(0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0)$	0
$(0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0)$	1
$(0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0)$	0
$(0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0)$	1
$(0,0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0)$	2
$(0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0)$	2
$(0,0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0)$	2
$(0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0)$	2
$(0,0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$	0
$(0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0)$	1
$(0,0,1,0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$	2
$(0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0)$	2
$(0,1,0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$	1
$(0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0)$	0
$(1,0,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$	1
$(2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0)$	0

La valeur majoritaire est 2. Comme m est impair, on prend $m_{x_3} = 1$. En procédant de même pour x_2 puis x_1, on a $m_{x_2} = 1$, $m_{x_1} = 0$. De plus, le dernier M_r obtenu étant $(0,0,1,2,1,1,2,2,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1)$, on choisit $m_1 = 1$.
En décodant, on a donc trouvé comme message $(1,0,1,1)$ qui correspond bien à notre message initial.

L'étude sur plusieurs exemples nous permet de faire la conjecture suivante :

Conjecture A.3.8. *Soit $0 \leq r \leq m(q-1)-1$, $r = t(q-1)+s$ avec $0 \leq s \leq q-2$. L'algorithme ci-dessus permet de corriger jusqu'à $\lceil \frac{1}{2}(q-s)q^{m-t-1} - 1 \rceil = \lceil \frac{1}{2}d - 1 \rceil$ erreurs sur le code de Reed-Muller généralisé $R_q(r,m)$.*

A.4 Complexité

A.4.1 Correction d'effacements

Supposons qu'il y ait e effacements. Il faut alors au pire $e\prod_{i=1}^{m}\binom{q}{1+k_i}$ comparaisons pour trouver un vecteur caractéristique associé au monôme $x_1^{k_1}\dots x_m^{k_m}$ qui s'annule en chaque effacement. Puis, comme le support d'un tel vecteur caractéristique est de cardinal $\prod_{i=1}^{m}(1+k_i)$, il faut $\prod_{i=1}^{m}(1+k_i)$ multiplications et $\prod_{i=1}^{m}(1+k_i)-1$ additions pour calculer le produit scalaire. Finalement, on doit faire $e\sum_{\substack{(k_1,\dots,k_m)\in\{0,\dots,q-1\}^m \\ \sum_{i=1}^{m} k_i \leq r}}\prod_{i=1}^{m}\binom{q}{1+k_i}$ comparaisons, $\sum_{\substack{(k_1,\dots,k_m)\in\{0,\dots,q-1\}^m \\ \sum_{i=1}^{m} k_i \leq r}}\prod_{i=1}^{m}(1+k_i)$ multiplications et $\sum_{\substack{(k_1,\dots,k_m)\in\{0,\dots,q-1\}^m \\ \sum_{i=1}^{m} k_i \leq r}}(\prod_{i=1}^{m}(1+k_i)-1)$ additions pour corriger e effacements.
Pour se donner une meilleure idée, regardons le cas $r = 1$. Pour $r = 1$,

$$\sum_{\substack{(k_1,\dots,k_m)\in\{0,\dots,q-1\}^m \\ \sum_{i=1}^{m} k_i \leq r}}\prod_{i=1}^{m}\binom{q}{1+k_i} = q^m + mq^m\frac{q-1}{2}$$

donc la complexité de cet algorithme est en $O(emq^m)$.

A.4.2 Corrections d'erreurs par vote majoritaire

Définition A.4.1. Soit $x_1,\dots,x_n$ une suite finie d'éléments de $\mathbb{F}_q$. Un élément $\omega \in \mathbb{F}_q$ est dit majoritaire s'il apparait plus de $\frac{n}{2}+1$ fois dans la suite.

Proposition A.4.2. *Soit $x_1,\dots,x_n$ une suite finie d'éléments de $\mathbb{F}_q$. Supposons qu'elle ait une valeur majoritaire. Alors la complexité pour trouver cette valeur majoritaire est linéaire en la longueur de la liste.*

Démonstration. Soit $i < j$ tel que $x_i \neq x_j$. On considère alors la suite à $n-2$ éléments $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n$. Cette suite à la même valeur majoritaire que $x_1, \ldots, x_n$. En effet, si x_i et x_j n'était pas valeur majoritaire alors $\frac{n}{2} + 1 \geq \frac{n-2}{2} + 1$. Si x_i est valeur majoritaire de $x_1, \ldots, x_n$. Alors il y a plus de $\frac{n}{2} = \frac{n-2}{2} + 1$ éléments égaux à x_i dans la nouvelle suite.
On considère alors l'algorithme suivant :

