RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ DE BATNA 2
FACULTÉ DES MATHÉMATIQUES ET D´INFORMATIQUE
DÉPARTEMENT DES MATHÉMATIQUES

THÈSE

Pour obtenir le titre de

Docteur en Sciences

de l'université de Batna 2

Spécialité : **MATHÉMATIQUES**

Présentée par

Karima CHATOUH

Construction et étude des codes linéaires

dirigée par

Lemnouar NOUI

Soutenue le :

Jury :

Guedjiba Said	Professeur , Université de batna 2	Président
Noui Lemnouar	Professeur , Université de batna 2	directeur de thèse
Trabelsi Nadir	Professeur , Université de setif 2	Examinateur
Badis Abdelhafid	Professeur , Université de Khenchela	Examinateur
Melkemi Lamine	Professeur , Université de batna 1	Examinateur
Guenda Kenza	MCA, Université USTHB , Algérie	Invité

Remerciements

Nulle oeuvre n´est exaltante que celle réalisée avec le soutien moral et financier des personnes qui nous sont proches.

Je tiens en tout premier lieu à remercier **Allah**, le miséricordieux, de m´avoir donné la force dans les moments difficiles d´éditer cette thèse.

Je tiens à exprimer ma plus profonde reconnaissance et gratitude à ma soeur Guenda Kenza pour sa disponibilité, ses conseils, et qui m´a aidé dans mes recherches.

Mes remerciements s´adressent également au Professeur Noui Lemnouar mon directeur de recherche d´avoir accepté de diriger ce travail.

J´adresse mes sincères remerciements aux membres du jury pour avoir accepté d´évaluer ce travail, à savoir : Messieurs les Professeurs Mr Guedjiba Said, Mr Trabelsi Nadir, Mr Badis Abdelhafid et Mr Melkemi Lamine.

Je remercie les professeurs Mr Benlahcene Moussa, Mme Boudiaf Naima et Mme Gadra Meriem pour toute l´aide qu´ils m´ont apporté.

J´adresse mes sincères remerciements au Professeur T. A. Gulliver de l´université Victoria du Canada pour sa collaboration.

Dédicace

Je dédie ce modeste travail à : Ceux qui m´ont donné la vie : mes parents.

Celui qui m´a été d´un grand soutien moral mon époux. Ceux que je leur ai donné ma vie : mes enfants, Anes, Tassnim, Gaza et Sadjida. À ceux qui ont participé de près ou de loin à réaliser cette thèse. À toute ma famille ainsi qu´à mes amis.

Abstract

The works of this thesis have reached this level by producing for papers, three of them are already published.

The first is entitled, "*On some classes of linear codes over $\mathbb{Z}_2\mathbb{Z}_4$ and their covering radii*", Journal of Applied Mathematics and Computing, 2016. In this paper, we have established a simples codes, and a MacDonald cdes of type α and β over $\mathbb{Z}_2\mathbb{Z}_4$. We have also examined the covering radius of these codes. In addition, we have examined the binary image of simplex codes of type β attained the Gilbert bound.

The second is entitled, "*Simplex and MacDonald codes over R_q*", Journal of Applied Mathematics and Computing, 2016. In this paper, we have given a new homogeneous weight as its Gray map of the ring R_q. We have created a simplex and MacDonald codes of type α and β over this ring as well. We have studied many characteristics, as their binary images.

The third is entitled, "Codes over $\mathbb{Z}_2$ $(\mathbb{Z}_2 + u\mathbb{Z}_2)$ and their covering radii". Journal of Algebra, Number Theory : Advances and Applications. Volume 16, Number 1, pp. 25-39, 2016. In this paper, we have created the first of order of Reed-Muller codes over $\mathbb{Z}_2$ $(\mathbb{Z}_2 + u\mathbb{Z}_2)$ starting from a simplex codes to type α over this ring, and calculated the exact value of the covering radius of these codes.

In the fourth is entitled, "*Secret Sharing Schemes Based on Gray Images of Linear Codes over $R_{q,m}$*, International Conference on Coding and Cryptography ICCC, USTHB, Algiers, Algeria, 2015 (communiqué par K. Chatouh). In this paper, the secret sharing schemes obtained from a class of linear codes are the Gray images of simplex and MacDonald codes of type α and β over $R_{q,m} = \mathbb{F}_{2^m}[u_1, u_2 \cdots u_q]/\langle u_i^2 = 0, u_i u_j - u_j u_i \rangle$, with $q \geq 2$

and $m \geq 1$.

The motivations in studying such codes comes form the fact that these codes are with few weights. They also find some other applications such as PSK modulation and some cryptographic purposes.

Key words : Simplex codes, MacDonald codes, Gray map, Homogeneous weight, Hamming weight, Lee weight, The covering radius.

Résumé

Les travaux de cette thèse résument le contenu de quatre papiers dont trois sont déjà publiés.

Le premier, intitulé "*On some classes of linear codes over* $\mathbb{Z}_2\mathbb{Z}_4$ *and their covering radii*", Journal of Applied Mathematics and Computing, 2016. Dans lequel, Nous avons construits les codes simplexes et les codes de Macdonald de types α et β sur $\mathbb{Z}_2\mathbb{Z}_4$. Nous avons examiné aussi le rayon de recouvrement de ces codes. De plus, nous avons étudié leurs images binaires, et nous avons prouvé que l´image binaire des codes simplexes de types β atteint la borne de Gilbert.

Le deuxième, intitulé "*Simplex and MacDonald codes over* R_q", Journal of Applied Mathematics and Computing, 2016. Dans lequel, nous avons donné un nouveau poids Homogène ainsi que son Gray map dans l´anneau R_q. Aussi, nous avons construit les codes simplexes et les codes de MacDonald de types α et β sur cet anneau, ainsi que leurs images binaires. En outre nous avons étudié plusieurs propriétés,

Le troisième, intitulé "Codes over $\mathbb{Z}_2\left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)$ and their covering radii". Journal of Algebra, Number Theory : Advances and Applications. Volume 16, Number 1, pp. 25-39, 2016. Dans lequel, nous avons construit Le premier ordre des codes de Reed-Müller sur $\mathbb{Z}_2\left(\mathbb{Z}_2 + u\mathbb{Z}_2\right)$ à partir des codes simplexes de type α sur cet anneau également nous avons calculé la valeur exacte de rayon de recouvrement de ces codes.

Le quatrième intitulé "*Secret Sharing Schemes Based on Gray Images of Linear Codes over* $R_{q,m}$, International Conference on Coding and Cryptography ICCC, USTHB, Algiers, Algeria, 2015 (communiqué par K. Chatouh). Dans lequel, Les schémas de partage d´ secret

sont obtenus à partir d´une classe de codes linéaires qui sont les images Gray des simplexes et des codes MacDonald de types α et β sur $R_{q,m} = \mathbb{F}_{2^m}[u_1, u_2 \cdots u_q]/\langle u_i^2 = 0, u_i u_j - u_j u_i \rangle$, avec $q \geq 2$ et $m \geq 1$.

Nos motivations dans l´étude de ces codes proviennent du fait que ces codes sont des poids connus. Il existe aussi quelques autres applications comme la modulation PSK et quelques fins cryptographiques.

Mots clés : Codes simplexes, Code de MacDonald, Gray map, Poids Homogène, Poids de Hamming, Poids de Lee, L´image binaire, Le rayon de recouvrement.

Notations

$\mathbb{F}_q$ =: Un corps fini de q éléments.

$r(C)$ =: Le rayon de recouvrement d´un code C de longueur n sur $\mathbb{F}_q$.

$\widehat{C}$ =: Le code étendu.

$\mathcal{R}$ =: Un anneau fini.

$S_k(q)$ =: Le code simplexe sur un corps fini $\mathbb{F}_q$.

$M_{k,u}(q)$ =: Le code de Macdonald sur un corps fini $\mathbb{F}_q$.

wt_E =: Le poids Euclidien.

wt_{Lee} =: Le poids de Lee.

wt_{Ham} =: Le poids de Hamming.

wt_{hom} =: Le poids homogène.

$C^{\sum_{j=1}^{7} n_j}$ =: Le code de répétition en bloc sur $\mathbb{Z}_2\mathbb{Z}_4$.

S_k^{α} =: Le code simplexe de type α sur $\mathbb{Z}_2\mathbb{Z}_4$.

S_k^{β} =: Le code simplexe de type β sur $\mathbb{Z}_2\mathbb{Z}_4$.

$\mathcal{M}_{k,u}^{\alpha}$ =: Le code de MacDonald de type α sur $\mathbb{Z}_2\mathbb{Z}_4$.

$\mathcal{M}_{k,u}^{\beta}$ =: Le code de MacDonald de type β sur $\mathbb{Z}_2\mathbb{Z}_4$.

$S_{(q,k)}^{\alpha}$ =: Le code simplexe de type α sur R_q.

$S_{(q,k)}^{\beta}$ =: Le code simplexe de type β sur R_q.

$\mathcal{M}_{(q,k,u)}^{\alpha}$ =: Le code de MacDonald de type α sur R_q.

$\mathcal{M}_{(q,k,u)}^{\beta}$ =: Le code de MacDonald de type β sur R_q.

$Tor_A(C)$ =: Le code de *torsion*.

Table des matières

Introduction

La théorie des anneaux commutatifs finis est le type de théories qui à développé rapidement. Elle à été appliquée dans plusieurs domaines théoriques comme la combinatoire, la géométrie finie et l´analyse des algorithmes.

Dans les deux dernières décennies, l´intérêt vers le développement de cette théorie a augmenté particulièrement dans la cryptographie algébrique et la théorie des codes. En effet, plusieurs codes sur un corps fini, ont été investis comme des images des codes sur des anneaux de Galois (en particulier sur l'anneau $\mathbb{Z}_4$). D´une part, la recherche mathématique appliquée a motivé une analyse plus systématique de l´algèbre commutative finie. D´autre part, les mathématiques pures ont offert des méthodes innovatrices dans la théorie du codage.

Il existe plusieurs codes non linéaires binaires ayant le double mots-code comme n´importe quel code linéaire de la même longueur et de même distance minimale, le code de Nadler [51] est un exemple, c´est un $[12, 5]$-code non linéaire systématique avec un rayon de recouvrement $\rho = 4$ et de distance minimale $d = 5$ [66]. Malgré que le code possède des meilleurs propriétés, il est ni efficace de l´utiliser à cause d´être non linéaire. Cependant, cela a été changé aprés la contribution de Nechaev [53] en 1989. Dans son ouvrage, certains de ces codes non linéaires ont donné une structure algébrique comme des codes linéaires sur l´anneau $\mathbb{Z}_4$ au moyen du nom de l´application **Gray**, ce qui fait la correspondance entre les coordonées binaires et les coordonées quaternaires. Elle joue un rôle fondamental dans l´étude des codes quaternaires. C´est une isométrie qui préserve la propriété de la distance mais pas la linéarité. De cela, a commencé l´intérêt d´étudier les codes linéaires définis sur

les anneaux finis. Le terme code linéaire sur $\mathbb{Z}_4$ a été utilisé tel un code non linéaire avec une structure algébrique sur $\mathbb{Z}_4$, cependant, les codes définis comme des sous-ensembles de $\mathbb{Z}_4$ ont été appelés codes linéaires quaternaires. Ce résultat ouvre une nouvelle direction de la théorie des codes, plusieurs articles ont été publiés sur ce thème.

Une contribution très importante est celle de Hammons, Kummar, Calderbank, Sloane et Solé [42] qui a défini plusieurs familles de codes quaternaires. Comme il y a des codes binaires non linéaires qui peuvent être vu comme des codes linéaires quaternaires sous le Gray map, il y a aussi quelques codes binaires non linéaires connus comme des codes linéaires sur $\mathbb{Z}_2\mathbb{Z}_4$, on peut donner une structure algébrique comme les sous groupes de $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Cette structure est appelée codes additifs sur $\mathbb{Z}_2\mathbb{Z}_4$ [1], [6], [13], [14] et [64], qui sont des codes binaires linéaires pour $\delta = 0$ et des codes quaternaires linéaires pour $\gamma = 0$.

Les codes additifs ont été d´abord définis par Delsarte en 1973 en terme de schéma d´association [26] et [29]. En général un code additif, d´après le schéma d´association de la transmission, est défini comme un sous groupe du groupe sous-adjacent abélien. D´autre part, la transmission invariante des codes de propelinear ont été définis pour la première fois en 1997 [61], où il est prouvé que tous ces codes binaires sont des groupes isomorphes aux sous-groupes de $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta \times \mathbb{Q}_8^\sigma$, où $\mathbb{Q}_8$ est le groupe de quaternions non commutatif de huit éléments. Dans le cas particulier où le schéma d´association est le schéma de Hamming binaire, et quand le groupe sous-adjacent abélien est d´ordre 2^n, les codes additifs coïncident avec la transmission invariante des codes de propelinear. Alors, comme il a été expliqué dans [29], les seules structures des codes abéliens sont celles de la forme $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$, avec $n = \gamma + 2\delta$. Donc, les sous-groupes de $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ sont les seuls codes additifs dans le schéma de Hamming binaire. Pour distinguer des codes additifs sur les corps finis [7], désormais, on va les appeler codes additifs sur $\mathbb{Z}_2\mathbb{Z}_4$.

L´image binaire des codes additifs sur $\mathbb{Z}_2\mathbb{Z}_4$ sous le Gray map étendu, définie dans le chapitre 2 est appelée les codes linéaires binaires sur $\mathbb{Z}_2\mathbb{Z}_4$.

La théorie des codes est un domaine de recherche vaste, identifie l´étude des codes simplexes sur les corps et les anneaux. Il est indispensable de donner les propriétés de ces codes sur les corps.

En effet, soit $\mathbb{F}_q = GF_{(q)} = \{\alpha_0, \alpha_1, \cdots, \alpha_{q-1}\}$, pour k, q données, soit $G_k(q)$ une matrice de taille $k \times \dfrac{\left(q^k-1\right)}{(q-1)}$ sur $\mathbb{F}_q$ dont les colonnes sont deux à deux linéairement indépendantes. Le code $S_k\left(q\right)$ généré par la matrice $G_k\left(q\right)$ est appelé code simplexe.

Notons que $S_k\left(q\right)$ est un $\left[\dfrac{\left(q^k-1\right)}{(q-1)}, k, q^{k-1}\right]$ −code. Tout code linéaire ayant ces paramètres est équivalents à $S_k\left(q\right)$ [34]. $G_k(q)$ peut être défini par :

$$G_k\left(q\right) = \left(\begin{array}{c|c|c|c|c|c} 00\cdots0 & 1 & 11\cdots1 & \alpha_3\cdots\alpha_3 & \cdots & \alpha_q\cdots\alpha_q \\ \hline G_{k-1}\left(q\right) & 0 & G_{k-1}\left(q\right) & G_{k-1}\left(q\right) & \cdots & G_{k-1}\left(q\right) \end{array}\right), \tag{1}$$

avec

$$G_2\left(q\right) = \left(\begin{array}{c|c|c|ccc} 0 & 1 & 1 & \alpha_3 & \cdots & \alpha_{q-1} \quad \alpha_q \\ \hline 1 & 0 & 1 & 1 & \cdots & 1 \quad\quad 1 \end{array}\right).$$

Chaque mots-code non nul de $S_k\left(q\right)$ a un poids égal à q^{k-1}. Le code simplexe binaire (généralement noté S_k) a été découvert par Ronald A. Fisher [32] en 1942.

La dualité du code simplexe est connue par le code de Hamming de paramètres

$$\left[\frac{q^k-1}{q-1}, \frac{q^k-1}{q-1} - k, 3\right].$$

Une méthode pour construire de nouveaux codes consiste à éliminer ou ajouter une ou plusieurs coordonnées d´un code connu .

Soit $1 \leq u \leq k-1$ et soit $G_{k,u}\left(q\right)$ la matrice obtenue de $G_k\left(q\right)$ par l´élimination des colonnes correspondantes aux colonnes de la matrice $G_u\left(q\right)$. c´est-à-dire :

$$G_{k,u}\left(q\right) = \left(G_k\left(q\right) \left\backslash \frac{0}{G_u\left(q\right)}\right.\right) \tag{2}$$

où 0 est la matrice nulle de taille $(k-u) \times \dfrac{q^u-1}{q-1}$ et $(A \setminus B)$ est la matrice obtenue de la matrice A par l´élimination des colonnes de la matrice B.

Le code $M_{k,u}\left(q\right)$ généré par la matrice $G_{k,u}\left(q\right)$ est le code poinçoné de $S_k\left(q\right)$, appelé un code de Macdonald. $M_{k,u}\left(q\right)$ est un code de paramètres $\left[\dfrac{q^k-q^u}{q-1}, k, q^{k-1}-q^{u-1}\right]$ dont chaque mots code non nul a un poids, soit q^{k-1} ou $q^{k-1}-q^{u-1}$ [48].

Les codes sur les anneaux étaient de grande importance comme un point d´intérêt pour les recherches depuis le travail de Hammons et al. [42], sur les codes sur $\mathbb{Z}_4$. Un nombre de ces résultats ont été étendu aux anneaux à chaîne finie comme l´anneau de Galois ou les anneaux de la forme $\mathbb{F}_2[u]/\langle u^m\rangle$. Récemment, comme une généralisation des études précédentes [68] et [70], Dougherty et Yildiz dans [31] ont considéré les codes sur une série d´anneaux, dénotés R_q. Ces anneaux sont finis et commutatifs, mais ne sont pas à chaîne finies, l´importance des codes simplexes et des codes de MacDonald qui sont définis sur quelques anneaux commutatifs finis est le motif principal de cette étude détaillé et approfondie.

Les codes simplexes de type α et β sur l´anneau $\mathbb{Z}_4$ ont été introduits dans [16], ce sont des généralisations des codes simplexes binaires. Ainsi dans [38], une généralisation de ces codes aux codes sur $\mathbb{Z}_{2^s}$ a été donnée.

Il y a un intérêt grandissant des recherches sur les codes simplexes et les codes de MacDonald de type α et β sur les anneaux finis, l´étude a été détaillée dans [2], [3], [16], [25], [38], [40] et [41] au cours des dernières années.

Notre contribution dans la présente thèse est resumée dans les trois points suivants :

► On a dévloppé une nouvelle approche pour une présentation algébrique des codes simplexes et des codes de MacDonald de type α et β sur certains anneaux à savoir l´anneau $\mathbb{Z}_2\mathbb{Z}_4$, l´anneau $R_q = \mathbb{F}_2[u_1, u_2, \ldots, u_q]/\langle u_i^2 = 0, u_iu_j = u_ju_i\rangle$, avec $q \geq 2$. et de plus l´anneau $R_{q,m} = \mathbb{F}_{2^m}[u_1, u_2, \ldots, u_q]/\langle u_i^2 = 0, u_iu_j = u_ju_i\rangle$, avec $q \geq 2$ et $m \geq 1$. Ce travail est un sujet de recherche intéressant et important vu les domaines d´application, en l´occurence, la cryptographie et les schémas de partage d´un secret basé sur les codes linéaires, voir [18], [19] et [20]. Ces résultats sont utilisés pour étudier le décodage algébrique des codes correcteurs d´erreurs, ainsi que pour analyser des attaques algébriques en cryptographie. Nous soulignons aussi à l´importance d´etudier les rayons de recouvrement des codes simplexes et des codes de MacDonald pour la stéganographie.

Pour la première fois dans [20], nous avons montré comment construire un code simplexe, et un code de MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$ à partir de la concaténation d´un code simplexe et d´un code de MacDonald de type α et β sur $\mathbb{Z}_2$, et sur $\mathbb{Z}_4$.

► On a construit les codes simplexes et les codes de MacDonald de type α et β sur une serie d´anneaux de Frobenius dans [18], où on a étudié :

◇ Les distributions de poids de Hamming, homogène et de Lee.

◇ Les images binaires de ces codes sur cette serie d´anneaux.

◇ En généralisant les rayons de recouvrement de ces codes.

► Une généralisation a été éffectuée de l´anneau R_q à l´anneau $R_{q,m}$, en construisant les codes simplexes et les codes de MacDonald de type α et β sur $R_{q,m}$ à partir de la construction des codes simplexes et des codes de MacDonald de type α et β sur R_q, nous avons ternminé par la construction des codes de *torsion*, des codes simplexes et des codes de MacDonald, puis on a réalisé une application du partage de secret sur les images Gray de ces codes (voir [19]).

Cette thèse est composée de cinq chapitres et un annexe consacré aux préliminaires mathématiques, qui nous permettent une compréhension plus aisée des autres chapitres.

• Le premier chapitre est consacré aux rappels sur les codes correcteurs d´erreurs sur un corps fini, nous donnons une introduction sur la théorie des codes, nous rappelons quelque codes correcteurs d´erreurs linéaires et nous donnons quelques bornes sur ces paramètres.

• Le deuxième chapitre est consacré, aux codes linéaires de longueur n sur un anneau fini $\mathcal{R}$ considérés comme sous-module du module $\mathcal{R}^n$ sur $\mathcal{R}$, en particulier, les codes linéaires sur l´anneau $\mathbb{Z}_4$, les codes linéaires sur l´anneau $\mathbb{Z}_2\mathbb{Z}_4$. Nous donnons la définition de la matrice génératrice des codes linéaires sur l´anneau $\mathbb{Z}_2\mathbb{Z}_4$, on définit aussi la dualité, et le type de ces codes.

• Dans le troisième chapitre , nous utilisons les résultats des deux chapitres précedents pour construire les codes simplexes et les codes de MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$. Les codes simplexes et les codes de MacDonald sur un corps fini et sur des anneaux finis ont été déja étudiés, Cela nous a donné la motivation de construire de nouveaux codes, c´est la concaténation des codes simplexes et des codes de MacDonald binaires et quaternaires de type α et β. Il résulte de ce qui précède la construction des codes simplexes et des codes de MacDonald sur $\mathbb{Z}_2\mathbb{Z}_4$, qui contiennent les codes binaires et les codes quaternaires correspondants comme des sous classes et nous donnons leur rayon de recouvrement, où ce

rayon est imporant pour déterminer la capacité de corriger les erreurs. Nous construisons aussi le code de répétition en blocs sur $\mathbb{Z}_2\mathbb{Z}_4$ en trouvant leurs rayons de recouvrements. Finalement, nous prenons en considération les images Gray binaires de ces codes. nous montrons que l´image binaire des codes simplexes de type β atteint la borne de Gilbert.

• Dans le quatrième chapitre, on construit les codes simplexes et les codes de MacDonald de type α et β sur l´anneau de Frobenius

$$R_q = \mathbb{F}_2[u_1, u_2, \ldots, u_q]/\left\langle u_i^2 = 0, u_i u_j = u_j u_i \right\rangle, \text{ avec } \ q \geq 2.$$

Dans ce travail nous proposons un nouveau poids homogène sur R_q, ainsi que son Gray map, nous construisons les codes simplexes et les codes de MacDonald de type α et β sur cet anneau où les propriétés de ces codes sont étudiées, particulièrement les distributions de poids et les rayons de recouvrement. En plus, les images binaires de ces codes sont considérées en utilisant différents Gray map.

• Le but essentiel du cinqième chapitre est l´application du schéma de partage d´un secret basé sur les images Gray des codes linéaires sur $R_{q,m}$. Nous appliquons le schéma de partage d´un secret basé sur une classe des codes linéaires qui sont les images Gray des codes simplexes et des codes de MacDonald de type α et β sur l´anneau

$R_{q,m} = \mathbb{F}_{2^m}[u_1, u_2, \ldots, u_q]/\left\langle u_i^2 = 0, u_i u_j = u_j u_i \right\rangle$, avec $\ q \geq 2$ et $\ m \geq 1$.

Nous avons ainsi achevé cette thèse par une conclusion et des perspectives.

Chapitre 1

Les codes linéaires sur les corps finis

1.1 Introduction

Le problème de la communication de l´information, en particulier le codage et le décodage de l´information pour la transmission fiable sur un canal "bruyant", est d´une grande importance aujourd´hui. En général, il faut transmettre un message qui est constitué en une chaîne de symboles finis qui sont des éléments d´un alphabet fini. Par exemple, si cet alphabet est constitué simplement de 0 et 1, le message peut être décrit comme un nombre binaire. En général, l´alphabet est un corps fini. Maintenant, la transmission de chaînes finies d´éléments de l´alphabet sur un canal de communication ne doit pas être parfaite dans le sens où chaque bit d´information est transmis inchangé sur ce canal. Comme il n´y a pas de canal idéal sans "bruit", le récepteur du message transmis peut obtenir de l´information déformée et peut faire des erreurs dans l´interprétation du signal transmis.

L´un des problèmes principaux de la théorie du codage est connaitre les erreurs qui se produisent par exemple en raison des canaux bruyants, très improbables. Les méthodes pour améliorer la fiabilité de la transmission dépendent des propriétés des corps finis.

L´idée de base la plus importante de la théorie de codage algébrique est de transmettre des informations redondantes avec le message que l´on veut communiquer, on étend la chaîne de symboles de message pour une chaîne plus longue d´une manière systématique.

Un modèle simple d´un système de communication, on suppose que les symboles de message et du message codé sont des éléments du même corps fini $\mathbb{F}_q$. Les moyens de codage pour coder un bloc de messages de k symboles $a_1a_2\cdots a_k,\ a_i \in \mathbb{F}_q$ en un mots code $c_1c_2\cdots c_n$ de n symboles $c_j \in \mathbb{F}_q$, où $n > k$. Nous considérons le mots code comme un vecteur ligne c dans $\mathbb{F}_q^n$.

Un simple type de codage on suppose que chaque bloc $a_1a_2\cdots a_k$ des symboles d´où, le message codé est un mots-code de la forme

$$a_1a_2\cdots a_kc_{k+1}c_{k+2}\cdots c_n$$

où les premiers k symboles sont les symboles du message original et $n-k$ symboles qui restent dans $\mathbb{F}_q$ sont des symboles de contrôle.

Dans ce chapitre nous présentons certains outils de la théorie du codage, nous donnons quelques définitions de base, et, des notations qui seront utilisées dans la dissertation. En plus de synthétiser les résultats classiques comme les codes linéaires, une synthèse sur des techniques et des définitions récentes relatives à la contribution jointe à ce document est inclue, ce qui va aider le lecteur à une bonne compréhension. Pour une introduction profonde à la théorie du codage, le lecteur se référe à [5], [7], [44], [49] et [57].

1.2 Les codes linéaires

Si l'alphabet $\mathcal{A}$ est un corps fini, alors $\mathcal{A}^n$ est un espace vectoriel. Tel est le cas si $\mathcal{A} = \{0, 1\}$, il est naturel de chercher des codes à $\mathcal{A}^n$ qui ont plus de structure, en particulier, qui sont des sous-espaces vectoriel.

L'alphabet $\mathcal{A} = \mathbb{F}_q$, qui est un corps fini de q éléments. Tout sous ensemble C de $\mathbb{F}_q^n$ est appelé code de longueur n sur $\mathbb{F}_q$.

Définition 1.2.1 (Les codes linéaires) *Un sous espace vectoriel C de $\mathbb{F}_q^n$ de dimension k est appelé code linéaire $[n, k]$. Les vecteurs de C sont dits mots du code.*

Un code linéaire est un sous-espace vectoriel de dimension k sur $\mathbb{F}_q$ contenant q^n mots code. La valeur $R = \dfrac{k}{n}$ est appelée taux de transmission ou rendement. Les mots d´un

code linéaire peuvent s´écrire de plusieurs manières selon le choix d´une base du code. On représente une base d´un code linéaire sous forme matricielle.

1.2.1 Paramètres d´un code linéaire

Soit C un code linéaire de dimension k et de longueur n.

Définition 1.2.2 (Matrice génératrice) *Une matrice génératrice de C est une matrice, notée généralement G, de taille $k \times n$ et à coefficients dans $\mathbb{F}_q$ dont les lignes forment une base de C.*

Propriété 1.2.3 *Soit G une matrice génératrice de C, alors la matrice MG, où M est une matrice inversible de taille $k \times k$ à coefficients dans $\mathbb{F}_q$ est aussi une matrice génératrice de C,*

Définition 1.2.4 *Une matrice génératrice G d´un code linéaire est dite sous forme systématique si et seulement si $G = (I_k|A)$, où I_k est la matrice identité de taille $k \times k$ et A une matrice de taille $k \times (n-k)$.*

Proposition 1.2.5 *Tout code linéaire C peut se mettre sous forme systématique à permutation près.*

Un code linéaire peut être défini par sa matrice génératrice ou sa matrice dite matrice de contrôle de parité de C donné par :

$$C = \{x \in \mathbb{F}_q^n, Hx^{\perp} = 0\}.$$

Définition 1.2.6 (Distance de Hamming) *La distance de Hamming de deux mots x et y de longueur fixe est*

$$d(x, y) = |\{i|1 \leq i \leq n, x_i \neq y_i\}|.$$

Définition 1.2.7 (Support d´un mot) *Le support d´un mot code $c = (c_1, c_2, \cdots, c_n) \in \mathbb{F}_q^n$ est défini comme suit :*

$$supp(c) = \{i|1 \leq i \leq n, c_i \neq 0\}.$$

Définition 1.2.8 (Poids de Hamming) *Le poids de Hamming d´un mot est le cardinal de son support. On notera $w(x)$ le poids de Hamming d´un mot x, alors on a :*

$$pour\ tout\ \ x, y \in \mathbb{F}_q^n, d(x,y) = w(x-y).$$

Sur les codes définis sur les corps finis, nous utiliserons seulement la distance de Hamming.

Définition 1.2.9 (Distance minimale) *La distance minimale d d´un code est le plus petit poids non nul de tous ces mots codes.*

1.2.2 Bornes sur les codes

Plusieurs théorèmes d´existence et non-existence des bornes sont connus, mais la borne exacte est en fait toujours un problème ouvert.

Nous avons introduit certains paramètres d´un code linéaire dans cette section. Dans la théorie du codage, un des problèmes les plus fondamentaux est de trouver la meilleure valeur d'un paramètre lorsque d´autres paramètres ont été donnés. Dans cette partie, nous discutons certaines bornes sur les paramètres de code.

Dans la borne suivante nous donnons la distance minimale et maximale d´un code avec une longueur et une dimension donnée. Cette borne est appelée borne de Singleton.

Théorème 1.2.10 (Borne de Singleton) *[57] Soit C un $[n,k,d]_d$ code, alors*

$$d \leq n - k + 1.$$

Définition 1.2.11 (Borne de Griesmer) *[57] Si C est un $[n,k,d]_d$ code avec $k > 0$, alors*

$$n \geq \sum_{i=0}^{i=k-1} \lceil \frac{d}{q^i} \rceil. \tag{1.1}$$

Dans les applications pratiques, compte tenu de la longueur et de la distance minimale, les codes qui ont plus de mots code (en d´autres termes, les codes de plus grande taille)

sont souvent préférés. Une question naturelle se pose, quelle est la taille maximale possible d´un code, compte tenu de la longueur et de la distance minimale ?. Notons $A_q(n,d)$ le nombre maximal de mots code dans un code sur $\mathbb{F}_q$ (qui peut être linéaire ou non linéaire) de longueur n et de distance minimale d. Le nombre maximal du mots-code d´un code linéaire est notée $B_q(n,d)$. Il est clair que $B_q(n,d) \leq A_q(n,d)$. Ce qui suit est bien connu par la borne supérieure pour $A_q(n,d)$.

Définition 1.2.12 (Borne de Hamming) *Le nombre de vecteurs dans* $B_t(x) = \{y \in \mathbb{F}_q^n, d(x,y) \leq t\}$ *la boule de rayon* $t = \lfloor \frac{d-1}{2} \rfloor$ *autour d´un vecteur donné* $x \in \mathbb{F}_q^n$ *est égale à* $V_q(n,t)$, *où*

$$V_q(n,t) = \sum_{i=0}^{t} \left(\begin{array}{c} n \\ i \end{array} \right) (q-1)^i . \tag{1.2}$$

Définition 1.2.13 (Borne de Gilbert)

$$log_q(A_q(n,d)) \geq n - log_q(V_q(n,d-1)). \tag{1.3}$$

Définition 1.2.14 (Rayon de recouvrement) *Le rayon de recouvrement* $r(C)$ *d´un code* C *de longueur* n *sur* $\mathbb{F}_q$ *est défini par :*

$$r(C) = max_{x \in \mathbb{F}_q^n} \{min_{y \in C} d(x,y)\}. \tag{1.4}$$

1.2.3 Propriétés d´un code

On note par $[n, M, d]_q$ un code C de longueur n, de cardinal M et de distance minimale d. Un code linéaire $[n, k, d]_q$ est un code linéaire de longueur n, de dimension k et de distance minimale d. On a l´égalité $|M| = q^k$.

Définition 1.2.15 (Isométrie linéaire) *Soit* $\mathbb{F}_q$ *un corps fini et* d *la distance de Hamming définie sur* $\mathbb{F}_q^n$. *Une isométrie, est une application linéaire*

$$f \ : \ \mathbb{F}_q^n \ \longrightarrow \ \mathbb{F}_q^n$$

qui est une isométrie pour d.

Théorème 1.2.16 *Soit* $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ *une application. Les assertions suivantes sont équivalentes :*

1. *f est une isométrie linéaire.*
2. *Il existe une permutation $\sigma \in S_n$ et des scalaires non nuls $\alpha_1, \alpha_2, \cdots, \alpha_n$ tels que pour tout $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_q^n$, on a :*

$$f(x_1, x_2, \cdots, x_n) = (\alpha_1 x_{\sigma(1)}, \alpha_2 x_{\sigma(2)}, \cdots, \alpha_n x_{\sigma(n)}) \tag{1.5}$$

Une application de la forme 1.5 est dite monômiale, si P est la matrice dans la base canonique d´une telle application, alors chaque ligne et chaque colonne de P contient un seul coefficient non nul.

Définition 1.2.17 (Codes équivalents) *Deux codes linéaires C et C' de longueur n sur $\mathbb{F}_q$ sont dit équivalents, s´il existe une isométrie linéaire f de $\mathbb{F}_q^n$ telle que $f(C) = C'$.*

Remarque 1.2.18 *Deux codes linéaires équivalents ont les mêmes propriétés métriques et les mêmes propriétés linéaires.*

1.3 Codes dérivés

Dans cette partie, nous discutons certaines méthodes classiques de construction de nouveaux codes en utilisant des codes connus. Il existe d´autres constructions, on pourrait également combiner des codes entre eux (exp. les codes concaténés, les codes produits, les turbo-codes).

