République Algérienne Démocratique et Populaire

Ministère de L'enseignement Supérieure et de la recherche Scientifique

Université El Hadj Lakhdar Batna

Faculté des Sciences

Département de Mathématiques

Laboratoire des Techniques Mathématiques

MEMOIRE

Présenté pour obtenir le diplôme de

MAGISTER

Thème

Codes auto- duaux sur $\mathrm{IF_q}$ et $\mathrm{Z_4}$

Option : Mathématiques Appliquée

Par

Abdous Fatiha

Soutenue le : 03/06/2007

Devant le jury

Mr. S. E.REBIAI	Professeur (U. de Batna)	Président
Mr. M. BENLAHCENE	Chargé de cours (U. de Batna)	Rapporteur
Mr. A.BOUDAOUD	Professeur (U. de M'sila)	Examinateur
Mr. D. MIHOUBI	Maître de conférence (U. de M'sila)	Examinateur

Table des matières

Notations

$\mathbb{F}_q$	Un corps fini à q éléments ;
$C\,(n,k,d)$	Code linéaire C de longueur n, de dimension k et de distance minimale d ;
G	Matrice génératrice de C ;
$C^{\perp}$	Code dual de C ;
H	Matrice de contrôle de C ;
$rg(H)$	Rang de H ;
$ppncld(H)$	Plus petit nombre de colonnes de H linéairement dépendantes ;
G^t	Transposée d'une matrice G ;
Id_k	Matrice identité de rang k ;
$G = (Id_k \| A)$	Matrice génératrice en forme systématique ;
$H = (-A \| Id_{n-k})$	Matrice de contrôle en forme systématique ;
$\omega\,(u)$	Poids de Hamming de u ;
$Lee\,(u)$	Poids de Lee de u ;
$Norm\,(u)$	Norme de u ;
S_n	Groupe symétrique de n éléments ;
G_r	Groupe du code C ;
$Aut\,(C)$	Groupe d'automorphisme de C ;
$C_1 \sim C_2$	Equivalence des codes ;
$W_C\,(x,y)$	Polynôme énumérateur des poids ;
$CW_C\,(x,x,...,x)$	Complément énumérateur des poids ;
$SW_C\,(x,y,z)$	Symétrie énumérateur des poids ;
A_i	Nombre des mots du code de poids i ;
B_i	Distance de distribution des poids i ;
N_C	Nombre des codes équivalents au code C ;

T_n	Nombre total de tous les codes auto- duaux de logueur n ;
$\binom{k}{n}_q$	Nombre des sous espace vectoriel de dimension k de $\mathbb{F}_q^n$;
χ	Un caractère ;
$I(G)$	Ensemble des invariants du G ;
$\overline{p}$	Moyenne polynomiale de p ;
S_C	Ombre du code C ;
$W_{S_C}(x,y)$	Polynôme énumérateurs des poids de S_C ;
$C = (C_1 C_2 ... C_t)^+$	Code indécomposable ;
$C = (C_1 C_2 ... C_t)$	Code décomposable ;
X	Une matrice dont les lignes est des vecteurs de colle ;

Introduction

Notre société est devenue dépendante de la communication sous toutes ses formes, notamment les messages numériques dont le volume augmente sans cesse. Il faut donc assurer l'intégrité des données à la réception, malgré des moyens de transmission qui ajoutent parfois des erreurs à l'information : ondes radio, ligne téléphonique, support magnétique, etc,.... C'est le rôle des codes correcteurs d'erreurs.

Le domaine d'étude des codes correcteurs a connu une évolution en définissant des classes des codes où chaque classe possède des propriétés concernant leurs construction, par exemple les codes de Hamming, les codes BCH, les codes auto- duau, etc,...

Les codes auto- duaux ont été le sujet d'étude durant les quarante dernières années, notamment par Gleason (1970) où il a caractérisé les codes auto- duaux (codes qui coicident avec leurs duaux) binaires de type II dans son fameux théorème où il a démontré que le polynôme énumérateur des poids d'un tel code est un élément de l'algèbre des invariants, d'un certain groupe fini d'ordre 192, engendrée par les polynômes énumérateurs des poids de code de Hamming étendu de longueur 8 et celui de Golay de longueur 24, une généralisation de ces résultats pour les autres familles des codes auto- duaux a été établie dans [2], [5], [11], [17].

Notons l'étroite connexion entre la théorie des codes et certains domaine mathématiques tel que l'analyse combinatoire, théorie de groupe, treillis et les treillis uni- modulaires (pour plus détails, voir [10], [13] entre autres).

L'objectif principal de ce mémoire est l'étude des codes auto- duaux, leurs propriétés (longueur, dimension, polynôme énumérateur des poids) et leur classification dans le cas binaire et ternaire. Une classification qui prend en considération pour une longueur donnée, la construction du code (sa matrice génératrice), l'ordre du groupe d'automorphismes, et le nombre de codes inéquivalents.

Le mémoire est composé de trois chapitres.

Dans le premier chapitre on présente les notions fondamentales de la théorie des codes (code linéaire, description matricielle des codes linéaires, distance minimale, équivalence des codes, groupe d'automorphismes, polynômes énumérateurs des poids, familles des codes...), qui servirons d'appui pour le développement ultérieur.

Dans le deuxième chapitre nous présentons une classe très importante de codes, c'est la classe des codes auto- duaux, où dans la première partie nous étudions les paramètres de ces codes tels que la longueur, la dimension, et le poids de Hamming. Dans la deuxième partie on s'intéresse aux polynômes énumérateurs des poids de ces codes.

Enfin dans le troisième chapitre nous traitons la classification des codes auto- duaux binaires (de type I, et de type II) et ternaires où nous utilisons la méthode de collage pour leurs construction, une méthode qui s'appuie sur les codes auto orthogonaux, et les propriétés étudiées dans le chapitre précédent. Dans notre étude nous donnons la classification des codes auto- duaux binaires jusqu' à la longueur 22, et ternaires jusqu' à la longueur 20.

Chapitre 1

Généralités sur les codes correcteurs d'erreurs

Nous rappelons, dans ce chapitre, quelques notions de base sur la théorie des codes. On commence par donner la définition de code, les codes linéaires et leurs paramètres, équivalence des codes, polynôme énumérateur des poids, familles des codes, les codes étendus et codes tronqués, qui seront utils dans la suite.

Les théorèmes et les propositions sont donnés sans démonstration, pour plus de détails voir [6], [14], [17].

1.1 Définitions et propriétés

1.1.1 Le code

Définition 1.1 On appelle un ensemble fini $\mathbb{F}$: l'alphabet.
Un code C sur $\mathbb{F}$ de longueur n est un sous ensemble de $\mathbb{F}^n$.

• Si $\mathbb{F}$ est un groupe additif, alors C est un code additif s'il est un sous groupe additif de $\mathbb{F}^n$.

• Si $\mathbb{F}$ est un anneau, alors C est un code linéaire s'il est un sous groupe additif de

$\mathbb{F}^n$ et stable par rapport à la multiplication par un élément de $\mathbb{F}$ (supposons que la multiplication dans $\mathbb{F}$ est commutative).

• Si $\mathbb{F}$ est un corps, alors C est un code linéaire de longueur n et de dimension k s'il est un sous espace vectoriel de dimension k de $\mathbb{F}^n$.

Les codes linéaires sur les corps finis de longueur n et de dimension k, sont notés par $C(n,k)$ ou $[n,k]$.