Algorithme 4

$C := x_1$; $M := 1$;
$i := 2$;
tant que $i \leq n$ faire
  si $x_i = C$ alors $M := M + 1$; sinon $M := M - 1$;
    si $M = 0$ alors $C := x_{i+1}$; $i := i + 2$; $M := 1$; sinon $i := i + 1$; fin si ;
  fin si ;
fin tant que ;

La valeur C est alors la valeur majoritaire. On a bien n comparaisons pour obtenir une valeur majoritaire. □

Le support de chaque vecteur caractéristique associé au monôme $x_1^{k_1} \ldots x_m^{k_m}$ est de cardinal $\prod_{i=1}^{m}(1+k_i)$. Puisqu'il y a $\prod_{i=1}^{m} \binom{q}{1+k_i}$ vecteurs caractéristiques associés à ce monôme, il faut $q^m \prod_{i=1}^{m} \binom{q-1}{k_i}$ multiplications et $q^m \prod_{i=1}^{m} \binom{q-1}{k_i} - \prod_{i=1}^{m} \binom{q}{k_i+1}$ additions pour calculer les produits scalaires de M_r avec les vecteurs caractéristiques de $x_1^{k_1} \ldots x_m^{k_m}$. Comme déterminer la valeur majoritaire parmi les produits scalaires est linéaire en la longueur de la suite, la complexité de notre algorithme est en $O\left(q^m \sum_{\substack{(k_1,\ldots,k_m)\in\{0,\ldots,q-1\}^m \\ \sum_{i=1}^{m} k_i \leq r}} \prod_{i=1}^{m} \binom{q-1}{k_i}\right)$

Comparons la complexité pour $r = 1$ de cet algorithme aux algorithmes précédents. Si $r = 1$, $\sum_{\substack{(k_1,\ldots,k_m)\in\{0,\ldots,q-1\}^m \\ \sum_{i=1}^{m} k_i \leq r}} \prod_{i=1}^{m} \binom{q-1}{k_i} = 1 + m(q-1)$ donc la complexité de cet algorithme est $O(mq^m)$.

Bibliographie

[AL96] Alexey E. Ashikhmin et Simon N. Litsyn : Fast decoding of non-binary first order Reed-Muller codes. *Appl. Algebra Engrg. Comm. Comput.*, 7(4):299–308, 1996.

[AMR10] Yves Aubry, Gary McGuire et François Rodier : A few more functions that are not APN infinitely often. *In Finite fields : theory and applications*, volume 518 de *Contemp. Math.*, pages 23–31. Amer. Math. Soc., Providence, RI, 2010.

[BBMM08] Carl Bracken, Eimear Byrne, Nadya Markin et Gary McGuire : New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields Appl.*, 14(3):703–714, 2008.

[BBMM11] Carl Bracken, Eimear Byrne, Nadya Markin et Gary McGuire : A few more quadratic APN functions. *Cryptogr. Commun.*, 3(1):43–53, 2011.

[BC93] Thierry Berger et Pascale Charpin : The automorphism group of generalized Reed-Muller codes. *Discrete Math.*, 117(1-3):1–17, 1993.

[BC08] Lilya Budaghyan et Claude Carlet : Classes of quadratic APN trinomials and hexanomials and related structures. *IEEE Trans. Inform. Theory*, 54(5): 2354–2357, 2008.

[BCFL06] Lilya Budaghyan, Claude Carlet, Patrick Felke et Gregor Leander : An infinite class of quadratic apn functions which are not equivalent to power mappings. *In Proceedings of ISIT 2006, Seattle, USA*, 2006.

[BCL09] Lilya Budaghyan, Claude Carlet et Gregor Leander : Constructing new APN functions from known ones. *Finite Fields Appl.*, 15(2):150–159, 2009.

[BCP07] Lilya Budaghyan, Claude Carlet et Alexander Pott : Another class of quadratic apn binomials over f2n : the case n divisible by 4. *In Proceedings of WCC 07*, pages 49–58, 2007.

[Ber77] Marcel Berger : *Géométrie. Vol. 1.* CEDIC, Paris, 1977. Actions de groupes, espaces affines et projectifs. [Actions of groups, affine and projective spaces].