Soit C un code linéaire de paramètres $[n, k, d]$.

Définition 1.3.1 (Produit sur $\mathbb{F}_q$) *Par analogie avec le produit scalaire usuel ,on définit un produit sur $\mathbb{F}_q^n$, pour $x, y \in \mathbb{F}_q^n$ on a :*

$$x \cdot y = \sum_{i=1}^{i=n} x_i y_i.$$

Définition 1.3.2 (Code dual) *Le dual de C est l´orthogonal $C^{\perp}$ de C dans $\mathbb{F}_q^n$.*

Exemple 1.3.3 *Sur $\mathbb{F}_2$ si :*

$$C = \{000, 111\}$$

alors,

$$C^{\perp} = \{000, 011, 110, 101\}.$$

Remarque 1.3.4 *$C^{\perp}$ est un code linéaire de paramètres $[n, n-k, d']$, et on a l´égalité*

$$dim(C) + dim(C^{\perp}) = n.$$

Définition 1.3.5 (Auto-dual) *Le code C est auto-dual si $C = C^{\perp}$.*

Définition 1.3.6 (Auto-orthogonal) *Le code C est auto-orthogonal si $C \subset C^{\perp}$.*

Définition 1.3.7 (Matrice de parité) *Une matrice de parité de C est une matrice, notée généralement H, de type $(n-k, n)$ dont les lignes forment une base de $C^{\perp}$. Il s´agit d´une matrice génératrice de $C^{\perp}$.*

Définition 1.3.8 (Code de répétition) *Le code de répétition sur $\mathbb{F}_q$ de longueur n est constitué de tous les mots sous forme $c = (c, c, \cdots, c)$ avec $c \in \mathbb{F}_q$. Ceci est un code linéaire de dimension 1 et distance minimale n.*

Remarque 1.3.9 *Le code de répétition de longueur n à une matrice génératrice*

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix}.$$

1.3.1 Construction des nouveaux codes à partir des anciens

Définition 1.3.10 (Code étendu) *Le code étendu $\widehat{C}$ d´un code q-aire C défini est :*

$$\widehat{C} = \{(c_1, \cdots, c_n, c_{n+1} = -\sum_{i=1}^{i=n} c_i), (c_1, \cdots, c_n) \in C\}$$

Remarque 1.3.11 *Pour $q = 2$, la dernière coordonnée de C est celle du bit de parité. Le code $\widehat{C}$ est linéaire, et admet comme paramètres $[n+1, k, \widehat{d}]$ avec $\widehat{d} = d$ ou $\widehat{d} = d+1$, dans le cas binaire, si d est impaire alors $\widehat{d} = d+1$.*

Il faut noter que si nous étendons un code puis éliminons la nouvelle coordonnée, nous finissons d´obtenir le code originale.

Soit Θ un ensemble de cardinal n, nous indexons les coordonnées des mots de $\mathbb{F}_q^n$ par cet ensemble, par exemple, $x = (x_\sigma)_{\sigma\in\Theta}$.

Définition 1.3.12 (Code poinçonné) *Le code poinçonné de C en I est composé de tous les mots code de C avec les coordonnées indexées par I remplaçées par zéros où I est un sous-ensemble de Θ.*

Définition 1.3.13 (Code de Hamming) *Soit $n = \dfrac{q^r-1}{q-1}$. Soit $H_r(q)$ une matrice de taille $r\times n$ sur $\mathbb{F}_q$ avec des colonnes non nulles, de sorte que deux colonnes sont dépendantes. Le code $\mathcal{H}_r(q)$ admet $H_r(q)$ comme matrice de contrôle de parité est appelé q-aire code de Hamming. Le code qui admet $H_r(q)$ comme matrice génératrice est appelé q-aire code simplexe, et est désigné par $\mathcal{S}_r(q)$.*

Remarque 1.3.14 *Soit $r \geq 2$. Alors le code de Hamming $\mathcal{H}_r(q)$ a des paramètres $[n = \dfrac{q^r-1}{q-1}, k = \dfrac{q^r-1}{q-1} - r, d = 3]$.*

Exemple 1.3.15 *Considérons le code de Hamming ternaire $\mathcal{H}_3(3)$ de dimension 3 et de longueur 13 admet comme matrice de contrôle de parité :*

$$H_3(3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 1 \end{bmatrix}$$

Définition 1.3.16 (Code simplexe) *Les duaux des codes de Hamming sont appelés codes simplexes sur $\mathbb{F}_q$ des paramètres $[\dfrac{q^r-1}{q-1}, r]$, et tous les mots code non nuls ont un poids constant égal à q^{r-1}.*

Nous donnons maintenant une construction des codes simplexes binaires. Soit $H_2(2)$ donnée par :

$$H_2(2) = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Pour $r \geq 3$, on définit $H_r(2)$ par récurrence :

$$H_r(2) = \left[\begin{array}{c|c|c} 0 \cdots 0 & 1 & 1 \cdots 1 \\ \hline & 0 & \\ H_{r-1}(2) & \vdots & H_{r-1}(2) \\ & 0 & \end{array}\right].$$

Définition 1.3.17 (Juxtaposition des Codes) *Soient C_1 est un $[n_1, k, d_1]$ code et C_2 un $[n_2, k, d_2]$ code avec G_1 et G_2 sont des marices génératrices de C_1 et C_2, respectivements. La juxtaposition des codes C_1 et C_2 est le code qui admet comme matrice génératrice*

$$G = \begin{bmatrix} G_1 & G_2 \end{bmatrix} \tag{1.6}$$

1.4 Conclusion

Dans ce chapitre nous avons donné des notions de base sur les codes correcteurs définis sur les corps finis, cela sera util pour étudier un cas particulier de ces codes qui sont les codes simplexes sur certains anneaux finis.

Chapitre 2

Les codes sur différents anneaux spéciaux, principalement commutatifs, ont été la cible des chercheurs depuis deux décennies, l´intérêt grandissant de ces codes est mesuré par la possibilité d´avoir le lien entre ces derniers et des codes sur les corps finis via une application particulières généralement connus par le Gray map.

Dans ce qui suit, on donne quelques définitions nécessaires de certain type de code sur les anneaux finis et leurs propriétés pour la meilleur compréhension du reste, pour plus de détails (voir l´annexe).

Définition 2.0.1 *Soit $\mathcal{R}$ un anneau fini, un code linéaire C de longueur n sur $\mathcal{R}$ est un sous-module du $\mathcal{R}$-module de $\mathcal{R}^n$, Qui peut être libre ou pas. Les vecteurs de C sont appelés les mots du code C.*

On munit $\mathcal{R}^n$ du produit suivant : $v.w = \sum v_i w_i$. Le code dual $C^\perp$ de C est défini par

$$C^\perp = \{v \in \mathcal{R}^n \mid v \cdot w = 0;\ \forall w \in C\}.$$

Si $C \subset C^\perp$, on dit que le code C est auto-orthogonal, et si $C = C^\perp$, on dit que le code C est auto-dual.

2.1 Les poids et distances sur l´anneau de Galois $\mathbb{Z}_q$

Soit C un code linéaire sur l´anneau de Galois $\mathbb{Z}_q$ de longueur n, où q est une puissance d´un nombre premier p, alors on peut associer au vecteur $x = (x_1, x_2, \cdots, x_n)$ différents

poids et différentes distances autres que le poids et la distance de Hamming. On a déjà défini le poids de Hamming $w_{Ham}(x)$ comme étant le nombre de composantes non nulles de x.

Le poids Euclidien :

$$wt_E(x) = \sum_{i=1}^{n} min\{x_i^2, (q - x_i^2)\} \tag{2.1}$$

Le poids de Lee :

$$wt_{Lee}(x) = \sum_{i=1}^{n} min\{|x_i|, |(q - x_i)|\} \tag{2.2}$$

De même pour la distance, on définit ces trois distances

La distance de Hamming :

$$d_{Ham}(x, y) = w_{Ham}(x - y)$$

La distance de Lee :

$$d_{Lee}(x, y) = w_{Lee}(x - y)$$

La distance Euclidienne :

$$d_E(x, y) = w_E(x - y)$$

La distance homogène :

$$d_{hom}(x, y) = w_{hom}(x - y)$$

Les définitions suivantes donnent les distributions de poids de Hamming, Lee, et homogène.

Définition 2.1.1 *les distributions de poids d`un code C, est le nombre des mots code de poids i dans C et noté par $A_{wt}(i)$.*

Définition 2.1.2 *[38] Pour tous* $1 \leq i \leq n$*, soient* $A_{Ham}(i)$*,* $A_{Lee}(i)$ *et* $A_{hom}(i)$*, les distributions de poids de* C *de Hamming, Lee et homogène, respectivement, d`un code sur* $\mathcal{R}$*. Alors on a :*

$$(A_{Ham}(0), A_{Ham}(1), \cdots, A_{Ham}(n)),$$
$$(A_{Lee}(0), A_{Lee}(1), \cdots, A_{Lee}(n)),$$
$$et$$
$$(A_{hom}(0), A_{hom}(1), \cdots, A_{hom}(n)),$$

2.2 Codes linéaires sur l´anneau $\mathbb{Z}_4$

Un code linéaire sur $\mathbb{Z}_4$ de longueur n est un sous-groupe additif de $\mathbb{Z}_4^n$. Un tel sous groupe est un sous-module de $\mathbb{Z}_4$, qui peut être libre ou pas.

Définition 2.2.1 *Un* $\mathbb{Z}_4$*-module* M *est libre, s´il existe un sous ensemble* B *de* M *tel que chaque élément de* M *peut être exprimé sous forme de* $\mathbb{Z}_4$ *combinaison linéaire d´éléments de* B*.*

Exemple 2.2.2 *Si* v *est un vecteur de* $\mathbb{Z}_4^n$ *de composantes égale à* 0 *ou* 2*, alors*

$$2v = 0,$$

ce qui implique qu´un tel vecteur ne peut pas être un vecteur de base d´un module libre de $\mathbb{Z}_4$*.*

On peut montrer que l´ensemble des mots suivants de $\mathbb{Z}_4$ *est un code linéaire sur* $\mathbb{Z}_4$ *de longueur* 4 *:*

$$0000 \quad 1113 \quad 2222 \quad 3331 \quad 0202 \quad 1311 \quad 2020 \quad 3133$$
$$0022 \quad 1131 \quad 2200 \quad 3313 \quad 0220 \quad 1333 \quad 2002 \quad 3111.$$

C´est un sous groupe additif de $\mathbb{Z}_4^4$*. Si c´est un* $\mathbb{Z}_4$*-module libre, alors, il existe une base de deux vecteurs* b_1 *et* b_2 *ayant au moins une composante égale à* 1 *ou* 3*. Tous les mots avec une composante égale à* 1 *ou* 3 *vérifient*

$$2b_1 = 2b_2 = 2222.$$

Alors $\{b_1, b_2\}$ *ne peuvent pas former une base ce qui implique que* C *n´est pas libre. Cependant on peut démontrer que tout mot de* C *peut s´écrire sous la forme*

$$xc_1 + yc_2 + zc_3$$

avec

$$c_1 = 1113,\ c_2 = 0202,\ c_3 = 0022,\ x \in \mathbb{Z}_4,\ y \text{ et } z \in \mathbb{Z}_2.$$

2.2.1 Matrice génératrice

Soit C le code de $\mathbb{Z}_4$ donné par l´exemple 1, on peut démontrer que

$$G = \begin{bmatrix} 1 & 1 & 1 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix},$$

est une matrice génératrice de C, dans le sens où tout mot de C peut s´écrire comme étant $(xyz)G$ pour certains $x \in \mathbb{Z}_4$, y *et* $z \in \mathbb{Z}_2$. Tout mot de C peut s´écrire sous la forme

$$\sum_{i=1}^{k_1} a_i c_i + \sum_{i=k_1}^{k_1+k_2} b_i c_i$$

avec $a_i \in \mathbb{Z}_4$ pour $1 \leq i \leq k_1$ et $b_i \in \mathbb{Z}_2$ pour $k_1 + 1 \leq i \leq k_1 + k_2$. En plus chaque c_i admet une composante égale à 1 ou 3 pour $1 \leq i \leq k_1$ et tout c_i est égale à 0 ou 2 pour $k_1 + 1 \leq i \leq k_1 + k_2$. Si $k_2 = 0$, le code C est un $\mathbb{Z}_4$-module libre.

Définition 2.2.3 *La matrice qui admet pour ligne* c_i *pour* $1 \leq i \leq k_1 + k_1$ *est appelée matrice génératrice de* C*. Le code* C *admet* $4^{k_1}2^{k_2}$ *mots et il est dit de type* $4^{k_1}2^{k_2}$*.*

Toute matrice d´un code linéaire sur $\mathbb{Z}_4$ peut être s´exprimer sous la forme

$$G = \begin{bmatrix} I_{k_1} & A & B_1 + 2B_2 \\ 0_{k_2 \times k_1} & 2I_{k_2} & 2C \end{bmatrix}$$

avec A, B_1,B_2 et C sont des matrice à coefficients dans $\mathbb{Z}_2$, et $0_{k_2 \times k_1}$ est une matrice nulle de taille $k_2 \times k_1$. Le code C est de type $4^{k_1}2^{k_2}$.

Théorème 2.2.4 *Tout code linéaire sur $\mathbb{Z}_4$ est équivalent à un code avec une matrice génératrice sous sa forme standard.*

2.2.2 Dual d´un code sur $\mathbb{Z}_4$

Il existe un produit scalaire modulo 4 sur $\mathbb{Z}_4$ défini par

$$x.y = \sum_{i=1}^{i=n} x_i y_i \ (mod\ 4)$$

où $x = (x_1, \cdots, x_n)$ et $y = (y_1, \cdots, y_n)$.

Définition 2.2.5 *Le code dual de C est définie par*

$$C^{\perp} = \{x \in \mathbb{Z}_4^n |\ x.c = 0 \ pour\ tout\ c \in C\}.$$

Définition 2.2.6 *Un $\mathbb{Z}_4$-linéaire est un code auto-orthogonal s´il vérifie $C \subset C^{\perp}$, il est dit auto-dual s´il vérifie $C = C^{\perp}$.*

Si C est un code dans sa forme standard, alors $C^{\perp}$ admet pour matrice génératrice

$$G^{\perp} = \begin{bmatrix} -(B_1 + 2B_2)^t - C^t A^t & C^t & I_{n-k_1-k_2} \\ 2A^t & 2I_{k_2} & 0_{k_2 \times (n-k_1-k_2)} \end{bmatrix}$$

où $0_{k_2 \times (n-k_1-k_2)}$ et la matrice nulle de taille $k_2 \times (n - k_1 - k_2)$. En particulier, $C^{\perp}$ est de type $4^{n-k_1-k_2}2^{k_2}$.

2.2.3 Poids et distances d´un code sur $\mathbb{Z}_4$

Sur $\mathbb{Z}_4$, il existe différents poids pour un vecteur de $\mathbb{Z}_4^n$, donc différentes distances minimales. Soit $x \in \mathbb{Z}_4^n$, supposons que $n_a(x)$ le nombre de composantes de x égale à a pour $a \in \mathbb{Z}_4$.

Le poids de Hamming, le poids de Lee et le poids Euclidien sont respectivement

$$\begin{aligned} wt_{Ham}(x) &= n_1(x) + n_2(x) + n_3(x) \\ wt_{Lee}(x) &= n_1(x) + 2n_2(x) + n_3(x) \\ wt_E(x) &= n_1(x) + 4n_2(x) + n_3(x) \end{aligned}$$

La distance d désigne, la distance de Hamming, Lee et la distance Euclidienne respectivement, alors la distance entre deux mots x et y est donnée par

$$d_d(x, y) = wt_d(x - y)$$

2.2.4 L´image Gray des codes sur $\mathbb{Z}_4$

Les codes quaternaires peuvent être donnés comme des codes binaires sous le Gray map. On définit d´abord l´application :

$$\begin{aligned} \phi \; : \; \mathbb{Z}_4 &\longrightarrow \mathbb{Z}_2^2 \\ 0 &\longmapsto \phi(0) = (0,0) \\ 1 &\longmapsto \phi(1) = (0,1) \\ 2 &\longmapsto \phi(2) = (1,1) \\ 3 &\longmapsto \phi(3) = (1,0), \end{aligned}$$

puis étendue cette application à $\mathbb{Z}_4^n$ dans $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$, on a :

$$\begin{aligned} \Phi \; : \; \mathbb{Z}_4^n &\longrightarrow \mathbb{Z}_2^n \times \mathbb{Z}_2^n \\ (a_1, \cdots, a_n) &\longmapsto ((u_1, \cdots, u_n), (v_1, \cdots, v_n)) \end{aligned}$$

Si $\mathbf{C}$ est un code linéaire quaternaire, alors le code binaire $C = \phi(\mathbf{C})$ est donné comme un code linéaire sur $\mathbb{Z}_4$. La notion du code dual quaternaire d´un code linéaire quaternaire $\mathbf{C}$, est notée par $\mathbf{C}^{\perp}$, ainsi la notion du code dual binaire sur $\mathbb{Z}_4$, est notée par $C_{\perp} = \phi(\mathbf{C}^{\perp})$. Ces derniers sont définis à la façon standard dans [42] et [49].

2.3 Codes sur $\mathbb{Z}_2\mathbb{Z}_4$

Dans cette partie, nous rappelons quelques définitions et concepts reliés aux codes additifs sur $\mathbb{Z}_2\mathbb{Z}_4$. Nous décrivons également leurs paramètres fondamentaux. Les outils de cette partie est un résumé des résultats présentés dans [12], [13] et [64].

Soient $\mathbb{Z}_2$ et $\mathbb{Z}_4$ l´anneau des entiers modulo 2 et 4 respectivement. $\mathbb{Z}_2^n$ est l´ensemble de tous les vecteurs binaires de longueur n, et $\mathbb{Z}_4^n$ est l´ensemble de tous les n-uples sur $\mathbb{Z}_4$, les éléments de $\mathbb{Z}_4^n$ seront ainsi appelés des vecteurs quaternaires de longueur n. N´importe quel sous ensemble non vide C de $\mathbb{Z}_2^n$ est un code binaire, et un sous groupe de $\mathbb{Z}_2^n$ est appelé un code linéaire binaire ou un code linéaire sur $\mathbb{Z}_2$. De la même façon, toute partie non vide $\mathbf{C}$ de $\mathbb{Z}_4^n$ est un code quaternaire, et un sous groupe de $\mathbb{Z}_4^n$ est appelé un code linéaire quaternaire.

2.3.1 le poids de Lee et Euclidien sur $\mathbb{Z}_2\mathbb{Z}_4$

Soient $u \in \mathbb{Z}_2^\gamma$ et $v \in \mathbb{Z}_4^\delta$. On note par $wt_{Ham}(u)$ le poid de Hamming de u, $wt_{Lee}(v)$ et $wt_E(v)$ sont les poids de Lee et Euclidien de v, respectivement, où

$$wt_E(v_i) = \begin{cases} 0 & \text{si} \quad v_i = 0 \\ 1 & \text{si} \quad v_i = 1 \text{ ou } 3 \\ 4 & \text{si} \quad v_i = 2 \end{cases}$$

et

$$wt_{Lee}(v_i) = \begin{cases} 0 & \text{si} \quad v_i = 0 \\ 1 & \text{si} \quad v_i = 1 \text{ ou } 3 \\ 2 & \text{si} \quad v_i = 2. \end{cases}$$

Soit :

$$x = (u, v) \in \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta, \text{ où } u = (u_1, \cdots, u_\gamma) \in \mathbb{Z}_2^\gamma \text{ et } v = (v_1, \cdots, v_\delta) \in \mathbb{Z}_4^\delta.$$

Alors le poid de Lee de x est défini par :

$$wt_{Lee}(x) = wt_{Ham}(u) + wt_{Lee}(v)$$

et le poid Euclidean de x est défini par :

$$wt_E(x) = wt_{Ham}(u) + wt_E(v).$$

2.3.2 Le Gray map sur $\mathbb{Z}_2\mathbb{Z}_4$

Soit $\mathbf{C}$ un code additif sur $\mathbb{Z}_2\mathbb{Z}_4$, qui est un sous groupe de groupe $\mathbb{Z}_2^{\lambda} \times \mathbb{Z}_4^{\mu}$. L´application défini par :

$$\phi \ : \ \mathbb{Z}_2 \times \mathbb{Z}_4 \ \rightarrow \ \mathbb{Z}_2^3 \ , \tag{2.3}$$

est le Gray map sur $\mathbb{Z}_2\mathbb{Z}_4$.

Nous allons prendre une extension de Gray map définie par l´équation (2.3).

$$\Phi \ : \ \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta} \ \rightarrow \ \mathbb{Z}_2^n \ , \text{ avec } n = \gamma + 2\delta,$$

donné par :

$$\Phi(u, v) = (u, \phi(v_1), \ldots, \phi(v_\delta)), \forall\ u \in \mathbb{Z}_2^{\gamma}, \forall\ (v_1, \ldots, v_\delta) \in \mathbb{Z}_4^{\delta}.$$

Ce Gray map est une isométrie qui transforme la distante de Lee définie dans $\mathbf{C}$ un code additif inclus dans $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$ à la distance de Hamming définie dans le code binaire $C = \phi(\mathbf{C})$.

Constatant que la longueur du code binaire C est $n = \gamma + 2\delta$.

2.3.3 Le type d´un code sur $\mathbb{Z}_2\mathbb{Z}_4$

Soit $\mathbf{C}$ un sous-groupe de $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$, il est aussi isomorphe à une structure abélienne comme $\mathbb{Z}_2^{\lambda} \times \mathbb{Z}_4^{\mu}$, toutefois, $\mathbf{C}$ est de type $2^{\lambda}4^{\mu}$ et on à :

$$|\mathbf{C}| = 2^{\lambda+2\mu} \tag{2.4}$$

le nombre des mots codes dans $\mathbf{C}$ d´ordre 2 est $2^{\lambda+\mu}$.

Soient X et Y deux ensembles de $\mathbb{Z}_2$ et $\mathbb{Z}_4$ respectivement, où

$$|X| = \gamma \; et \; |Y| = \delta$$

L´ensemble X correspondant à la première coordonnée γ et Y correspondant à la dernière coordonnée δ.

Nous appelons $\mathbf{C}_X$ (resp., $\mathbf{C}_Y$) le code poinçonné de $\mathbf{C}$ par l´élimination des coordonées en dehors de X (resp., Y). Soit $\mathbf{C}_b$ le sous code de $\mathbf{C}$ qui contient tous les mots-code d´ordre deux, et soit k la dimension de $(\mathbf{C}_b)_X$ qui est un code linéaire binaire pour $\gamma = 0$, et dans ce cas nous allons écrire $k = 0$.

Prenant en considération tous ces paramètres, nous dirons que $\mathbf{C}$ (ou de manière équivalente $C = \Phi(\mathbf{C})$) est de type $(\gamma, \delta; \lambda, \mu; k)$.

On constate que :

(1) $\mathbf{C}_Y$ est un code linéaire quaternaire de type $(0, \delta; \lambda_Y, \mu; 0)$, où $0 \leq \lambda_Y \leq \lambda$

(2) $\mathbf{C}_X$ est un code linéaire binaire de type $(\gamma, 0; \lambda_X, 0; \lambda_X)$, où $k \leq \lambda_X \leq k + \lambda$.

Définition 2.3.1 *Soit* $\mathbf{C}$ *un code additif sur* $\mathbb{Z}_2\mathbb{Z}_4$*, est un sous groupe de* $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$*. Nous disons que l´image binaire* $C = \Phi(\mathbf{C})$ *est un code linéaire sur* $\mathbb{Z}_2\mathbb{Z}_4$ *de longueur* $n = \lambda + 2\mu$ *et de type* $(\gamma, \delta; \lambda, \mu; k)$*, où* λ*,* μ *et* k *sont définis comme ci-dessus.*

Remarque 2.3.2 *Un code linéaire sur* $\mathbb{Z}_2\mathbb{Z}_4$ *est une généralisation de code linéaire binaire et le code linéaire sur* $\mathbb{Z}_4$*.*

1. *Si* $\delta = 0$*,*

   le code binaire $C = \mathbf{C}$ *correspond à un code linéaires binaire.*

2. *Si,* $\gamma = 0$*,*

   le code linéaire sur $\mathbb{Z}_2\mathbb{Z}_4$ *est un code linéaire quaternaire et son code binaire correspondant* $C = \Phi(\mathbf{C})$ *est un code linéaire sur* $\mathbb{Z}_4$*.*

2.3.4 L´équivalence monômiale des codes additifs

Deux codes additifs $\mathbf{C}_1$ et $\mathbf{C}_2$ sur $\mathbb{Z}_2\mathbb{Z}_4$ de type $(\gamma, \delta; \lambda, \mu; k)$ sont considérés équivalents monômialement, si l´un peut être obtenu à partir de l´autre par une permutation des coordonnées, et (si nécessairement) en changeant les signes de certaines coordonnées de $\mathbb{Z}_4$.

Définition 2.3.3 *Deux codes additives sur $\mathbb{Z}_2\mathbb{Z}_4$ sont des équivalents de permutations, s´ils se diffèrent seulement par une permutation des coordonnées*

Proposition 2.3.4 *Si deux codes additifs $\mathbf{C}_1$ et $\mathbf{C}_2$ sur $\mathbb{Z}_2\mathbb{Z}_4$ de type $(\gamma, \delta; \lambda, \mu; k)$ sont équivalents monômialement donc, d´aprés le Gray map les codes additifs linéaires sur $\mathbb{Z}_2\mathbb{Z}_4$ correspondant $C_1 = \Phi(\mathbf{C}_1)$ et $C_2 = \Phi(\mathbf{C}_2)$, sont isomorphes comme des codes binaires.*

Remarque 2.3.5 *l´inverse n´est pas toujours vrai.*

2.3.5 Matrice génératrice d´un code sur $\mathbb{Z}_2\mathbb{Z}_4$

Soit $\mathbf{C}$ un code additif sur $\mathbb{Z}_2\mathbb{Z}_4$. Le code $\mathbf{C}$ n´est pas un module libre, chaque mots-code exprémé uniquement sous la forme :

$$\sum_{i=1}^{\lambda} \zeta_i u^{(i)} + \sum_{j=\lambda+1}^{\lambda+\mu} \eta_j v^{(j)}, \tag{2.5}$$

où $\zeta_i \in \mathbb{Z}_2$ pour $1 \leq i \leq \lambda$, $\eta \in \mathbb{Z}_4$, $\lambda + 1 \leq j \leq \lambda + \mu$, et $u^{(i)}, v^{(j)}$ sont des vecteurs dans $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$ d´ordre deux et d´ordre quatre, respectivement.

Pour les vecteurs $u^{(i)}$ et $v^{(j)}$ on obtient une matrice génératrice $\mathcal{G}$ de taille $(\lambda+\mu)\times(\gamma+\delta)$ de code $\mathbf{C}$. En plus nous pouvons écrire $\mathcal{G}$ comme :

$$\mathcal{G} = \left[\begin{array}{c|c} B_1 & 2B_3 \\ \hline B_2 & Q \end{array}\right], \tag{2.6}$$

où B_1 et B_2 sont des matrices sur $\mathbb{Z}_2$ de taille $\lambda \times \gamma$ et $\mu \times \delta$, respectivement, B_3 est une matrice sur $\mathbb{Z}_4$ de taille $\lambda \times \delta$ avec toutes les entrées dans $\mathbb{Z}_2 \subset \mathbb{Z}_4$, et Q est une matrice sur $\mathbb{Z}_4$ de taille $\mu \times \delta$ avec des vecteurs lignes d´ordre quatre.

Exemple 2.3.6 *Soit* $\mathbf{C}$ *un code additif sur* $\mathbb{Z}_2\mathbb{Z}_4$ *de type* $(1,3;1,2;1)$*, de matrice génératrice :*

$$\mathcal{G} = \left[\begin{array}{c|ccc} 1 & 2 & 2 & 2 \\ \hline 0 & 1 & 1 & 0 \\ 1 & 1 & 2 & 3 \end{array}\right],$$

le code $\mathbf{C}$ *peut être aussi généré par la matrice :*

$$\left[\begin{array}{c|ccc} 1 & 2 & 2 & 2 \\ \hline 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 3 \end{array}\right].$$

2.3.6 Dualité des codes sur $\mathbb{Z}_2\mathbb{Z}_4$

Pour les codes linéaires sur les corps finis, et les anneaux finis, il éxiste un concept de dualité.

Dans cette partie, on va étudier la dualité des codes additifs sur $\mathbb{Z}_2\mathbb{Z}_4$ en utilisant leur structure de groupe abélien.

Nous définissons le produit scalaire des vecteurs $u, v \in \mathbb{Z}_2^{\gamma}\mathbb{Z}_4^{\delta}$ par :

$$\langle u, v\rangle_{\mathbb{Z}_2\mathbb{Z}_4} = 2\left(\sum_{i=1}^{\gamma} u_i v_i\right) + \sum_{j=\gamma+1}^{\gamma+\delta} u_j v_j \in \mathbb{Z}_4. \tag{2.7}$$

Soit $\mathbf{C}$ un code additif sur $\mathbb{Z}_2\mathbb{Z}_4$ de type $(\gamma, \delta; \lambda, \mu; k)$ et soit $C = \Phi(\mathbf{C})$ le code linéaire sur $\mathbb{Z}_2\mathbb{Z}_4$ correspondant. Le code additif orthogonal de $\mathbf{C}$, noté par $\mathbf{C}^{\perp}$ est défini d´une façon standard :

$$\mathbf{C}^{\perp} = \left\{ v \in \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta} \,\middle|\, \langle u, v\rangle_{\mathbb{Z}_2\mathbb{Z}_4} = 0;\ \text{por tout } u \in C \right\}. \tag{2.8}$$

Nous allons appeler $\mathbf{C}^{\perp}$ le code additif dual de $\mathbf{C}$. Le code binaire correspondant $\Phi(\mathbf{C}^{\perp})$ est noté par $C_{\perp}$, il s´appelle code dual de $\mathbf{C}$ sur $\mathbb{Z}_2\mathbb{Z}_4$.

Lemme 2.3.7 *Soient* $\mathbf{C}$ *un code additif sur* $\mathbb{Z}_2\mathbb{Z}_4$ *de type* $(\gamma, \delta; \lambda, \mu; k)$*, et* $\mathbf{C}^{\perp}$ *son code additif dual. Alors,* $|\mathbf{C}||\mathbf{C}^{\perp}| = 2^n$*, où* $n = \gamma + 2\delta$*.*

2.4 Les rayons de recouvrement des codes sur l´anneau $\mathcal{R}$

Dans cette partie, le rayon de recouvrement d´un code C sur $\mathcal{R}$ est introduit. D´abord, nous rappelons la définition du rayon de recouvrement d´un code binaire .

Pour un code binaire C, son rayon de recouvrement $r(C)$ est donné par :

$$r(C) = \max_{u \in \mathbb{Z}_2} \left\{ \min_{c \in C} d_{Ham}(u, c) \right\} \tag{2.9}$$

Cette définition est l´équivalent de dire que le rayon de recouvrement est le plus petit des nombres r telle que les sphères de rayon r autour des mots codes recouvrent $\mathbb{F}_2$. L´extension de cette définition aux codes sur $\mathcal{R}$ est que le rayon de recouvrement d'un code C est le plus petit des nombres r telles que les sphères de rayon r autour les mots codes recouvrent $\mathcal{R}$. Par conséquent, en respectant les distances de Lee et euclidiennes, les rayons de recouvrement d´un code C sur $\mathcal{R}$, sont donnés par :

$$r_{Lee}(C) = \max_{u \in \mathcal{R}^n} \left\{ \min_{c \in C} d_{Lee}(u, c) \right\} \text{ et } r_E(C) = \max_{u \in \mathcal{R}^n} \left\{ \min_{c \in C} d_E(u, c) \right\}, \tag{2.10}$$

respectivement.

Il est clair que $r_{Lee}(C)$ et $r_E(C)$ sont les valeurs minimales r_{Lee} et r_E telles que :

$$\mathcal{R}^n = \cup_{c \in C} S_{r_{Lee}}(c),$$

et

$$\mathcal{R}^n = \cup_{c \in C} S_{r_E}(c),$$

respectivement, où

$$S_{r_{Lee}}(u) = \{v \in \mathcal{R}^n; d_{Lee}(u, v) \leq r_{Lee}\},$$

et

$$S_{r_E}(u) = \{v \in \mathcal{R}^n; d_E(u, v) \leq r_E\},$$

pour $u \in \mathcal{R}^n$.

les résultats suivants sont utiles pour déterminer le rayon de recouvrement des codes sur les anneaux finis. C´est une généralisation du résultat dans [23] pour les codes sur un corps fini.

Proposition 2.4.1 *Si C_0 et C_1 sont des codes sur $\mathcal{R}$ de longueur n_0 et n_1, de distance minimale d_0 et d_1, générés par G_0 et G_1, respectivement, et si C est le code généré par :*

$$G = \left[\begin{array}{c|c} 0 & G_1 \\ \hline G_0 & A \end{array}\right],$$

donc

$$r_d(C) \leq r_d(C_0) + r_d(C_1),$$

est le rayon de recouvrement de la concaténation de C_0 et C_1, noté par C_c, satisfait l´inégalité suivante :

$$r_d(C_c) \geq r_d(C_0) + r_d(C_1)$$

pour toutes les distances d sur $\mathcal{R}$.