1.1.2 Le produit scalaire

Soit $\mathbb{F}$ un corps fini, un produit scalaire $\langle , \rangle_{\mathbb{F}}$ sur $\mathbb{F}$ est une application de $\mathbb{F} \times \mathbb{F}$ vers $\mathbb{F}$ telle que

1. $\forall x, y, z \in \mathbb{F}; \langle x+y, z\rangle_{\mathbb{F}} = \langle x, z\rangle_F + \langle y, z\rangle_{\mathbb{F}}$
2. $\forall x, y, z \in \mathbb{F}; \langle x, y+z\rangle_{\mathbb{F}} = \langle x, y\rangle_{\mathbb{F}} + \langle x, z\rangle_{\mathbb{F}}$
3. $\forall x \in \mathbb{F}; \langle x, y\rangle_{\mathbb{F}} = 0 \Longrightarrow y = 0$
4. $\forall y \in \mathbb{F}; \langle x, y\rangle_{\mathbf{F}} = 0 \Longrightarrow x = 0$

Le produit scalaire sur $\mathbb{F}$ définit le produit scalaire sur l'espace vectoriel $\mathbb{F}^n$ comme suit : $\langle x, y\rangle_{\mathbb{F}^n} = \sum_{i=1}^{n} \langle x_i, y_i\rangle_{\mathbb{F}}; \forall x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n) \in \mathbb{F}^n$

1.2 Description matricielle des codes linéaires

1.2.1 La matrice génératrice

Soit $C = C(n,k)$ un code linéaire sur $\mathbb{F}$ dont $\{g_1, g_2, ..., g_k\}$ est une base.

Alors tous les éléments du code linéaire C s'écrivent sous la forme

$$C = \left\{u \in \mathbb{F}^n; u = aG, a \in \mathbb{F}^k\right\} \tag{1.1}$$

avec $G = \begin{pmatrix} g_1 \\ g_2 \\ . \\ . \\ . \\ g_k \end{pmatrix}$ une matrice de type $k \times n$.

Définition 1.2 La matrice G est appelée la matrice génératrice de C et tous les vecteurs de C sont appelés les mots code de C.

Remarque 1.1 • Le rang de la matrice génératrice G est k .

• À partir de la matrice génératrice G, on peut aussi considérer le code linéaire $C = C(n,k)$ comme l'image d'une application linéaire f telle que

$$\begin{aligned} f : \mathbb{F}^k &\longrightarrow \mathbb{F}^n \\ a &\longmapsto f(a) = aG \end{aligned} \tag{1.2}$$

L'application f est appelée la fonction de codage et a le mot d'information.

Définition 1.3 Soit $C(n,k)$ un code linéaire et u un élément de $\mathbb{F}_q^n$, l'ensemble

$$u + C = \left\{ v \in \mathbb{F}_q^n ; v = u + c, \forall c \in C \right\} \tag{1.3}$$

est appelé le translaté de C dont u est un représentant.

Proposition 1.1 [17] Pour un code linéaire $C(n,k)$, il existe q^{n-k} translatés différents constituant une partition de l'espace vectoriel $\mathbb{F}_q^n$.

1.2.2 La matrice de contrôle

Soit $\mathbb{F}$ un espace vectoriel muni d'un produit scalaire $\langle , \rangle_{\mathbb{F}}$.

Définition 1.4 On dit que deux vecteurs x, y dans $\mathbb{F}^n$ sont orthogonaux si $\langle x, y \rangle_{\mathbb{F}^n} = 0$.

Proposition 1.2 [17]] Soit $C = C(n,k)$ un code linéaire sur $\mathbb{F}$, alors l'ensemble

$$C^{\perp} = \{u \in \mathbb{F}^n; \langle u, c\rangle = 0, \forall c \in C\} \tag{1.4}$$

est un sous espace vectoriel de $\mathbb{F}^n$ de dimension $n-k$, appelé l'espace dual de C ou l'orthogonal de C.

Donc $C^{\perp}$ est un code linéaire de longueur n et de dimension $n-k$ engendré par une matrice H de type $(n-k)\times n$. Cette matrice est appelée la matrice de contrôle de C ou la matrice de test.

On a la relation suivante entre la matrice génératrice G et la matrice de contrôle H d'un code

$$H^t G = 0 \tag{1.5}$$

Remarque 1.2 Nous remarquons que les propriétés du code dual d'un code linéaire sur un corps fini peuvent être tout à fait différentes de ceux de l'espace dual d'un espace vectoriel sur les nombres réel, par exemple si W est un espace vectoriel d'un espace vectoriel de dimension fini sur $\mathbb{R}$ on a $W \cap W^{\perp} = \{0\}$, puisque aucun vecteur n'est orthogonal à lui même, ce n'est pas toujours pour les codes linéaires, malgré $C \cap C^{\perp}$ n'est pas le code zéro mais on a

$$\dim C + \dim C^{\perp} = n \tag{1.6}$$

1.3 La distance minimale d'un code linéaire

Soit $\mathbb{F}$ un espace vectoriel.

Définition 1.5 • On définit le poids d'un vecteur $v = (v_1, v_2, ..., v_n)$ de $\mathbb{F}^n$, noté $\omega(v)$ comme étant le nombre de ses composantes non nulles.

• La distance de Hamming entre deux vecteurs u et v, notée $d(u,v)$, est le poids de $u-v$, c'est-à-dire le nombre des positions où elles sont différentes.

La distance de Hamming est une fonction $d : \mathbb{F}^n \times \mathbb{F}^n \longrightarrow \mathbb{N}$ satisfaisant les propriétés

suivantes :

- $\forall x, y \in \mathbb{F}^n; d(x,y) \geq 0$
- $\forall x, y \in \mathbb{F}^n; d(x,y) = d(y,x)$
- $\forall x, y \in \mathbb{F}^n; d(x,y) = 0 \iff x = y$
- $\forall x, y, z \in \mathbb{F}^n; d(x,y) \leq d(x,z) + d(z,y)$

Définition 1.6 La distance minimale d'un code linéaire $C = C(n,k)$, notée d est la plus petite distance de Hamming entre deux mots code différents

$$d = \min_{\substack{u \neq v \\ u,v \in C}} d(u,v) \tag{1.7}$$

Un code C de distance minimale d peut détecter $d-1$ erreurs et peut corriger $\left[\frac{d-1}{2}\right]$ erreurs, d'où elle vient la définition C est $d-1$ détecteur d'erreurs, et $\left[\frac{d-1}{2}\right]$ correcteur d'erreurs.

La longueur, la dimension et la distance minimale jouent un rôle fondamental dans la description des codes, lorsqu'on veut les mentionner on dit qu'on a affaire à un $[n,k,d]$ code, si l'on ne veut pas préciser la valeur de d on dit simplement qu'on a faire à un $[n,k]$ code.

Proposition 1.3 [6] La distance minimale d'un code linéaire $C = C(n,k)$ est le plus petit poids des mots code non nul

$$d = \min_{u \in C - \{0\}} \omega(u) \tag{1.8}$$

Théorème 1.1 *Soit $C = C(n,k,d)$ un code linéaire ayant comme matrice de contrôle une matrice H alors :*

• *Il existe un mot code de poids ω si est seulement s'il existe ω colonnes de H linéairement dépendantes.*

• *$d \geq \omega$ si est seulement si tout ensemble de $\omega - 1$ colonnes de H est une famille libre.*

• *Si $ppncld(H)$ est le plus petit nombre de colonnes de H linéairement dépendantes, alors*

on a

$$ppncld\left(H\right) \leq rg\left(H\right)+1 \tag{1.9}$$

où $rg\left(H\right)$ *est le rang de* H.