[BK10] Jurgen Bierbrauer et Gohar M. Kyureghyan : On the projection construction of planar and apn mappings. *In YACC*, 2010.

[BON84] P.G.A. BONNEAU : *CODES ET COMBINATOIRE.* Univ. Pierre et Marie Curie, 1984.

[Bos61] R. C. BOSE : On some connections between the design of experiments and information theory. *Bull. Inst. Internat. Statist.*, 38:257–271, 1961.

[Bou07] N. BOURBAKI : *Éléments de mathématique. Algèbre. Chapitre 9.* Springer-Verlag, Berlin, 2007. Reprint of the 1959 original.

[BW72] Elwyn R. BERLEKAMP et Lloyd R. WELCH : Weight distributions of the cosets of the (32, 6) Reed-Muller code. *IEEE Trans. Information Theory*, IT-18:203–207, 1972.

[CCZ98] Claude CARLET, Pascale CHARPIN et Victor ZINOVIEV : Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[CH10] Yves CRAMA et Peter L. HAMMER, éditeurs. *Boolean models and methods in mathematics, computer science, and engineering*, volume 134 de *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, Cambridge, 2010.

[CM97] Robert S. COULTER et Rex W. MATTHEWS : Planar functions and planes of Lenz-Barlotti class II. *Des. Codes Cryptogr.*, 10(2):167–184, 1997.

[DGM70] P. DELSARTE, J.-M. GOETHALS et F. J. MACWILLIAMS : On generalized Reed-Muller codes and their relatives. *Information and Control*, 16:403–442, 1970.

[Die71] Jean A. DIEUDONNÉ : *La géométrie des groupes classiques.* Springer-Verlag, Berlin, 1971. Troisième édition, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5.

[DK00] Peng DING et Jennifer D. KEY : Minimum-weight codewords as generators of generalized Reed-Muller codes. *IEEE Trans. Inform. Theory*, 46(6):2152–2158, 2000.

[DMM+03] Hans DOBBERTIN, Donald MILLS, Eva Nuria MÜLLER, Alexander POTT et Wolfgang WILLEMS : APN functions in odd characteristic. *Discrete Math.*, 267(1-3):95–112, 2003. Combinatorics 2000 (Gaeta).

[DO68] Peter DEMBOWSKI et T. G. OSTROM : Planes of order n with collineation groups of order n^2. *Math. Z.*, 103:239–258, 1968.

[Dob99a] Hans DOBBERTIN : Almost perfect nonlinear power functions on GF(2^n) : the Niho case. *Inform. and Comput.*, 151(1-2):57–72, 1999.

[Dob99b] Hans DOBBERTIN : Almost perfect nonlinear power functions on GF(2^n) : the Welch case. *IEEE Trans. Inform. Theory*, 45(4):1271–1275, 1999.

[Dob99c] Hans DOBBERTIN : Another proof of Kasami's theorem. *Des. Codes Cryptogr.*, 17(1-3):177–180, 1999.

[Dob01] Hans DOBBERTIN : Almost perfect nonlinear power functions on GF(2^n) : a new case for n divisible by 5. *In Finite fields and applications (Augsburg, 1999)*, pages 113–121. Springer, Berlin, 2001.

[DY06] Cunsheng DING et Jin YUAN : A family of skew Hadamard difference sets. *J. Combin. Theory Ser. A*, 113(7):1526–1535, 2006.

[Ful89] William FULTON : *Algebraic curves.* Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[Gru90] I. I. GRUSHKO : Majority decoding of generalized Reed-Muller codes. *Problemy Peredachi Informatsii*, 26(3):12–20, 1990.

[Hir98] J. W. P. HIRSCHFELD : *Projective geometries over finite fields.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second édition, 1998.

[HKM78] Tor HELLESETH, Torleiv KLØVE et Johannes MYKKELTVEIT : On the covering radius of binary codes. *IEEE Trans. Inform. Theory*, 24(5):627–628, 1978.

[HM09] Fernando HERNANDO et Gary MCGUIRE : Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and apn functions. *CoRR*, abs/0903.2016, 2009.

[Hou93] Xiang Dong HOU : Further results on the covering radii of the Reed-Muller codes. *Des. Codes Cryptogr.*, 3(2):167–177, 1993.

[Hou96] Xiang-Dong HOU : Covering radius of the Reed-Muller code $R(1,7)$—a simpler proof. *J. Combin. Theory Ser. A*, 74(2):337–341, 1996.