Preuve 2.4.2 *Nous définissons la matrice génératrice de C_c comme*

$$\left[\begin{array}{cc} G_0' & G_1 \end{array}\right],$$

alors C_c est un code de longueur $n_0 + n_1$ et de distance minimale d, où

$$d \geq \min\{d_0, d_1\}.$$

D´où le rayon de recouvrement satisfait :

$$r_d(C_c) \geq r_d(C_0) + r_d(C_1).$$

Proposition 2.4.3 *Soient C est un code sur $\mathcal{R}$, et $\Phi(C)$ est l´image de C sous le Gray map, alors :*

$$r_{Lee}(C) = r(\Phi(C)).$$

Dans la cas où $\mathcal{R} = \mathbb{Z}_2\mathbb{Z}_4$

Nous examinons le rayon de recouvrement du code dual de code sur $\mathbb{Z}_2\mathbb{Z}_4$.

Les résultats suivants, donnés par Aoki et al. dans [4, Proposition 3.2] pour les codes sur $\mathbb{Z}_4$ sont encore valides pour les codes sur $\mathbb{Z}_2\mathbb{Z}_4$. Cela est vérifié, en utilisant la définition du rayon de recouvrement, et par le fait que le Gray map Φ est une application préservant le poids [20].

Soit C un code sur $\mathbb{Z}_2\mathbb{Z}_4$ et

$$s\left(C^{\perp}\right) = |\left\{i;\, A_i\left(C^{\perp}\right) \neq 0, i \neq 0\right\}|,$$

où $A_i\left(C^{\perp}\right)$ est le nombre du mots code de poids i dans $C^{\perp}$.

Lemme 2.4.4 *Pour tout code C sur $\mathbb{Z}_2\mathbb{Z}_4$, on a :*

$$r_{Lee}\left(C\right) \leq r_E\left(C\right) \leq 2r_{Lee}\left(C\right).$$

Preuve 2.4.5 *Le résultat est vrai du fait que $d_{Lee}(x,y) \leq d_E(x,y) \leq 2d_{Lee}(x,y)$ pour tous deux vecteurs x et y.*

Delsarte [27] montre que le rayon de recouvrement $r(B)$ d´un code binaire B et le nombre de poids non nuls distincts de la distribution des distances du dualité de B noté par $s(B^{\perp})$,vérifie l´inégalité suivante, connue par la borne de Delsarte

$$r(B) \leq s(B^{\perp}). \tag{2.11}$$

Maintenant, nous étendons la borne de Delsarte aux codes sur $\mathbb{Z}_2\mathbb{Z}_4$ [20].

Théorème 2.4.6 *Soit C un code sur $\mathbb{Z}_2\mathbb{Z}_4$, alors :*

$$r_{Lee}\left(C\right) \leq \left(C^{\perp}\right) \text{ et } r_E\left(C\right) \leq 2s\left(C^{\perp}\right). \tag{2.12}$$

Preuve 2.4.7 *Les distributions de poids de $\Phi(C)$ et $\Phi(C^{\perp})$ sont liées par la transformation de MacWilliams binaire. C´etait prouvé pour les codes sur $\mathbb{Z}_4$. Pour les codes sur $\mathbb{Z}_2\mathbb{Z}_4$, il est possible de voir [26]. Et aprés le résultat est obtenu de la transformation de MacWilliams , lemme 2.4.4, et du fait que n´importe quel code sur $\mathbb{Z}_2\mathbb{Z}_4$ est une distance-invariante.*

2.5 Conclusion

L´objectif de ce chapitre est l´étude générale des codes additifs sur $\mathbb{Z}_2\mathbb{Z}_4$ et des codes additifs linéaires sur $\mathbb{Z}_2\mathbb{Z}_4$ correspondants. Nous avons définis les matrices génératrices des codes additifs sur $\mathbb{Z}_2\mathbb{Z}_4$, ainsi que le concept de la dualité des codes additifs sur $\mathbb{Z}_2\mathbb{Z}_4$ qui définissent le produit scalaire approprié.

Chapitre 3

Codes simplexes et code de MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$

Dans ce chapitre, nous définissons les codes simplexes et les codes de MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$. Ce-ci sont des généralisations des codes simplexes binaires. De plus, nous étudions l´image binaire de ces codes et nous prouvons que l´image binaire des codes simplexes de type β atteint la borne de Gilbert [20].

3.1 Le rayon de recouvrement d´un code de répétition en bloc sur $\mathbb{Z}_2\mathbb{Z}_4$

Pour déterminer les rayons de recouvrements des codes simplexes et des codes de MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$, nous construisons d´abord certaines classes de code en blocs sur $\mathbb{Z}_2\mathbb{Z}_4$ et la méthode utilisée dans [63] pour obtenir leur rayon de recouvrement.

Le code de répétition en bloc sur $\mathbb{Z}_2\mathbb{Z}_4$

Le code de répétition en bloc C^n sur $\mathbb{Z}_2\mathbb{Z}_4$ est un code additif sur $\mathbb{Z}_2\mathbb{Z}_4$ de longueur $n = \sum_{j=1}^{7} n_j$ et de matrice génératrice :

$$G = \left[\overbrace{01\cdots01}^{n_1} \overbrace{02\cdots02}^{n_2} \overbrace{03\cdots03}^{n_3} \overbrace{10\cdots10}^{n_4} \overbrace{11\cdots11}^{n_5} \overbrace{12\cdots12}^{n_6} \overbrace{13\cdots13}^{n_7} \right].$$

Si pour i fixé avec $1 \leq i \leq 7$ nous avons pour tout $1 \leq j \neq i \leq 7$, $n_j = 0$, le code $C^n = C^{n_i}$ noté par C_i.

Exemple 3.1.1 *Pour $i = 1$, nous avons :*

$$C_1 \;=\; \{(00\cdots00), (01\cdots01), (02\cdots02), (03\cdots03)\},$$

un code additif de longueur $n = n_1$ généré par :

$$G_1 \;=\; [0101\cdots01].$$

Les théorèmes suivants donnent les rayons de recouvrement des codes de répétition en blocs C_j, $1 \leq j \leq 7$.

Théorème 3.1.2 *le rayon de recouvrement de C_j, $1 \leq j \leq 7$, par rapport au poids euclidien est donné par :*

(i) $r_E(C_1) = r_E(C_3) \leq \dfrac{5n}{2}$,

(ii) $r_E(C_2) \leq \dfrac{3n}{2}$,

(iii) $r_E(C_4) \leq \dfrac{9n}{2}$,

(iv) $n \leq r_E(C_5) = r_E(C_7) \leq 2n$,

(v) $r_E(C_6) \leq \dfrac{5n}{2}$.

Preuve 3.1.3 *Pour $c \in C_j$, $1 \leq j \leq 7$, soit $t_i(c)$, $0 \leq i \leq 7$ le nombre d´occurrences de symbole i dans le mots-code c. Pour démontrer ce théorème il suffit de démontrer (iv), on à :*

$$r_E(C_j) = \max_{x \in (\mathbb{Z}_2\mathbb{Z}_4)^n} \{d_E(x, C_j; 1 \leq j \leq 7)\}.$$

Soit $x \in (\mathbb{Z}_2\mathbb{Z}_4)^n$, *si* x *est donné par* $(t_0, t_1, t_2, t_3, t_4, t_5, t_6, t_7)$, *où* $\sum_{j=0}^{7} t_i = n$, *alors*

$d_E\left(x, \overline{00}\right) = n - t_0 + 3t_2 + t_5 + 4t_6 + t_7,$

$d_E\left(x, \overline{03}\right) = n - t_1 + 3t_3 + t_4 + t_6 + 4t_7,$

$d_E\left(x, \overline{02}\right) = n - t_2 + 3t_0 + 4t_4 + t_5 + t_7,$

$d_E\left(x, \overline{01}\right) = n - t_3 + 3t_1 + t_4 + 4t_5 + t_6,$

$d_E\left(x, \overline{10}\right) = n - t_4 + t_1 + 4t_2 + t_3 + 3t_6,$

$d_E\left(x, \overline{13}\right) = n - t_5 + t_0 + t_2 + 4t_3 + 3t_7,$

$d_E\left(x, \overline{12}\right) = n - t_6 + 4t_0 + t_1 + t_3 + 3t_4,$

$d_E\left(x, \overline{11}\right) = n - t_7 + t_0 + 4t_1 + t_2 + 3t_5.$

Par conséquent, $d_E(x, C_5) = \min\{(n - t_0 + 3t_2 + t_5 + 4t_6 + t_7),\ (n - t_1 + 3t_3 + t_4 + t_6 + 4t_7),$ $(n - t_2 + 3t_0 + 4t_4 + 3t_5 + t_7),\ (n - t_3 + 3t_1 + t_4 + 4t_5 + t_6), (n - t_4 + t_1 + 4t_2 + t_3 + 3t_6), n - t_5 + 3t_0 + t_2 + 4t_3 + 3t_7, (n - t_6 + 4t_0 + t_1 + t_3 + 3t_4), (n - t_7 + t_0 + 4t_1 + t_2 + 3t_5)\}$ $\leq \dfrac{8n + 8(t_0 + t_1 + t_2 + t_3 + t_4 + t_5 + t_6 + t_7)}{8}.$

Donc,

$$r_E(C_5) \leq 2n.$$

Si

$$x = \overbrace{00\cdots00}^{\frac{n}{8}}\overbrace{01\cdots01}^{\frac{n}{8}}\overbrace{02\cdots02}^{\frac{n}{8}}\overbrace{03\cdots03}^{\frac{n}{8}}\overbrace{10\cdots10}^{\frac{n}{8}}\overbrace{11\cdots11}^{\frac{n}{8}}\overbrace{12\cdots12}^{\frac{n}{8}}\overbrace{13\cdots13}^{\frac{n}{8}} \in (\mathbb{Z}_2\mathbb{Z}_4)^n,$$

alors,

$d_E\left(x, \overline{00}\right) = d_E\left(x, \overline{01}\right) = d_E\left(x, \overline{02}\right) = d_E\left(x, \overline{03}\right) = d_E\left(x, \overline{10}\right) = d_E\left(x, \overline{11}\right) = d_E\left(x, \overline{12}\right) = d_E\left(x, \overline{13}\right) = \dfrac{n}{16} + 4\left(\dfrac{n}{16}\right) + \dfrac{n}{16} + \dfrac{n}{16} + \dfrac{n}{8} + \dfrac{n}{16} + 4\left(\dfrac{n}{16}\right) + \dfrac{n}{8} = n.$ *Ainsi*

$$r_E(C_5) \geq n,$$

et alors,

$$n \leq r_E(C_5) \leq 2n.$$

Les preuves pour les équations (i), (ii), (iii) *et* (iv) *sont obtenues en utilisant une procédure similaire.*

Théorème 3.1.4 *Le rayon de recouvrement de C_j, $1 \leq j \leq 7$, par rapport au poids de Lee est donné par :*

(i) $r_{Lee}(C_1) = r_{Lee}(C_3) = \dfrac{n}{2}$,

(ii) $r_{Lee}(C_2) = n$,

(iii) $r_{Lee}(C_4) = \dfrac{n}{2}$,

(iv) $r_{Lee}(C_5) = r_{Lee}(C_7) = \dfrac{n}{2}$,

(v) $r_{Lee}(C_6) = \dfrac{n}{2}$.

Preuve 3.1.5 *Pour démontrer ce théorème il suffit de démontrer (iv), l´image Gay du code C_5 est*

$$\Phi(C_5) = \begin{array}{l}\{000\cdots000, 001\cdots001, 011\cdots011, 010\cdots010,\\ 100\cdots100, 101\cdots101, 110\cdots110, 111\cdots111\}\end{array},$$

Par la proposition 2.4.3, on a :

$$r_{Lee}(C_5) = r(\Phi(C_5)) = \frac{n}{2}.$$

Les preuves pour les équations (i), (ii), (iii) et (v) sont obtenues en utilisant une procédure similaire.

Les résultats ci-dessus sont utilisés pour déterminer le rayon de recouvrement de code C^n avec les paramètres

$(n = n_1+n_2+n_3+n_4+n_5+n_6+n_7, 2^3, d_L = 2n, d_E = \min\{(n_1+4n_2+n_3+n_4+2n_5+5n_6+2n_7), (n_1+4n_2+n_3+n_5+4n_6+n_7), (4n_1+n_2+4n_3+4n_5+n_6+4n_7), (n_4+n_5+n_6+n_7), (4n_1+4n_3+n_4+5n_5+n_6+5n_7)\}$.

Théorème 3.1.6 *le rayon de recouvrement du code de répétition en bloc C^n a les propriétés suivantes ;*

$$r_E\left(C^{\sum_{j=1}^{7} n_j}\right) \leq \frac{1}{2}\left[5(n_1+n_3+n_6)+3n_2+9n_4\right]+2(n_5+n_7),$$

et si $n_1 = \cdots = n_7 = n$

$$r_{Lee}\left(C^{7n}\right) = 2n.$$

Preuve 3.1.7 *Par la proposition 2.4.1, le théorème 3.1.2 et le théorème 3.1.4, on a pour* $x = x_1x_2x_3x_4x_5x_6x_7 \in (\mathbb{Z}_2\mathbb{Z}_4)^{\sum_{j=1}^{7} n_j}$ *avec* $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ *donné par*

$$(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7), (b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7), (c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7),$$
$$(d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7), (e_0, e_1, e_2, e_3, e_4, e_5, e_6, e_7), (f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7),$$
$$(g_0, g_1, g_2, g_3, g_4, g_5, g_6, g_7),$$

respectivement, tel que

$$n_1 = \sum_{j=0}^{7} a_j, n_2 = \sum_{j=0}^{7} b_j, n_3 = \sum_{j=0}^{7} c_j, n_4 = \sum_{j=0}^{7} d_j, n_5 = \sum_{j=0}^{7} e_j, n_6 = \sum_{j=0}^{7} f_j, n_7 = \sum_{j=0}^{7} g_j.$$

Alors

$d_E\left(x, \overline{00}\right) = n_1 - a_0 + 3a_2 + a_5 + 4a_6 + a_7 + n_2 - b_0 + 3b_2 + b_5 + 4b_6 + b_7 + n_3 - c_0 + 3c_2 + c_5 + 4c_6 + c_7 + n_4 - d_0 + 3d_2 + d_5 + 4d_6 + d_7 + n_5 - e_0 + 3e_2 + e_5 + 4e_6 + e_7 + n_6 - f_0 + 3f_2 + f_5 + 4f_6 + f_7 + n_7 - g_0 + 3g_2 + g_5 + 4g_6 + g_7,$ *où*

$$\overline{00} = \overbrace{00\cdots0}^{n_1}\overbrace{00\cdots0}^{n_2}\overbrace{00\cdots0}^{n_3}\overbrace{00\cdots0}^{n_4}\overbrace{00\cdots0}^{n_5}\overbrace{00\cdots0}^{n_6}\overbrace{00\cdots00}^{n_7},$$

est le premier vecteur de $C^{\sum_{j=1}^{7} n_j}$.

$d_E\left(x, \overline{y_1}\right) = n_1 - a_3 + 3a_1 + a_4 + 4a_5 + a_6 + n_2 - b_2 + 3b_0 + 4b_4 + b_5 + b_7 + n_3 - c_1 + 3c_3 + c_4 + c_6 + 4c_7 + n_4 - d_4 + d_1 + 4d_2 + d_3 + 3d_6 + n_5 - e_7 + e_0 + 4e_1 + e_2 + 3e_5 + n_6 - f_6 + 4f_0 + f_1 + f_3 + 3f_4 + n_7 - g_5 + g_0 + g_2 + 4g_3 + 3g_7,$ *où*

$$\overline{y_1} = \overbrace{01\cdots0}^{n_1}\overbrace{102\cdots0}^{n_2}\overbrace{203\cdots0}^{n_3}\overbrace{310\cdots1}^{n_4}\overbrace{011\cdots1}^{n_5}\overbrace{112\cdots1}^{n_6}\overbrace{213\cdots13}^{n_7},$$

est le deuxième vecteur de $C^{\sum_{j=1}^{7} n_j}$.

$d_E\left(x, \overline{y_2}\right) = n_1 - a_3 + 3a_1 + a_4 + 4a_5 + a_6 + n_2 - b_2 + 3b_0 + 4b_4 + b_5 + b_7 + n_3 - c_1 + 3c_3 + c_4 + c_6 + 4c_7 + n_4 - d_0 + 3d_2 + d_5 + 4d_6 + d_7 + n_5 - e_3 + 3e_1 + e_4 + 4e_5 + e_6 + n_6 - f_2 + 3f_0 + 4f_4 + f_5 + f_7 + n_7 - g_1 + 3g_3 + g_4 + g_6 + 4g_7,$ *où*

$$\overline{y_2} = \overbrace{01\cdots0}^{n_1}\overbrace{102\cdots0}^{n_2}\overbrace{203\cdots0}^{n_3}\overbrace{300\cdots0}^{n_4}\overbrace{001\cdots0}^{n_5}\overbrace{102\cdots0}^{n_6}\overbrace{203\cdots03}^{n_7},$$

est le troisième vecteur de $C^{\sum_{j=1}^{7} n_j}$.

$d_E(x, \overline{y_3}) = n_1 - a_2 + 3a_0 + 4a_4 + a_5 + a_7 + n_2 - b_0 + 3b_2 + b_5 + 4b_6 + b_7 + n_3 - c_2 + 3c_0 + 4c_4 + c_5 + c_7 + n_4 - d_0 + 3d_2 + d_5 + 4d_6 + d_7 + n_5 - e_2 + 3e_0 + 4e_4 + e_5 + e_7 + n_6 - f_0 + 3f_2 + f_5 + 4f_6 + f_7 + n_7 - g_2 + 3g_0 + 4g_4 + g_5 + g_7$, *où*

$$\overline{y_3} = \overbrace{02\cdots02}^{n_1}\overbrace{00\cdots00}^{n_2}\overbrace{02\cdots02}^{n_3}\overbrace{00\cdots00}^{n_4}\overbrace{02\cdots02}^{n_5}\overbrace{00\cdots00}^{n_6}\overbrace{02\cdots02}^{n_7},$$

est le quatrième vecteur de $C^{\sum_{j=1}^{7} n_j}$.

$d_E(x, \overline{y_4}) = n_1 - a_1 + 3a_3 + a_4 + a_6 + 4a_7 + n_2 - b_2 + 3b_0 + 4b_4 + b_5 + b_7 + n_3 - c_3 + 3c_1 + c_4 + 4c_5 + c_6 + n_4 - d_0 + 3d_2 + d_5 + 4d_6 + d_7 + n_5 - e_1 + 3e_3 + e_4 + e_6 + 4e_7 + n_6 - f_2 + 3f_0 + 4f_4 + f_5 + f_7 + n_7 - g_3 + 3g_1 + g_4 + 4g_5 + g_6$, *où*

$$\overline{y_4} = \overbrace{03\cdots03}^{n_1}\overbrace{02\cdots02}^{n_2}\overbrace{01\cdots01}^{n_3}\overbrace{00\cdots00}^{n_4}\overbrace{03\cdots03}^{n_5}\overbrace{02\cdots02}^{n_6}\overbrace{01\cdots01}^{n_7},$$

est le cinquième vecteur de $C^{\sum_{j=1}^{7} n_j}$.

$d_E(x, \overline{y_5}) = n_1 - a_0 + 3a_2 + a_5 + 4a_6 + a_7 + n_2 - b_0 + 3b_2 + b_5 + 4b_6 + b_7 + n_3 - c_0 + 3c_2 + c_5 + 4c_6 + c_7 + n_4 - d_4 + d_1 + 4d_2 + d_3 + 3d_6 + n_5 - e_4 + e_1 + 4e_2 + e_3 + 3e_6 + n_6 - f_4 + f_1 + 4f_2 + f_3 + 3f_6 + n_4 - g_4 + g_1 + 4g_2 + g_3 + 3g_6$, *où*

$$\overline{y_5} = \overbrace{00\cdots00}^{n_1}\overbrace{00\cdots00}^{n_2}\overbrace{00\cdots00}^{n_3}\overbrace{10\cdots10}^{n_4}\overbrace{10\cdots10}^{n_5}\overbrace{10\cdots10}^{n_6}\overbrace{10\cdots10}^{n_7},$$

est le sixième vecteur de $C^{\sum_{j=1}^{7} n_j}$.

$d_E(x, \overline{y_6}) = n_1 - a_2 + 3a_0 + 4a_4 + a_5 + a_7 + n_2 - b_0 + 3b_2 + b_5 + 4b_6 + b_7 + n_3 - c_2 + 3c_0 + 4c_4 + c_5 + c_7 + n_4 - d_4 + d_1 + 4d_2 + d_3 + 3d_6 + n_6 - e_6 + 4e_0 + e_1 + e_3 + 3e_4 + n_6 - f_4 + f_1 + 4f_2 + f_3 + 3f_6 + n_7 - g_6 + 4g_0 + g_1 + g_3 + 3g_4$, *où*

$$\overline{y_6} = \overbrace{02\cdots02}^{n_1}\overbrace{00\cdots00}^{n_2}\overbrace{02\cdots02}^{n_3}\overbrace{10\cdots10}^{n_4}\overbrace{12\cdots12}^{n_5}\overbrace{10\cdots10}^{n_6}\overbrace{12\cdots12}^{n_7},$$

est le septième vecteur de $C^{\sum_{j=1}^{7} n_j}$.

$d_E(x, \overline{y_7}) = n_1 - a_1 + 3a_3 + a_4 + a_6 + 4a_7 + n_2 - b_2 + 3b_0 + 4b_4 + b_5 + b_7 + n_3 - c_3 + 3c_1 + c_4 + 4c_5 + c_6 + n_4 - d_4 + d_1 + 4d_2 + d_3 + 3d_6 + n_7 - e_5 + 3e_0 + e_2 + 4e_3 + 3e_7 + n_2 -$

$f_6 + 4f_0 + f_1 + f_3 + 3f_4 + n_5 - g_7 + g_0 + 4g_1 + g_2 + 3g_5$, *où*

$$\overline{y_7} = \overbrace{03\cdots}^{n_1}\overbrace{0302\cdots}^{n_2}\overbrace{0201\cdots}^{n_3}\overbrace{0110\cdots}^{n_4}\overbrace{1013\cdots}^{n_5}\overbrace{1312\cdots}^{n_6}\overbrace{1211\cdots 11}^{n_7},$$

est le huitième vecteur de $C^{\sum_{j=1}^{7} n_j}$.

Ainsi :

$$\begin{aligned} r_E\left(C^{\sum_{j=1}^{7} n_j}\right) \leq\ & \frac{8n_1 + 4(a_0 + a_1 + a_2 + a_3) + 12(a_4 + a_5 + a_6 + a_7)}{8} \\ & + \frac{8n_3 + 4(c_0 + c_1 + c_2 + c_3) + 12(c_4 + c_5 + c_6 + c_7)}{8} \\ & + \frac{8n_6 + 4(f_0 + f_1 + f_2 + f_3) + 12(f_4 + f_5 + f_6 + f_7)}{8} \\ & + \frac{8n_2 + 8(b_0 + b_2 + b_5 + b_7) + 16(b_4 + b_6)}{8} \\ & + \frac{8n_4 - 4(d_0 + d_4) + 4(d_1 + d_3 + d_5 + d_7) + 28(d_1 + d_6)}{8} \\ & + \frac{8n_5 + 8(e_0 + e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + e_7)}{8} \\ & + \frac{8n_5 + 8(g_0 + g_1 + g_2 + g_3 + g_4 + g_5 + g_6 + g_7)}{8}. \end{aligned}$$

$$\begin{aligned} r_E\left(C^{\sum_{j=1}^{7} n_j}\right) \leq\ & \frac{8n_1 + 12(a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7)}{8} \\ & + \frac{8n_3 + 12(c_0 + c_1 + c_2 + c_3 + c_4 + c_5 + c_6 + c_7)}{8} \\ & + \frac{8n_6 + 12(f_0 + f_1 + f_2 + f_3 + f_4 + f_5 + f_6 + f_7)}{8} \\ & + \frac{8n_2 + 4(b_0 + b_1 + b_2 + b_3 + b_4 + b_5 + b_6 + b_7)}{8} \\ & + \frac{8n_4 + 28(d_0 + d_1 + d_2 + d_3 + d_4 + d_5 + d_6 + d_7)}{8} \\ & + \frac{8n_5 + 8(e_0 + e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + e_7)}{8} \\ & + \frac{8n_5 + 8(g_0 + g_1 + g_2 + g_3 + g_4 + g_5 + g_6 + g_7)}{8}. \end{aligned}$$

Par conséquent :

$$r_E\left(C^{\sum_{j=1}^{7} n_j}\right) \leq \frac{1}{2}\left[5(n_1 + n_3 + n_6) + 3n_2 + 9n_4\right] + 2(n_5 + n_7).$$

Pour la deuxième partie, nous avons $\Phi(C^{7n})$*, l´ensemble donné par :*

$$\{000\cdots000000\cdots000000\cdots000000\cdots000000\cdots000000\cdots000000\cdots000,$$
$$001\cdots001011\cdots011010\cdots010100\cdots100101\cdots101111\cdots111110\cdots110,$$
$$001\cdots001011\cdots011010\cdots010000\cdots000001\cdots001011\cdots011010\cdots010,$$
$$011\cdots011001\cdots001011\cdots011000\cdots000011\cdots011001\cdots001011\cdots011,$$
$$010\cdots010011\cdots011001\cdots001000\cdots000010\cdots010100\cdots100001\cdots001,$$
$$000\cdots000000\cdots000000\cdots000100\cdots100100\cdots100100\cdots100100\cdots100,$$
$$011\cdots011000\cdots000011\cdots011100\cdots100111\cdots111100\cdots100111\cdots111,$$
$$010\cdots010011\cdots011001\cdots001100\cdots100110\cdots110111\cdots111101\cdots101\}.$$

Alors :

$$r_{Lee}(C^{7n}) = r(\Phi(C^{7n})) = 2n.$$

3.2 Les codes simplexes de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$

Dans cette partie, nous prenons en considération la construction des codes simplexes de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$.

3.2.1 Les codes simplexes de type α

Soit $m^{\alpha}_{2,k}$ la matrice génératrice de $S^{\alpha}_{2,k}$, le code simplexe binaire de type α, est défini par :

$$m^{\alpha}_{2,k} = \left[\begin{array}{c|c} 00\cdots0 & 11\cdots1 \\ \hline m^{\alpha}_{2,k-1} & m^{\alpha}_{2,k-1} \end{array}\right], \quad \text{pour } k \geq 2,$$

où

$$m^{\alpha}_{2,1} = \left[\begin{array}{cc} 0 & 1 \end{array}\right].$$

Dans [16], les codes simplexes $S^{\alpha}_{4,k}$ de type α sur $\mathbb{Z}_4$ étaient définis. la matrice génératrice $G^{\alpha}_{4,k}$ de $S^{\alpha}_{4,k}$ est

$$G^{\alpha}_{4,k} = \left[\begin{array}{c|c|c|c} 00\cdots0 & 11\cdots1 & 22\cdots2 & 33\cdots3 \\ \hline G^{\alpha}_{4,k-1} & G^{\alpha}_{4,k-1} & G^{\alpha}_{4,k-1} & G^{\alpha}_{4,k-1} \end{array}\right], \quad \text{pour } k \geq 2,$$

où

$$G_{4,1}^{\alpha} = \left[\begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \right].$$

En utilisant les deux matrices précédentes, on a pu construire un nouveau code, et établir une étude complète sur les propriétés algébriques nécéssaires.

Construisons S_k^{α} le code simplexe de type α sur $\mathbb{Z}_2\mathbb{Z}_4$, à partir de la concaténation de 2^{2k} copies de la matrice génératrice de $S_{2,k}^{\alpha}$ et 2^k copies de la matrice génératrice de $S_{4,k}^{\alpha}$ donnée par :

$$\Theta_k^{\alpha} = \left[\begin{array}{c|c|c|c|c|c|c} m_{2,k}^{\alpha} & m_{2,k}^{\alpha} & \cdots & m_{2,k}^{\alpha} & G_{4,k}^{\alpha} & G_{4,k}^{\alpha} & \cdots & G_{4,k}^{\alpha} \end{array} \right], \quad \text{pour } k \geq 1. \tag{3.1}$$

où la forme standard de Θ_k^{α}, la matrice génératrice de S_k^{α}, est

$$\Theta_k^{\alpha} = \left[\begin{array}{c|c|c|c} 00\ 00\cdots00 & 01\ 01\cdots01 & \cdots & 13\ 13\cdots13 \\ \hline \Theta_{k-1}^{\alpha} & \Theta_{k-1}^{\alpha} & \cdots & \Theta_{k-1}^{\alpha} \end{array} \right], \text{ for} k \geq 2,$$

avec

$$\Theta_1^{\alpha} = \left[\begin{array}{cccccccc} 00 & 01 & 02 & 03 & 10 & 11 & 12 & 13 \end{array} \right].$$

Propriétés algébrique du nouveau code

- La longueur du code simplexe de type α sur $\mathbb{Z}_2\mathbb{Z}_4$ est égal à 2^{3k+1}.
- Le nombre de mots-code est égal à $2^{k_0}4^{k_1}$ pour certains k_0 et k_1.

Exemple 3.2.1 *Dans le cas où $k = 1$ avec $k_0 = 0$ et $k_1 = 1$, on a tous les mots- code du code simplexe S_1^{α} générés par Θ_1^{α}, qui sont :*

00 00 00 00 00 00 00 00,

00 01 02 03 10 11 12 13,

00 02 00 02 00 02 00 02,

00 03 02 01 10 13 12 11.

3.2.2 Les codes simplexes de type β

Construisons le code simplxe S_k^β de type β, à partir de la concaténation de 2^k copies de la matrice génératrice de $S_{2,k}^\beta$ et 2^{k-1} copies de la matrice génératrice de $S_{4,k}^\beta$ définie par :

$$\Theta_k^\beta = \left[\begin{array}{c|c|c|c|c|c|c} m_{2,k}^\beta & m_{2,k}^\beta & \cdots & m_{2,k}^\beta & G_{4,k}^\beta & \cdots & G_k^\beta \end{array} \right], \quad \text{pour } k \geq 2, \tag{3.2}$$

où $m_{2,k}^\beta$ est une matrice génératrice du code simplexe binaire de type β définie par :

$$\left[\begin{array}{c|c} 11\cdots1 & 00\cdots0 \\ \hline m_{2,k-1}^\alpha & m_{2,k-1}^\beta \end{array} \right], \quad \text{pour } k \geq 3,$$

avec

$$m_{2,2}^\beta = \left[\begin{array}{c|c} 11 & 0 \\ \hline 01 & 1 \end{array} \right],$$

et $G_{4,k}^\beta$ est une matrice génératrice du code simplexe sur $\mathbb{Z}_4$ de type β définie par :

$$\left[\begin{array}{c|c|c} 11\cdots1 & 00\cdots0 & 22\cdots2 \\ \hline G_{4,k-1}^\alpha & G_{4,k-1}^\beta & G_{4,k-1}^\beta \end{array} \right], \quad \text{pour } k \geq 3,$$

avec

$$G_{4,2}^\beta = \left[\begin{array}{c|c|c} 1111 & 0 & 2 \\ \hline 0123 & 1 & 1 \end{array} \right].$$

Propriétés algébrique du nouveau code

- Le code simplexe S_k^β de type β est le code poinçonné de S_k^α.
- Le nombre de mots code est $2^{k_0}4^{k_1}$ pour certains k_0 et k_1.
- La longueur de ces codes est $2^k(2^{k-2}+1)(2^k-1)$.

3.2.3 Les rayons de recouvrement des codes simplexes de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$

Les théorèmes suivants fournissent les bornes supérieures sur le rayon de recouvrement des codes simplexes sur $\mathbb{Z}_2\mathbb{Z}_4$ par rapport aux poids de Lee et euclidien.

Théorème 3.2.2 *Les bornes supérieurs des rayons de recouvrement des codes simplexes sur $\mathbb{Z}_2\mathbb{Z}_4$ de type α sont donnés par :*

$$r_{Lee}(S_k^\alpha) \leq 3.2^{3k-1} \text{ et } r_E(S_k^\alpha) \leq 2^k \left(\frac{7 \cdot 2^{2k} - 1}{3}\right).$$

Preuve 3.2.3 *Les codes simplexes sur $\mathbb{Z}_2\mathbb{Z}_4$ de type α a un poids de Lee égal à 2^{3k} ou $3 \cdot 2^{3k-1}$. Ainsi à partir de l´équation (2.9), la proposition 2.4.1 et le théorème 3.1.6, on a :*

$$\begin{aligned}
r_{Lee}(S_k^\alpha) &\leq r_{Lee}(2^{2k} S_{2,k}^\alpha) + r_{Lee}(2^k S_{4,k}^\alpha) \\
&\leq 2^{2k} r_{Lee}(S_{2,k}^\alpha) + 2^k r_{Lee}(S_{4,k}^\alpha) \\
&\leq 2^{2k} r_{Ham}(S_{2,k}^\alpha) + 2^k r_{Lee}(S_{4,k}^\alpha) \\
&\leq 2^{2k}\left(2^{k-1}\right) + 2^k\left[\left(3 \cdot 2^{2(k-1)} + 3 \cdot 2^{2(k-2)} + \cdots + 3 \cdot 2^{2\cdot 1}\right) + r_L(S_{4,1}^\alpha)\right] \\
&\leq 2^{3k-1} + 2^k\left[\left(2^{2k} - 1\right) + 1\right] \\
&\leq 2^{3k-1} + 2^k \cdot 2^{2k} \\
&\leq 2^{3k-1} + 2^{3k} \\
&\leqslant 3 \cdot 2^{3k-1}.
\end{aligned}$$

D´où, $r_{Lee}(S_k^\alpha) \leq 3 \cdot 2^{3k-1}$. Des arguments similaires, en utilisant l´équation (2.9), la proposition 2.4.1 et le théorème 3.1.6 on obtient le résultat suivant :

$$\begin{aligned}
r_E(S_k^\alpha) &\leq r_E(2^{2k} S_{2,k}^\alpha) + r_E(2^k S_{4,k}^\alpha) \\
&\leq 2^{2k} r_E(S_{2,k}^\alpha) + 2^k r_E(S_{4,k}^\alpha) \\
&\leq 2^{2k} r_{Ham}(S_{2,k}^\alpha) + 2^k r_E(S_{4,k}^\alpha) \\
&\leq 2^{2k} \cdot 2^{k-1} + 2^k \left(\frac{11\left(2^{2k}-1\right)+9}{6}\right) \\
&\leq 2^k \left[2^{2k-1} + \left(\frac{11\left(2^{2k}-1\right)+9}{6}\right)\right] \\
&\leq 2^k \left(\frac{7 \cdot 2^{2k}-1}{3}\right).
\end{aligned}$$

Les rayons de recouvrement des codes simplexes sur $\mathbb{Z}_2\mathbb{Z}_4$ de type β sont donnés dans le théorème suivant :

Théorème 3.2.4 *Les rayons de recouvrements des codes simplexes sur $\mathbb{Z}_2\mathbb{Z}_4$ de type β sont donnés par :*

(i) $r_{Lee}(S_k^{\beta}) \leq 2^{k-1}\left[(2^{k-1}+1)(2^k-1)-2\right]$,

(ii) $r_E(S_k^{\beta}) \leq 2^{k-1}\left(\frac{14\cdot 2^{2k}-449}{6}\right)$.