Corollaire 1.1 [6] Soit H une matrice de contrôle d'un code $C=C\left(n,k\right)$ alors

- $\dim\left(C\right)=k=n-rg\left(H\right)$
- $d=ppncld\left(H\right)$
- $d\leq n-k+1$

Le théorème suivant montre l'existence d'un code linéaire sur $\mathbb{F}_q$ si ses paramètres n, k et d vérifient une certaine condition.

Théorème 1.2 [6] (Borne de Gilbert- Varshamov) : *Si* $q^{n-k}\succ\sum_{i=0}^{i=d-2}\complement_{n-1}^{i}\left(q-1\right)^{i}$, *alors on peut construire un* $[n,k]$ *code linéaire sur* $\mathbb{F}_q$, *de distance minimale inférieure ou égale à* d.

1.4 Les codes équivalents

Définition 1.7 Soient δ une permutation de $\{1,2,..,n\}$ et

$$\begin{array}{c}\Pi_i:\mathbb{F}_q\longrightarrow\mathbb{F}_q\\ s\longmapsto\Pi_i\left(s\right)=\alpha_i\times s\text{ où }\alpha_i\in\mathbb{F}_q^*\end{array}\qquad\forall i=1,...,n \tag{1.10}$$

alors l'application

$$\begin{array}{c}\Gamma:\mathbb{F}_q^n\longrightarrow\mathbb{F}_q^n\\ \left(c_1,c_2,...,c_n\right)\longmapsto\Gamma\left(c_1,c_2,...,c_n\right)=\Pi_1\left(c_{\delta(1)}\right)\Pi_2\left(c_{\delta(2)}\right)...\Pi_n\left(c_{\delta(n)}\right)\end{array} \tag{1.11}$$

est appelée une transformation monômiale de degré n.

Définition 1.8 Deux codes $C_1=C\left(n,k\right)$, $C_2=C\left(n,k\right)$ sur $\mathbb{F}_q$ sont équivalents s'il existe une transformation monômiale μ de degré n telle que

$$\mu\left(C_1\right)=C_2\text{ où }\mu\left(C_1\right)=\{\mu\left(c\right);c\in C_1\}$$

Pour les codes linéaires sur $\mathbb{F}_2$ on a la définition suivante :

Définition 1.9 Deux codes binaires $C_1 = C(n,k)$, $C_2 = C(n,k)$ sont équivalents s'il existe une permutation qui transforme chaque mot code de C_1 à un mot code de C_2 c'est-à- dire

$$[C_1 \backsim C_2] \Longleftrightarrow [\exists\ \delta \in S_n;\ \ (\forall u \in C_1 \Longrightarrow \delta(u) \in C_2)] \tag{1.12}$$

1.4.1 Le groupe d'automorphismes d'un code

On associe à chaque code sur $\mathbb{F}_q$ un certain groupe, appelé le groupe d'automorphismes du code. Ce groupe est util dans l'étude du nombre de codes équivalents à un code donné.

Définition 1.10 Soit C un code de longueur n sur $\mathbb{F}_q$, le groupe d'automorphismes de C noté $Aut(C)$, est l'ensemble de toutes les transformations monômiale μ de degré n tel que :

$$\forall c \in C; \mu(c) \in C \tag{1.13}$$

Définition 1.11 Soit $C(n,k)$ un code sur $\mathbb{F}_2$, le groupe d'automorphismes de C est

$$Aut(C) = \{\sigma \in S_n; \sigma(c) \in C, \forall c \in C\} \tag{1.14}$$

Exemple 1.1 Soit $C = \{0000, 0011, 1100, 1111\}$

$Aut(C) = \{(1234), (2134), (1243), (2143), (4321), (3412), (1324), (1423)\}$

1.4.2 Forme systématique d'un code linéaire

Définition 1.12 Un code linéaire $C = C(n,k)$ est dit sous la forme systématique lorsque le mot d'information a de $\mathbb{F}_q^k$ se trouve dans des coordonneés préfixées du mot code correspondant.

En général on exige que ces positions préfixées soient les k premières positions, dans ce cas la matrice génératrice est sous la forme $G = (I_k \parallel A)$ où A est une matrice de type $k \times (n-k)$, c'est la forme standard de G

Remarque 1.3 La matrice de contrôle d'un code linéaire sous la forme systématique est $H = (-A^t \parallel I_{n-k})$

Proposition 1.4 [17] Tout code linéaire $C = C(n,k)$ est équivalent à un code linéaire sous la forme systématique.

1.5 Le polynôme énumérateur des poids

Dans cette partie on présente un certain polynôme associé à un code, ce polynôme caractérise les poids de tous les mots code, appelé le polynôme énumérateur des poids. Il existe une relation très importante entre les polynômes énumérateurs des poids d'un code et son dual appelée identité de Mac Williams qu'on reparlera ultérieurement.

Définition 1.13 Soit $C(n,k)$ un code linéaire, le polynôme homogène de deux variables x et y suivant

$$W_C(x,y) = \sum_{c \in C} x^{n-w(c)} y^{w(c)} \tag{1.15}$$

est appelé polynôme énumérateur des poids de C.

De (1.15) on déduit une autre définition du polynôme énumérateur des poids de C. En effet :

$$\begin{aligned} W_C(x,y) &= \sum_{c \in C} x^{n-w(c)} y^{w(c)} \\ &= \sum_{i=0}^{n} \sum_{\substack{w(c)=i \\ c \in C}} x^{n-i} y^i \\ &= \sum_{i=0}^{n} \left(\sum_{\substack{w(c)=i \\ c \in C}} 1 \right) x^{n-i} y^i \\ &= \sum_{i=0}^{n} A_i x^{n-i} y^i \end{aligned} \tag{1.16}$$

où A_i est le nombre des mots code de poids i.

Dans le polynôme énumérateur des poids les coefficients $A_0, A_1, ..., A_n$ sont appelés la distribution des poids.

Définition 1.14 On définit le polynôme énumérateur des poids d'un code non linéaire C de longueur n par :

$$W_C(x,y) = \sum_{i=0}^{n} B_i x^{n-i} y^i \tag{1.17}$$

tels que

$$B_i = \frac{1}{\mid C \mid} \mid \{(u,v) \diagup u, v \in C, d(u,v) = i\} \mid \tag{1.18}$$

Les nombres $B_o, B_1, ..., B_n$ sont appelés la distance de distribution des poids.

1.5.1 Poids énumérateur complément

Soit $\mathbb{F}_q = \{\zeta_1, \zeta_2, ...\zeta_q\}$ un corps fini, on associe à chaque élément ζ_i de $\mathbb{F}_q$ une variable x_i.

On définit le poids énumérateur complément d'un code C sur $\mathbb{F}_q$, noté CW_C, comme suit :

$$CW_C(x_1, x_2, ..., x_q) = \sum_{u \in C} x_1^{n_1(u)} x_2^{n_2(u)} ... x_q^{n_q(u)} \tag{1.19}$$

où $n_\nu(u)$ est le nombre des composantes de u égale à ζ_ν.

Pour les codes sur $\mathbb{F}_4$ on définit le poids énumérateur symétrisé SW_C par

$$\begin{aligned} SW_C(x,y,z) &= \sum_{u \in C} x^{n_0(u)} y^{n_1(u)} z^{N_w(u)} \\ &= CW_C(x,y,z,z) \end{aligned} \tag{1.20}$$

où $n_0(u), n_1(u)$ sont définis ci dessus et $N_w(u)$ est le nombre des composantes dans u égal à w ou $\overline{w}$.

1.6 Familles des codes

Les codes linéaires peuvent être répartis sur des familles suivant l'alphabet $\mathbb{F}$ et le produit scalaire défini sur $\mathbb{F}$.