[HRS99] Tor HELLESETH, Chunming RONG et Daniel SANDBERG : New families of almost perfect nonlinear power mappings. *IEEE Trans. Inform. Theory*, 45(2): 474–485, 1999.

[HS97] Tor HELLESETH et Daniel SANDBERG : Some power mappings with low differential uniformity. *Appl. Algebra Engrg. Comm. Comput.*, 8(5):363–370, 1997.

[Jed07] David JEDLICKA : APN monomials over $\mathrm{GF}(2^n)$ for infinitely many n. *Finite Fields Appl.*, 13(4):1006–1028, 2007.

[JW93] H. JANWA et R. M. WILSON : Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in char. 2 and some applications to cyclic codes. *In Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993)*, volume 673 de *Lecture Notes in Comput. Sci.*, pages 180–194. Springer, Berlin, 1993.

[KDY10] Selçuk KAVUT et Melek DIKER YÜCEL : 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class. *Inform. and Comput.*, 208(4):341–350, 2010.

[KLP68] Tadao KASAMI, Shu LIN et W. Wesley PETERSON : New generalizations of the Reed-Muller codes. I. Primitive codes. *IEEE Trans. Information Theory*, IT-14:189–199, 1968.

[KP08] Gohar M. KYUREGHYAN et Alexander POTT : Some theorems on planar mappings. *In Arithmetic of finite fields*, volume 5130 de *Lecture Notes in Comput. Sci.*, pages 117–122. Springer, Berlin, 2008.

[Lan91a] Philippe LANGEVIN : Covering radius of RM(1, 9) in RM(3, 9). *In Eurocode '90 (Udine, 1990)*, volume 514 de *Lecture Notes in Comput. Sci.*, pages 51–59. Springer, Berlin, 1991.

[Lan91b] Philippe LANGEVIN : On the orphans and covering radius of the Reed-Muller codes. *In Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991)*, volume 539 de *Lecture Notes in Comput. Sci.*, pages 234–240. Springer, Berlin, 1991.

[Led10a] E. LEDUCQ : A new proof of Delsarte, Goethals and Mac Williams theorem on minimal weight codewords of generalized Reed-Muller code. *ArXiv e-prints*, janvier 2010.

[Led10b] E. LEDUCQ : A proof of two conjectures on APN functions. *ArXiv e-prints*, juin 2010.

[Led10c] E. LEDUCQ : Fonctions PN sur une infinite d extensions de Fp, p impair. *ArXiv e-prints*, juin 2010.

[Led11] E. LEDUCQ : On the covering radius of first order generalized Reed-Muller codes. *ArXiv e-prints*, février 2011.

[LN97] Rudolf LIDL et Harald NIEDERREITER : *Finite fields*, volume 20 de *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second édition, 1997. With a foreword by P. M. Cohn.

[Luc78] Edouard LUCAS : Theorie des Fonctions Numeriques Simplement Periodiques. [Continued]. *Amer. J. Math.*, 1(3):197–240, 1878.

[MS77a] F. J. MACWILLIAMS et N. J. A. SLOANE : *The theory of error-correcting codes. I.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[MS77b] F. J. MACWILLIAMS et N. J. A. SLOANE : *The theory of error-correcting codes. II.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[Myk80] Johannes J. MYKKELTVEIT : The covering radius of the (128, 8) Reed-Muller code is 56. *IEEE Trans. Inform. Theory*, 26(3):359–362, 1980.

[NH07] Geir Jarle NESS et Tor HELLESETH : A new family of ternary almost perfect nonlinear mappings. *IEEE Trans. Inform. Theory*, 53(7):2581–2586, 2007.

[Nyb94] Kaisa NYBERG : Differentially uniform mappings for cryptography. *In Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993)*, volume 765 de *Lecture Notes in Comput. Sci.*, pages 55–64. Springer, Berlin, 1994.

[PHB98] V. S. PLESS, W. C. HUFFMAN et R. A. BRUALDI, éditeurs. *Handbook of coding theory. Vol. I, II.* North-Holland, Amsterdam, 1998.

[PW83] N. J. PATTERSON et Douglas H. WIEDEMANN : The covering radius of the (2^{15}, 16) Reed-Muller code is at least 16 276. *IEEE Trans. Inform. Theory*, 29(3):354–356, 1983.