Preuve 3.2.5 *D´aprés les équations (3.2), (2.9), la proposition 2.4.1 et le théorème 3.1.6, on a :*

$$\begin{aligned} r_{Lee}(S_k^{\beta}) &\leq r_{Lee}(2^k S_{2,k}^{\beta}) + r_{Lee}(2^{k-1} S_{4,k}^{\beta}) \\ &\leq 2^k r_{Lee}(S_{2,k}^{\beta}) + 2^{k-1} r_{Lee}(S_{4,k}^{\beta}) \\ &\leq 2^k r_{Ham}(S_{2,k}^{\beta}) + 2^{k-1} r_{Lee}(S_{4,k}^{\beta}) \\ &\leq 2^k\left(\tfrac{2^k-1}{2}\right) + 2^{k-1}\left[2^{k-1}\left(2^k-1\right)-2\right] \\ &\leq 2^{k-1}(2^k-1) + 2^{k-1}\left[2^{k-1}\left(2^k-1\right)-2\right] \\ &\leq 2^{k-1}\left[(2^{k-1}+1)(2^k-1)-2\right]. \end{aligned}$$

Des arguments analogues, en utilisant l´équation (2.9), la proposition 2.4.1 et le théorème 3.1.6, donnent ce résultat

$$\begin{aligned} r_E(S_k^{\beta}) &\leq r_E(2^k S_{2,k}^{\beta}) + r_E(2^{k-1} S_{4,k}^{\beta}) \\ &\leq 2^k r_E(S_{2,k}^{\beta}) + 2^{k-1} r_E(S_{4,k}^{\beta}) \\ &\leq 2^k r_{Ham}(S_{2,k}^{\beta}) + 2^{k-1} r_E(S_{4,k}^{\beta}) \\ &\leq 2^k\left(\tfrac{2^k-1}{2}\right) + 2^{k-1}\left[2^k\left(2^{k+1}-1\right) + \tfrac{1}{3}\left(2^{2k}-1\right) - \tfrac{147}{2}\right] \ (since\ r_E(S_2^{\beta}) \leq 25) \\ &\leq 2^{k-1}\left(2^k-1\right) + 2^{k-1}\left[2^k\left(2^{k+1}-1\right) + \tfrac{1}{3}\left(2^{2k}-1\right) - \tfrac{147}{2}\right] \\ &\leq 2^{k-1}\left[2^k\left(2^{k+1}-1\right) + \tfrac{1}{3}\left(2^{2k}-1\right) + \left(2^k-1\right) - \tfrac{147}{2}\right] \\ &\leq 2^{k-1}\left(\tfrac{14\cdot 2^{2k}-449}{6}\right). \end{aligned}$$

Théorème 3.2.6 *Le rayon de recouvrement du code dual de code simplexe de type α et β est donné par :*

$$r_{Lee}(S_k^{\alpha^{\perp}}) = r_{Lee}(S_k^{\beta^{\perp}}) = 1, r_E(S_k^{\alpha^{\perp}}) \leq 2 \ et\ r_{Lee}(S_k^{\beta^{\perp}}) \leq 2.$$

Preuve 3.2.7 *La borne de Delsarte donne $r_{Lee}(S_k^{\alpha^{\perp}}) \leq 1$ et $r_{Lee}(S_k^{\beta^{\perp}}) \leq 1$, de sorte que l´égalité est satisfaite. Les autres inégalités se définissent du lemme 2.4.4.*

Exemple 3.2.8 *Pour $k = 2$, $k_0 = 1$ et $k_1 = 1$, le code simplexe S_2^β a $2^1 4^1 = 8$ mots-code et de longueur 24. La matrice génératrice de S_2^β est donné par :*

$$\Theta_2^\beta = \left[\begin{array}{cccc|cc} 110 & 110 & 110 & 110 & 111102 & 111102 \\ 011 & 011 & 011 & 011 & 012311 & 012311 \end{array}\right].$$

Les mots-code de S_2^β sont :

$$\begin{array}{l} 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00, \\ 00\ 01\ 02\ 03\ 10\ 11\ 12\ 13\ 11\ 11\ 11\ 11, \\ 00\ 02\ 00\ 02\ 00\ 02\ 00\ 02\ 02\ 02\ 02\ 02, \\ 00\ 03\ 02\ 01\ 10\ 13\ 12\ 11\ 13\ 13\ 13\ 13, \\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 00\ 00\ 02\ 02, \\ 11\ 12\ 13\ 10\ 01\ 02\ 03\ 00\ 11\ 11\ 13\ 13, \\ 11\ 13\ 11\ 13\ 11\ 13\ 11\ 13\ 02\ 02\ 00\ 00, \\ 11\ 10\ 13\ 12\ 01\ 00\ 03\ 02\ 13\ 13\ 11\ 11. \end{array}$$

Le rayon de recouvrement du code simplexe S_2^β satisfait :

$$r_{Lee}(S_2^\beta) \leq 14 \text{ et } r_E(S_2^\beta) \leq 25.$$

3.3 Les Codes de MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$

Le code de MacDonald $\mathcal{M}_{k,u}(q)$ sur un corps fini $\mathbb{F}_q$ est le $\left[\frac{q^k-q^u}{q-1}, k, q^{k-1}-q^{u-1}\right]$ −code dont n´importe quel mots-code non nul a un poids soit q^{k-1} ou $q^{k-1}-q^{u-1}$.

Soit $m_{2,k}^\alpha$ (resp., $m_{2,k}^\beta$) la matrice génératrice de $S_{2,k}^\alpha$ (resp., $S_{2,k}^\beta$), pour $1 \leq u \leq k-1$, on définit $m_{2,k,u}^\alpha$ (resp. ; $m_{2,k,u}^\beta$) comme une matrice obtenue à partir de $m_{2,k}^\alpha$ (resp., $m_{2,k}^\beta$), par l´élimination des colonnes correspondantes aux colonnes de $m_{2,u}^\alpha$ et $0_{2^u\times(k-u)}$ (resp., $m_{2,u}^\beta$ et $0_{(2^u-1)\times(k-u)}$), qui est la matrice génératrice de $\mathcal{M}_{2,k,u}^\alpha$ (resp., $\mathcal{M}_{2,k,u}^\beta$), le code de MacDonald binaire de type α (resp., β), donné par :

$$m_{2,k,u}^\alpha = \left[\begin{array}{ccc} m_{2,k}^\alpha & \setminus & \frac{0_{2^u\times(k-u)}}{m_{2,u}^\alpha} \end{array}\right], \quad \text{pour } k \geq 2, \tag{3.3}$$

$$(\text{resp. } m^{\beta}_{2,k,u} = \left[\begin{array}{cc} m^{\beta}_{2,k} & \backslash \quad \frac{0_{(2^u-1)\times(k-u)}}{m^{\beta}_{2,u}} \end{array} \right], \text{ pour } k \geq 3). \tag{3.4}$$

Dans [25], les codes de MacDonald de type α et β sur $\mathbb{Z}_4$ ont été définis en utilisant les matrices génératrices des codes simplexes des types α et β sur $\mathbb{Z}_4$. Pour $1 \leq u \leq k-1$, soit $G^{\alpha}_{4,k,u}$ (resp., $G^{\beta}_{4,k,u}$) la matrice génératrice de $\mathcal{M}^{\alpha}_{4,k,u}$ (resp., $\mathcal{M}^{\beta}_{4,k,u}$), le code de MacDonald de type α (resp., β) sur $\mathbb{Z}_4$ est obtenu de $G^{\alpha}_{4,k}$ (resp., $G^{\beta}_{4,k}$) par l´élimination des colonnes correspondantes aux colonnes de $G^{\alpha}_{4,u}$ et $0_{2^{2u}\times(k-u)}$ (resp., $G^{\beta}_{4,u}$ et $0_{2^{(u-1)}(2^u-1)\times(k-u)}$) est le suivant :

$$G^{\alpha}_{4,k,u} = \left[\begin{array}{cc} G^{\alpha}_{4,k} & \backslash \quad \frac{0_{2^{2u}\times(k-u)}}{G^{\alpha}_{4,u}} \end{array} \right], \text{ pour } k \geq 2, \tag{3.5}$$

$$(\text{resp. } G^{\beta}_{4,k,u} = \left[\begin{array}{cc} G^{\beta}_{4,k} & \backslash \quad \frac{0_{2^{(u-1)}(2^u-1)\times(k-u)}}{G^{\beta}_{4,u}} \end{array} \right], \text{ pour } k \geq 3). \tag{3.6}$$

Maintenant nous construisons $\mathcal{M}^{\alpha}_{k,u}$ et $\mathcal{M}^{\beta}_{k,u}$, les codes de MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$. Soit $\Theta^{\alpha}_{k,u}$, $1 \leq u \leq k-1$, la matrice génératrice du code de MacDonald de type α sur $\mathbb{Z}_2\mathbb{Z}_4$ obtenu par la concaténation de 2^{2k} des copies de la matrice génératrice de $\mathcal{M}^{\alpha}_{2,k,u}$ et 2^k des copies de la matrice génératrice de $\mathcal{M}^{\alpha}_{4,k,u}$. on a, alors :

$$\Theta^{\alpha}_{k,u} = \left[\begin{array}{c|c|c|c|c} m^{\alpha}_{2,k,u} & \cdots & m^{\alpha}_{2,k,u} & G^{\alpha}_{4,k,u} & \cdots & G^{\alpha}_{4,k,u} \end{array} \right], \text{ pour } k \geq 2, \tag{3.7}$$

Pour $k \geq 2$ la matrice $\Theta^{\alpha}_{k,u}$ prend la forme :

$$\left[\begin{array}{c|c} \overbrace{m^{\alpha}_{2,k}\backslash\frac{0_{2^u\times(k-u)}}{m^{\alpha}_{2,u}}\cdots m^{\alpha}_{2,k}\backslash\frac{0_{2^u\times(k-u)}}{m^{\alpha}_{2,u}}}^{2^{2k}} & \overbrace{G^{\alpha}_{4,k}\backslash\frac{0_{2^{2u}\times(k-u)}}{G^{\alpha}_{4,u}}\cdots G^{\alpha}_{4,k}\backslash\frac{0_{2^{2u}\times(k-u)}}{G^{\alpha}_{4,u}}}^{2^k} \end{array} \right],$$

et avec un réarrangement nous obtenons :

$$\left[\begin{array}{c|c} \overbrace{m^{\alpha}_{2,k}\cdots m^{\alpha}_{2,k}}^{2^{2k}}\overbrace{G^{\alpha}_{4,k}\cdots G^{\alpha}_{4,k}}^{2^k} & \overbrace{\backslash\frac{0_{2^u\times(k-u)}}{m^{\alpha}_{2,u}}\cdots\backslash\frac{0_{2^u\times(k-u)}}{m^{\alpha}_{2,u}}}^{2^{2k}}\overbrace{\backslash\frac{0_{2^{2u}\times(k-u)}}{G^{\alpha}_{4,u}}\cdots\backslash\frac{0_{2^{2u}\times(k-u)}}{G^{\alpha}_{4,u}}}^{2^k} \end{array} \right],$$

de sorte que

$$\Theta^{\alpha}_{k,u} = \left[\begin{array}{c|c} \Theta^{\alpha}_{k} & \overbrace{\backslash\frac{0_{2^u\times(k-u)}}{m^{\alpha}_{2,u}}\cdots\backslash\frac{0_{2^u\times(k-u)}}{m^{\alpha}_{2,u}}}^{2^{2k}}\overbrace{\backslash\frac{0_{2^{2u}\times(k-u)}}{G^{\alpha}_{4,u}}\cdots\backslash\frac{0_{2^{2u}\times(k-u)}}{G^{\alpha}_{4,u}}}^{2^k} \end{array} \right], \text{ pour } k \geq 2.$$

Soit $\Theta_{k,u}^{\beta}$, $1 < u \leq k-1$, la matrice génératrice de code de MacDonal de type β sur $\mathbb{Z}_2\mathbb{Z}_4$ obtenue par la concaténation des 2^k copies de matrice génératrice de $\mathcal{M}_{2,k,u}^{\beta}$ et 2^{k-1} des copies de matrice génératrice de $\mathcal{M}_{4,k,u}^{\beta}$. On a :

$$\Theta_{k,u}^{\beta} = \left[\begin{array}{c|c|c|c|c} m_{2,k,u}^{\beta} & \cdots & m_{2,k,u}^{\beta} & G_{4,k,u}^{\beta} & \cdots & G_{4,k,u}^{\beta} \end{array} \right], \text{ pour } k \geq 3, \tag{3.8}$$

Pour $k \geq 3$, la matrice $\Theta_{k,u}^{\beta}$ prend la forme :

$$\left[\begin{array}{c|c} \overbrace{m_{2,k}^{\beta} \backslash \frac{0_{(2^u-1)\times(k-u)}}{m_{2,u}^{\beta}} \cdots m_{2,k}^{\beta} \backslash \frac{0_{(2^u-1)\times(k-u)}}{m_{2,u}^{\beta}}}^{2^k} & \overbrace{G_{4,k}^{\beta} \backslash \frac{0_{2^{(u-1)}(2^u-1)\times(k-u)}}{G_{4,u}^{\beta}} \cdots G_{4,k}^{\beta} \backslash \frac{0_{2^{(u-1)}(2^u-1)\times(k-u)}}{G_{4,u}^{\beta}}}^{2^{k-1}} \end{array} \right],$$

et avec un réarrangement nous obtenons :

$$\Theta_{k,u}^{\beta} = \left[\begin{array}{c|c} \Theta_{k}^{\beta} & \overbrace{\backslash \frac{0_{(2^u-1)\times(k-u)}}{m_{2,u}^{\beta}} \backslash \cdots \frac{0_{(2^u-1)\times(k-u)}}{m_{2,u}^{\beta}} \backslash \frac{0_{2^{(u-1)}(2^u-1)\times(k-u)}}{G_{4,u}^{\beta}} \cdots \backslash \frac{0_{2^{(u-1)}(2^u-1)\times(k-u)}}{G_{4,u}^{\beta}}}^{2^k \quad\quad 2^{k-1}} \end{array} \right].$$

Propriétés algébrique du nouveau code

• Le code de MacDonald $\mathcal{M}_{k,u}^{\alpha}$ (resp., $\mathcal{M}_{k,u}^{\beta}$), de type α (resp., β) sur $\mathbb{Z}_2\mathbb{Z}_4$ a des paramètres $\left[2^{3k+1} - 2^{k+u}\left(2^k + 2^u\right)\right]$ (resp., $[2^k\left(2^{k-2}+1\right)\left(2^k-1\right) - 2^k\left(2^{u-2}+1\right)\left(2^u-1\right)]$),

• Il y a $2^{k_0}4^{k_1}$ mots-code pour chaque k_0 et k_1.

• D´après la définition de Gray map, le poids de Lee minimal du code de MacDonald $\mathcal{M}_{k,u}^{\alpha}$ (resp., $\mathcal{M}_{k,u}^{\beta}$), de type α (resp., β) sur $\mathbb{Z}_2\mathbb{Z}_4$ est $d_{Lee} = 3 \cdot 2^{3k-1} + 2^{k+u}(2^{k-1} - 2^u)$ (resp., $d_{Lee} = 2^{k-1}[(2^{k-1}+1)(2^k-1) - (2^{k+u-1}+1)(2^u-1)]$).

3.3.1 Les rayons de recouvrement des codes de MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$

Les bornes suivantes donnent les rayons de recouvrement des codes de MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$.

Théorème 3.3.1 *Pour $u \leq r \leq k$, les rayons de recouvrement des codes de MacDonald*

de type α sur $\mathbb{Z}_2\mathbb{Z}_4$ sont donnés par :

$$\begin{aligned} r_{Lee}(\mathcal{M}^{\alpha}_{k,u}) &\leq \left[3\cdot 2^{3k-1} - 2^{k+r-1}\left(2^{r+1}+2^k\right)\right] + \left[2^{2k} r_{Ham}(\mathcal{M}^{\alpha}_{2,r,u}) + 2^k r_{Lee}(\mathcal{M}^{\alpha}_{4,r,u})\right] \\ r_{E}(\mathcal{M}^{\alpha}_{k,u}) &\leq \tfrac{1}{3}\left[7\cdot 2^{3k} - 2^{k+r-1}\left(3\cdot 2^k + 11\cdot 2^r\right)\right] + \left[2^{2k} r_{Ham}(\mathcal{M}^{\alpha}_{2,r,u}) + 2^k r_{E}(\mathcal{M}^{\alpha}_{4,r,u})\right] \end{aligned}$$

Preuve 3.3.2 *Pour $u \leq r \leq k$*

$$\begin{aligned} r_{Lee}(\mathcal{M}^{\alpha}_{k,u}) &\leq r_{Lee}(2^{2k}\mathcal{M}^{\alpha}_{2,k,u}) + r_{Lee}(2^k \mathcal{M}^{\alpha}_{4,k,u}) \\ &\leq 2^{2k} r_{Lee}(\mathcal{M}^{\alpha}_{2,k,u}) + 2^k r_{Lee}(\mathcal{M}^{\alpha}_{4,k,u}) \\ &\leq 2^{2k} r_{Ham}(\mathcal{M}^{\alpha}_{2,k,u}) + 2^k r_{Lee}(\mathcal{M}^{\alpha}_{4,k,u}) \\ &\leq \left[2^{2k}\left(2^{k-1}-2^{r-1}\right) + 2^{2k} r_{Ham}(\mathcal{M}^{\alpha}_{2,r,u})\right] + \left[2^k\left(2^{2\cdot k}-2^{2r}\right) + 2^k r_{Lee}(\mathcal{M}^{\alpha}_{2,r,u})\right] \\ &\leq \left[3\cdot 2^{3k-1} - 2^{k+r-1}\left(2^{r+1}+2^k\right)\right] + \left[2^{2k} r_{Ham}(\mathcal{M}^{\alpha}_{2,r,u}) + 2^k r_{Lee}(\mathcal{M}^{\alpha}_{4,r,u})\right]. \end{aligned}$$

Les mêmes arguments pour $r_E(\mathcal{M}^{\alpha}_{k,u})$.

En utilisant les équations (3.8), (2.9), la proposition 2.4.1 et le théorème 3.1.6, les bornes suivantes sont obtenues par les rayons de recouvrement des codes de MacDonald de type β.

Théorème 3.3.3 *Pour $u \leq r \leq k$, les rayons de recouvrement des codes de MacDonald de type β sont donnés par :*

$$r_{Lee}(\mathcal{M}^{\beta}_{k,u}) \leq \left[2^{2k-2}\left(2^k+1\right) - 2^{k+r-2}\left(2^r+1\right)\right] + \left[2^{2k} r_{Ham}(\mathcal{M}^{\beta}_{2,r,u}) + 2^k r_{Lee}(\mathcal{M}^{\beta}_{4,r,u})\right],$$

et

$$r_{E}(\mathcal{M}^{\beta}_{k,u}) \leq \left[\tfrac{1}{3}\cdot 2^{2k-3}(3+11\cdot 2^k) - 2^{k+r-3}(\tfrac{5}{3}\cdot 2^r+1)\right] + \left[2^k r_{Ham}(\mathcal{M}^{\beta}_{2,r,u}) + 2^{k-1} r_{E}(\mathcal{M}^{\beta}_{4,r,u})\right].$$

Preuve 3.3.4

$$\begin{aligned} r_{Lee}(\mathcal{M}^{\beta}_{k,u}) &\leq r_{Lee}(2^k\mathcal{M}^{\beta}_{2,k,u}) + r_{Lee}(2^{k-1} \mathcal{M}^{\beta}_{4,k,u}) \\ &\leq 2^k r_{Lee}(\mathcal{M}^{\beta}_{2,k,u}) + 2^{k-1} r_{Lee}(\mathcal{M}^{\beta}_{4,k,u}) \\ &\leq 2^k r_{Ham}(\mathcal{M}^{\beta}_{2,k,u}) + 2^{k-1} r_{Lee}(\mathcal{M}^{\beta}_{4,k,u}) \\ &\leq 2^k\left(2^{k-1}-2^{r-1}\right) + 2^k r_{Ham}(\mathcal{M}^{\beta}_{2,r,u}) \\ &\quad +2^{k-1}\left[2^{k-1}\left(2^k-1\right) - 2^{r-1}\left(2^r-1\right)\right] + 2^{k-1} r_{Lee}(\mathcal{M}^{\beta}_{4,r,u}) \\ &\leq \left[2^{2k-2}\left(2^k+1\right) - 2^{k+r-2}\left(2^r+1\right)\right] + \left[2^k r_{Ham}(\mathcal{M}^{\beta}_{2,r,u}) + 2^{k-1} r_{Lee}(\mathcal{M}^{\beta}_{4,r,u})\right]. \end{aligned}$$

Les mêmes arguments pour $r_E(\mathcal{M}^{\beta}_{k,u})$.

Exemple 3.3.5 *Pour $k = 2$, $k_0 = 1$, $k_1 = 1$ et $u = 1$, le code de MacDonald $\mathcal{M}^{\alpha}_{2,1}$ a $2^1 4^1 = 8$ mots-code, de longueur 80, et de matrice génératrice :*

$$\Theta^{\alpha}_{2,1} = \left[\begin{array}{ccc|cccccccc} 11 & \cdots & 11 & 1111 & 2222 & 3333 & \cdots & 1111 & 2222 & 3333 \\ 01 & & 01 & 0123 & 0123 & 0123 & & 0123 & 0123 & 0123 \end{array}\right],$$

où la matrice $\begin{bmatrix} 11 \\ 01 \end{bmatrix}$ *est répété 2^4 fois dans $\Theta^{\alpha}_{2,1}$ et la matrice :*

$$\begin{bmatrix} 1111 & 2222 & 3333 \\ 0123 & 0123 & 0123 \end{bmatrix}$$

est répétée 2^2 fois dans $\Theta^{\alpha}_{2,1}$. Le rayon de recouvroument de code de MacDonald $\mathcal{M}^{\alpha}_{2,1}$ est égal à :

$$r_{Lee}(\mathcal{M}^{\alpha}_{2,1}) \leq \left[3 \cdot 2^{3\times 2-1} - 2^{2+r-1}\left(2^{r+1} + 2^2\right)\right] + \left[2^4 r_{Ham}(\mathcal{M}^{\alpha}_{2,r,1}) + 2^2 r_{Lee}(\mathcal{M}^{\alpha}_{4,r,1})\right].$$

Pour $r = 2$ on a

$$r_{Lee}(\mathcal{M}^{\alpha}_{2,1}) \leq \left[2^4 r_{Ham}(\mathcal{M}^{\alpha}_{2,2,1}) + 2^2 r_{Lee}(\mathcal{M}^{\alpha}_{4,2,1})\right],$$

de sorte que

$$r_{Lee}(\mathcal{M}^{\alpha}_{2,1}) \leq 64,$$

et

$$r_E(\mathcal{M}^{\alpha}_{2,1}) \leq 88.$$

Théorème 3.3.6 *Pour $u \leq r \leq k$, Le rayon de recouvrement du code dual de code de MacDonald sur $\mathbb{Z}_2\mathbb{Z}_4$ de type α et β est donné par :*

$$r_{Lee}(\mathcal{M}^{\alpha^{\perp}}_{k,u}) = r_{Lee}(\mathcal{M}^{\beta^{\perp}}_{k,u}) = 2, r_E(\mathcal{M}^{\alpha^{\perp}}_{k,u}) \leq 4 \text{ et } r_E(\mathcal{M}^{\beta^{\perp}}_{k,u}) \leq 4.$$

Preuve 3.3.7 *La preuve est semblable à celle du Théorème 3.2.6.*

3.4 Les images binaires par le Gray map des codes simplexes et MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$

3.4.1 Les images binaires des codes simplexes de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$

L´image binaire par le Gray map de S_k^α est une concaténation du code simplexe binaire $S_{2,k}^\alpha$ qui est donnée par le théorème suivant :

Théorème 3.4.1 *Soit S_k^α le code simplexe sur $\mathbb{Z}_2\mathbb{Z}_4$ de type α avec un poids de Lee minimal d_{Lee} alors $\Phi(S_k^\alpha)$ est une concaténation des $3 \cdot 2^{2k}$ copies de code simplexe binaire de paramètres $[3 \cdot 2^{3k}; k; d_H = 3 \cdot 2^{3k-1}]$.*

Preuve 3.4.2 *Si Θ_k^α est la matrice génératrice de code simplexe S_k^α de type α sur $\mathbb{Z}_2\mathbb{Z}_4$, alors $\Phi(\Theta_k^\alpha)$ possède la forme suivante :*

$$\Phi(\Theta_k^\alpha) = \left[\overbrace{\begin{array}{c|c|c|c} m_{2,k}^\alpha & m_{2,k}^\alpha & \cdots & m_{2,k}^\alpha \end{array}}^{3\cdot 2^{2k}} \right],$$

où $m_{2,k}^\alpha$ est la matrice génératrice du code simplexe binaire $S_{2,k}^\alpha$. Le résultat alors s´en suit par l´induction sur k.

L´image binaire par le Gray map de S_k^β est une concaténation du code simplexe binaire $S_{2,k}^\beta$ est donnée par le théorème suivant.

Théorème 3.4.3 *Soit S_k^β un code simplexe sur $\mathbb{Z}_2\mathbb{Z}_4$ de type β avec un poids de Lee minimale d_{Lee}, alors $\Phi(S_k^\beta)$ est une concaténation des $2^k\left(2^{k-1}+1\right)$ copies de code simplexe binaire de paramètres $[2^k(2^{k-1}+1)(2^k-1); k; d_{Ham} = 2^{k-1}(2^{k-1}+1)(2^k-1)]$.*

Preuve 3.4.4 *La même que celui du théorème 3.4.1.*

Le lemme suivant sera utile pour prouver que l´image binaire des codes simplexes de type β atteint la borne de Gilbert.

Lemme 3.4.5 *Soit C un code de longueur n et de type $2^{k_0}4^{k_1}$ sur $\mathbb{Z}_2\mathbb{Z}_4$, et soit d_{Lee} la distance minimale de C, alors le rayon de recouvrement $r_{Lee}(C)$ satisfait :*

$$\left\lfloor \frac{d_{Ham}}{2} \right\rfloor \leq r_{Lee}(C) \leq 2(n-k_1) - k_0, \tag{3.9}$$

et par conséquent :

$$\left\lfloor \frac{d_{Lee}}{2} \right\rfloor \leq r_{Lee}(C) \leq d_{Lee} - 1. \tag{3.10}$$

Preuve 3.4.6 *Soient x et y deux mots-code de C avec $x = x_1x_2$ et $y = y_1y_2$, alors on a :*

$$d_{Lee}(x,y) = d_{Ham}(x_1,y_1) + d_{Lee}(x_2,y_2).$$

La borne de rayon d´emballage du code sur $\mathbb{Z}_4$ voir [[4], Théorème 4.3], est donnée par :

$$d_{Lee}(x,y) \geq d_{Ham}(x_1,y_1) + \left\lfloor \frac{d_{Lee}}{2} \right\rfloor,$$

qui implique

$$d_{Lee}(x,y) \geq \left\lfloor \frac{d_{Lee}}{2} \right\rfloor,$$

on obtient

$$r_{Lee}(C) \geq \left\lfloor \frac{d_{Lee}}{2} \right\rfloor.$$

Le reste de l´équation (3.9) est obtenu par la borne de redondance voir [[4], Théorème 4.6].

Théorème 3.4.7 *Soit S_k^β un code simplexe de type β sur $\mathbb{Z}_2\mathbb{Z}_4$. Alors le code binaire $\Phi(S_k^\beta)$ obtenu de S_k^β par l´image de Gay map atteint la borne de Gilbert.*

Preuve 3.4.8 *Supposons que $\Phi(S_k^\beta)$ le code binaire de distance minimale d_{Ham}, qui est la même distance minimale de S_k^β, lorsque le Gray map est une application préservant le poids, et par la proposition 2.4.3 on a :*

$$r(\Phi(S_k^\beta)) = r_{Lee}(S_k^\beta),$$

donc, d´aprés la borne de rayon d´emballage, le lemme 3.4.5, le théorème 3.2.2 et le théorème 3.4.1, on a :

$$2^{k-1}\left[(2^{k-1}+1)(2^k-1)-2\right] \leq 2^{k-1}(2^{k-1}+1)(2^k-1)-1, \text{ pour } k \geq 2.$$

Alors, on peut conclure que :

$$r_{Lee}(S_k^{\beta}) \leq d_{Ham} - 1 \text{ for } k \geq 2,$$

lorsque $\Phi(S_k^{\beta})$ *a un rayon de recouvrement moins de* $d_{Lee} - 1$. *Il est dans [[44], p. 87], qu´un code sur* $\mathbb{F}_q$ *avec une distance minimale* d_{Ham} *et rayon de recouvrement* $d_{Ham} - 1$ *atteint la borne de Gilbert .*

3.4.2 Les images binaires des codes de MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$

Les images binaires par le Gray map de $\mathcal{M}_{k,u}^{\alpha}$ et $\mathcal{M}_{k,u}^{\beta}$ sont des concaténations des codes de MacDonald binaires de type α et β, respectivement, donnés par les théorèmes suivants.

Théorème 3.4.9 *Soit* $\mathcal{M}_{k,u}^{\alpha}$ *un code de MacoDonald sur* $\mathbb{Z}_2\mathbb{Z}_4$ *de type* α *et un poids de Lee minimal* d_{Lee}, *alors* $\Phi(\mathcal{M}_{k,u}^{\alpha})$ *est une concaténation de* $3 \cdot 2^{2k} + 2^{k+u+1}$ *copies du code de MacDonald binaire de paramètres*

$$[3 \cdot 2^{3k} - 2^{k+u}(2^k + 2^{u+1}); k; d_{Ham} = 3 \cdot 2^{3k-1} + 2^{k+u}(2^{k-1} - 2^u)].$$

Preuve 3.4.10 *La même que celle du théorème 3.4.1.*

Théorème 3.4.11 *Soit* $\mathcal{M}_{k,u}^{\beta}$ *un code de MacDonald sur* $\mathbb{Z}_2\mathbb{Z}_4$ *de type* β *et un poids de Lee minimal* d_{Lee}, *alors* $\Phi(\mathcal{M}_{k,u}^{\beta})$ *est une concaténation des* $\frac{2^k\left[(2^{k-1}+1)(2^k-1)-(2^{k+u-1}+1)(2^u-1)\right]}{2^k-2^u}$ *copies du code de MacDonald binaire de paramètres*

$$[2^k[(2^{k-1}+1)(2^k-1)-(2^{k+u-1}+1)(2^u-1)]; k; d_{Ham} = 2^{k-1}[(2^{k-1}+1)(2^k-1)-(2^{k+u-1}+1)(2^u-1)]].$$

Preuve 3.4.12 *La même preuve que celle du théorème 3.4.1.*

3.5 Conclusion

Dans ce chapitre, les bornes de rayon de recouvrement des codes simplexes et des codes de MacDonald de type α et β sur $\mathbb{Z}_2\mathbb{Z}_4$ ont été calculées. Les valeurs exactes ont été

obtenues dans certains cas. Les images binaires sous le Gray map de ces codes ont été présentées.

Chapitre 4

Les codes simplexes et les codes de MacDonald de type α et β sur R_q

Dans ce chapitre, nous donnons quelques résultats préliminaires concernant l´anneau de Frobenius R_q et les codes sur cet anneau. En plus, nous définissons le poids homogène et son Gray map, nous présentons les propriétés des codes simplexes et des codes de MacDonald de type α et de type β, et spécialement les images binaires et les rayons de recouvrement [18].

4.1 Préliminaires

Soit $q \geq 2$ un entier positif, alors l´anneau $R_q = \mathbb{F}_2[u_1, u_2, \ldots, u_q]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle$ est donné d´une façon récurrente par :

$$R_q = \mathbb{F}_2[u_1, u_2, \cdots, u_q]/\left\langle u_i^2 = 0, u_i u_j = u_j u_i \right\rangle = R_{q-1} + u_q R_{q-1}.$$

Pour chaque sous-ensemble $A \subseteq \{1, 2, \cdots, q\}$ on a :

$$u_A = \prod_{i \in A} u_i,$$

accord que $u_\emptyset = 1$, alors tous les éléments de R_q peuvent s´exprimer par :

$$\sum_{A \subseteq \{1,2,\ldots,q\}} c_A u_A, \text{avec } c_A \in \mathbb{F}_2.$$

Les lemmes suivants prouvés dans [31] et [69] donnent quelques propriétés importantes de R_q.

Lemme 4.1.1 *L´anneau R_q est un anneau commutatif local avec $|R_q| = 2^{2^q}$. L´unique idéal maximal m_q se constitué de tous les diviseurs de zéro et*

$$|m_q| = \frac{|R_q|}{2}.$$

Lemme 4.1.2

(i) Pour tout $a \in R_q$, on a :

$$a \cdot (u_1 u_2 \cdots u_q) \;=\; \begin{cases} 0 & \text{si } a \text{ et un diviseur de zéro ,} \\ u_1 u_2 \cdots u_q & \text{si } a \text{ est une unité.} \end{cases}$$

(ii) Pour toute unité $a \in R_q$ et $x \in R_q$, on a :

$$a \cdot x = u_1 u_2 \cdots u_q \Leftrightarrow x = u_1 u_2 \cdots u_q.$$

On note l'ensemble des unités de R_q par $\mathfrak{U}(R_q)$, et les diviseurs de zéro par $\mathfrak{D}(R_q)$. Il est clair que :

$$|\mathfrak{U}(R_q)| = |\mathfrak{D}(R_q)| = 2^{2^q-1} \text{ et } \mathfrak{U}(R_q) = \mathfrak{D}(R_q) + 1.$$

Un code linéaire de longueur n sur R_q est défini comme un R_q-sous module de R_q^n.