1. Si $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$, et le produit scalaire $\langle x, y \rangle_{\mathbb{F}_2} = xy$, alors C est un sous espace vectoriel de $\mathbb{F}_2^n$ et on dit que C est un code linéaire binaire sur $\mathbb{F}_2$.

2. Si $\mathbb{F} = \mathbb{F}_3 = \{0, 1, 2\}$, et le produit scalaire $\langle x, y \rangle_{\mathbb{F}_3} = xy$, alors C est un sous espace vectoriel de $\mathbb{F}_3^n$ et on dit que C est un code linéaire ternaire sur $\mathbb{F}_3$.

3. Si $\mathbb{F} = \mathbb{F}_4 = \{0, 1, w, \overline{w}\}$, où $w^2 + w + 1 = 0$, $w^3 = 1$, $\overline{x} = x^2$ pour tout x de $\mathbb{F}_4$, on a deux familles de codes linéaires et deux familles de codes additifs à partir du produit scalaire.

3.i. Si le produit scalaire est hermitien $\langle x, y \rangle_{4^H} = x\overline{y}$, alors C est un sous espace vectoriel de $\mathbb{F}_4^n$ et on dit que C est un code linéaire quaternaire hermitien sur $\mathbb{F}_4$. La famille notée par $\left(4^H\right)$.

3.ii. Si le produit scalaire est euclidien $\langle x, y \rangle_{4^E} = xy$, alors C est un sous espace vectoriel de $\mathbb{F}_4^n$ et on dit que C est un code linéaire quaternaire euclidien sur $\mathbb{F}_4$. Cette famille est notée par $\left(4^E\right)$.

3.iii. Si le produit scalaire est donné par $\langle x, y \rangle_{4^{H_+}} = x\overline{y} + \overline{x}y = trace\left(x\overline{y}\right)$ (la trace de $\mathbb{F}_4$ vers $\mathbb{F}_2$), alors C est un sous groupe additif de $\mathbb{F}_4^n$. Cette famille est notée par $\left(4^{H_+}\right)$.

3.iv. Si le produit scalaire est donné par $\langle x, y \rangle_{4^{E_+}} = xy + \overline{xy} = trace\left(xy\right)$ (la trace de $\mathbb{F}_4$ vers $\mathbb{F}_2$), alors C est un sous groupe additif de $\mathbb{F}_4^n$. Cette famille est notée par $\left(4^{E_+}\right)$.

4. Si $\mathbb{F} = \mathbb{F}_q$, où $q = p^2$ et p premier avec $\overline{x} = x^{\sqrt{q}}$ pour tout x de $\mathbb{F}_q$, alors on a deux familles de codes linéaires, une hermitienne et l'autre euclidienne.

4.i. Pour le produit scalaire hermitien $\langle x, y \rangle_{q^H} = x\overline{y}$, alors C est un sous espace vectoriel de $\mathbb{F}_q^n$, et la famille correspondante est notée par $\left(q^H\right)$.

4.ii. Pour le produit scalaire euclidien $\langle x, y\rangle_{q^E} = xy$, alors C est un sous espace vectoriel de $\mathbb{F}_q^n$, et la famille correspondante est notée par $\left(q^E\right)$.

5. Si $\mathbb{F} = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ et le produit scalaire $\langle x, y\rangle_{\mathbb{Z}_4} = xy \pmod 4$, alors C est un sous groupe additif de $\mathbb{Z}_4^n$ et on dit que C est un code linéaire sur $\mathbb{Z}_4$.

1.7 Codes étendus et codes tronqués

Parfois il est intéressant de trouver des nouveaux codes à partir de codes déjà connus, pour améliorer les paramètres du code original, c'est le cas des codes étendus et des codes tronqués.

1.7.1 Code étendu

Soit $C(n, k, d)$ un code linéaire. On considère le code linéaire étendu $\hat{C}(n+1, k)$ de distance minimale d ou $d+1$, où chaque mot code $\tilde{u} = (u_1, u_2, ..., u_{n+1})$ est tel que : $u = (u_1, u_2, ..., u_n) \in C$ et $\sum_{k=1}^{n+1} u_k = 0$, on a alors tous les mots code de $\hat{C}$ de poids pair.

La matrice de contrôle $\hat{H}$ de $\hat{C}$ s'obtient en ajoutant à la matrice de contrôle H de C une ligne de 1 et une colonne avec un 0 dans les $n-k$ premiers positions et un 1 dans la $n-k+1^{ième}$.

Exemple 1. 2 Soit $C = C(7, 3, 4)$ un code de matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

et de matrice de contrôle $H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

alors $\hat{C} = \hat{C}\,(8,3,4)$ telle que $\hat{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & \mathbf{0} \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & \mathbf{0} \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & \mathbf{0} \end{pmatrix}$ et

$$\hat{H} = \begin{pmatrix} 1 & 0 & 0 & 0 & \mathbf{0} & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & \mathbf{0} & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & \mathbf{0} & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & \mathbf{0} & 1 & 1 & 0 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

1.7.2 Code tronqué

Soit $C\,(n,k,d)$ un code linéaire.

On déduit un code linéaire tronqué $C^{\star}\,(n,k)$, en supprimant une ou plusieurs coordonnées de chaque mot de $C\,(n,k,d)$, la longueur diminue d'une unité tandis que la dimension reste constante, la distance minimale peut diminuer d'une unité, mais par fois on peut supprimer une coordonnée qui n'effecte pas la distance minimale.

Chapitre 2

Codes auto- duaux et théorie des invariants

Ce chapitre est composé de deux sections. Dans la première nous examinons d'une part les codes auto- duaux et les propriétés de leurs longueurs, dimension et poids des mots codes, d'autre part on étudie les codes auto- duaux de longueur n sur l'anneau $\mathbb{Z}_4$ comme un sous groupe additif de $\mathbb{Z}_4^n$ et leurs propriétés. Dans la deuxième, on s'intéresse à la présentation du polynôme énumérateur des poids comme un invariant d'un groupe fini, et l'ombre d'un code et son polynôme énumérateur des poids.

2.1 Codes auto- duaux

2.1.1 Les codes auto- orthogonaux

Puisque les codes auto- duaux appartiennent à la classe des codes auto- orthogonaux, on rappele dans ce paragraphe, quelques notions fondamentales des codes auto- orthogonaux.

Définition 2.1 Un code linéaire $C = C(n, k)$ est appelé auto- orthogonal si $C \subset C^{\perp}$.

Le théorème suivant donne les conditions nécessaires et suffisantes en terme de la

matrice génératrice, pour qu'un code linéaire soit auto- orthogonal sur $\mathbb{F}_q$.

Théorème 2.1 [14] *Soit G une matrice génératrice d'un code linéaire sur le corps $\mathbb{F}_q$, alors C est un code auto- orthogonal si est seulement si les lignes distinctes de G sont orthogonales et ont un poids divisible par q.*

Le théorème suivant caractérise les codes linéaires binaires auto- orthogonaux.

Théorème 2.2 *Si les différentes lignes dans la matrice génératrice d'un code linéaire binaire C sont orthogonales et leur poids est divisible par quatre, alors C est un code auto- orthogonal et tous les poids des mots code sont divisibles par quatre.*

Pour montrer ce théorème on utilise le lemme suivant :

Lemme 2.1 Pour tout x, y dans $\mathbb{F}_2^n$ ona :

$$\omega(x+y) = \omega(x) + \omega(y) - 2\omega(x \cap y) \tag{2.1}$$

où $x \cap y = z = (z_1, z_2, ..., z_n)$ et $z_i = \begin{cases} 1 & \text{si } x_i = y_i = 1 \\ 0 & \text{si non} \end{cases}$

Preuve : Soit $x = (x_1, x_{2,}..., x_n)$ et $y = (y_1, y_2, ..., y_n)$

on a $x \cap y = (x_1y_1, x_2y_2, ...x_ny_n)$

et $x = (x_1, 0, ..., 0) + (0, x_2, ..., 0) + (0, ..., 0, x_n) = x^1 + x^2 + ... + x^n$.