[PW90] Nick J. Patterson et Douglas H. Wiedemann : Correction to : “The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16 276” [IEEE Trans. Inform. Theory **29** (1983), no. 3, 354–356 ; MR0712397 (85h :94031)]. *IEEE Trans. Inform. Theory*, 36(2):443, 1990.

[Ree54] Irving S. Reed : A class of multiple-error-correcting codes and the decoding scheme. *Trans. I.R.E.*, PGIT-4:38–49, 1954.

[Rom06] Steven Roman : *Field theory*, volume 158 de *Graduate Texts in Mathematics*. Springer, New York, second édition, 2006.

[Sor91] Anders Bjaert Sorensen : A Note on Algorithms Deciding Rationality and Absolutely Irreducibility Based on the Number of Rational Solutions. RISC Report Series 91-37, Research Institute for Symbolic Computation (RISC), University of Linz, Schloss Hagenberg, 4232 Hagenberg, Austria, 1991.

[vL99] J. H. van Lint : *Introduction to coding theory*, volume 86 de *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third édition, 1999.

[Wei48] André Weil : *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

[Wel68] Edward J. Weldon, Jr. : New generalizations of the Reed-Muller codes. II. Nonprimitive codes. *IEEE Trans. Information Theory*, IT-14:199–205, 1968.

[ZKW09] Zhengbang Zha, Gohar M. Kyureghyan et Xueli Wang : Perfect nonlinear binomials and their semifields. *Finite Fields Appl.*, 15(2):125–133, 2009.

[ZW09] Zhengbang Zha et Xueli Wang : New families of perfect nonlinear polynomial functions. *J. Algebra*, 322(11):3912–3918, 2009.

[ZW10] ZhengBang Zha et XueLi Wang : Power functions with low uniformity on odd characteristic finite fields. *Sci. China Math.*, 53(8):1931–1940, 2010.

Liste des tableaux

3.1 Exposants pour lesquels [HRS99] ne donne pas de famille infinie 79

4.1 Singularités de g 101
4.2 Singularités de h pour $d \equiv 1 \mod p$ 102

A.1 Calcul de m_{x_3}. 122

Index des notations

$\#A$, 17
$\left(\frac{a}{p}\right)$, 17
$< x, y >$, 21
$\lceil x \rceil$, 17
$\lfloor x \rfloor$, 17
1_A, 29

1_u, 24

A^c, 17
$\mathrm{Aut}(C)$, 20

B_m^q, 24

$\overline{c}^\omega$, 49
χ, 17
$C^\perp$, 21

$d(.,.)$, 17
$\deg(f)$, 17
Δ, 26
Δ_d, 65
Δ_f, 64
$\delta_{i,j}$, 30

$f(x, y)$, 93
$\widehat{f}$, 47
$\widetilde{f}$, 96
$\overline{f}$, 96
$\mathbb{F}_q$, 17
$\mathbb{F}_q[x_1, \ldots, x_m]$, 17
$\widetilde{F}^v$, 90
$F_x(a, b)$, 89
$F_y(a, b)$, 89

$G_{q,r}$, 40
$g(x, y)$, 93
$\mathrm{GA}_m(\mathbb{F}_q)$, 17
$\Gamma(F)$, 89
$\mathrm{GL}_m(\mathbb{F}_q)$, 17
$\mathrm{GSA}_m(\mathbb{F}_q)$, 41

$h(x, y)$, 94
$\widetilde{h}$, 96
$\overline{h}$, 96

$I_P(F, G)$, 90

$\Lambda_{a,i}(x)$, 20

$m_P(F)$, 89

$N_f(a, b)$, 64
$N(Q)$, 46

$O_P(F)$, 89
ord_P^F, 91

$\mathcal{P}(\mathbb{F}_2^m)$, 26
p, 17
$\mathrm{pgcd}(a, b)$, 17
φ_q, 40
$\phi_{\Pi,\sigma}$, 20
$\mathrm{Pol}(m, \mathbb{F}_q)$, 24

q, 17

$R(r, m)$, 26
$\mathrm{rg}(F)$, 34
$\rho(1, m)$, 43
$\rho(C)$, 21
$\rho_r(1, m)$, 43
$R_q(r, m)$, 28
$R_q(r, m)^*$, 29

$\sigma.f$, 26
$\mathcal{S}_n$, 17
$\mathrm{Supp}(f)$, 17

$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$, 30

U_v, 90

$W(f)$, 69
wt_q, 30

$\overline{x_i}$, 110