4.1.1 Le poids de Lee, homogène sur R_q et le Gray Map

Le poids de Lee sur R_q et le Gray Map

Soit l´ordre des sous-ensembles de l´ensembles $\{1, 2, \ldots, q\}$ est donné par :

$$\{1, 2, \ldots, q\} = \{1, 2, \ldots, q-1\} \cup \{q\}.$$

Avec cet ordre, Le Gray map est défini par :

$$\Psi_{Lee} \;:\; R_q \;\rightarrow\; \mathbb{F}_2^{2^q},$$

avec

$$\Psi_{Lee}\left(u_A\right) = \left(c_B\right)_{B\subset\{1,2,\ldots,q\}},$$

et

$$c_B = \begin{cases} 1 & \text{si } B \subset A, \\ 0 & \text{d´autre part.} \end{cases}$$

On peut étendre Ψ_{Lee} à tous les éléments de R_q et on peut définir le poids de Lee d´un élément dans R_q comme le poids de Hamming de son image. C´est une distance linéaire préservant le Gray map R_q^n à $\mathbb{F}_2^{2^q n}$. II s´ensuit immédiatement que :

$$w_{Lee}(u_A) = 2^{|A|}.$$

Nous avons donc le lemme suivant.

Lemme 4.1.3 *Si C est un code linéaire sur R_q de longueur n, de cardinal 2^k et de poids de Lee minimal d_{Lee}, alors $\Psi_{Lee}(C)$ est un code linéaire binaire de paramètres $[2^{2^q}n, k, d_{Lee}]$.*

Le poids homogène sur R_q et le Gray Map

Plusieurs poids peuvent être définis sur les anneaux. Un poids sur un code C sur l´anneau R_q est appelé homogène s´il satisfait la définition suivante.

Définition 4.1.4 *[37, p. 19] Une fonction réelle w sur l´anneau fini R_q s´appelle un poids homogène à gauche si $w(0) = 0$ et vérifie les propriétés suivantes :*

(i) Pour tous $x, y \in R_q$, $R_q x = R_q y \Rightarrow w(x) = w(y)$.

(ii) Il existe un nombre réel η tel que :

$$\sum_{y\in R_q x} w(y) = \eta|R_q x| \text{ pour tout } x \in R_q - \{0\}.$$

Le nombre η est la valeur moyenne de w dans R_q, et par la condition (i) on peut déduire que η est constante sur tout idéal principal non nul de R_q.

Honold [43] décrit le poids homogène sur R_q concernant le caractére générateur.

Proposition 4.1.5 *[43] Soit R_q un anneau fini de caractère générateur χ, donc tous les poids homogènes sur R_q sont de la forme :*

$$\begin{array}{rccl} w & : & R_q & \to & \mathbb{R} \\ & & x & \mapsto & \gamma\left[1-\frac{1}{\left|R_q^{\times}\right|}\sum_{u\in R_q^{\times}}\chi(xu)\right] \end{array}$$

Le poids homogène sur R_q est obtenu en utilisant la proposition 4.1.5. Basé sur le résultat de [31] et [69] ce qui suit est un caractère générateur de l´anneau R_q

$$\chi\left(\sum_{\substack{A\subseteq\{1,2,\ldots,q\}\\ c_{\varnothing}=0\vee A\neq\varnothing}} c_A u_A\right) = (-1)^{wt(c)},$$

où $wt(c)$, est le poids de Hamming du vecteur de coordonnées dans $\mathbb{F}_2$ d´un élément dans la base $\{u_A; A\subseteq\{1,2,\cdots,q\}\}$. On a

$$\begin{aligned} &\chi(0)=1\\ &\chi(1)=\chi(u_1)=\cdots=\chi(u_q)=\chi(u_1u_2)=\cdots=\chi(u_1u_2\cdots u_q)=-1\\ &\chi(1+u_1)=\chi(u_1+u_2)=\cdots=\chi(u_q+u_1u_2\cdots u_q)=1\\ &\chi(1+u_1+u_2)=\chi(u_1+u_2+u_3)=\cdots=\chi(u_{q-1}+u_q+u_1u_2\cdots u_q)=-1\\ &\vdots\\ &\chi\left(1+\sum_{\substack{A\subseteq\{1,2,\ldots,q\}\\ c_{\varnothing}=0\vee A\neq\varnothing}} c_A u_A\right)=1. \end{aligned}$$

Le théorème suivant est un résultat principale pour les poids homogènes dans R_q.

Théorème 4.1.6 *le poids homogène dans R_q est*

$$w_{hom}(x) = \begin{cases} 0 & si\ x=0,\\ 2\gamma & si\ x=u_1u_2\cdots u_q,\\ \gamma & autrement\ . \end{cases}$$

Le lemme suivant dans [43, Théorème 2] sera la clé pour prouver le théorème principale concernant le poids homogène dans R_q.

Lemme 4.1.7 *Soit x un élément dans R_q tel que $x \neq 0$ et $x \neq u_1u_2\cdots u_q$, alors*

$$\sum_{a\in R_q} \chi(a\cdot x) = 0.$$

Preuve 4.1.8 *Soit $x = u_1u_2\cdots u_q$. Alors par le lemme 4.1.2 on a :*

1) $a\cdot x = x$ pour tout $a \in \mathfrak{U}(R_q)$

2) $\chi(a\cdot x) = -1$ pour tout $a \in \mathfrak{U}(R_q)$.

Par conséquent, par la proposition 4.1.5 on a :

$$w_{hom}(x) = \gamma\left[1 - \frac{1}{|\mathfrak{U}(R_q|}\sum_{a\in\mathfrak{U}(R_q} (-1)\right] = 2\gamma.$$

Si $x \neq 0$ et $x \neq u_1u_2\cdots u_q$, par le lemme 4.1.7 on a :

$$\sum_{a\in R_q} \chi(a\cdot x) = 0.$$

nous obtenons ainsi :

$$w_{hom}(x) = \gamma\left[1 - \frac{1}{|\mathfrak{U}(R_q|}0\right] = \gamma.$$

On propose une définition pour le poids homogène pour un mots-code $x = (x_1, x_2, \cdots, x_n) \in R_q^n$ comme suit :

$$w_{hom}(x_i) = \begin{cases} 0 & \text{si } x_i = 0, \\ 2^{q+1} & \text{si } x_i = u_1u_2\cdots u_q, \\ 2^q & \text{autrement.} \end{cases}$$

On obtient le Gray map correspondant suivant :

$$\Psi_{hom} \;:\; R_q \;\to\; \mathbb{F}_2^{2^{q+1}}$$

où

$$\begin{aligned} \Psi_{hom}(0) &= 0000\cdots00 \\ \Psi_{hom}(1) &= 0101\cdots01 \\ \vdots &\quad \vdots \qquad \vdots \\ \Psi_{hom}\left(\sum_{\substack{A\subseteq\{1,2,\ldots,q\} \\ c_\varnothing=0\vee A\neq\varnothing}} c_A u_A\right) &= 1111\cdots11 \end{aligned}$$

D´où le lemme suivant.

Lemme 4.1.9 *Si C est un code linéaire sur R_q de longueur n, de cardinale 2^k et de poids homogène minimal d_{hom}, alors $\Psi_{hom}(C)$ est un code linéaire binaire de paramètres $[2^{2^{q+1}}n, k, d_{hom}]$.*

En utilisant les informations de [30], le code de *torsion* de C sur R_q est défini par :

$$Tor_A(C) = \{v \in \mathbb{F}_2^n;\, u_A v \in C, A \subset \{1, \cdots, 2^q\}\}. \tag{4.1}$$

l´ensemble :

$$Tor_\varnothing(C) = \{v \in \mathbb{F}_2^n;\, u_\varnothing v \in C, A = \varnothing\}$$

est appelé le code de résidus, il est souvent désigné par :

$$Res(C) = \{u \in \mathbb{F}_2^n; \exists v \in \mathbb{F}_2^n; u + u_A v \in C\}.$$

En général, nous avons l´inclusion suivante du codes de *torsion*

$$Tor_\varnothing(C) \subseteq Tor_{\{i\}\subset\{1,\cdots,2^q\}}(C) \subseteq \cdots \subseteq Tor_{\{1,\cdots,2^q\}}(C). \tag{4.2}$$

Ainsi, pour un code C sur R_q

$$|C| = |Tor_\varnothing(C)|\,|Tor_{\{i\}\subset\{1,\cdots,2^q\}}(C)|\cdots|Tor_{\{1,\cdots,2^q\}}(C)|.$$

4.2 Codes simplexes de type α sur R_q

Soient q et k des entiers positifs avec $q \geq 1$, et soit $G^\alpha_{(q,k)}$ la matrice de taille $k \times 2^{2^q \cdot k}$ défini par :

$$G^\alpha_{(q,k)} = \left[\begin{array}{c|c|c} G^\alpha_{(q,k-1)} & \cdots & G^\alpha_{(q,k-1)} \\ \hline 0_{2^{2^q\cdot(k-1)}} & \cdots & \left(1 + \sum_{\substack{A\subseteq\{1,2,\ldots,q\} \\ c_\varnothing = 0 \vee A \neq \varnothing}} c_A u_A\right) \times 1_{2^{2^q\cdot(k-1)}} \end{array}\right], \tag{4.3}$$

pour $k \geq 2$, où

$$G^{\alpha}_{(q,1)} = \left[0\ 1\ u_1\ \cdots\ \left(1 + \sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_{\varnothing}=0 \vee A \neq \varnothing}} c_A u_A \right) \right],$$

est une matrice avec une ligne et 2^{2^q} colonnes contient tous les éléments de R_q. Les colonnes de $G^{\alpha}_{(q,k)}$ constitués des tous les k-uples distinctes sur R_q. Le code $S^{\alpha}_{(q,k)}$ généré par $G^{\alpha}_{(q,k)}$ s´appelle code simplexe de type α sur R_q. Ce code a la longueur $2^{2^q k}$.

Remarque 4.2.1 *Si A_{k-1} est la matrice de taille $2^{2^q \cdot (k-1)} \times 2^{2^q \cdot (k-1)}$ constitué de tous les mots-code dans $S^{\alpha}_{(q,k-1)}$, et J est la matrice dont toutes les composantes égal à 1, alors le tableau de tous les mots-code de $S^{\alpha}_{(q,k)}$ est donné par la matrice de taille $2^{2^q \cdot k} \times 2^{2^q \cdot k}$*

$$\begin{bmatrix} A_{k-1} & A_{k-1} & \cdots & A_{k-1} \\ A_{k-1} & J + A_{k-1} & \cdots & \left(1 + \sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_{\varnothing}=0 \vee A \neq \varnothing}} c_A u_A \right) J + A_{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k-1} & \left(1 + \sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_{\varnothing}=0 \vee A \neq \varnothing}} c_A u_A \right) J + A_{k-1} & \cdots & J + A_{k-1} \end{bmatrix}, \tag{4.4}$$

où A_1 est le tableau des opérations de multiplication dans R_q, qui sont donnés par :

$\cdot$	0	1	u_1	$\cdots$	$\left(1 + \sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_{\varnothing}=0 \vee A \neq \varnothing}} c_A u_A \right)$
0	0	0	0	$\cdots$	0
1	0	1	u_1	$\cdots$	$\left(1 + \sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_{\varnothing}=0 \vee A \neq \varnothing}} c_A u_A \right)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
$\cdot$	0	$\left(1 + \sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_{\varnothing}=0 \vee A \neq \varnothing}} c_A u_A \right)$	$\left(\sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_{\varnothing}=0 \vee A \neq \varnothing}} c_A u_A \right)$	$\cdots$	1

Remarque 4.2.2 *Si $l_1, l_2, \ldots, l_k$ sont les lignes de $G^{\alpha}_{(q,k)}$, alors :*

1. $w_{Ham}(l_i) = (2^{2^q}-1)2^{2^q\cdot k-2^q}$, $w_{Ham}(u_1 l_i) = w_{Ham}(u_2 l_i) = \ldots = w_{Ham}(u_q l_i) = (2^{2^q}-1)2^{2^q\cdot k-2^q}$, $w_{Ham}(u_1 u_2 \ldots u_q l_i) = 2^{2^q\cdot k-1}$.
2. $w_{Lee}(l_i) = w_{Lee}(u_1 l_i) = w_{Lee}(u_2 l_i) = \ldots = w_{Lee}(u_1 u_2 \ldots u_q l_i) = 2^{2^q\cdot k+(q-1)}$.
3. $w_{hom}(l_i) = w_{hom}(u_1 l_i) = w_{hom}(u_2 l_i) = \ldots = w_{hom}(u_1 u_2 \ldots u_q l_i) = 2^{2^q k}$.

Dans la matrice $G^{\alpha}_{(q,k)}$, il est clair que chaque élément de R_q, est répété $2^{2^q\cdot(k-1)}$ fois dans chaque ligne. Ainsi, nous avons le lemme suivant.

Lemme 4.2.3 *Soit $c \in S^{\alpha}_{(q,k)}$ non nul. Si une coordonnée de c est une unité, alors chaque élément de R_q est répété $2^{2^q\cdot(k-1)}$ fois dans c.*

Preuve 4.2.4 *Par la remarque 4.2.1, pour chaque $x \in S^{\alpha}_{(q,k-1)}$ nous avons les mots-code suivants :*

$$\begin{aligned}
c_1 &= (x|x|x|\cdots|x)\\
c_2 &= \left(x|1+x|u_1+x|\cdots|\left(1+\sum_{\substack{A\subseteq\{1,2,\ldots,q\}\\ c_\varnothing=0\vee A\neq\varnothing}} c_A u_A\right)+x\right)\\
&\vdots\\
c_{2^{2^q}} &= \left(x|\left(1+\sum_{\substack{A\subseteq\{1,2,\cdots,q\}\\ c_\varnothing=0\vee A\neq\varnothing}} c_A u_A\right)+x|\cdots|x\right).
\end{aligned}$$

Le résultat est obtenu par récurrence sur k et la remarque 4.2.1.

Pour obtenir les codes de *torsion* sur R_q, il est nécessaire d´introduire les codes binaires simplexes de type α et β.

Le code simplexe binaire de type α, noté par S_k, a des paramètres $[2^k; k; d_{Ham} = 2^{k-1}]$ et une matrice génératrice :

$$G_k = \left[\begin{array}{c|c} 00\cdots0 & 11\cdots1 \\ \hline G_{k-1} & G_{k-1} \end{array}\right], \tag{4.5}$$

pour $k \geqslant 2$, où $G_1 = [0|1]$.

Le code simplexe binaire de type β, noté par $\widehat{S}_k$, a des paramètres $[2^k-1; k; d_{Ham} = 2^{k-1}]$ et une matrice génératrice :

$$\widehat{G}_k = \left[\begin{array}{c|c} 11\cdots 1 & 00\cdots 0 \\ \hline G_{k-1} & \widehat{G}_{k-1} \end{array}\right], \tag{4.6}$$

pour $k \geqslant 3$, où

$$\widehat{G}_2 = \left[\begin{array}{c|c} 11 & 0 \\ \hline 01 & 1 \end{array}\right]. \tag{4.7}$$

Lemme 4.2.5 *Le code de torsion de $S^{\alpha}_{(q,k)}$ est la concaténation $2^{(2^q-1)k}$ de code S_k.*

Preuve 4.2.6 *Le code de torsion de $S^{\alpha}_{(q,k)}$ est l´ensemble des mots-code obtenu en remplaçant $u_1u_2\cdots u_q$ avec 1 dans tout $u_1u_2\ldots u_q$- des combinaisons linéaires des lignes de $u_1\cdots u_qG^{\alpha}_{(q,k)}$ (où $G^{\alpha}_{(q,k)}$ est la matrice génératrice de $S^{\alpha}_{(q,k)}$ définie dans l´équation (4.3)). La preuve se fait par récurrence sur k. Pour $k = 2$, le résultat est vrai. Si $u_1u_2\cdots u_qG^{\alpha}_{(q,k-1)}$ est la matrice obtenue par la concaténation des $2^{(2^q-1)(k-1)}$ de la matrice $u_1u_2\cdots u_qG_{k-1}$, de sorte que $u_1u_2\cdots u_qG^{\alpha}_{(q,k)}$ prend la forme :*

$$\left[\begin{array}{c|c|c} u_1u_2\cdots u_qG_{k-1}\cdots u_{1u_2}\cdots u_qG_{k-1} & \cdots & u_1u_2\cdots u_qG_{k-1}\cdots u_1u_2\cdots u_qG_{k-1} \\ \hline 0_{\,2^{2^q\cdot(k-1)}} & \cdots & (u_1u_2\ldots u_q)\times 1_{\,2^{2^q\cdot(k-1)}} \end{array}\right]. \tag{4.8}$$

On regroupe les colonnes basées sur l´quation (4.5), on obtient le résultat.

Pour $q \geq 2$, nous définissons l´homomorphisme linéaire suivant :

$$\begin{array}{rccc} \Gamma_q & : & R_q & \to & R_{q-1} \\ & & 1+\sum\limits_{\substack{A\subseteq\{1,2,\cdots,q\}\\ c_\varnothing=0\vee A\neq\varnothing}} c_Au_A & \longmapsto & \Gamma_q\left(1+\sum\limits_{\substack{A\subseteq\{1,2,\cdots,q\}\\ c_\varnothing=0\vee A\neq\varnothing}} c_Au_A\right), \end{array}$$

où

$$\Gamma_q\left(1+\sum_{\substack{A\subseteq\{1,2,\cdots,q\}\\ c_\varnothing=0\vee A\neq\varnothing}} c_Au_A\right) = 1+\sum_{\substack{A\subseteq\{1,2,\cdots,q-1\}.\\ c_\varnothing=0\vee A\neq\varnothing}} c_Au_A.$$

on a

$$Im(\Gamma_q) = R_{q-1},$$

et pour n un entier positif cet homomorphisme peut être étendu à R_q^n

$$\Gamma_q \ : \ R_q^n \ \longrightarrow \ R_{q-1}^n.$$

Théorème 4.2.7 *Soit $S^{\alpha}_{(q,k)}$ le code simplexe de type α sur R_q, alors $\Gamma_q(S^{\alpha}_{(q,k)})$ est la concaténation des $2^{2^{q-1}k}$ codes simplexes de type α sur R_{q-1}.*

Preuve 4.2.8 *Si $G^{\alpha}_{(q,k)}$ est la matrice génératrice de code simplexe $S^{\alpha}_{(q,k)}$ de type α sur R_q, alors $\Gamma_q(G^{\alpha}_{(q,k)})$ est de la forme :*

$$\Gamma_q(G^{\alpha}_{(q,k)}) = \left[\overbrace{\begin{array}{c|c|c|c} G^{\alpha}_{(q-1,k)} & G^{\alpha}_{(q-1,k)} & \cdots & G^{\alpha}_{(q-1,k)} \end{array}}^{2^{2^{q-1}k}} \right],$$

où

$$G^{\alpha}_{(q-1,k)} = \left[\begin{array}{c|c|c|c} G^{\alpha}_{(q-1,k-1)} & G^{\alpha}_{(q-1,k-1)} & \cdots & G^{\alpha}_{(q-1,k-1)} \\ \hline 0_{2^{2^{q-1}(k-1)}} & 1_{2^{2^{q-1}(k-1)}} & \cdots & \left(1 + \sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_{\varnothing}=0 \vee A \neq \varnothing}} c_A u_A \right) \times 1_{2^{2^{q-1}(k-1)}} \end{array} \right],$$

est la matrice génératrice du code simplexe de type α sur R_{q-1}.

Théorème 4.2.9 *Si $S^{\alpha}_{(q,k)}$ est le code simplexe de type α sur R_q, alors :*

$$\Gamma_q\left(\Gamma_{q-1}\cdots\left(\Gamma_2\left(S^{\alpha}_{(2,k)}\right)\right)\right) = \overbrace{S^{\alpha}_{(1,k)}S^{\alpha}_{(1,k)}\cdots S^{\alpha}_{(1,k)}}^{2^{2^q\left(\frac{q-1}{q}\right)}k},$$

est la concaténation des $2^{2^q\left(\frac{q-1}{q}\right)}k$ codes $S^{\alpha}_{(1,k)}$, où $S^{\alpha}_{(1,k)}$ est le code simplexe de type α sur R_1.

Preuve 4.2.10 *La preuve est par récurrence sur q, et en utilisant le Théorème 4.2.9.*

Pour $q = 2$, si $G^{\alpha}_{(2,k)}$ est la matrice génératrice de code simplexe sur R_2, alors :

$$\Gamma_2\left(G^{\alpha}_{(2,k)}\right) = \left[\overbrace{G^{\alpha}_{(1,k)} \mid G^{\alpha}_{(1,k)} \mid \cdots \mid G^{\alpha}_{(1,k)}}^{2^{2k}}\right],$$

où $G^{\alpha}_{(1,k)}$ est la matrice génératrice de code simplexe sur R_1. Si

$$\Gamma_{q-1}\left(\Gamma_{q-2}\cdots\left(\Gamma_2\left(G^{\alpha}_{(2,k)}\right)\right)\right) = \left(2^{2^{q-1}k}\cdots\left(2^{2^2k}G^{\alpha}_{(1,k)}\right)\right),$$

est la matrice génératrice obtenue par la concaténation des $2^{2^{(q-2)}\left(\frac{q+1}{2}\right)k}$ codes simplexes de type α sur R_1, alors :

$$\Gamma_q\left(\Gamma_{q-1}\cdots\left(\Gamma_2\left(G^{\alpha}_{(2,k)}\right)\right)\right) = \left(2^{2^q k}\cdots\left(2^{2^2k}G^{\alpha}_{(1,k)}\right)\right) = \left(\overbrace{G^{\alpha}_{(1,k)} \mid G^{\alpha}_{(1,k)} \mid \cdots \mid G^{\alpha}_{(1,k)}}^{2^{2^q\left(\frac{q-1}{2}\right)k}}\right).$$

Soient $S_0 = \{0\}$, $S_1 = \{0, u_1u_2\cdots u_q\},\cdots$, $S_{q-1} = \{0, u_1, u_2, \cdots, u_1u_2\cdots u_q\}$, et $S_q = R_q$. Notons que S_{q-1} est l´ensemble de tous les diviseurs de zéro de R_q. Un mots-code $c = (c_1, c_2, \cdots, c_n) \in S^{\alpha}_{(q,k)}$ est concidéré de *type* m, $0 \leq m \leq q$, si tous ses composantes appartiennent à l´ensemble S_m. Pour $G^{\alpha}_{(q,k)}$, on a chaque élément de R_q se trouve également dans chaque ligne de $G^{\alpha}_{(q,k)}$.

Pour déterminer le nombre de mots-code de type m dans $S^{\alpha}_{(q,k)}$, $0 \leq m \leq q$, nous définissons la matrice D_m, tel que :

$$D_0 = \begin{bmatrix} u_1u_2\dots u_ql_1 \\ u_1u_2\dots u_ql_2 \\ \vdots \\ u_1u_2\dots u_ql_k \end{bmatrix},\ D_1 = \begin{bmatrix} u_1\dots u_{q-1}l_1 \\ u_1\dots u_ql_1 \\ u_1\dots u_{q-1}l_2 \\ u_1\dots u_ql_2 \\ \vdots \\ u_1\dots u_{q-1}l_k \\ u_1\dots u_ql_k \end{bmatrix},\ \cdots,\ D_q = \begin{bmatrix} l_1 \\ u_1l_1 \\ \vdots \\ u_1\dots u_qR_1 \\ l_2 \\ u_1l_2 \\ \vdots \\ u_1\dots u_ql_2 \\ \vdots \\ l_k \\ u_1l_k \\ \vdots \\ u_1\dots u_ql_k \end{bmatrix},$$

où l_i la i^{th} ligne de $G^{\alpha}_{(q,k)}$. Notons que les mots-code générés par D_0 ont des éléments qui sont, soit 0 ou $u_1u_2\dots u_q$, et D_q génère $S^{\alpha}_{(q,k)}$, soit $C^{(m)}$ le sous-code de C généré par les lignes de D_m, alors on a :

$$C^{(0)} \subset C^{(2)} \subset \cdots \subset C^{(q)},$$

et $C^{(m)}$ a 2^{mk} mots-code. Pour $0 \leq m \leq q$, les mots-code de type m sont répétés $2^{mk} - 2^{(m-1)k}$ fois dans $S^{\alpha}_{(q,k)}$. Cela prouve le lemme suivant.

Lemme 4.2.11 *Pour $0 \leq m \leq q$, le nombre de mots-code de type m dans $S^{\alpha}_{(q,k)}$ est $2^{(m-1)k}(2^k - 1)$.*

Théorème 4.2.12 *Les distributions de poids de Hamming, Lee et homogène de $S^{\alpha}_{(q,k)}$ sont :*

(i) $A_{Ham}(0) = 1$, $A_{Ham}((2^{(2^{qk-m})})(2^{2^m} - 1)) = 2^{(m-1)k}(2^{2^m} - 1)$, *pour* $0 \leq m \leq q$.

(ii) $A_{Lee}(0) = 1, A_{Lee}(2^{2^{qk+(q-1)}}) = 2^{2^{qk}} - 1$.

(iii) $A_{hom}(0) = 1, A_{hom}(2^{2^q k}) = 2^{2^q k} - 1.$

Preuve 4.2.13 *Soit* $c \in S^{\alpha}_{(q,k)}$ *un mots-code de type* m $(\neq 0)$*, alors par le lemme 4.2.11 on a :*

$$A_{Ham}(2^{2^q - m}(2^{2^m} - 1)) = 2^{(m-1)k}(2^{2^m} - 1),$$

pour $m = 0$*, et* $A_{Ham}(0) = 1$*. De plus, d´après le lemme 4.2.3 on a :*

$$A_{Lee}(c) = 2^{2^q \cdot k} - 1,$$

qui est indépendant de m*, de sorte que tous les mots-code de type* m $(\neq 0)$ *ont les mêmes poids de Lee et homogènes.*

4.2.1 Les images Gray binaires des codes simplexes de type α

Les images Gray Binaires des codes simplexes $S^{\alpha}_{(q,k)}$ sur R_q sont données dans les deux théorèmes suivants :

Théorème 4.2.14 *Soit* $S^{\alpha}_{(q,k)}$ *un code simplexe sur* R_q *de longueur* $2^{2^q k}$ *et de poids de Lee minimale* d_{Lee}*, alors* $\Psi_{Lee}(S^{\alpha}_{(q,k)})$ *est la concaténation de* $2^{(2^q-1)k+q}$ *codes simplexes binaires a des paramètres* $[2^{2^q k+q}; k; d_{Ham} = 2^{2^q k+q-1}]$.

Preuve 4.2.15 *Soit* $G^{\alpha}_{(q,k)}$ *une matrice génératrice de code simplexe* $S^{\alpha}_{(q,k)}$ *sur* R_q*, alors* $\Psi_{Lee}(G^{\alpha}_{(q,k)})$ *est de la forme :*

$$\Psi_{Lee}(G^{\alpha}_{(q,k)}) = \left[\overbrace{G_k \mid G_k \mid \cdots \mid G_k}^{2^{(2^q-1)k+q}} \right],$$

où G_k *est une matrice génératrice du code simplexe binaire* S_k*. La démonstration est par récurrence sur* k*.*

Théorème 4.2.16 *Soit* $S^{\alpha}_{(q,k)}$ *un code simplexe sur* R_q *de longueur* $2^{2^q k}$ *et un poids homogène minimale* d_{hom}*, alors* $\Psi_{hom}(S^{\alpha}_{(q,k)})$ *est la concaténation des* $2^{(2^q-1)k+q+1}$ *codes simplexes binares a de paramètres* $[2^{2^q k+q+1}; k; d_{Ham} = 2^{2^q k+q}]$.

Preuve 4.2.17 *La preuve est analogue au Théorème 4.2.14.*

4.3 Codes simplexes de type β sur R_q

Soit $G^{\beta}_{(q,k)}$ la matrice de taille $k \times 2^{(2^q-1)(k-1)}(2^k-1)$ définie par :

$$G^{\beta}_{(q,k)} = \left[\begin{array}{c|c|c|c} 1_{2^{2^q\cdot(k-1)}} & 0_{2^{2^q(k-2)}\left(2^{k-1}-1\right)} & \cdots & \left(\sum_{\substack{A\subseteq\{1,2,\ldots,q\}\\ c_\varnothing=0\vee A\neq\varnothing}} c_A u_A\right)_{2^{2^q(k-2)}\left(2^{k-1}-1\right)} \\ \hline G^{\alpha}_{(q,k-1)} & G^{\beta}_{(q,k-1)} & \cdots & G^{\beta}_{(q,k-1)} \end{array}\right],$$

pour $k > 2$, et

$$G^{\beta}_{(q,2)} = \left[\begin{array}{c|c|c|c} 1_{2^{2^q\cdot(k-1)}} & 0 & \cdots & \sum_{\substack{A\subseteq\{1,2,\ldots,q\}\\ c_\varnothing=0\vee A\neq\varnothing}} c_A u_A \\ \hline 0\ 1\ \ldots \left(1+\sum_{\substack{A\subseteq\{1,2,\ldots,q\}\\ c_\varnothing=0\vee A\neq\varnothing}} c_A u_A\right) & 1 & \cdots & 1 \end{array}\right],$$

où $G^{\alpha}_{(q,k-1)}$ est une matrice génératrice de $S^{\alpha}_{(q,k-1)}$.

Le code simplexe $S^{\beta}_{q,k}$ de type β est le code poinçonné de $S^{\alpha}_{q,k}$. Ce code est de longueur $2^{(2^q-1)(k-1)}(2^k-1)$.

Remarque 4.3.1 *(i) A_{k-1} (B_{k-1}) désigne l´ensemble des mots-code dans $S^{\alpha}_{(q,k-1)}$ (resp. $S^{\beta}_{(q,k-1)}$), et J la matrice dont tous les éléments égaux à 1.*

(ii) L´ensemble de tout les mots-code de $S^{\beta}_{(q,k)}$ est donné par la matrice suivante :

$$\left[\begin{array}{cccc} A_{k-1} & B_{k-1} & \cdots & B_{k-1} \\ J+A_{k-1} & B_{k-1} & \cdots & \left(\sum\limits_{\substack{A\subseteq\{1,2,\ldots,q\}\\ c_\varnothing=0\vee A\neq\varnothing}} c_A u_A\right) J+B_{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ \left(1+\sum\limits_{\substack{A\subseteq\{1,2,\ldots,q\}\\ c_\varnothing=0\vee A\neq\varnothing}} c_A u_A\right) J+A_{k-1} & B_{k-1} & \cdots & \left(\sum\limits_{\substack{A\subseteq\{1,2,\ldots,q\}\\ c_\varnothing=0\vee A\neq\varnothing}} c_A u_A\right) J+B_{k-1} \end{array}\right].$$

$\mathfrak{U}(\mathfrak{R}_{\mathfrak{q}})$ et $\mathfrak{D}(\mathfrak{R}_{\mathfrak{q}})$ deux ensembles, l´ensemble des unités et l´ensemble des diviseurs de zéro de R_q, respectivement. La proposition suivante donne les distributions de poids de $S^{\beta}_{(q,k)}$.

Proposition 4.3.2 *Pour $2 \leq j \leq k$, Soit l_j la j^{th} ligne de $G^{\beta}_{(q,k)}$. Alors on a :*

(i) $\sum_{i \in \mathfrak{U}(\mathfrak{R}_q)} w_i = 2^{2^q \cdot (k-1)}$, *et chaque diviseur de zéro dans* R_q *se trouve* $2^{(2^q-1)\cdot(k-2)}(2^{k-1}-1)$ *fois dans* l_j.

(ii) $w_{Ham}(l_j) = 2^{(2^q-1)(k-1)-2^q}((2^{2^q}-1)(2^k-1)+1)$.

1. $w_{Lee}(l_1) = 2^{2^q(k-1)} + 2^{2^q \cdot k-(2^q-1)} - 2^{4k-(2^q-2)}$.

(iii) $w_{hom}(l_j) = 2^{(2^q-1)k-1}(2^k-1)$.

Preuve 4.3.3 *La démonstration résulte en utilisant la définition de* l_j.

La proposition suivante donne la structure des mots-code de $S^{\beta}_{(q,k)}$.

Proposition 4.3.4 *Considérons un mots-code* $c \in S^{\beta}_{(q,k)}$. *Si une coordonnée de* c *est une unité alors* $\sum_{i \in \mathfrak{U}(\mathfrak{R}_q)} w_i = 2^{2^q \cdot (k-1)}$, *et chaque diviseur de zéro de* R_q *se trouve* $2^{(2^q-1)\cdot(k-2)}(2^{k-1}-1)$ *fois dans* c.

Preuve 4.3.5 *Par la remarque 4.3.1, il existe* $x_1 \in S^{\alpha}_{(q,k-1)}$, *et* $x_2 \in S^{\beta}_{(q,k-1)}$ *tel que* c *prend des* 2^{2^q} *formes suivantes :*

$$\begin{aligned}
c_1 &= (x_1|x_2|x_2|\cdots|x_2) \\
c_2 &= \left(1 + x_1|x_2|u_1 + x_2|\cdots|\left(\sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_\varnothing = 0 \vee A \neq \varnothing}} c_A u_A\right) + x_2\right) \\
&\vdots \\
c_{2^{2^q}} &= \left(\left(1 + \sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_\varnothing = 0 \vee A \neq \varnothing}} c_A u_A\right) + x_1|\cdots|\left(\sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_\varnothing = 0 \vee A \neq \varnothing}} c_A u_A\right) + x_2\right).
\end{aligned}$$

Le résultat alors par induction sur k.