$\omega(x) = \sum_{i=1}^{n} \omega(x^i)$ et $\omega(x^i) = \begin{cases} 1 & \text{si } x_i = 1 \\ 0 & \text{si } x_i = 0 \end{cases}$

donc

$$\omega(x^i + y^i) = \omega(x^i) + \omega(y^i) - 2\omega(x^i \cap y^i)$$

alors

$$\begin{aligned} \omega(x+y) &= \sum_{i=1}^{n} \omega\left(x^i + y^i\right) = \sum_{i=1}^{n} \omega\left(x^i\right) + \sum_{i=1}^{n} \omega\left(y^i\right) - 2\sum_{i=1}^{n} \omega\left(x^i \cap y^i\right) \\ &= \omega(x) + \omega(y) - 2\omega(x \cap y) \end{aligned}$$

■

Preuve du théorème 2.2 : D'après le théorème précédent on a tout code binaire est auto- orthogonal, reste à montrer que tous les poids des mots code sont divisibles par quatre.

Dans le lemme précédent on a

$$\omega(x+y) = \omega(x) + \omega(y) - 2\omega(x \cap y) \text{ .et } \omega(x \cap y) = \sum_{i=1}^{n} x_i y_i = \langle x, y \rangle \equiv 0 \pmod 2$$

alors $\omega(x \cap y)$ est pair, donc $\omega(x+y)$ est divisible par quatre. ■

2.1.2 Les codes auto- duaux

Nous allons maintenant étudier les codes auto- duaux et leurs propriétés qui sont la longueur, la dimension et le poids de Hamming des mots code qui nous serons utiles ultérierement.

Définition 2.2 Un code linéaire $C(n,k)$ est dit auto- dual si $C = C^{\perp}$.

Remarque 2.1 Soit C un code linéaire sur $\mathbb{F}$ de longueur n ; on a

$$|C| \left|C^{\perp}\right| = |\mathbb{F}|^n \tag{2.2}$$

Pour les codes auto- duaux on a

$$|C| = |\mathbb{F}|^{\frac{n}{2}} \tag{2.3}$$

Si $|\mathbb{F}|$ n'est pas carré donc n doit être pair.

En particulier si C est un code linéaire auto- dual sur un corps fini on a

$$\dim C = \frac{n}{2} \tag{2.4}$$

car $\dim C + \dim C^{\perp} = n$

donc C est un sous espace vectoriel de dimension $\frac{n}{2}$ et n est pair.

Corollaire 2.1 Soit $C(n,k)$ un code linéaire.Alors $C(n,k)$ est auto- orthogonal et de

dimension $\frac{n}{2}$ si est seulement si C est code auto- dual.

Remarque 2.2 Il est facile de remarquer que dans les codes auto- duaux binaires le poids de Hamming de chaque vecteur est pair. Dans les codes ternaires auto- duaux le poids de Hamming de chaque vecteur est divisible par trois. Il existe enfin des codes auto-duaux binaires dont chaque vecteur a un poids de Hamming divisible par quatre.

Il y a deux types de poids qui sont utils pour étudier les codes non binaires.

Définition 2.3 On défini le poids de Lee et la norme euclidienne d'un vecteur u dans $\mathbb{F}$ par

$$\begin{aligned} Lee\,(u) &= \min\{\mid u \mid, \mid \mathbb{F} \mid - \mid u \mid\} \\ Norme\,(u) &= (Lee\,(u))^2 \end{aligned} \tag{2.5}$$

Pour un vecteur $u = (u_1, u_2, ..., u_n)$ dans $\mathbb{F}^n$ on pose

$$\begin{aligned} Lee\,(u) &= \sum_{i=0}^{n} Lee\,(u_i) \\ Norme\,(u) &= \sum_{i=0}^{n} Norme\,(u_i) \end{aligned} \tag{2.6}$$

2.1.3 Quelques exemples sur les codes auto- duaux

Les codes binaires

a. Le code de répétition, noté par i_2, de matrice génératrice (11) c-à-d $i_2 = \{00, 11\}$ et de polynôme énumérateur des poids $W_{i_2}(x, y) = x^2 + y^2$

b. Le code de Hamming étendu $e_8 = C\,(8, 4, 4)$ de matrice génératrice

$$\left(\begin{array}{c||cccc} & 0 & 1 & 1 & 1 \\ & 1 & 0 & 1 & 1 \\ I_4 & 1 & 1 & 0 & 1 \\ & 1 & 1 & 1 & 0 \end{array} \right) \tag{2.7}$$

et de polynôme énumérateur des poids $W_{e_8}(x,y) = x^8 + 14x^4y^4 + y^8$.

En 1947, Marcel Golay introduit deux codes linéaires auto- duaux binaire et ternaire noté par g_{24}, g_{12} appelé les codes de Golay.

c. Le code de Golay $g_{24} = C(24, 12, 8)$, est de matrice génératrice

$$G_{g_{24}}= \begin{pmatrix} 1&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1 \end{pmatrix} \tag{2.8}$$

et de polynôme énumérateur des poids

$$W_{g_{24}}(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$$

Les codes ternaires

a. Le tetracode $t_4 = [4,2,3]_3$, est de matrice génératrice

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} \tag{2.9}$$

avec $W_{t_4}(x,y) = x^4 + 8xy^3$

$$CW_{t_4}(x,y,z) = .x^4 + xy^3 + xz^3 + 3xy^2z + 3xyz^2$$

b. Le code de Golay $[12,6,6]_3$ est de matrice génératrice

$$\left(\begin{array}{c|c} & 1 \; 1 \; 2 \; 1 \; 0 \; 2 \\ & 1 \; 0 \; 1 \; 2 \; 2 \; 2 \\ & 1 \; 1 \; 1 \; 0 \; 1 \; 1 \\ I_6 & 2 \; 1 \; 0 \; 2 \; 1 \; 2 \\ & 1 \; 2 \; 2 \; 2 \; 1 \; 0 \\ & 0 \; 1 \; 2 \; 2 \; 2 \; 1 \end{array}\right) \tag{2.10}$$

avec $W_{g_{12}}(x,y) = x^{12} + 264x^6y^6 + 440x^4y^9 + 24y^{12}$

$$\begin{aligned} CW_{g_{12}}(x,y,z) = x^{12} + y^{12} + z^{12} + 22\,(x^6y^6 + y^6z^6 + x^6z^6) \\ +220\,(x^6y^3z^3 + x^3y^6z^3 + x^3y^3z^6) \end{aligned}$$

Les codes quaternaires hermitiens sur $\mathbb{F}_4$

a. Le code de répétition $i_2 = C(2,1,2)_{4^H}$ est de matrice génératrice (11) c-à-d

$i_2 = \{00, 11, \omega\omega, \varpi\varpi\}$

avec $W_{i_2}(x,y) = x^2 + 3y^2$

$$SW_{i_2}(x,y,z) = x^2 + y^2 + 2z^2$$

$$CW_{i_2}(x,y,z,t) = x^2 + y^2 + z^2 + t^2$$

b. L'hexacode $h_6 = [6,3,4]_{4^H}$ est de matrice génératrice

$$\left(\begin{array}{c||ccc} & 1 & \omega & \omega \\ I_3 & \omega & 1 & \omega \\ & \omega & \omega & 1 \end{array}\right) \tag{2.11}$$

avec $W_{h_6}(x,y) = x^6 + 45x^2y^4 + 18y^6$

$$SW_{h_6}(x,y,z) = x^6 + y^6 + 2z^6 + 15\left(2x^2y^2z^2 + x^2z^4 + y^2z^4\right)$$
$$CW_{h_6}(x,y,z,t) = x^6 + y^6 + z^6 + t^6 + 15\left(x^2y^2z^2 + x^2y^2t^2 + x^2z^2t^2 + y^2z^2t^2\right)$$

Les codes quaternaires euclidiens sur $\mathbb{F}_4$

a. Le code de Reed Solomon noté par $(R,S) = [4,2,3]_{4^E}$ est de matrice génératrice

$$\left(\begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & \omega & \varpi \end{array}\right) \tag{2.12}$$

avec $W_{(R,S)}(x,y) = x^4 + 12xy^3 + 3y^4$

$$SW_{(R,S)}(x,y,z) = x^4 + y^4 + 2z^4 + 12xyz^2$$
$$CW_{(R,S)}(x,y,z,t) = x^4 + y^4 + z^4 + t^4 + 12xyzt$$

Le théorème suivant mis en évidence la relation entre la longueur n et q d'un code auto- dual $C\left(n, \frac{n}{2}\right)$ sur le corps $\mathbb{F}_q$.

Théorème 2.3 [14] *Il existe un $\left[n, \frac{n}{2}\right]$ code auto- dual sur $\mathbb{F}_q$ si est seulement si l'une des propriétés suivantes est satisfaite :*

- *q et n sont pair.*
- *$q \equiv 1 \pmod 4$ et n pairs.*
- *$q \equiv 3 \pmod 4$ et n est divisible par quatre.*

En particulier, on remarque qu' il existe un code binaire (quaternaire) auto- dual pour tout n pair, et il existe un code ternaire auto- dual pour n divisible par quatre.

Les codes de type I et de type II

• Un code auto- dual binaire dont le poids de Hamming de chacun de ses vecteurs est multiple de quatre est dit doublement pair ou de type II. S'il admet un vecteur de poids de Hamming non multiple de quatre, il est alors dit simplement pair ou de type I.
On note les codes binaires auto- duaux de type I par (2_I), et de type II par (2_{II}) .
On général on dit qu' un code binaire de type II si tous les poids de Hamming sont divisibles par quatre, et de type I s'il existe un vecteur de poids non divisible par quatre.

• Les codes auto- duaux sur $\mathbb{F}_3$ sont appelés de type III .

• Enfin les codes auto- duaux hermitien sur $\mathbb{F}_4$ sont appelés de type IV.

Le théorème suivant montre que la distance minimale d'un code auto- dual est bornée.

Théorème 2.4 [12] *La distance minimale d'un code auto- dual de longueur n est infèrieure ou égale à d^*, donné dans le tableau suivant* :

de type	d^*
(I)	$2\left[\frac{n}{8}\right]+2$
(II)	$4\left[\frac{n}{24}\right]+4$
(III)	$3\left[\frac{n}{12}\right]+3$
(IV)	$2\left[\frac{n}{6}\right]+2$

La seule borne existante pour la distance minimale d d'un code auto- dual de longueur n sur $\mathbb{F}_q$ et $q \geq 5$ est la borne de Singleton i e

$$d \leq \frac{n}{2}+1 \tag{2.13}$$

Définition 2.4 • Un code auto- dual est dit extrémal si sa distance minimale rencontre la borne correspondante.

• Un code auto- dual est dit optimal si sa distance minimale est le plus grand connu

pour sa longueur et sa dimension.

2.1.4 Le nombre de codes auto- duaux

Le but de cette partie est de déterminer le nombre total des codes auto- duaux différents.

Soit G_r le groupe de toutes les transformations d'ordre $\mid G_r \mid$ (par exemple pour les codes binaires $\mid G_r \mid = n!$, pour les codes ternaires $\mid G_r \mid = 2^n n!$).

Le nombre des codes équivalents à un code C est

$$N_C = \frac{\mid G_r \mid}{\mid Aut\,(C) \mid} \tag{2.14}$$

ce que implique que

$$\mid Aut\,(C) \mid = \frac{\mid G_r \mid}{N_C} \tag{2.15}$$

C'est-à-dire les codes équivalents sont des codes ayant le même ordre de groupe d'automorphismes mais l'inverse n'est pas vrai.

On peut déterminer le nombre total T_n des codes auto- duaux différents de longueur n.

En effet, soit

$$T_n = \sum_{C \text{ inéquivalent}} N_C \tag{2.16}$$

donc

$$\frac{T_n}{\mid G_r \mid} = \sum_{C \text{ inéquivalent}} \frac{1}{\mid Aut\,(C) \mid} \tag{2.17}$$

L'équation (2.17) est appelée la formule de masse.

Le nombre des codes binaires auto- duaux

Un argument de compte relativement simple peut être employé pour compter le nombre de codes auto- duaux binaires. Cette argument a été généralisé dans [13] aux

codes sur $\mathbb{F}_q$. On commence par une définition et un résultat préliminaire qui est d'intérêt indépendant.

Définition 2.5 Un code linéaire est dit faiblement auto- dual si $1 \in C \subset C^{\perp}$.

Lemme 2.2 Si q est une puissance d'un élément premier ($q = p^m$, p premier) alors

$$\binom{k}{n}_q = \frac{(q^n-1)(q^{n-1}-1)...(q-1)}{(q^k-1)(q^{k-1}-1)...(q-1)(q^{n-k}-1)(q^{n-k-1}-1)...(q-1)} \tag{2.18}$$

est le nombre des sous espaces vectoriels de dimension k de $\mathbb{F}_q^n$.

Les expressions $\binom{k}{n}_q$ où $k \in \{1, 2, ..., n\}$ sont appelés les coefficients de Gauss.

Preuve : Soit $S(n,k)$ le nombre des sous espace vectoriel de $\mathbb{F}_q^n$ de dimension k, et soit $N(n,k)$ le nombre des vecteurs $(v_1, v_2, ..., v_k)$ dans $\mathbb{F}_q^n$ linéairement indépendant

On choisit

v_1 parmi $(q^n - 1)$ possibilités.

v_2 parmi $(q^n - q)$ possibilités.

$\vdots$

v_k parmi $\left(q^n - q^{k-1}\right)$ possibilités.

donc

$$N(n,k) = (q^n-1)\left(q^{n-1}-q\right)...\left(q^n-q^{k-1}\right)$$

Dans chaque sous espace vectoriel de dimension k, le nombre de vecteurs de k composantes sont linéairement indépendants dans $\mathbb{F}_q^k$ est

$$\left(q^k-1\right)\left(q^k-q\right)...\left(q^k-q^{k-1}\right)$$

alors

$$N(n,k) = S(n,k) \times \left(q^k-1\right)\left(q^{k-1}-q\right)...\left(q^k-q^{k-1}\right)$$

donc

$$\begin{aligned} S(n,k) &= \frac{N(n,k)}{(q^k-1)(q^{k-1}-q)...(q^k-q^{k-1})} \\ &= \frac{(q^n-1)(q^n-q)...\left(q^n-q^{k-1}\right)}{(q^k-1)(q^{k-1}-q)...(q^k-q^{k-1})} \\ &= \frac{(q^n-1)(q^{n-1}-1)...\left(q^{n-k+1}-1\right)\times\left(q^{n-k}-1\right)\left(q^{n-k-1}-1\right)...(q-1)}{(q^k-1)(q^{k-1}-1)...(q-1)\times(q^{n-k}-1)(q^{n-k-1}-1)...(q-1)} \\ &= \frac{(q^n-1)(q^{n-1}-1)...(q-1)}{(q^k-1)(q^{k-1}-1)...(q-1)\times(q^{n-k}-1)(q^{n-k-1}-1)...(q-1)} \\ &= \binom{k}{n}_q \end{aligned}$$

■

Théorème 2.5 *Soit $C = C(n,k)$ un code binaire faiblement auto- dual, le nombre des codes faiblement auto- duaux $\left[n, \frac{n}{2}\right]$ contenant C est $\prod_{i=1}^{\frac{n}{2}-k}(2^i+1)$.*

Preuve : *S*oit $\sigma_{n,m}$ le nombre des $[n,m]$ codes faiblement auto- duaux, qui contient C et $k \leq m \leq \frac{n}{2}$.