Lemme 4.3.6 *Le code de torsion de* $S^{\beta}_{(q,k)}$ *est la concaténation des* $2^{(2^q-1)\cdot(k-2)}$ *codes simplexes binaires de type* β *notée par* $\widehat{S}_k$.

Preuve 4.3.7 *La même démonstration que dans le lemme 4.2.5.*

Théorème 4.3.8 *Les distributions de poids de Hamming et homogéne* $S^{\beta}_{(q,k)}$ *sont :*

(i) $A_{Ham}(0) = 1$, $A_{Ham}(2^{(2^q-1)(k-1)}[(2^{k-m}(2^{2^m}-1)+(2^{1-m}-1)]) = 2^{(m-1)k}(2^{2^m}-1)$, $0 \leq m \leq q$.

(ii) $A_{hom}(0) = 1$, $A_{hom}(2^{(2^q-1)k-1}(2^k-1) = 2^k(2^{(2^q-1)k}-1)$.

Preuve 4.3.9 *La preuve est semblable à celle du Théorème 4.2.12.*

Théorème 4.3.10 *Soit $S^{\beta}_{(q,k)}$ le code simplexe de type β sur R_q, alors $\Gamma_q(S^{\beta}_{(q,k)})$ est la concaténation des $2^{2^{q-1}k}$ codes simplexes de type β sur R_{q-1}.*

Preuve 4.3.11 *Si $G^{\beta}_{(q,k)}$ est la matrice génératrice de code simplexe de type β sur R_q, alors $\Gamma_q(G^{\beta}_{(q,k)})$ est sous forme :*

$$\Gamma_q(G^{\beta}_{(q,k)}) = \left[\overbrace{G^{\beta}_{(q-1,k)} \,\middle|\, G^{\beta}_{(q-1,k)} \,\middle|\, \cdots \,\middle|\, G^{\beta}_{(q-1,k)}}^{2^{2k}}\right],$$

où $G^{\beta}_{(q-1,k)}$ est la matrice génératrice de code simplexe $S^{\beta}_{(q,k-1)}$ de type β sur R_{q-1}.

Théorème 4.3.12 *Si $S^{\beta}_{(q,k)}$ est le code simplexe de type β sur R_q, alors*

$$\Gamma_q\left(\Gamma_{q-1}\cdots\left(\Gamma_2\left(S^{\beta}_{(2,k)}\right)\right)\right) = \overbrace{S^{\beta}_{(1,k)}S^{\beta}_{(1,k)}\cdots S^{\beta}_{(1,k)}}^{2^{2^q\left(\frac{q-1}{2}\right)_k}},$$

est la concaténation des $2^{2^q\left(\frac{q-1}{2}\right)k}$ codes simplexes de type β sur R_1, notée par $S^{\beta}_{(1,k)}$.

Preuve 4.3.13 *La preuve est par récurrence sur q et le Théorème 4.3.10.*

Pour $q = 2$, $G^{\beta}_{(2,k)}$ est une matrice génératrice pour le code simplexe de type β sur R_2, alors

$$\Gamma_2\left[G^{\beta}_{(2,k)}\right) = \left(\overbrace{G^{\beta}_{(1,k)} \,\middle|\, G^{\beta}_{(1,k)} \,\middle|\, \cdots \,\middle|\, G^{\beta}_{(1,k)}}^{2^{2k}}\right],$$

où $G^{\beta}_{(1,k)}$ est une matrice génératrice du code simplexe de type β sur R_1. Si

$$\Gamma_{q-1}\left(\Gamma_{q-2}\cdots\left(\Gamma_2\left(G^{\beta}_{(2,k)}\right)\right)\right) = \left(2^{2^{q-1}k}\cdots\left(2^{2^2k}G^{\beta}_{(1,k)}\right)\right),$$

alors cette dernière est la matrice génératrice obtenue par la concaténation $2^{2^q\left(\frac{q-1}{2}\right)_k}$ *de* $S^{\beta}_{(1,k)}$*, où* $S^{\beta}_{(1,k)}$ *est le code simplexe de type* β *sur* R_1*, alors :*

$$\Gamma_q\left(\Gamma_{q-1}\cdots\left(\Gamma_2\left(S^{\beta}_{(2,k)}\right)\right)\right) = \overbrace{S^{\beta}_{(1,k)} \mid S^{\beta}_{(1,k)} \mid \cdots \mid S^{\beta}_{(1,k)}}^{2^{2^{(q-2)}\left(\frac{q+1}{2}\right)_k}}.$$

4.3.1 Les images Gray binaires des codes simplexes de type β

Les images Gray binaires des codes simplexes de type β sur R_q sont données dans les théorèmes suivants :

Théorème 4.3.14 *Soit* $S^{\beta}_{(q,k)}$ *le code simplexe sur* R_q *de longueur* $2^{(2^q-1)(k-1)}(2^k-1)$ *et de poids de Lee minimal* d_{Lee}*, alors* $\Psi_{Lee}(S^{\beta}_{(q,k)})$ *est la concaténation de* $2^{(2^q-1)(k-1)+q}$ *codes simplexes binaires a de paramètres* $[2^{(2^q-1)(k-1)+q}(2^k-1); k; d_{Ham} = 2^{(2^{q-1}-2)k+q}]$.

Preuve 4.3.15 *Si* $G^{\beta}_{(q,k)}$ *est la matrice génératrice de code simplexe* $S^{\beta}_{(q,k)}$ *sur* R_q*, alors* $\Psi_{Lee}(G^{\alpha}_{(q,k)})$ *est de la forme :*

$$\Psi_{Lee}(G^{\alpha}_{(q,k)}) = \left[\overbrace{G_k \mid G_k \mid \cdots \mid G_k}^{2^{(2^q-1)(k-1)+q}}\right],$$

où G_k *est la matrice génératrice du code simplexe binaire* S_k*. en utilisant la récurrence sur* k*, on obtient le résultat.*

Théorème 4.3.16 *Soit* $S^{\beta}_{(q,k)}$ *le code simplexe sur* R_q *de longueur* $2^{(2^q-1)(k-1)}(2^k-1)$*, et de poids homogenène* d_{hom}*, alors* $\Psi_{\hom}(S^{\beta}_{(q,k)})$ *est la concaténation de* $2^{(2^q-1)(k-1)+(q+1)}$ *codes simplexes binaires a de paramètres* $[2^{(2^q-1)(k-1)+(q+1)}(2^k-1); k; d_{Ham} = 2^{(2^q-2)(k-1)+(q+1)}]$.

Preuve 4.3.17 *Le même raisennement que celui du théorème 4.3.14.*

4.4 Codes de MacDonald de type α et β sur R_q

Dans [56], l´auteur a défini le code binaire de MacDonald sur un corps fini $\mathbb{F}_2$, et le code de MacDonald $\mathcal{M}_{k,u}(q)$ sur un corps fini $\mathbb{F}_q$, est de paramètres $\left[\frac{q^k-q^u}{q-1}, k, q^{k-1}-q^{u-1}\right]$, dans lequel chaque mots-code non nul a un poids soit q^{k-1} ou $q^{k-1}-q^{u-1}$.

Soit $G^{\alpha}_{(q,k)}$ (resp., $G^{\beta}_{(q,k)}$), des matrices génératrices des codes simplexes de type α et β sur R_q, respectivement. Pour $1 \leq u \leq k-1$, nous construisons $G^{\alpha}_{(q,k,u)}$ (resp., $G^{\beta}_{(q,k,u)}$), la matrice génératrice de code de MacDonald $\mathcal{M}^{\alpha}_{(q,k,u)}$ (resp., $\mathcal{M}^{\beta}_{(q,k,u)}$), obtenue de $G^{\alpha}_{(q,k)}$ (resp., $G^{\beta}_{(q,k)}$), par l´élémination des colonnes correspondantes aux colonnes de $G^{\alpha}_{(q,u)}$ et $0_{2^{2q}u\times(k-u)}$ (resp., $G^{\beta}_{(q,u)}$ et $0_{2^{(2q-1)(u-1)}(2^u-1)\times(k-u)}$), comme suit :

$$G^{\alpha}_{(q,k,u)} = \left[\begin{array}{c|c} G^{\alpha}_{(q,k)} & \begin{array}{c} 0_{2^{2q}u\times(k-u)} \\ \hline G^{\alpha}_{(q,u)} \end{array} \end{array}\right], \tag{4.9}$$

$$(\text{resp. } G^{\beta}_{(q,k,u)} = \left[\begin{array}{c|c} G^{\beta}_{(q,k)} & \begin{array}{c} 0_{2^{(2q-1)(u-1)}(2^u-1)\times(k-u)} \\ \hline G^{\beta}_{(q,u)} \end{array} \end{array}\right]). \tag{4.10}$$

Le code $\mathcal{M}^{\alpha}_{(q,k,u)}$ (resp., $\mathcal{M}^{\beta}_{(q,k,u)}$), généré par $G^{\alpha}_{(q,k,u)}$ (resp., $G^{\beta}_{(q,k,u)}$), est un code poinçonné de $S^{\alpha}_{(q,k)}$ (resp., $S^{\beta}_{(q,k)}$), et est un code de MacDonald de type α (resp., β). Le code de MacDonald $\mathcal{M}^{\alpha}_{(q,k,u)}$ est un code sur R_q de longueur $2^{2q}k - 2^{2q}u$.

Le code de MacDonald $\mathcal{M}^{\beta}_{(q,k,u)}$ est un code sur R_q de longueur $2^{(2q-1)(k-1)}(2^k-1) - 2^{(2q-1)(u-1)}(2^u-1)$.

Exemple 4.4.1 *Dans le cas où $q=2$, $k=3$ et $1 \leq u \leq 2$. Il y a deux codes de MacDonald de type α et deux codes de MacDonald de type β, $\mathcal{M}^{\alpha}_{(2,3,1)}$ et $\mathcal{M}^{\alpha}_{(2,3,2)}$ (resp., $\mathcal{M}^{\beta}_{(2,3,1)}$ et $\mathcal{M}^{\beta}_{(2,3,2)}$). Les matrices génératrices de ces codes est données par :*

$$G^{\alpha}_{(2,3,1)} = \left[\begin{array}{c|c|c|c} \overbrace{1\cdots 1}^{256} & \overbrace{u_1\cdots u_1}^{256} & \cdots & \overbrace{\mathcal{U}_{\{1,2\}}\cdots\mathcal{U}_{\{1,2\}}}^{256} \\ \hline G^{\alpha}_{(2,2)} & G^{\alpha}_{(2,2)} & \cdots & G^{\alpha}_{(2,2)} \end{array}\right],$$

$$G^{\alpha}_{(2,3,2)} = \left[\begin{array}{c|c|c|c} \overbrace{0\cdots0}^{240} & \overbrace{1\cdots1}^{256} & \cdots & \overbrace{\mathcal{U}_{\{1,2\}}\cdots\mathcal{U}_{\{1,2\}}}^{256} \\ \hline \overbrace{1\cdots1}^{16}\cdots\overbrace{\mathcal{U}_{\{1,2\}}\cdots\mathcal{U}_{\{1,2\}}}^{16} & \overbrace{0\cdots0}^{16}\cdots\overbrace{\mathcal{U}_{\{1,2\}}\cdots\mathcal{U}_{\{1,2\}}}^{16} & \cdots & \overbrace{0\cdots0}^{16}\cdots\overbrace{\mathcal{U}_{\{1,2\}}\cdots\mathcal{U}_{\{1,2\}}}^{16} \\ \hline G^{\alpha}_{(2,1)} \setminus \overbrace{01\cdots\mathcal{U}_{\{1,2\}}}^{16} & G^{\alpha}_{(2,1)} & \cdots & G^{\alpha}_{(2,1)} \end{array}\right]$$

$$G^{\beta}_{(2,3,1)} = \left[\begin{array}{c|c|c|c} \overbrace{1\cdots1}^{256} & \overbrace{0\cdots0}^{23} & \cdots & \overbrace{\mathcal{V}_{\{1,2\}}\cdots\mathcal{V}_{\{1,2\}}}^{24} \\ \hline \overbrace{0\cdots0}^{16}\cdots\overbrace{\mathcal{U}_{\{1,2\}}\cdots\mathcal{U}_{\{1,2\}}}^{16} & \overbrace{1\cdots1u_1\cdots\mathcal{V}_{\{1,2\}}}^{16\quad 7} & \cdots & \overbrace{1\cdots10u_1\cdots\mathcal{V}_{\{1,2\}}}^{16\quad 8} \\ \hline \overbrace{G^{\alpha}_{(2,1)}}^{16}\cdots\overbrace{G^{\alpha}_{(2,1)}}^{16} & \overbrace{G^{\alpha}_{(2,1)}1\cdots1}^{16\quad 7} & \cdots & \overbrace{G^{\alpha}_{(2,1)}1\cdots1}^{16\quad 8} \end{array}\right]$$

$$G^{\beta}_{(2,3,2)} = \left[\begin{array}{c|c|c|c} \overbrace{1\cdots1}^{256} & \overbrace{u_1\cdots u_1}^{24} & \cdots & \overbrace{\mathcal{V}_{\{1,2\}}\cdots\mathcal{V}_{\{1,2\}}}^{24} \\ \hline G^{\alpha}_{(2,2)} & G^{\beta}_{(2,2)} & \cdots & G^{\beta}_{(2,2)} \end{array}\right]$$

avec, $\mathcal{U}_{\{1,2\}} = 1 + u_1 + u_2 + u_1u_2$ *et* $\mathcal{V}_{\{1,2\}} = u_1 + u_2 + u_1u_2$

Sous les notations précédentes, nous avons les résultats suivants :

Théorème 4.4.2 *Soit* $\mathcal{M}^{\alpha}_{(q,k,u)}$ *et* $\mathcal{M}^{\beta}_{(q,k,u)}$ *les codes de MacDonald de type* α *et* β*, respectivement, sur* R_q*, alors* $\Gamma_q(\mathcal{M}^{\alpha}_{(q,k,u)})$ *et* $\Gamma_q(\mathcal{M}^{\beta}_{(q,k,u)})$ *sont la concaténation de* $2^{2^{q-1}k}$ *codes de MacDonald de type* α *et* β*, respectivement, sur* R_{q-1}*.*

Preuve 4.4.3 *La preuve est similaire à celles des théorèmes 4.2.7 et 4.3.10.*

Théorème 4.4.4 *Si* $\mathcal{M}^{\alpha}_{(q,k,u)}$ *est le code de MacDonald de type* α *sur* R_q*, alors :*

$$\Gamma_q\left(\Gamma_{q-1}\cdots\left(\Gamma_2\left(\mathcal{M}^{\alpha}_{(2,k,u)}\right)\right)\right) = \left(\mathcal{M}^{\alpha}_{(1,k,u)}\mathcal{M}^{\alpha}_{(1,k,u)}\cdots\mathcal{M}^{\alpha}_{(1,k,u)}\right)$$

est la concaténation des $2^{2^{q\left(\frac{q-1}{2}\right)k}}$ $\mathcal{M}^{\alpha}_{(1,k,u)}$*(où* $\mathcal{M}^{\alpha}_{(1,k,u)}$ *est le code de MacDonald de type* α *sur* R_1*).*

Si $\mathcal{M}^{\beta}_{(q,k,u)}$ *est le code de MacDonald de type* β *sur* R_q*, alors :*

$$\left(\Gamma_q\left(\Gamma_{q-1}\cdots\left(\Gamma_2\left(\mathcal{M}^{\beta}_{(2,k,u)}\right)\right)\right) = \left(\mathcal{M}^{\beta}_{(1,k,u)}\mathcal{M}^{\beta}_{(1,k,u)}\cdots\mathcal{M}^{\beta}_{(1,k,u)}\right)\right),$$

est la concaténation des $2^{2^{q\left(\frac{q-1}{2}\right)k}}$ $\mathcal{M}^{\beta}_{(1,k,u)}$*(où* $\mathcal{M}^{\beta}_{(1,k,u)}$ *est le code de MacDonald de type* β *sur* R_1*).*

Preuve 4.4.5 *La preuve est semblable à celles des théorèmes 4.2.9 et 4.3.12.*

Dans le reste du chapitre, on note $\mathcal{M}_{T,\alpha}$ et $\mathcal{M}_{T,\beta}$ les codes de *torsion* de $\mathcal{M}^{\alpha}_{(q,k,u)}$ et $\mathcal{M}^{\beta}_{(q,k,u)}$, respectivement. D´aprés, les distributions de poids de Hamming des codes de *torsion* $\mathcal{M}_{T,\alpha}$ et $\mathcal{M}_{T,\beta}$ on a les résultats suivants.

Théorème 4.4.6 *Le code de torsion $\mathcal{M}_{T,\alpha}$ est un code linéaire avec les paramètres $[2^{2^q k} - 2^{2^q u}; k; 2^{2^q k-1} - 2^{2^q u-1}]$. Le nombre de mots-code a un poids de Hamming $2^{2^q k-1} - 2^{2^q u-1}$ est égal à $2^k - 2^{k-u}$, Le nombre de mots-code a un poids de Hamming $2^{2^q k-1}$ est égal à $2^{k-u} - 1$, et il est un seul mots-code de poids zéro.*

Preuve 4.4.7 *La matrice génératrice du code de torsion $\mathcal{M}_{T,\alpha}$ obtenu en remplaçant $u_1u_2\cdots u_q$ dans la matrice $u_1u_2\cdots u_qG^{\alpha}_{(q,k,u)}$ par 1. similaire à la preuve de [3, Lemma 3.1], la preuve est achevé par récurrence sur k et u.*

- *Il est clair que le résultat est vrai pour $k = 2$ et $u = 1$.*
- *Supposons que le résultat est vrai pour $k-1$ et $1 \leq u \leq k-2$.*

Alors :

pour k et $1 \leq u \leq k-1$, la matrice $u_1u_2\cdots u_qG^{\alpha}_{(q,k,u)}$ prend la forme :

$$u_1u_2\cdots u_qG^{\alpha}_{(q,k,u)} = \left[\begin{array}{c|c} u_1u_2\cdots u_qG^{\alpha}_{(q,k)} & \begin{array}{c} 0_{2^{2^u}\times(k-u)} \\ \hline u_1u_2\cdots u_qG^{\alpha}_{(q,u)} \end{array} \end{array}\right]. \tag{4.11}$$

D´où, chaque mots-code non nul de $u_1u_2\cdots u_qG^{\alpha}_{(q,k,u)}$ a un poids de Hamming $2^{2^q k-1}-2^{2^q u-1}$ ou $2^{2^q k-1}$, et la dimension du code de torsion $\mathcal{M}_{T,\alpha}$ est égal k. Par conséquent, le nombre de mots-code ayant un poids de Hamming $2^{2^q k-1} - 2^{2^q u-1}$ est $2^k - 2^{k-u}$, et le nombre de mots-code ayant un poids de Hamming $2^{2^q k-1}$ est $2^{k-u} - 1$.

Théorème 4.4.8 *Les distributions de poids de Hamming, Lee et homogenène de $\mathcal{M}^{\alpha}_{(q,k,u)}$ sont :*

(i) $A_{Ham}(0) = 1$, $A_{Ham}(2^{2^q k-1} - 2^{2^q u-1}) = 2^k - 2^{k-u}$, *et* $A_{Ham}(2^{2^q k-1}) = 2^{k-u} - 1$.

(ii) $A_{Lee}(0) = 1$, $A_{Lee}(2^{2^q k+1}) = 2^{2^q(k-u)} - 1$, *et* $A_{Lee}(2^{2^q k+1} - 2^{2^q u+1}) = 2^{2^q(k-u)}(2^{2^q u} - 1)$.

(iii) $A_{hom}(0) = 1$, $A_{hom}(2^{2^q k+1}) = 2^{2^q(k-u)} - 1$, *et* $A_{hom}(2^{2^q k+1} - 2^{2^q u+1}) = 2^{2^q(k-u)}(2^{2^q u} - 1)$.

Preuve 4.4.9 *Par le lemme 4.2.3 et l´équation (4.9), il y a des mots-codes de* $\mathcal{M}^{\alpha}_{(q,k,u)}$ *a un poids de Hamming* $2^{2^q k-1} - 2^{2^q u-1}$ *ou* $2^{2^q k-1}$*, les poids de Lee et homogenène est* $2^{2^q k+1}$ *ou* $2^{2^q k+1} - 2^{2^q u+1}$*. De plus par le théorème 4.4.6 , la dimension du code de torsion* $\mathcal{M}_{T,\alpha}$ *est* k*. Ainsi, nous avons* $2^{k-u} - 1$ *mots-code de poids de Hamming* $2^{2^q k-1}$*.*

Alors, le nombre de mots -code ayant un poids de Hamming $2^{2^q k-1} - 2^{2^q u-1}$ *est* $2^k - 2^{k-u}$*.*

Théorème 4.4.10 *Le code de torsion* $\mathcal{M}_{T,\beta}$ *est un code linéaire de paramètres*

$$[2^{(2^q-1)(k-1)}(2^k-1) - 2^{(2^q-1)(u-1)}(2^u-1); k; 2^{2^q k-2^q} - 2^{2^q u-2^q}].$$

Le nombre de mots-code a un poids de Hamming $2^{2^q k-2^q} - 2^{2^q u-2^q}$ *est* $2^k - 2^{k-u}$*, le nombre de mots-code a un poids de Hamming* $2^{2^q k-2^q}$ *est* $2^{k-u} - 1$*, et il y a un seul mots code de poids* 0*.*

Preuve 4.4.11 *Résultat de la preuve du théorème 4.4.6.*

4.4.1 Les images binaires sous le Gray map des codes de Macdonald de type α et β sur R_q

Les images binaires sous le Gray map des codes de Macdonald de type α et β sont pris en considération dans ce qui suit :

Les images binaires sous le Gray map de code de MacDonald de type α

Dans cette partie nous déterminons les images binaires du code de MacDonald de type α sur R_q, dans le premier théorème nous pouvons utiliser le poids de Lee et dans le deuxième théorème nous pouvons utiliser le poids homogène.

Théorème 4.4.12 *Soit* $\mathcal{M}^{\alpha}_{(q,k,u)}$*, le code de MacDonald de type* α *sur* R_q *de longueur* $2^{2^q k} - 2^{2^q u}$*, et de poids de Lee minimal* d_{Lee}*, alors* $\Psi_{Lee}(S^{\alpha}_{(q,k)})$ *est la concaténation de* $\dfrac{2^{2^q k+q} - 2^{2^q u+q}}{2^k - 2^u}$ *codes de MacDonald binaires de paramètres.*

$$[2^{2^q k+q} - 2^{2^q u+q}; k; d_{Ham} = 2^{2^q k+q-1} - 2^{2^q u+q-1}].$$

Preuve 4.4.13 *La preuve est similaire à celle du Théorème 4.2.14.*

Théorème 4.4.14 *Soit $\mathcal{M}^{\alpha}_{(q,k,u)}$, le code de MacDonald de type α sur R_q de longueur $2^{2^q k} - 2^{2^q u}$, et de poids homogène minimal d_{hom}, alors $\Psi_{hom}(S^{\alpha}_{(q,k)})$ est la concaténation de $\dfrac{2^{2^q k+q+1} - 2^{2^q u+q+1}}{2^k - 2^u}$ codes de MacDonald binaires de paramètres.*

$$[2^{2^q k+q+1} - 2^{2^q u+q+1}; k; d_{Ham} = 2^{2^q k+q} - 2^{2^q u+q}].$$

Preuve 4.4.15 *La preuve est similaire à celle du Théorème 4.2.14.*

Les images binaires sous le Gray map de code de MacDonald de type β

Les images binaires sous le Gray map de code de MacDonald de Type β, sont données par :

Théorème 4.4.16 *Soit $\mathcal{M}^{\beta}_{(q,k,u)}$, le code de MacDonald de type β, sur R_q de longueur $2^{(2^q-1)(k-1)}(2^k-1)-2^{(2^q-1)(u-1)}(2^u-1)$ et de poids de Lee minimal d_{Lee}, alors $\Psi_{Lee}(S^{\beta}_{(q,k)})$ est la concaténation de $\dfrac{2^{(2^q-1)(k-1)+q}(2^k-1) - 2^{(2^q-1)(u-1)+q}(2^u-1)}{2^k - 2^u}$ codes de MacDonald binaires de paramètres.* $[2^{(2^q-1)(k-1)+q}(2^k-1)-2^{(2^q-1)(u-1)+q}(2^u-1); k; d_{Ham} = 2^{(2^q-1)(k-1)+q-1}(2^k-1) - 2^{(2^q-1)(u-1)+q-1}(2^u-1)]$.

Preuve 4.4.17 *La preuve est similaire à celle du Théorème 4.2.14.*

Théorème 4.4.18 *Soit $\mathcal{M}^{\beta}_{(q,k,u)}$, le code de MacDonald de type β, sur R_q de longueur $2^{(2^q-1)(k-1)}(2^k-1)-2^{(2^q-1)(u-1)}(2^u-1))$ et de poids homogène minimal d_{hom}, alors $\Psi_{hom}(S^{\beta}_{(q,k)}))$ est la concaténation des $\dfrac{2^{(2^q-1)(k-1)+(q+1)}(2^k-1) - 2^{(2^q-1)(u-1)+(q+1)}(2^u-1)}{2^k - 2^u}$ codes de MacDonald binaires de paramètres.* $[2^{(2^q-1)(k-1)+(q+1)}(2^k-1)-2^{(2^q-1)(u-1)+(q+1)}(2^u-1); k; d_{Ham} = 2^{(2^q-1)(k-1)+q}(2^k-1) - 2^{(2^q-1)(u-1)+q}(2^u-1)]$.

Preuve 4.4.19 *La preuve est similaire à celle du Théorème 4.2.16 et 4.3.16.*

4.5 Les rayons de recouvrement des codes Simplexes et MacDonald de type α et β

4.5.1 Les rayons de recouvrement des codes de répétitions sur R_q

Le code de répétition C sur un corps fini $\mathbb{F}_q$ est un $[n;1;n]$-code linéaire. Le rayon de recouvrement de C est $\lfloor \frac{n(q-1)}{q} \rfloor$ [40]. Soit

$$\mathcal{U}_A = \left(1 + \sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_\varnothing = 0 \vee A \neq \varnothing}} c_A u_A \right),$$

et

$$\mathcal{V}_A = \sum_{\substack{A \subseteq \{1,2,\ldots,q\} \\ c_\varnothing = 0 \vee A \neq \varnothing}} c_A u_A.$$

Il éxiste deux types de code de répétition qui sont définis sur R_q.

Type 1 Le code de répétition C_c généré par :

$$G_c = \left[\overbrace{cc\cdots c}^{n} \right]$$

où c est un élément de $R_q - \{0, u_1u_2\cdots u_q\}$.

Type 2 Le code de répétition $C_{u_1u_2\cdots u_q}$ généré par :

$$G_{u_1u_2\cdots u_q} = \left[\overbrace{u_1u_2\cdots u_qu_1u_2\cdots u_q\cdots u_1u_2\cdots u_q}^{n} \right].$$

Théorème 4.5.1 *Les rayons de recouvrement des codes de répétition sur R_q sont donnés par :*

(i) $r_{hom}(C_c) = 2^q n$ *et* $r_{Lee}(C_c) = 2^q n$.

(ii) $r_{hom}(C_{u_1u_2\cdots u_q}) = 2^{q+1} n$ *et* $r_{Lee}(C_{u_1u_2\cdots u_q}) = 2^q n$.

Preuve 4.5.2 *pour la partie (i), par la définition de* $r_{hom}(C_c) = \max_{x \in (R_q)^n} d\{x, C_c\}$. *Soit*

$$x \in (R_q - \{0, u_1u_2\cdots u_q\})^n.$$

Alors, comme une conséquence directe, pour tout $y \in C_c$ on a $d\{x, y\} = 2^q n$, de sorte que $r_{hom}(C_c) = 2^q n$. Par la proposition 2.4.3, on obtient $r_{Lee}(C_c) = r_{Ham}(\Psi_{Lee}(C_c)) = 2^q n$. Même preuve de la partie (ii).

Soit C le code linéaire sur R_q généré par la matrice

$$G = \left[\overbrace{11\cdots1}^{n}\overbrace{u_1u_1\cdots u_1}^{n}\cdots\overbrace{\mathcal{U}_A\mathcal{U}_A\cdots\mathcal{U}_A}^{n}\right].$$

Alors C est le code de répétition de longueur $(2^{2^q} - 1)n$.

Théorème 4.5.3 *Un code linéaire C généré par la matrice*

$$G = \left[\overbrace{11\cdots1}^{n}\overbrace{u_1u_1\cdots u_1}^{n}\cdots\overbrace{\mathcal{U}_A\mathcal{U}_A\cdots\mathcal{U}_A}^{n}\right],$$

a un rayon de recouvrement donné par :

$$r_{hom}(C) = 2^{2^q+q}n \text{ et } r_{Lee}(C) = (2^{2^q} - 1)2^{q-1}n.$$

Preuve 4.5.4 *Les vecteurs de C générés par G peuvent être divisés en trois classes.*

Classe 1 *Les vecteurs de C avec des composantes de tous les éléments de R_q*

$$x_a = (x_1x_2\cdots x_n) \in C, x_i \in R_q \text{ pour tout } 1 \leq i \leq n.$$

Classe 2 *Les vecteurs de C avec des composantes qui sont des diviseurs de zéro de R_q*

$$x_b = (x_1x_2\cdots x_n) \in C, x_i \in \mathfrak{D}(R_q) \text{ pour tout } 1 \leq i \leq n.$$

Classe 3 *Les composantes des vecteurs de C sont 0 ou $u_1u_2\cdots u_q$*

$$x_c = (x_1x_2\cdots x_n) \in C, x_i \in \{0, u_1u_2\cdots u_q\} \text{ pour tout } 1 \leq i \leq n.$$

Pour $x \in (R_q)^n$, nous avons :

$$d(x, x_a) = d(x, x_b) = d(x, x_c) = 2^{2^q+q}n,$$

ainsi

$$r_{hom}(C) \geqslant 2^{2^q+q}n.$$

Pour le premier cas *si* $x = (11\cdots1) \in (R_q)^n$ *et* $x_a = (1u_1\cdots\mathcal{U}_A) \in (R_q)^n$, *on a*

$$x + x_a = (0(1+u_1)\cdots\mathcal{V}_A),$$

est une permutation équivalente à x_a *c´est-à-dire*

$$x + x_a = \sigma(x_a),$$

alors :

$$d(x, x_a) \leq 2^{2^q+q}n,$$

par conséquent

$$r_{hom}(C) \leq 2^{2^q+q}n.$$

Pour le deuxième cas *si* $x = (11\cdots1) \in (R_q)^n$ *et* $x_b = (u_1u_2\cdots\mathcal{V}_A) \in (\mathfrak{D}(R_q))^n$, *on a :*

$$x + x_b = ((1+u_1)(1+u_2)\cdots\mathcal{U}_A) \in (\mathfrak{U}(R_q))^n,$$

alors :

$$d(x, x_b) \leq 2^{2^q+q}n,$$

ainsi

$$r_{hom}(C) \leq 2^{2^q+q}n.$$

Pour le troisième cas *si* $x = (11\cdots1) \in (R_q)^n$ *et* $x_c = (0(u_1u_2\cdots u_q)\cdots(u_1u_2\cdots u_q)) \in (\mathfrak{D}(R_q))^n$, *on a :*

$$x + x_c = (1(1+u_1u_2\cdots u_q)\cdots(1+u_1u_2\cdots u_q)) \in (\mathfrak{U}(R_q))^n,$$

alors :

$$d(x, x_c) \leq 2^{2^q+q}n,$$

d´où :

$$r_{hom}(C) \leq 2^{2^q+q}n.$$

Par la Proposition 2.4.3 on a :

$$r_{Lee}(C) = r_{Ham}(\Psi_{Lee}(C)) = (2^{2^q}-1)2^{q-1}n.$$

4.5.2 Les rayons de recouvrement des codes simplexes de type α et β

Les rayons de recouvrement des codes simplexes de type α et β sur R_q sont donnés par les théorèmes suivants.

Théorème 4.5.5 *Les rayons de recouvrement des codes simplexes de type α sur R_q, par rapport aux poids homogène et le poids de Lee sont :*

(i) $r_{hom}(S^{\alpha}_{(q,k)}) = k \cdot 2^{2^q k+q}$.

(ii) $r_{Lee}(S^{\alpha}_{(q,k)}) = 2^{(2^q+1)k+1}$.

Preuve 4.5.6 *Pour la partie (i), si $x \in (R_q)^n$, on a :*

$$d_{hom}(x, S^{\alpha}_{(q,k)}) = k \cdot 2^{2^q k+q}.$$

Par la définition de rayon de recouvrement l´inégalité suivante est vraie

$$r_{hom}(S^{\alpha}_{(q,k)}) \geqslant k \cdot 2^{2^q k+q}.$$

D´autre part, en appliquant la proposition 2.4.1, et le théorème 4.5.3 on obtient :

$$\begin{aligned} r_{hom}(S^{\alpha}_{(q,k)}) &\leq r_{hom}\left(\left[\overbrace{11\cdots1}^{2^{2^q}(k-1)}\overbrace{u_1u_1\cdots u_1}^{2^{2^q}(k-1)}\cdots\overbrace{\mathcal{U}_A\mathcal{U}_A\cdots\mathcal{U}_A}^{2^{2^q}(k-1)}\right]\right) + 2^{2^q}\cdot r_{hom}(S^{\alpha}_{(q,k-1)}) \\ &\leq 2^{2^q k+q} + 2^{2^q(k-1)+q}\cdot 2^{2^q} + \cdots + 2^{q\cdot 2^q}\cdot r_{hom}(S^{\alpha}_{(q,1)}) \\ &\leq 2^{2^q k+q} + 2^{2^q(k-1)+q}\cdot 2^{2^q} + \cdots + 2^{2^q(k-q)+q}\cdot 2^{q\cdot 2^q} \\ &\leq k \cdot 2^{2^q k+q}. \end{aligned}$$

Pour la partie (ii), Par la proposition 2.4.3 on a

$$r_{Lee}(S^{\alpha}_{(q,k)}) = r_{Ham}(\Psi_{Lee}(S^{\alpha}_{(q,k)})) = 2^{(2^q+1)k+1}.$$

Théorème 4.5.7 *Le rayon de recouvrement des codes simplexes de type β sur R_q, par rapport aux poids homogène et au poids de Lee sont :*

(i) $r_{hom}(S^{\beta}_{(q,k)}) = 2^{2^q(k-2)+q}\left[2^{2^q}(k-2^{-q}) + 4 - 2^{-q+1}\right]$.