On compte le nombre des couples (D,E) telle que $C \subset D \subset E$, $D = C(n,m)$ et $E = C(n,m+1)$ sont des codes faiblement auto- duaux .

Premièrement on fixe D : comme $D \subset E$ et $\dim E = \dim D + 1$ alors E engendré par D et un vecteur non nul $x \notin D$.

Si $x \in E \backslash D$ alors $E = D \cup \{x+D\}$, de plus E est un code faiblement auto- dual donc

$$x \in E \subset E^{\perp} \subset D^{\perp}$$

alors on peut prendre $E = D \cup \{x+D\}$ et $x \in D^{\perp} \backslash D$.

mais $D \cup \{x+D\} = D \cup \{y+D\}$ si est seulement si x et y dans la même translaté de D dans $D^{\perp}$.

Par conséquent le nombre des différents codes de la forme $E = D \cup \{x+D\}$ est le nombre des différents translatés non triviaux de D dans $D^{\perp}$ qui est

$$\frac{2^{n-m}}{2^m} - 1 = 2^{n-2m} - 1$$

alors le nombre des couples (D,E) est $\sigma_{n,m}(2^{n-2m}-1)$.

Deuxièment on fixe E : on a le nombre des sous espace vectoriel de dimension m dans E de dimension $m+1$ est

$$\binom{m}{m+1}_2 = \binom{m-k}{m-k+1}_2 = 2^{m-k+1} - 1$$

donc le nombre des couples (D, E) est $\sigma_{n,m+1}\left(2^{m-k+1}-1\right)$

alors

$$\sigma_{n,m}\left(2^{n-2m}-1\right) = \sigma_{n,m+1}\left(2^{m-k+1}-1\right)$$

donc

$$\sigma_{n,m+1} = \sigma_{n,m}\frac{(2^{n-2m}-1)}{(2^{m-k+1}-1)}$$

On remarque que $\sigma_{n,k} = 1$, alors

$$\begin{aligned}
\sigma_{n,\frac{n}{2}} &= \sigma_{n,\frac{n}{2}-1}\frac{2^2-1}{2^{\frac{n}{2}-k}-1} \\
&= \sigma_{n,\frac{n}{2}-2}\frac{2^4-1}{2^{\frac{n}{2}-k-1}-1} \times \frac{2^2-1}{2^{\frac{n}{2}-k}-1} \\
&= \sigma_{n,k}\frac{2^{n-2k}-1}{2-1} \times \frac{2^{n-2k-2}-1}{2^2-1} \times ... \times \frac{2^4-1}{2^{\frac{n}{2}-k-1}-1} \times \frac{2^2-1}{2^{\frac{n}{2}-k}-1} \\
&= \left(2^{\frac{n}{2}-k}+1\right)\left(2^{\frac{n}{2}-k-1}+1\right)...\left(2^2+1\right)(2+1) \\
&= \prod_{i=1}^{\frac{n}{2}-k}\left(2^i+1\right)
\end{aligned}$$

■

Corollaire 2.2 Le nombre des codes binaires auto- duaux $\left[n, \frac{n}{2}\right]$ est

$$T_n = \prod_{i=1}^{\frac{n}{2}-1}\left(2^i+1\right) \tag{2.19}$$

Preuve : Comme tous les codes binaires auto- duaux contient le vecteur 1^n puisque pour tout $u \in C$ on a $\langle u, 1\rangle = \omega(u) \equiv 0 \pmod 2$ donc $1^n \in C^\perp = C$.
D'après le théorème précédent, considérons le code faiblement auto- dual est le code de répétition c-à-d $C(n,k) = C(n,1) = \{0^n, 1^n\}$ et le nombre des codes auto- duaux est

$T_n = \prod_{i=1}^{\frac{n}{2}-1} (2^i + 1)$. ■

Théorème 2. 6 [13] Le nombre total des codes auto duaux de longueur n

- $T_n = 2 \prod_{i=1}^{\frac{n}{2}-2} (2^i + 1)$; pour les codes binaires de type II.
- $T_n = 2 \prod_{i=1}^{\frac{n}{2}-1} (3^i + 1)$; pour les codes ternaires.
- $T_n = \prod_{i=0}^{\frac{n}{2}-1} (2^{2i+1} + 1)$; pour les codes quaternaires hermitiens.
- $T_n = \prod_{i=1}^{\frac{n}{2}-1} (2^{2i} + 1)$; pour les codes quaternaires euclidiens.

2.1.5 Les codes sur $\mathbb{Z}_4$

Les codes sur un anneau sont probablement moins familiers que les codes sur un corps. Dans cette partie on étudie les codes sur l'anneau $\mathbb{Z}_4$, ([4], [13]).

Chaque code sur $\mathbb{Z}_4$ est équivalent à un code de matrice génératrice de forme

$$A = \begin{pmatrix} I_{k_1} & X & Y_1 + 2Y_2 \\ 0 & 2I_{k_2} & 2Z \end{pmatrix} \tag{2.20}$$

où X, Y_1, Y_2, Z sont des matrices binaires.

Alors un code C sur $\mathbb{Z}_4$ est un groupe additif de type $4^{k_1}2^{k_2}$ qui contient $2^{2k_1+k_2}$ c-à-d $\mid C \mid = 2^{2k_1+k_2}$.

Pour définir le dual d'un code de longueur n sur $\mathbb{Z}_4$ on définit le produit scalaire sur $\mathbb{Z}_4^n$ comme suit

$\langle x, y \rangle = \left(\sum_{k=1}^{n} x_k y_k \right) (\mathrm{mod}\, 4)\,; \forall x = (x_1, x_2, ...x_n)\,, y = (y_1, y_2, ..., y_n) \in \mathbb{Z}_4^n$

Le dual de C est engendré par la matrice

$$A^{\perp} = \begin{pmatrix} -(Y_1 + 2Y_2)^t - Z^t X^t & Z^t & I_{n-k_1-k_2} \\ 2X^t & 2I_{k_2} & 0 \end{pmatrix} \tag{2.21}$$

où $\mid C^{\perp} \mid = 4^{n-k_1-k_2}2^{k_2}$.

Proposition 2.1 [4] • Il y a deux codes binaires $C^{(1)} = C\,(n, k_1)$ et $C^{(2)} = C\,(n, k_1 + k_2)$ associés à C et engendrés respectivement par les deux matrices $G^{(1)} = \begin{pmatrix} I_{k_1} & X & Y_1 \end{pmatrix}$ et

$$G^{(2)} = \begin{pmatrix} I_{k_1} & X & Y_1 \\ 0 & I_{k_2} & Z \end{pmatrix}.$$

• Si C un code auto- orthogonal alors $C^{\ (1)}$ est un code de type II et $C^{(1)} \subset C^{(2)} \subset C^{(1)\perp}$, par conséquent si C un code auto- dual alors $C^{(2)} = C^{(1)^{\perp}}$.