(ii) $r_{Lee}(S^{\beta}_{(q,k)}) = 2^{(2^q-1)(k-1)+(q-1)}(2^k-1)$.

Preuve 4.5.8 *Pour la partie (i), si* $x \in (R_q)^n$, *on a :*

$$d_{hom}(x, S^{\beta}_{(q,k)}) = 2^{2^q(k-2)+q}\left[2^{2^q}(k-2^{-q})) + 4 - 2^{-q+1}\right],$$

par la définition de rayon de recouvrement, on a :

$$r_{hom}(S^{\beta)}_{(q,k)} \geqslant 2^{2^q(k-2)+q}\left[2^{2^q}(k-2^{-q})) + 4 - 2^{-q+1}\right].$$

D´autre part, en appliquant la proposition 2.4.1 et le Théorème 4.5.3 on obtient :

$$\begin{aligned}
r_{hom}(S^{\beta}_{(q,k)}) &\leq r_{hom}\left(\left[\overbrace{1\cdots 1}^{2^{2^q}(k-1)} \cdots \overbrace{\mathcal{V}_A\cdots\mathcal{V}_A}^{2^{(2^q-1)(k-1)}(2^k-1)}\right]\right) + r_{hom}(S^{\alpha}_{(q,k-1)}) + 2^{2^q-1}\cdot r_{hom}(S^{\beta}_{(q,k-1)}) \\
&\leq 2^{2^q(k-2)+q}\left(2^{2^q-1}+2\right) + \cdots + 2^{2^q(k-2)+q}(k-1) + 2^{q\cdot 2^q-q}\cdot r_{hom}(S^{\beta}_{(q,2)}) \\
&\leq 2^{2^q(k-2)+q}(2^{2^q-1}+2)(2-2^{-q}) + \cdots + 2^{2^q(k-2)+q}(k-1) \\
&\leq 2^{2^q(k-2)+q}\left[2^{2^q}(k-2^{-q})) + 4 - 2^{-q+1}\right],
\end{aligned}$$

et le reste, à partir d´une approche similaire à la preuve de la partie (ii) du théorème 4.5.5.

4.5.3 Les rayons de recouvrement des codes de MacDonald de type α et β

Les rayons de recouvrement des codes de MacDonald de type α et β sur R_q sont donnés par les théorèmes suivants.

Théorème 4.5.9 *Les rayons de recouvrement des codes de MacDonald de type* α *sur* R_q *par rapport aux poids homogène et poids de Lee sont :*

(i) Pour $u \leq e \leq k$, $r_{hom}(\mathcal{M}^{\alpha}_{(q,k,u)}) \leq 2^{2^q k} - 2^{2^q u} + r_{hom}(\mathcal{M}^{\alpha}_{(q,e,u)})$.

(ii) $r_{Lee}(\mathcal{M}^{\alpha}_{(q,k,u)}) = 2^{2^q k+(q-1)} - 2^{2^q u+(q-1)}$.

Preuve 4.5.10 *Pour la première partie, on applique la proposition 2.4.1, et le théorème 4.5.3, si $u \leq e \leq k$, on a :*

$$\begin{aligned} r_{hom}(\mathcal{M}^{\alpha}_{(q,k,u)}) &\leq (2^{2^q}-1)(2^{2^qk-2^q}) + r_{hom}(\mathcal{M}^{\alpha}_{(q,k-1,u)}) \\ &\leq (2^{2^q}-1)(2^{2^qk-2^q}) + (2^{2^q}-1)(2^{2^qk-(2^q-2)}) + \cdots + (2^{2^q}-1)2^{2^qe} \\ &\quad + r_{hom}(\mathcal{M}^{\alpha}_{(q,e,u)}) \\ &\leq 2^{2^qk} - 2^{2^qe} + r_{hom}(\mathcal{M}^{\alpha}_{(q,e,u)}). \end{aligned}$$

Pour la deuxième partie, par la proposition 2.4.3, on obtient :

$$r_{Lee}(\mathcal{M}^{\alpha}_{(q,k,u)}) = r_{Ham}(\Psi_{Lee}(\mathcal{M}^{\alpha}_{(q,k,u)})) = 2^{2^qk+(q-1)} - 2^{2^qu+(q-1)}.$$

Théorème 4.5.11 *Les rayons de recouvrements des codes de MacDonald de type β sur R_q par rapport aux poids homogènes, et poids de Lee sont :*

(i) Pour $u \leq e \leq k$, $r_{hom}(\mathcal{M}^{\beta}_{(q,k,u)}) \leq 2^{(2^q-1)(k-1)}(2^k-1) - 2^{(2^q-1)(u-1)}(2^u-1) + r_{hom}(\mathcal{M}^{\beta}_{(q,e,u)})$.

(ii) $r_{Lee}(\mathcal{M}^{\beta}_{(q,k,u)}) = 2^{(2^q-1)(k-1)+(q-1)}(2^k-1) - 2^{(2^q-1)(u-1)+(q-1)}(2^u-1)$.

Preuve 4.5.12 *Pour la première partie, on applique la proposition 2.4.1, et le théorème 4.5.3, si $u \leq e \leq k$, on a :*

$$\begin{aligned} r_{hom}(\mathcal{M}^{\beta}_{(q,k,u)}) &\leq (2^{2^q}-1)2^{(2^q-1)(k-1)-(2^q-1)}(2^k-1) + r_{hom}(\mathcal{M}^{\beta}_{(q,k-1,u)}) \\ &\leq (2^{2^q}-1)2^{(2^q-1)(k-1)-(2^q-1)}(2^k-1) + (2^{2^q}-1)2^{(2^q-1)(k-1)-((2^q-1)-2)}(2^k-1) \\ &+ \cdots + (2^{2^q}-1)2^{(2^q-1)(k-1)-(2^e-1)}(2^k-1) + r_{hom}(\mathcal{M}^{\beta}_{(q,e,u)}) \\ &\leq 2^{(2^q-1)(k-1)}(2^k-1) - 2^{(2^q-1)(e-1)}(2^e-1) + r_{hom}(\mathcal{M}^{\beta}_{(q,e,u)}). \end{aligned}$$

Pour la deuxième partie, par la proposition 2.4.3, on obtient que

$$r_{Lee}(\mathcal{M}^{\beta}_{(q,k,u)}) = r_{Ham}(\Psi_{Lee}(\mathcal{M}^{\beta}_{(q,k,u)})) = 2^{(2^q-1)(k-1)+(q-1)}(2^k-1) - 2^{(2^q-1)(u-1)+(q-1)}(2^u-1).$$

Chapitre 5

Schémas de partage d´un secret basé sur les codes linéaires

5.1 Introduction

L´étude des schémas du partage d´un secret a été crée pour la premiére fois par Shamir et Blakely en 1979. Depuis ce moment là, les auteurs ont commencé à construire les schémas du partage d´un secret en utilisant les codes correcteurs d´erreurs linéaires. En plus, Massey a utilisé les codes linéaires pour découvrir les schémas du partage d´un secret, puis il construit la relation entre l´accès structure, et les mots-code minimal du code dual des codes sous-adjacents [50].

Les schémas de partage d´un secret sont des outils utilisés dans plusieur protocoles cryptographiques. Ils contiennentt un **dealer** qui a un secret, un ensemble de $n-1$ parties, et une collection $\mathcal{A}$ de sous-ensembles des partis qui s´appellent la structure d´accès. Plusieurs auteurs ont examiné certains codes linéaires et ont caractérisé d´accès structure des schémas de partage d´un secret à partir de leurs codes duals [46] et [50].

Dans ce chapitre, nous construisons les codes de *torsion* des codes de MacDonald de type α et β sur l´anneau $R_{q,m}$ et aussi les images Gray des codes simplexes sur cet anneau et nous donnons la construction des schémas de partage d´un secret à partir de ces codes

linéaires [19].

5.2 L´anneau $R_{q,m}$

Soit $R_{q,m}$ l´anneau $\mathbb{F}_{2^m}[u_1, u_2 \cdots u_q]/\langle u_i^2 = 0, u_i u_j - u_j u_i \rangle$, avec $R_{0,m} = \mathbb{F}_{2^m}$, et $R_{q,1} = R_q = \mathbb{F}_2[u_1, u_2 \cdots u_q]/\langle u_i^2 = 0, u_i u_j - u_j u_i \rangle$. Nous rappelons certaines propriétés de base, l´anneau $R_{q,m}$ est un anneau commutatif de Frobenius local avec $|R_{q,m}| = 2^{m2^q}$.

Pour tout sous-ensemble $A \subseteq \{1, 2, \cdots, q\}$, on a :

$$u_A = \prod_{i \in A} u_i,$$

avec la convention $u_\emptyset = 1$, alors tous les éléments de $R_{q,m}$ peu veut exprimés par :

$$\mathcal{U}_A = \sum_{A \subseteq \{1,2,\ldots,q\}} c_A u_A, \text{avec } c_A \in \mathbb{F}_{2^m}.$$

On note l´ensemble des unités de $R_{q,m}$ par $\mathcal{U}(R_{q,m})$ et les non-unités par $\mathcal{D}(R_{q,m})$. Il apparaît clairement que $|\mathcal{U}(R_{q,m})| = |\mathcal{D}(R_{q,m})| = 2^{m2^q - 1}$.

Si $\mathcal{U}_{A \subset \{1,2,\cdots,q\}} \in \mathcal{U}(R_{q,m})$ et $\mathcal{V}_{A \subset \{1,2,\cdots,q\}} \in \mathcal{V}(R_{q,m})$, alors $\mathcal{V}_A = \mathcal{U}_A + 1$.

Un code linéaire de longueur n sur $R_{q,m}$ est défini comme un $R_{q,m}$-sous module de $R_{q,m}^n$.

Le code de *torsion* de code C sur $R_{q,m}$ est défini par :

$$Tor_A(C) = \{v \in \mathbb{F}_{2^m}^n;\ u_A v \in C, A \subset \{1, \cdots, q\}\}.$$

5.3 Lien entre les schémas du partage de secret et les codes linéaires

Soit $[n; k; d; q]$-code C un sous espace linéaire de $\mathbb{F}_q^n$ de dimension k, et un poids de Hamming non nul minimal d. Si

$$G = [g_0, g_1, \cdots, g_{n-1}]$$

est une matrice génératrice d´un $[n, k, d; q]$-code, c´est-à-dire, les vecteurs lignes de G génèrent le sous-espace linéaire C.

Pour tous les codes linéaires mentionnés dans ce chapitre, nous supposons toujours que tout les vecteurs colonnes de toutes les matrices génératrice sont non nuls.

• le schéma de partage de secret construit à partir de C, est un élément de $\mathbb{F}_q$, le dealer P_0 est inclus dans les $n-1$ parties $P_1, P_2, \cdots, P_{n-1}$.

• Pour calculer les actions concernant un secret s, le dealer choisit aléatoirement un vecteur

$$u = (u_0, u_1, \cdots, u_{k-1}) \in \mathbb{F}_q^k,$$

comme $s = ug_0$. Il y a q^{k-1} vecteur $u \in \mathbb{F}_q^k$.

• Le dealer donc traite u comme un vecteur d´information et calcule le mot code correspondant

$$v = uG = (v_0, v_1, \cdots, v_{n-1}).$$

Donc, il donne v_i une partie de P_i comme action pour chaque $i \geqslant 1$.

• Tant que $s = v_0 = ug_0$, alors l´ensemble des actions $(v_{i_1}, v_{i_2}, \cdots, v_{i_m})$ détermine le secret s si et seulement si la colonne g_0 de la matrice génératrice G est une combinaison linéaire des colonnes $g_{i_1}, g_{i_2}, \cdots, g_{i_m}$ de G. C´est pour ça nous avons la proposition suivante [46].

Proposition 5.3.1 *Soit G une matrice génératrice d´un $[n; k; d; q]$-code C. Dans le schéma de partage du secret basé sur C, l´ensemble des actions $(v_{i_1}, v_{i_2}, \cdots, v_{i_m})$ détermine le secret si et seulement s´il existe un mots-code*

$$(1, 0, \cdots, 0, c_{i_1}, 0, \cdots, c_{i_m}, 0, \cdots, 0).$$

dans $C^{\perp}$ avec $c_{i_j} \neq 0$ pour au moins un j, $1 \leqslant i_1 \leqslant \cdots \leqslant i_m \leqslant n-1$ et $1 \leqslant m \leqslant n-1$

S´il y a un mots-code qui vérifie les hypothèses de la proposition ci-dessus, donc

$$g_0 = \sum_{j=1}^{m} a_j g_{i_j},$$

le secret s est récupéré par calcule de :

$$s = \sum_{j=1}^{m} a_j v_{i_j}$$

.

Si un groupe des participants peut récupérer le secret en combinant leurs actions, donc chaque groupe des participants qui contient ce groupe peut aussi récupérer le secret. Un groupe des participants est appelé un ensemble d´accès minimal s´ils peuvent récupérer le secret avec leurs actions. Pour déterminer l´ensemble des ensembles d´accès minimal, nous avons le concept de mots code minimal.

Définition 5.3.2 • *Le support d´un mots-code* $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbb{F}_q^n$ *est défini comme suit :*

$$supp(c) = \{i | 0 \leqslant i \leqslant n-1; c_i \neq 0\}.$$

• *Soit* c *et* $c^{'}$ *deux mots-code du code* C*. On dit que* c *est un recouvrement de* $c^{'}$ *si et seulement si* $wt(c \otimes c^{'}) = wt(c^{'})$*, où,* $c \otimes c^{'} = (c_0 c_0^{'}, c_1 c_1^{'}, \cdots, c_{n-1} c_{n-1}^{'})$*,* $c = (c_0, c_1, \cdots, c_{n-1})$ *et* $c^{'} = (c_0^{'}, c_1^{'}, \cdots, c_{n-1}^{'})$*. Un mots-code non nul* $c \in C$ *est dit minimal si les seuls mots-code de recouvrement sont les scalaires multiples.*

Moyennant la proposition 5.3.1, et le définition 5.3.2, il est clair qu'il n'y a un-à-un correspondance entre l´ensemble des ensembles d´accès minimale et l´ensemble des mots-code minimaux du code dual $C^{\perp}$.

5.4 Codes simplexes et les codes de MacDonald de type α et β sur $R_{q,m}$

Dans cette partie, nous allons construire les codes simplexes et Macdonald sur $R_{q,m}$ de type α et β, et nous donnons les distributions de poids de Hamming des codes de *torsion*, des codes simplexes et des codes de MacDonald.

Les codes simplexes sur R_q de type α et β ont été construit dans [18]. Même dans [18] un code simplexe $S^{\alpha}_{(q,m,k)}$ de type α sur $R_{q,m}$ à une longueur 2^{m2^qk} est un code linéaire sur $R_{q,m}$ admet la matrice génératrice suivante :

$$G^{\alpha}_{(q,m,k)} = \left[\begin{array}{c} 1_{2^{m2^q\cdot(k-1)}} \otimes G^{\alpha}_{(q,m,k-1)} \\ \hline (012\cdots\mathcal{U}_{\{1,2,\cdots,q\}}) \otimes 1_{2^{m2^q\cdot(k-1)}} \end{array} \right], \text{ pour } \ k \geq 2 \tag{5.1}$$

où,

$$G^{\alpha}_{(q,m,1)} = \left[0\ 1\ u_1\ \cdots\ \mathcal{U}_{\{1,2,\cdots,q\}}\right].$$

Les codes simplexes $S^{\beta}_{(q,m,k)}$ de type β sur $R_{q,m}$ sont construit en omettant certaines colonnes de $G^{\alpha}_{(q,m,k)}$. Soit $G^{\beta}_{(q,m,k)}$ une matrice de taille $k \times \frac{2^{m(2^q-1)(k-1)}(2^{mk}-1)}{2^m-1}$ défini par :

$$G^{\beta}_{(q,m,k)} = \left[\begin{array}{c|c} 1_{2^{m2^q\cdot(k-1)}} & (024\cdots\mathcal{V}_{\{1,2,\cdots,q\}}) \otimes 1_{\frac{2^{m2^q(k-2)}\left(2^{m(k-1)}-1\right)}{2^m-1}} \\ \hline G^{\alpha}_{(q,m,k-1)} & 1_{\frac{2^{m2^q(k-2)}\left(2^{m(k-1)}-1\right)}{2^m-1}} \otimes G^{\beta}_{(q,m,k-1)} \end{array} \right], \tag{5.2}$$

pour $k > 2$, et

$$G^{\beta}_{(q,m,2)} = \left[\begin{array}{c|c} 1_{2^{m2^q}} & 024\cdots\mathcal{V}_{\{1,2,\cdots,q\}} \\ \hline 0\ 1\ \ldots\mathcal{U}_{\{1,2,\cdots,q\}} & 1_{2^{m2^q-1}} \end{array} \right],$$

Les codes de MacDonald de type α et β sur R_q sont définis dans [17]. Nous obtenons les codes de MacDonald de type α et β sur $R_{q,m}$, après les mêmes étapes dans [18]. Pour $1 \leq u \leq k-1$, le code de MacDonald $\mathcal{M}^{\alpha}_{(q,m,k,u)}$ est un code sur $R_{q,m}$ de longueur $2^{m2^qk} - 2^{m2^qu}$, il est généré par :

$$G^{\alpha}_{(q,m,k,u)} = \left[\begin{array}{c} G^{\alpha}_{(q,m,k)} \\ \setminus \\ \frac{0_{2^{m2^qu}\times(k-u)}}{G^{\alpha}_{(q,m,u)}} \end{array} \right], \tag{5.3}$$

et le code de MacDonald $\mathcal{M}^{\beta}_{(q,m,k,u)}$ est un code sur $R_{q,m}$ de longueur

$$\frac{2^{m(2^q-1)(k-1)}(2^{mk}-1) - 2^{m(2^q-1)(u-1)}(2^{mu}-1)}{2^m-1},$$

il est généré par :

$$G^{\beta}_{(q,m,k,u)} = \left[\begin{array}{c} G^{\beta}_{(q,m,k)} \\ \setminus \\ \frac{0_{\frac{2^{m(2^q-1)(u-1)}(2^{mu}-1)\times(k-u)}{2^m-1}}}{G^{\beta}_{(q,m,u)}} \end{array} \right]. \tag{5.4}$$

où, $(A \setminus B)$ désigne la matrice obtenue à partir de la matrice A par l´élimination de la matrice B.

Cette construction nous permet de définir de nouveaux codes linéaires sur $\mathbb{F}_{2^m}$ qui sont les codes de *torsion*.

Maintenant, soient $\mathcal{S}_{(T,\alpha)}$ et $\mathcal{S}_{(T,\beta)}$ les codes de *torsion* de $S^{\alpha}_{(q,m,k)}$ et $S^{\beta}_{(q,m,k)}$, respectivement, et soient $\mathcal{M}_{(T,\alpha)}$ et $\mathcal{M}_{(T,\beta)}$ les codes de *torsion* de $\mathcal{M}^{\alpha}_{(q,m,k,u)}$ et $\mathcal{M}^{\beta}_{(q,m,k,u)}$, respectivement.

Les distributions de poids de Hamming de ces codes de *torsion* sont données dans les théorèmes suivants.

Théorème 5.4.1 *La distribution des poids de Hamming des codes de torsion $S_{T,\alpha}$ et $S_{T,\beta}$ à des paramètres $[2^{m2^q k}; k; 2^{m2^q(k-1)}]$ et $[\frac{2^{m(2^q-1)(k-1)}(2^{mk}-1)}{2^m-1}; k; 2^{m2^q(k-1)}]$ sont donnés par :*

(i) Pour $S_{T,\alpha}$ on a, $A_H((2^{(m2^q k-t)})(2^t-1)) = 2^{(t-1)k}(2^t-1)$, pour $0 \leq t \leq q$.

(ii) Pour $S_{T,\beta}$ on a, $A_{Ham}(2^{(2^q-1)(k-1)}[(2^{k-t}(2^t-1)+(2^{1-t}-1)]) = 2^{(t-1)k}(2^t-1)$, pour $0 \leq t \leq q$.

Preuve 5.4.2 *Pour la première partie, la matrice génératrice du code de torsion $S_{T,\alpha}$ est obtenue par le remplacement de $u_{\{1,2,\cdots,q\}}$ dans la matrice $c_{\{1,2,\cdots,q\}}u_{\{1,2,\cdots,q\}}G^{\alpha}_{(q,m,k)}$, où $c_{\{1,2,\cdots,q\}} \in \mathbb{F}^*_{2^m}$ par 1.*

La matrice $c_{\{1,2,\cdots,q\}}u_{\{1,2,\cdots,q\}}G^{\alpha}_{(q,m,k)}$ est de la forme :

$$c_{\{1,2,\cdots,q\}}u_{\{1,2,\cdots,q\}}G^{\alpha}_{(q,m,k)} = \left[\begin{array}{c} (0\ c_{\{1,2,\cdots,q\}}u_{\{1,2,\cdots,q\}}) \otimes 1_{2^{m2^q-1}} \\ \hline 1_{2^{m2^q}} \otimes c_{\{1,2,\cdots,q\}}u_{\{1,2,\cdots,q\}}G^{\alpha}_{(q,m,k-1)} \end{array}\right]. \tag{5.5}$$

On remplace maintenant $u_{\{1,2,\cdots,q\}}$ par 1, on a :

$$\widehat{G}_{q,mk} = \left[\begin{array}{c} (0\ c_{\{1,2,\cdots,q\}}) \otimes 1_{2^{m2^q-1}} \\ \hline 1_{2^{m2^q}} \otimes c_{\{1,2,\cdots,q\}}\widehat{G}_{k-1} \end{array}\right]. \tag{5.6}$$

Le code de torsion $S_{T,\alpha}$ est un code linéaire $\mathbb{F}_{2^m}$ de dimension k généré par $\widehat{G}_{q,m,k}$. Chaque mots-code non nul de $S_{T,\alpha}$ a un poids de Hamming $(2^{(m2^q k-t)})(2^t-1)$, pour $0 \leq t \leq q$. Même démonstration pour la deuxièmes partie.

Théorème 5.4.3 *Les distributions de poids de Hamming des codes de torsion $\mathcal{M}_{T,\alpha}$ et $\mathcal{M}_{T,\beta}$ a des paramètres*

$$[2^{m2^qk} - 2^{m2^qu}; k; 2^{m2^qk-1} - 2^{m2^qu-1}]$$

et

$$[\frac{2^{(m2^q-1)(k-1)}(2^k-1) - 2^{(m2^q-1)(u-1)}(2^u-1)}{2^m-1}; k; 2^{m2^qk-2^q} - 2^{m2^qu-2^q}]$$

sont donnés par :

1. *Pour $\mathcal{M}_{T,\alpha}$ on a, $A_H(2^{m2^qk-1}-2^{m2^qu-1}) = 2^{mk}-2^{m(k-u)}$ et $A_H(2^{m2^qk-1}) = 2^{m(k-u)}-1$*
2. *Pour $\mathcal{M}_{T,\beta}$ on a,$A_H(2^{m2^qk-2^q}-2^{m2^qu-2^q}) = 2^{mk}-2^{m(k-u)}$ et $A_H(2^{m2^qk-2^q}) = 2^{m(k-u)}-1$*

Preuve 5.4.4 *Similaire à la démonstration du théorème 5.4.1.*

5.5 Accès structure des schémas de partage de secret basé sur les codes de *torsion*

Dans cette partie, en se basant sur le résultat [46], qui montre les ensembles d´accès minimales du schéma de partage de secret basé sur $C^\perp$, nous allons étudier les schémas de partage de secrets obtenus à partir des codes duaux des codes de *torsion* des codes simplexes, et des codes de MacDonald de types α et β sur $R_{q,m}$.

Théorème 5.5.1 *Soit C un $[n; k; d]$-code linéaire sur $\mathbb{F}_q$ a une matrice génératrice*

$$G = [g_0, g_1, \cdots, g_{n-1}]$$

et soit $C^\perp$ son code dual de distance minimale $d^\perp$. Si chaque mots-code non nul de C est minimal, alors dans le schéma de partage de secret basé sur $C^\perp$ il y a q^{k-1} ensembles d´accès minimales est :

1. *Si* $d^{\perp} = 2$,

   a) Si g_i *est un multiple de* g_0, $1 \leqslant i \leqslant n-1$, *alors le participant* P_i *doit être dans chaque ensemble d´accès minimal.*

   b) Si g_i *n´est pas un multiple de* g_0, $1 \leqslant i \leqslant n-1$, *Alors le participant* P_i *doit être dans* $(q-1)q^{k-2}$ *ensemble d´accès minimal.*

2. *Si* $d^{\perp} \geqslant 2$,

$$1 \leqslant t \leqslant min\{k-1, d^{\perp}-1\}$$

   chaque groupe de t participants est impliqué dans

$$(q-1)^t q^{k-(t+1)}$$

   ensemble d´accès minimal.

La condition suffisante de poids, est décrite par le lemme suivant.

Lemme 5.5.2 *Soit* C *un* $[n; k; d; q]$*-code linéaire sur un corps fini* $\mathbb{F}_q$. *Soient* w_{min} *et* w_{max} *les poids minimaux et maximaux non nulles de* C, *respectivement. Si*

$$\frac{w_{min}}{w_{max}} \geqslant \frac{q-1}{q},$$

alors tous les mots-code non nuls de C *sont minimaux.*

Nous allons appliquer les schémas de partage de secret sur les codes de *torsion* des codes simplexes de type β et les codes de MacDonald de type α et β, nous avons les résultats suivants :

Théorème 5.5.3 *Soit* $S_{T,\beta}$ *un code de torsion sur* $\mathbb{F}_{2^m}$ *de* $S^{\beta}_{(q,m,k)}$, *alors dans le schéma de partage du secret basé sur* $S^{\perp}_{T,\beta}$, *Il y a en tout* $2^{m(k-1)}$ *ensembles d´accès minimal et* $\frac{2^{m(2^q-1)(k-1)}(2^{mk}-1)}{2^m-1} - 1$ *participants. De plus, chaque participant* P_i *est impliqué dans* $(2^m - 1)2^{mk-2}$ *ensembles d´accès minimal.*

Preuve 5.5.4 *D´après le théorème 5.4.1 on a,* $w_{min} = w_{max}$, *alors le lemme 5.5.2, est vérifié et tous les mots-code non nuls de* $S_{T,\beta}$ *sont minimaux.*

Théorème 5.5.5 *Soit $\mathcal{M}_{T,\alpha}$ (resp., $\mathcal{M}_{T,\beta}$) un code de torsion sur $\mathbb{F}_{2^m}$ de $\mathcal{M}^{\alpha}_{(q,m,k,u)}$ (resp., $\mathcal{M}^{\beta}_{(q,m,k,u)}$), alors dans le schéma de partage du secret basé sur $\mathcal{M}^{\perp}_{T,\alpha}$ (resp., $\mathcal{M}^{\perp}_{T,\beta}$), Il y a en tout $2^{m(k-1)}$ ensembles d´accès minimal et $2^{m2^qk}-2^{m2^qu}-1$ (resp., $\frac{2^{m(2^2-1)(k-1)}(2^{mk}-1)}{2^m-1}-\frac{2^{m(2^2-1)(u-1)}(2^{mu}-1)}{2^m-1}-1$) participants. De plus, chaque participant P_i est impliqué dans $(2^m-1)2^{mk-2}$ ensembles d´accès minimal.*

Preuve 5.5.6 *Soient w_{min} et w_{max} le poids minimal et maximal non nuls du code de torsion $\mathcal{M}_{T,\alpha}$. Alors, par le théorème 5.4.3, pour tout $1 \leqslant u \leqslant k-1$:*

$$\begin{aligned} \frac{w_{min}}{w_{max}} &= \frac{2^{m2^qk-1}-2^{m2^qu-1}}{2^{m2^qk-1}} = 1-\frac{2^{m2^qu-1}}{2^{m2^qk-1}} \\ &> \frac{2^m-1}{2^m} \\ &\geq \frac{1}{2}. \end{aligned}$$

Par conséquent, nous pouvons obtenir le minimal de tous les mots-codes non nuls de code de torsion $\mathcal{M}_{T,\alpha}$ par le Lemme 5.5.2. La même preuve pour $\mathcal{M}_{T,\beta}$.

Exemple 5.5.7 *Soient $m=2$ et $q=1$, nous considérons l´anneau $R_{1,2}=\mathbb{F}_4+u_1\mathbb{F}_4$ avec $u_1^2=0$. Nous étudions le code de torsion $S_{T,\beta}$, pour $k=2$. Dans ce cas, nous avons*

$$\widehat{G}_{1,2,2}=\left[\begin{array}{c|c} 1111111111111111 & 02020202 \\ \hline 0123012301230123 & 11111111 \end{array}\right],$$

la matrice génératrice du code de torsion $S_{T,\beta}$ sur $\mathbb{F}_4$.

Le code de torsion $S_{T,\beta}$ est un 2-ary $[24;2;20]$-code. Ces distributions de poids de Hamming sont $A_H(0)=1$, $A_H(20)=15$.

Alors nous construisons le SSS basé sur $S^{\perp}_{T,\beta}$. Le résultat suivant représente sa structure d´accès correspondante. On a 23 participants et 4 ensembles qualifiés minimaux. Les 4 ensembles qualifiés minimaux sont

$$c_1 = 11111111111111102020202,$$

$$c_2 = 12301230123012301313131 3,$$

$$c_3 = 131313131313131320202020,$$

$$c_4 = 10321032103210323131313 1.$$

L´ensemble des participants contiennent les sous-ensembles suivants

$\{1,2,3\}$, $\{2,4,6\}$, $\{3,6,9\}$, $\{1,2\}$, $\{2,4\}$, $\{3,6\}$, $\{1,2,3,4\}$, $\{1,2,3,4,5,7\}$, $\{1,3,4,5,7,10\}$, $\{1,2,3,4,5\}$, $\{2,4,6,8\}$, $\{2,3,5,8,7,11\}$, $\{1,3,4,5,6,7\}$, $\{2,3,5,7,8,9\}$, $\{3,6,9,12\}$.

5.6 Les schémas de partage de secret basés sur les images Gray des codes simplexes et MacDonald

Cette partie étudie le schéma de partage de secret basé sur les images Gray des codes simplex et Macdonald de type α et β sur $R_{q,m}$. Ces images sont des concaténations de quelque codes simplexes et des codes de MacDonald de type α et β sur $\mathbb{F}_{2^m}$.

5.6.1 Les images Gray des codes simplexes et des codes de Macdonald

Tout d´abord, nous présentons le Gray map en utilisant le poids homogène sur $R_{q,m}$, où le poids homogène sur $R_{q,m}$ est défini comme suit :

$$w_{hom}(x) = \begin{cases} 0 & \text{si } x = 0, \\ 2^{2q-1} & \text{si } x = c_{\{1,2,\cdots,q\}}\mathcal{V}_{\{1,2,\cdots,q\}}, c_{\{1,2,\cdots,q\}} \in \mathbb{F}_{2^m}, \\ 2^{2q-2} & \text{autrement.} \end{cases}$$

Soit

$$\Psi_{hom} : R_{q,m} \to \mathbb{F}_{2^m}^{2^{2q-1}}.$$

L´application Ψ_{hom} vérifie la propriété suivante.

Théorème 5.6.1 *L´application Ψ_{hom} défini ci-dessus est une isométrie préservant la distance ($R_{q,m}$, la distance homogène) à ($\mathbb{F}_{2^m}^{2^{2q}-1}$, la distance de Hamming).*

Les théorèmes suivants, qui sont déjà indiqués dans [18], donnent la caractérisation des images Gray des codes simplexes et MacDonald de type α and β sur $R_{q,m}$.

Théorème 5.6.2 *Soit $S^{\alpha}_{(q,m,k)}$ un code simplexe de type α sur $R_{q,m}$ de longueur 2^{m2^qk} et de poids homogène minimal d_{hom}, alors $\Psi_{hom}(S^{\alpha}_{(q,m,k)})$ est la concaténation des $2^{2mk(2^q-1)}$ codes simplexes $\widehat{\mathcal{S}}^{\alpha}_{(q,m,k)}$ de type α sur $\mathbb{F}_{2^m}$ de paramètres $[2^{2^q(mk+1)-1}; k]$.*

Preuve 5.6.3 *Soit $G^{\alpha}_{(q,m,k)}$ la matrice génératrice de $S^{\alpha}_{(q,m,k)}$, et $\Psi_{hom}(G^{\alpha}_{(q,m,k)})$ est une matrice d´un code linéaire sur $\mathbb{F}_{2^m}$. La matrice $\Psi_{hom}(G^{\alpha}_{(q,m,k)})$ est la concaténation des $2^{2mk(2^q-1)}$ matrices $\mathcal{G}_{(q,m,k)}$, et on a :*

$$\Psi_{hom}(G^{\alpha}_{(q,m,k)}) = \left[\; 1_{2^{2mk(2^q-1)}} \otimes \mathcal{G}^{\alpha}_{(q,m,k-1)} \; \right], \tag{5.7}$$

où

$$\mathcal{G}^{\alpha}_{(q,m,k)} = \left[\frac{(0123\cdots(2^m-1)) \otimes 1}{1 \otimes \mathcal{G}^{\alpha}_{(q,m,k-1)}} \right], \; \textit{pour } k \geqslant 2, \tag{5.8}$$

avec

$$\mathcal{G}^{\alpha}_{1} = [0123\cdots(2^m-1)]\,.$$

$\mathcal{G}^{\alpha}_{(q,m,k)}$ est la matrice génératrice de code simplexe $\widehat{\mathcal{S}}^{\alpha}_{(q,m,k)}$ de type α sur $\mathbb{F}_{2^m}$.

Théorème 5.6.4 *Soit $S^{\beta}_{(q,m,k)}$ un code simplexe de type β sur $R_{q,m}$ de longueur $\dfrac{2^{m(2^q-1)(k-1)}(2^{mk}-1)}{2^m-1}$ et de poids homogène minimal d_{hom}, alors $\Psi_{hom}(S^{\beta}_{(q,m,k)})$ est la concaténation des $\dfrac{2^{(2^q-1)(m(k-1)+1)}(2^{mk}-1)}{(2^m-1)2^{(m-1)(k-1)}(2^k-1)}$ codes simplexes $\widehat{\mathcal{S}}^{\beta}_{(q,m,k)}$ de type β sur $\mathbb{F}_{2^m}$ de paramètres $[\dfrac{2^{(2^q-1)(m(k-1)+1)}(2^{mk}-1)}{2^m-1}; k]$.*

Preuve 5.6.5 *La preuve est la même du théorème 5.6.2.*

Théorème 5.6.6 *Soit $\mathcal{M}^{\alpha}_{(q,m,k)}$ un code de MacDonald de type α sur $R_{q,m}$ de longueur $2^{m2^qk}-2^{m2^qu}$ et de poids homogène minimal d_{hom}, alors $\Psi_{hom}(\mathcal{M}^{\alpha}_{(q,m,k)})$ est la concaténation des $\frac{2^{2^q(mk+1)-1}-2^{2^q(mu+1)-1}}{2^{mk}-2^{mu}}$ codes de MacDonald $\widehat{\mathcal{M}}^{\alpha}_{(q,m,k)}$ de type α sur $\mathbb{F}_{2^m}$ de paramètres $[2^{2^q(mk+1)-1}-2^{2^q(mu+1)-1}; k]$.*

Preuve 5.6.7 *La preuve est la même du théorème 5.6.2.*

Théorème 5.6.8 *Soit $\mathcal{M}^{\beta}_{(q,m,k)}$ un code de MacDonald de type β sur $R_{q,m}$ de longueur $\frac{2^{m(2^q-1)(k-1)}(2^{mk}-1)-2^{m(2^q-1)(u-1)}(2^{mu}-1)}{2^m-1}$ et de poids homogène minimal d_{hom}, alors $\Psi_{hom}(\mathcal{M}^{\beta}_{(q,m,k)})$ est la concaténation des $\frac{2^{(2^q-1)(m(k-1)+1)}(2^{mk}-1)-2^{(2^q-1)(m(u-1)+1)}(2^{mu}-1)}{(2^m-1)2^{(m-1)(k-1)}(2^k-1)}$ codes de MacDonald $\widehat{\mathcal{M}}^{\beta}_{(q,m,k)}$ de type β sur $\mathbb{F}_{2^m}$ de paramèters*

$$[\frac{2^{(2^q-1)(m(k-1)+1)}(2^{mk}-1)-2^{(2^q-1)(m(u-1)+1)}(2^{mu}-1)}{2^m-1}; k]$$

.

Preuve 5.6.9 *La preuve est la même que celle du théorème 5.6.2.*

Les schémas de partage de secret basés sur les images Gray des codes simplexes et MacDonald sur $R_{q,m}$

Nous appliquons le schéma de partage de secret basé sur les images Gray des codes simplexes et des codes de Mcdonald sur $R_{q,m}$, nous avons les résultats suivants :

Théorème 5.6.10 *Soit $\Psi_{hom}(S^{\beta}_{(q,m,k)})$ un code linéaire sur $\mathbb{F}_{2^m}$, alors dans le schéma de partage du secret basé sur $\Psi_{hom}(S^{\beta}_{(q,m,k)})^{\perp}$, il y a en tout $2^{m(k-1)}$ ensembles d´accès minimal et $(\frac{2^{(2^q-1)(m(k-1)+1)}(2^{mk}-1)}{2^m-1}-1)$ participants. De plus, chaque participant P_i est impliqué dans $(2^m-1)2^{mk-2}$ ensembles d´accès minimal.*

Preuve 5.6.11 *La preuve est la même du théorème 5.5.3 et du théorème 5.5.5.*

Théorème 5.6.12 *Soit $\Psi_{hom}(\mathcal{M}^{\alpha}_{(q,m,k)})$ (resp., $\Psi_{hom}(\mathcal{M}^{\beta}_{(q,m,k)})$) un code linéaire sur $\mathbb{F}_{2^m}$, alors dans le schéma de partage du secret basé sur $\Psi_{hom}(\mathcal{M}^{\alpha}_{(q,m,k)})^{\perp}$ (resp., $\Psi_{hom}(\mathcal{M}^{\beta}_{(q,m,k)})^{\perp}$), il y a $2^{m(k-1)}$ ensembles d´accès minimal et $2^{2^q(mk+1)-1}-2^{2^q(mu+1)-1}-1$ (resp., $\frac{2^{(2^q-1)(m(k-1)+1)}(2^{mk}-1)-2^{(2^q-1)(m(u-1)+1)}(2^{mu}-1)}{2^m-1}-1$) participants.*

De plus, chaque participant P_i est impliqué dans $(2^m-1)2^{mk-2}$ ensembles d´accès minimal.

Preuve 5.6.13 *La preuve est la même du théorème 5.5.3 et du théorème 5.5.5.*

Quelques propriétés des codes $\widehat{\mathcal{S}}^{\beta}_{(q,m,k)}$ et $\Psi_{hom}(S^{\beta}_{(q,m,k)})$ ont la même structure d´accès minimal. L´explication serait incluse dans le théorème suivant.

Théorème 5.6.14 *Soient Γ_1 et Γ_2 les ensembles d´accès minimal des codes $\widehat{\mathcal{S}}^{\beta}_{(q,m,k)}$ et $\Psi_{hom}(S^{\beta}_{(q,m,k)})$, alors $\Gamma_1 = \Gamma_2$*

Preuve 5.6.15 *Si Γ_1 et Γ_2 sont les ensembles d´accès minimal des codes $\widehat{\mathcal{S}}^{\beta}_{(q,m,k)}$ et $\Psi_{hom}(S^{\beta}_{(q,m,k)})$ respectivement, soit $\mathcal{P}(2^{2^{mk}-1})$ l´ensemble de toutes les parties dans $\{1, 2, \cdots, 2^{mk}-1\}$, pour prouver que,*

$$\forall\ X \in \mathcal{P}(2^{2^{mk}-1}), X \subset \Gamma_1 \Leftrightarrow X \subset \Gamma_2.$$

Il suffit de prouver que

$$X \subset \Gamma_2 \Rightarrow X \subset \Gamma_1.$$

Si $X = \{P_i\}_{i\in\{1,2,\cdots,2^{2^{q(mk+1)-1}}-1\}} \subset \Gamma_2$, par l´équation (5.7) nous avons tous les vecteurs colonnes de la matrice $\Psi_{hom}(G^{\beta}_{(q,m,k)})$ sont des vecteurs colonnes de la matrice $\mathcal{G}^{\beta}_{(q,m,k)}$, alors $X = \{P_i\}_{i\in\{1,2,\cdots,2^{mk}-1\}} \subset \Gamma_1$.

Remarque 5.6.16 *Le dernier résultat est appliqué sur les codes $\Psi_{hom}(\mathcal{M}^{\alpha}_{(q,m,k)})$ et $\Psi_{hom}(\mathcal{M}^{\beta}_{(q,m,k)})$.*

5.7 Conclusions

Les avantages d´un partage de secret basé sur les codes linéaires est le vecteur aléatoire $u = (u_0, u_1, \cdots, u_{k-1})$ qui appartient à un espace fini d´un cardinal grand, car il y a exactement $2^{m(k-1)}$ vecteurs $u \in \mathbb{F}^k_{2^m}$ tel que $s = ug_0$, qui évite l´attaque par la force brute. L´ensemble des structures d´accès minimal est vraiment plus grande pour $[n, k]-$code, nous avons $2^{m(k-1)}$ ensemble d´accès minimal. La structure d´accès basée sur les codes linéaires sont meilleures que le schéma de Shamir car la méthode de Shamir a une structure d´accès très simple, c´est pour que n´importe quelle partition de n est capable de récupérer le secret.

Dans ce chapitre, nous avons construit les codes simplexes et les codes de McDonald de type α et β sur $R_{q,m}$ et leurs images Gray, nous avons donné les distributions de poids des codes de *torsion*, des codes simplexes et des codes de MacDonald. Puis nous avons déterminé l´accès structure du schéma de partage du secret basés sur leurs dual.

Conclusion et Perspectives

Ce travail a permis de résoudre certains problèmes dans la théorie des codes correcteurs, spécialement la construction de certains type des codes sur quelques anneaux finis. Au cours de cette étude, nous avons effectué plusieurs constructions des codes simplexes et des codes de MacDonald de type α et β sur des anneaux finis (commutatif et non commutatif).

Dans la première partie de cette thèse nous avons découvert que la construction de ces codes sur l´anneau $\mathbb{Z}_2\mathbb{Z}_4$ c´est la juxtaposition des codes simplexes et des codes de MacDonald de types α et β sur $\mathbb{Z}_2$, et les codes simplexes et les codes de MacDonald de types α et β sur $\mathbb{Z}_4$. Nous avons vu aussi que l´image Gray binaire des codes simplexes de type β sur $\mathbb{Z}_2\mathbb{Z}_4$ atteint la borne de Gilbert.

Puis dans la deuxième partie, nous avons étudié les codes simplexes et les codes de MacDonald de types α et β sur certains anneaux de Frobenius comme l´anneau :

$\diamond$ $R_q = \mathbb{F}_2[u_1, u_2, \ldots, u_q]/\langle u_i^2 = 0, u_iu_j = u_ju_i\rangle$, avec $q \geq 2$

$\diamond$ $R_{q,m} = \mathbb{F}_{2^m}[u_1, u_2 \cdots u_q]/\langle u_i^2 = 0, u_iu_j - u_ju_i\rangle$, avec $q \geq 2$ et $m \geq 1$.

Enfin, nous avons décrit dans la troisième partie, les applications de schéma de partage d´un secret sur ces nouveaux codes en utilisant les codes de *torsion* et les images Gray de ces codes.

Ces thèmes de recherche, a travers lesquels s´inscrit ma thèse offrent des questions et des perspectives de nombreuses recherches variées.

$\triangleright$ Il serait intéressant de voir les domaines d´applications de ces codes spécialement dans la cryptographie et la stéganographie.

$\triangleright$ Pour les codes définis sur les anneaux, nous avons travaillé dans le cas où ces anneaux

sont locaux, il serait intéressant de voir l´autre cas.

▷ On a appliqué les schémas de partage d´un secret basé sur les images Gray des codes linéaires sur $R_{q,m}$, il serait intéressant de voir cette application basée sur les codes linéaires sur certains anneaux finis.

Annexe

Dans cette annexe, on présentera quelques structures algébriques. Nous donnerons un certain nombre de propriétés que nous utilisons dans cette thèse. Nous allons définir les anneaux, les idéaux et les modules qui sont des outils de base pour effectuer la définition des codes sur les anneaux. Nous nous intéresserons essentiellement aux familles des codes sur les anneaux de Frobenius

5.8 Généralités sur les anneaux finis, les idéaux et les Modules

5.8.1 Anneaux et corps

Définition 5.8.1 *Un anneau $\mathcal{R}$ est un ensemble non vide muni de deux lois, $+$ (addition) et $\cdot$ (multiplication), telles que :*

1. *$(\mathcal{R}, +)$ est un groupe abélien, c.-à-d.,*
   - **(i)** *$+$ est associative, c.-à-d., $a + (b + c) = (a + b) + c$, pour tout $a, b, c \in \mathcal{R}$.*
   - **(ii)** *$+$ est commutative, c.-à-d., $a + b = b + a$, pour tout $a, b \in \mathcal{R}$.*
   - **(iii)** *$\mathcal{R}$ possède un élément 0 tel que $0 + a = a$ pour tout $a \in \mathcal{R}$.*
   - **(iv)** *Tout $a \in \mathcal{R}$ admet un opposé noté $(-a)$, tel que $a + (-a) = 0$.*
2. *La loi $\cdot$ est associative (c.-à-d., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pour tout $a, b, c \in \mathcal{R}$, et $\mathcal{R}$ admet un élément neutre 1 tel que $1 \cdot a = a = a \cdot 1$, pour tout a.*

3. *La loi $\cdot$ est distributive (à gauche et à droite) sur l´addition, c.-à-d., pour tout $a, b, c \in \mathcal{R}$, on a : $a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$.*

Enfin, on dit que $\mathcal{R}$ est un anneau commutatif si, de plus, la loi $\cdot$ est commutative.

Définition 5.8.2 *Un élément inversible de $\mathcal{R}$ est un élément $a \neq 0$ de $\mathcal{R}$ qui divise 1 c.-à-d., $a \cdot b = 1$ pour un certain $b \neq 0$ dans $\mathcal{R}$.*

On note $\mathcal{R}^{\times}$ l´ensemble des éléments inversibles de $\mathcal{R}$.

Définition 5.8.3 *Un élément a d´un anneau $\mathcal{R}$ est un diviseur de zéro si et seulement s´il est non nul et s´il existe $b \in R$ non nul tel que $a \cdot b = 0$.*

Définition 5.8.4 *Si $k \neq 0$, alors un corps est un anneau commutatif dans lequel tout élément non nul est inversible.*

Homomorphisme d´anneaux

Soient $\mathcal{R}$ et $\mathcal{R}'$ deux anneaux. Une application $f : \mathcal{R} \to \mathcal{R}'$ est un homomorphisme d´anneaux si et seulement si :

1. $f(a + b) = f(a) + f(b)$ pour tous $a, b \in \mathcal{R}$,
2. $f(a \cdot b) = f(a) \cdot f(b)$ pour tous $a, b \in \mathcal{R}$,
3. $f(1_{\mathcal{R}}) = 1_{\mathcal{R}'}$.

5.8.2 Anneaux et idéaux

Soit $\mathcal{R}$ un anneau, toujours supposé commutatif.

Idéaux

Définition 5.8.5 *Un idéal $\mathcal{I}$ de $\mathcal{R}$ est un sous ensemble non vide qui est un sous groupe pour l´addition (c.-à-d., $x, y \in I \Rightarrow x - y \in \mathcal{I}$) et qui est stable par la multiplication pour tout élément de $\mathcal{R}$, c.-à-d., $x \in \mathcal{I}$, $a \in \mathcal{R}, a \cdot x \in \mathcal{I}$.*

Définition 5.8.6 *(**Idéal premier**) Soit $\mathcal{R}$ un anneau et $\mathcal{I}$ un idéal de $\mathcal{R}$. L´ideal $\mathcal{I}$ est un idéal premier de $\mathcal{R}$ si et seulement si :*

$$\forall (a,b) \in \mathcal{R} \times \mathcal{R},\ a \cdot b \in \mathcal{I} \Rightarrow a \in \mathcal{I} ou\ b \in \mathcal{I}.$$

Théorème 5.8.7 *Soit $\mathcal{R}$ un anneau commutatif unitaire, un idéal $\mathcal{I}$ de $\mathcal{R}$ est dit maximal si et seulement si $\mathcal{R}/\mathcal{I}$ est un corps.*

Corollaire 5.8.8 *Tout élément non inversible de $\mathcal{R}$ est contenu dans un idéal maximal.*

Définition 5.8.9 *(**Idéal principal**) Un idéal $\mathcal{I}$ d´un anneau $\mathcal{R}$ est dit principal s´il existe un élément $a \in \mathcal{I}$ tel que $\mathcal{I} = \langle a \rangle$, où $\langle a \rangle = a \cdot x,\ x \in \mathcal{R}$.*

Définition 5.8.10 *(**Anneau local**) Un anneau $\mathcal{R}$ est dit anneau local si et seulement s´il admet un seul idéal maximal.*

5.8.3 Modules

Définition 5.8.11 *Soit $(\mathcal{M}, +)$ un groupe commutatif , on dit que $\mathcal{M}$ est un $\mathcal{R}$-module s´il existe une application $\mathcal{R} \times \mathcal{M} \ : \ \rightarrow \ \mathcal{M}$, où on note $a \cdot x$ l´image de (a, x), telle que :*

1. *$a \cdot (x + y) = a \cdot x + a \cdot y$ pour $a \in \mathcal{R}$ et $x, y \in \mathcal{M}$,*
2. *$(a + b) \cdot x = a \cdot x + b \cdot x$ pour $a, b \in \mathcal{R}$ et $x \in \mathcal{M}$,*
3. *$1 \cdot x = x$ et $a \cdot (b \cdot x) = (ab) \cdot x$ pour $a, b \in \mathcal{R} et x \in \mathcal{M}$.*

Si l´anneau $\mathcal{R}$ est un corps $\mathcal{K}$, on dit que $\mathcal{M}$ est un $\mathcal{K}$-espace vectoriel.

Définition 5.8.12 *Soit $\mathcal{M}$ un $\mathcal{R}$-module. Un sous groupe $\mathcal{N}$ de $\mathcal{M}$ tel que $a \cdot x \in \mathcal{N}$ pour $a \in \mathcal{R}$ et $x \in \mathcal{N}$ est un sous-module de $\mathcal{M}$.*

Il est claire qu´un sous ensemble $\mathcal{N}$ de $\mathcal{M}$ est un sous module de $\mathcal{M}$ si et seulement si

$$x, y \in \mathcal{N} \text{et}\ a, b \in \mathcal{R} \Rightarrow a \cdot x + b \cdot y \in \mathcal{N}.$$

Définition 5.8.13 *Soit $\mathcal{M}$ un $\mathcal{R}$-module et soit $\mathcal{B}$ un sous ensemble de $\mathcal{M}$. On dit que $\mathcal{B}$ est une partie libre de $\mathcal{M}$ si les éléments de $\mathcal{B}$ sont linéairement indépendants sur $\mathcal{R}$ c.-à-d., si la propriété suivante est vérifiée, pour tout $n \geq 1$ si $a_1, \cdots, a_n \in \mathcal{B}$ sont deux à deux distincts et si, $\alpha_1 a_1 + \cdots + \alpha_n a_n = 0$, alors $\alpha_i = 0$ pour tout $i = 1, \cdots, n$.*

5.9 Les anneaux de Frobenius

Aprés leur première apparition dans le travail de T. Nakayama [52], l´anneau de Frobenius et quasi-Frobenius ont fait l´objet d´études approfondies par des mathématiciens. Dans cette partie, nous allons revoir la définition de l´anneau Frobenius.

Définition 5.9.1 *Si $\mathcal{R}$ et $\mathcal{S}$ sont deux anneaux, alors un $\mathcal{R}$-$\mathcal{S}$-bimodule est un groupe abélien $\mathcal{M}$ tel que :*

1. *$\mathcal{M}$ est un $\mathcal{R}$-module à gauche et un $\mathcal{S}$-module à droite.*
2. *Pour tout $r \in \mathcal{R}$, $s \in \mathcal{S}$ et $m \in \mathcal{M}$ on a, $(rm)s = r(ms)$.*

Soit $\mathcal{R}$ un anneau fini unitaire. Le groupe des caractères du groupe additif $\mathcal{R}$ est noté par $\widehat{\mathcal{R}} = Hom_{\mathbb{Z}}(\mathcal{R}, \mathbb{C}^{\times})$. Ce groupe a une structure d´un $\mathcal{R}$-$\mathcal{R}$-bimodule en définissant $\chi^r(x) = \chi(rx)$ et ${}^r\chi(x) = \chi(xr)$ pour tout $r, x \in \mathcal{R}$, et pour tout $\chi \in \widehat{\mathcal{R}}$. Après tous ces concepts nous arrivons à la définition suivante.

Définition 5.9.2 *Un anneau fini $\mathcal{R}$ est appelé un anneau de Frobenius si ${}_{\mathcal{R}}\widehat{\mathcal{R}} =_{\mathcal{R}} \mathcal{R}$.*

On peut voir que si $\mathcal{R}$ est un anneau de Frobenius fini, donc $\mathcal{R}$ et $\widehat{\mathcal{R}}$ sont isomorphes aussi comme $\mathcal{R}$-modules à droite. Par conséquent, il existe des caractères χ et ψ telle que :

$$\widehat{\mathcal{R}} = \{{}^r\chi | r \in \mathcal{R}\} = \{\psi^r | r \in \mathcal{R}\}.$$

Ces caractères sont appelés des générateurs à gauche ou générateurs à droite, respectivement.

On constate deux cas :

• Caractère générateur à gauche est à droite à la fois.

• Caractère générateur ou bien à gauche ou bien à droite et cela si et seulement si son noyau ne contient aucun idéal non nul à gauche ou à droite de $\mathcal{R}$.

La classe des anneaux de Frobenius finie est assez grande, d´après la proposition suivante.

Proposition 5.9.3 *1. Tout anneau principal fini est un anneau de Frobenius.*

2. Si $\mathcal{R}$ et $\mathcal{S}$ sont des anneaux de Frobenius, alors $\mathcal{R} \times \mathcal{S}$ est un anneau de Frobenius.

3. Si $\mathcal{R}$ est un anneau de Frobenius, alors $M_n(\mathcal{R})$, l´anneau de toutes les matrices de taille $n \times n$ sur $\mathcal{R}$, est un anneau de Frobenius.

4. Si $\mathcal{R}$ est un anneau de Frobenius, et G un groupe fini, alors l´anneau de groupe $\mathcal{R}[G]$ est un anneau de Frobenius.

Bibliographie

[1] T. Abualrub, I. Siap, and N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-*additive cyclic codes*, IEEE Trans. Inform. Theory 60(3), pp.115-121, 2014.

[2] M. AL-Ashker, *Simplex codes over the ring* $\mathbb{F}_2 + u\mathbb{F}_2$, The Arabian Journal for Science and Engineering, 2005, 30 : pp.0227-285.

[3] M. Al-Ashker, *Simplex codes over the ring* $\sum_{n=0}^{s} u^n\mathbb{F}_2$, Turk .J. Math, vol. 29, pp.221-233, 2005.

[4] T. Aoki, P. Gaborit, M. Harada, M. Ozeki, and P. Solé, *On the covering radius of* $\mathbb{Z}_4$*-codes and their lattices*, IEEE Trans. Inform. Theory 45(6), pp.2162-2168, 1999.

[5] A. Batoul, Construction des codes auto-duaux, Ph.D. Thesis, 2013.

[6] M. Bilal, J. Borges, S.T. Dougherty, and C. Fernández-Córdoba, *Maximum distance separable codes over* $\mathbb{Z}_4$ *and* $\mathbb{Z}_2\mathbb{Z}_4$, Des. Codes Cryptogr. 61(1) pp.31-40, 2011.

[7] J. Bierbrauer, *Introduction to Coding Theory*, Chapman and Hall/CRC. Boca Raton. FL 2005.

[8] J. Borges, S.T. Dougherty, and C. Fernández-Córdoba, *Characterization and constructions of self-dual codes over* $\mathbb{Z}_2\mathbb{Z}_4$, Adv. Math. Commun. 6(3), pp.287-303, 2012.

[9] J. Borges, C. Fernández, K.T. Phelps, *Quaternary Reed Muller codes*, IEEE Trans. Inform. Theory, 51(7), pp.2686-2691, 2005.

[10] J. Borges, C. Fernández, K.T. Phelps, *ZRM codes*, IEEE Trans. Inform. Theory 54(1), pp.380-386, 2008.

[11] J. Borges, C. Fernández-Córdoba, J. Rifá, *Every $\mathbb{Z}_{2k}$-code is a binary propelinear code*, In : COMB´01. Electronic Notes in Discrete Mathematics. Elsevier Science. Amsterdam, vol. 10, pp.100-102, November 2001.

[12] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifá, and M. Villanueva, *$\mathbb{Z}_2\mathbb{Z}_4$-linear codes : Generator matrices and duality*, Des. Codes Cryptogr. 54(2), pp.167-179, 2010.

[13] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifá, and M. Villanueva, *On $\mathbb{Z}_2\mathbb{Z}_4$-linear codes and duality*, V Jornades de Matemàtica Discreta i Algorísmica, Soria (Spain), pp.171-177, 2006.

[14] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifá, and M. Villanueva,*On $\mathbb{Z}_2\mathbb{Z}_4$-linear codes and duality*, VJMDA. Ciencias, 23. Secr. Publ. Intercamb. Ed., Valladolid, pp.171-177, 2006.

[15] J. Borges, C. Fernandez-Cóordoba, J. Pujol, J. Rifá and M. Villanueva, *$\mathbb{Z}_2\mathbb{Z}_4$-additive codes*. A MAGMA package. Autonomous University of Barcelona (UAB). Bellaterra. Barcelona, http ://www.ccsg.uab.cat, 2007.

[16] M.C. Bhandari, M.K. Gupta, and A.K. Lal, *On $\mathbb{Z}_4$-simplex codes and their gray images*, Applied Algebra. Algebraic Algorithms and Error-Correcting Codes. AAECC-13. Lecture Notes in Computer Science 1719, pp.170-180, 1999.

[17] K. Chatouh, K. Guenda, T. A. Gulliver and L. Noui, *Simplex and MacDonald codes over R_q*, 21st Conference on Applications of Computer Algebra, ACA 2015 July 20-23, 2015.

[18] K. Chatouh, K. Guenda, T. A. Gulliver and L. Noui, *Simplex and MacDonald codes over R_q*, J. Appl. Math. Comput. DOI 10.1007/s12190-016-1045-4, 2016.

[19] K. Chatouh, K. Guenda, T.A. Gulliver and L. Noui, *Secret Sharing Schemes Based on Gray Images of Linear Codes over $R_{q,m}$*, International Conference on Coding and Cryptography ICCC, USTHB, Algiers, Algeria, November 2-5, 2015.

[20] K. Chatouh, K. Guenda, T.A. Gulliver and L. Noui, *On some classes of linear codes over $\mathbb{Z}_2\mathbb{Z}_4$ and their covering radii*, Journal of Applied Mathematics and Computing, pp.1-22, First online : 16 January 2016.

[21] K. Chatouh,L. Noui, M. Bin Mamat, *Codes over* $\mathbb{Z}_2\left(\mathbb{Z}_2+u\mathbb{Z}_2\right)$ *and their covering radii*. Journal of Algebra, Number Theory : Advances and Applications. Volume 16, Number 1, pp. 25-39, 2016.

[22] J. Chen, Y. Huang, B. Fu, J. Li, *Secret sharing schemes from a class of linear codes over finite chain ring*, Journal of Computational Information Systems 9 : 7, pp.2777-2784, 2013.

[23] G.D. Cohen, M.G. Karpovsky, H.F. Mattson, and J.R. Schatz, *Covering radius-Survey and recent results*, IEEE Trans. Inform. Theory 31(3), pp.328-343, 1985.

[24] G. Cohen, S. Mesnager and A. Patey, *On minimal and quasi minimal linear codes*, Proceedings of Fourteenth International Conference on Cryptography and Coding. Oxford. United Kingdom, IMACC 2013. LNCS 8308 Springer. Heidelberg. pages pp.85-98, 2013.

[25] C.J. Colbourn and M.K. Gupta, *On quaternary MacDonald codes*, Proc. Int. Conf. on Inform. Tech. : Coding and Computing, pp.212-215, 2003.

[26] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Rep. Suppl. 10, 1973.

[27] P. Delsarte, *Four fundamental parameters of a code and their combinatorial significance*, Inform. Contr. 23, pp.407-438, 1973.

[28] P. Delsarte and J. M. Goethals, *Alternating bilinear forms over* $GF(q)$, J. Comb. Theory. 19, pp.26-50, 1975.

[29] P. Delsarte and V. Levenshtein, *Association schemes and coding theory*, IEEE Trans. Inform. Theory 44(6), pp.2477-2504, 1998.

[30] S.T. Dougherty, T.A. Gulliver, and J.N.C. Wong, *Self-dual codes over* $\mathbb{Z}_8$ *and* $\mathbb{Z}_9$, Des. Codes Cryptogr. 41, pp.235-249, 2006.

[31] S.T. Dougherty, B. Yildiz, and S. Karadeniz, *Codes over* R_k *Gray maps and their binary images*, Finite Fields Appl, vol. 17, no. 3, pp.205-219, May 2011.

[32] R. A. Fisher, *The theory of confounding in factorial experiments in relation to the theory of groups*, Ann. Eugenics. 11,pp.341-353, 1942.

[33] R. A. Fisher, *A system of confounding for factors with more than two alternatives, giving completely orthogonal cubes and higher powers*, Ann. Eugenics. 12, pp.2283-2290, 1945.

[34] M. S. Garg, *On Optimum Codes and their Covering Radii*, PhD thesis. IIT Kanpur. India, 1990.

[35] J. M. Goethals, *Two dual families of nonlinear binary codes*, Electronics Letters, 10, pp.471-472, 1974.

[36] J. M. Goethals, *Nonlinear codes defined by quadratic forms over* $GF(2)$, Inform. Control. 31, pp.43-74, 1976.

[37] M. Greferath and S. E. Schmidt, *Finite-ring combinatorics and MacWilliams equivalence theorem*, J. Combin. Theory Ser. A, 92, pp.17-28, 2000.

[38] M.K. Gupta, *On Some Linear Codes over* $\mathbb{Z}_{2^s}$, Ph.D. Thesis, IIT, Kanpur, 1999.

[39] M.K. Gupta and C. Durairajan, *On the covering radius of some modular codes*, arXiv :1206.3038 v2 [cs.IT] Jun. 2012.

[40] M.K. Gupta and C. Durairajan, *On the covering radius of Some modular codes*, Adv. Math. Commun., vol. 8, no. 2, pp.129-137, 2014.

[41] M.K. Gupta, D.G. Glynn, and T.A. Gulliver, *On Senary Simplex Codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science, vol. 2227, pp.112–121, 2001.

[42] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory 40, pp.301-319, 1994.

[43] T. Honold, *Characterization of finite Frobenius rings*, Arch. Math., 76, pp.406-415, 2001.

[44] W.C. Huffman and V. Pless, *Fundamentals of Error-correcting Codes*, New York : Cambridge University Press, 2003.

[45] X.-D. Hou, J. T. Lahtonen, and S. Koponen. *The reed-muller code $r(r, m)$ is not $\mathbb{Z}_4$-linear for* $3 \leq r \leq m-2$, IEEE Trans. Inform. Theory. 44(2), pp.798-799, 1998.

[46]] E. D. Karnin, J. W. Greene, and M. E. Hellman, *On secret sharing systems*, IEEE Trans. Inf. Theory, vol. IT-29, no. 1, pp.35-41, Jan. 1983.

[47] A. M. Kerdock, *A class of low-rate nonlinear codes*, Inform. Control, 20, pp.182-187, 1972.

[48] B. Lindström, *Group partitions and mixed perfect codes*, Can. Math. Bull, 18, pp.57-60, 1975.

[49] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company. Amsterdam. New York, Oxford 1977.

[50] J. L. Massey, *Some applications of coding theory in cryptography*, Codes and Ciphers : Cryptography and Coding IV, Formara Ltd, Esses, England, pp.33- 47, 1995.

[51] M. Nadler, *A 32-point n=12, d=5 code*, IRE Transation on information Theory, 8 :58, 1962.

[52] T. Nakayama, *On Frobeniusean algebras*, II. Annals of Math. 42, pp.1-21 1941.

[53] A. A. Nechaev, *The Kerdock code in a cyclic form*, Diskret Math., 1(4) :123-139, 1989. English translation in Dscrete Math. Appl. 1, pp.365-384, 1991.

[54] A. W. Nordstrom and J. P. Robinson, *An optitum nonlinear code*, Inform. Control. 11, pp.613-616, 1967.

[55] P. C. Pandian and C. Duruairajan, *On the covering radius of some code over* $R = \mathbb{Z}_2 + u\mathbb{Z}_2$, *where* $u^2 = 0$, Int, Journal of Research in Applied, Matural and Social Sciences 2(1), pp.61-70, Jan. 2014.

[56] A. M. Patel, *Maximual q-ary codes with large minimum distance*, IEEE Trans. Inform. Theory, 21 : pp. 106-110, 1975.

[57] R. Pellikaan, Xin-Wen Wu, S. Bulygin and R. Jurrius, *Error-correcting codes and cryptology*, Cambridge, 2012.

[58] J. Pujol, J. Rifà, F. Solovéva, *Construction of $\mathbb{Z}_4$-linear Reed Muller codes*, IEEE Trans. Inform. Theory 55(1), pp.99-104, 2009.

[59] J. Pujol, J. Rifà, and L. Ronquillo, *Construction of additive Reed Muller codes*, arXiv :0909.3185v2 [cs.IT] 28 Dec. 2011.

[60] J. Pujol and J. Rifà,*Additive Reed Muller codes*,Proc. IEEE Int. Symp. on Inform. Theory, 508, Jun.-Jul. 1997.

[61] J. Pujol and J. Rifà, *Translation invariant propelinear codes*, IEEE Trans. Inform. Theory 43, pp.590-598, 1997.

[62] F. P. Preparata, *A class of optimum nonlinear double-error-correcting codes*, Inform. Control. 13, pp.378-400, 1968.

[63] M.K. Raut and M.K. Gupta, *On octonary codes and their covering radii*, arXiv :1411.1822v3 [cs.IT] Dec. 2014.

[64] J. Rifà, J.M. Basart, L. Huguet, *On completely regular propelinear codes*, In : Proceedings of 6th International Conference. AAECC-6. LNCS. Springer, vol. 357, pp.341-355, Berlin 1989 .

[65] C. E. Shannon, *A mathematical theory of communication*, The Bell System Technical Journal, 27, pp.379-423, 1948.

[66] J. H. van Lint, *Intrduction to coding theory*, Springer-Verlag New York. Inc. Secaucus NJ. USA, 1982.

[67] V.V. Vazirani, H. Sran and B.S. Rajan, *An efficient algorithm for constructing minimal trellises for codes over finite abelian groups*, IEEE Trans. Inform. Theory, 42(6), pp.1839-1854, 1996.

[68] B. Yildiz and S. Karadeniz, *Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$*, Designs. Codes. Crypt, vol. 54, no. 1, pp. 61-81, 2010.

[69] B. Yildiz and I.G. Kelebek, *The homogeneous weight for R_k, related Gray map and new binary quasicyclic codes*, arXiv :1504.04111v1 [cs.IT] 16 Apr 2015.

[70] B. Yildiz and S. Karadeniz, *Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$*, Designs. Codes. Crypt, vol. 58, no. 1, pp.221-234, 2011.