Remarque 2.3 • Si C est un code auto- orthogonal alors

$$k_1 + k_2 \leq n - k_1 \Longrightarrow n \geq 2k_1 + k_2 \tag{2.22}$$

• Si C est un code auto- dual alors

$$k_1 + k_2 = n - k_1 \Longrightarrow n = 2k_1 + k_2 \tag{2.23}$$

Le théorème suivant donne l'inverse de la proposition précédente.

Théorème 2.7 *Si A et B sont des codes binaires avec $A \subseteq B$ alors il existe un code C sur $\mathbb{Z}_4$ avec $C^{(1)} = A$ et $C^{(2)} = B$.*
Si A est de type II et $B \subseteq A^{\perp}$ alors C est un code auto- orthogonal, si $B = A^{\perp}$ alors C est un code auto- dual.

Preuve : Supposons que A et B sont engendrés par les deux matrices

$$G_A = \begin{pmatrix} I_{k_1} & X & Y_1 \end{pmatrix}, G_b = \begin{pmatrix} I_{k_1} & X & Y_1 \\ 0 & I_{k_2} & Z \end{pmatrix}$$

alors C est engendré par la matrice

$$G = \begin{pmatrix} I_{k_1} & X & Y \\ 0 & 2I_{k_2} & 2Z \end{pmatrix} \tag{2.24}$$

où $Y = Y_1 + 2Y_2$

Pour établir la deuxième assertion, il faut modifier (2.24) telle que C soit un code auto- orthogonal. On accomplir ceci en remplaçant l'élément $(j,i)^{ième}$ dans (2.24)) par le produit scalaire modulo 4 de lignes i, et j pour $1 \leq i \leq k_1$, $1 \leq j \leq k_1 + k_2$. Dans ce cas chaque code binaire auto- orthogonal de type II correspond à un ou plusieurs codes auto- duaux sur $\mathbb{Z}_4$. ■

Le théorème suivant montre comment choisir Y_2 dans (2.24) pour déterminer un code auto- dual sur $\mathbb{Z}_4$.

Théorème 2.8 [13] *Un code sur $\mathbb{Z}_4$ de matrice génératrice G (2.24) est un code auto-dual si est seulement si $C^{(1)}$ est de type II et $C^{(2)} = C^{(1)^\perp}$ et Y_2 est choisi comme suit, si $M = Y_1 Y_2^t$ alors $M_{ij} + M_{ji} \equiv \frac{1}{2}\omega(v_i \cap v_j)$ où $v_1, v_2, ...v_{k_1}$ sont des lignes dans la matrice $G^{(1)}$.*

Exemple 2.1 Soit A le code binaire de type II de matrice génératrice

$$G_A = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

et le deuxième code B de matrice génératrice $G_B = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

telle que $A^\perp = B$.

alors $Y_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $Y_1 Y_2^t = M$ ce que implique que $Y_2^t = M$.

Si $Y_2 = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}$ on a $\begin{cases} y_{12} + y_{21} = 0 \\ 2y_{11} = 2 \\ 2y_{22} = 2 \end{cases}$

alors $Y_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ou $Y_2 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

donc on a deux codes auto- duaux sur $\mathbb{Z}_4$ de matrices génératrices

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 3 \\ 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 3 & 2 \\ 0 & 1 & 0 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \end{pmatrix}$$

Les propriétés des codes auto- duaux sur $\mathbb{Z}_4$ [13]

1/ Toutes les normes des mots code sont divisibles par quatre.

2/ Un code auto- dual de longueur quelconque (pair ou impair) sur l'anneau $\mathbb{Z}_4$ existe toujours.

3/ Chaque code auto- dual sur $\mathbb{Z}_4$ de longueur n peut être tronqué à un code auto-dual de longueur $n-1$ en supprimant une composante de la manière suivante :

i) Si la projection de C sur la $i^{ième}$ composante, qui contient tout les éléments de $\mathbb{Z}_4$ le code tronqué est obtenu par trouver ces mots de C qui sont 0 ou 2, dans la $i^{ième}$ composante et supprimer cette composante.

ii) Si la projection de C sur la $i^{ième}$ composante qui contient 0 et 2, on trouve les mots code de C qui sont 0 dans la $i^{ième}$ composante et supprimer cette composante.

Transformation un code auto- dual binaire à un code auto- dual sur $\mathbb{Z}_4$

Dans un code binaire, il y a des transformations qui transforment 0 vers 0 ou 2 et 1 vers 1 ou 3 pour obtenir un code sur $\mathbb{Z}_4$.

Par exemple, la première transformation de code de Hamming étendu e_8 au code

auto- dual sur $\mathbb{Z}_4$ est l'octacode O_8 de matrice génératrice

$$\left(\begin{array}{c||cccc} & 2 & 1 & 1 & 1 \\ & 3 & 2 & 1 & 3 \\ I_4 & 3 & 3 & 2 & 1 \\ & 3 & 1 & 3 & 2 \end{array}\right) \tag{2.25}$$

avec le poids minimal de Lee est 6 et la norme minimale est 8.

La deuxième transformation de code de Hamming étendu e_8 au code auto- dual sur $\mathbb{Z}_4$ noté par ζ_8 de matrice génératrice

$$\left(\begin{array}{c||cccc} & 0 & 1 & 1 & 1 \\ & 3 & 0 & 1 & 3 \\ I_4 & 3 & 3 & 0 & 1 \\ & 3 & 1 & 3 & 0 \end{array}\right) \tag{2.26}$$

avec le poids minimal de Lee et la norme minimale quatre.

Par contre, on ne peut pas transformer chaque code binaire auto- dual à un code auto- dual sur $\mathbb{Z}_4$, par exemple le code de répétition $i_2 = \{00, 11\}$.

Le théorème suivant montre la condition nécessaire et suffisante sur un code binaire auto- dual transformé à un code auto- dual sur $\mathbb{Z}_4$.

Théorème 2.9 *Soit $C = C(2k, k)$ un code binaire auto- dual.*
La condition nécessaire et suffisante sur C transformé à un code auto- dual $\widehat{C}$ sur $\mathbb{Z}_4$ est tous les poids de Hamming de C sont divisibles par quatre.

Preuve : La condition nécessaire

Supposons que $v \in C$ et $\omega(v) \neq 0 \pmod 4$ et soit $\widehat{v} \in \widehat{C}$ est la transformation de v

alors $norm(\widehat{v}) \equiv norm(v) \pmod 4$ (car pour les nombres entiers si $x \equiv y \pmod 2$ donc $x^2 \equiv y^2 \pmod 4$).

alors $norm(\widehat{v}) \neq 0 \pmod 4$ contradiction .

La condition suffisante

Sans perdre la généralité, C possède une matrice génératrice de forme standard $(I_k \| A_k)$ où $AA^t \equiv -I_k \pmod 2$

Soit B une transformation de A sur $\mathbb{Z}_4$, on veut trouver $\widehat{A} = B + 2M$ où M est une matrice binaire telle que $\widehat{A}\widehat{A}^t \equiv -I_k \pmod 4$, en addition on peut prendre $\widehat{C} = \left(I_k \| \widehat{A}\right)$ on a

$$\widehat{A}\widehat{A}^t \equiv \left(BB^t + 2\left(MB^t + BM^t\right)\right) \pmod 4$$

La condition sur C implique que $BB^t + I_k$ ayant des coefficients pairs et zéro sur la diagonale, mais il existe une matrice binaire $\overline{M}$ telle que $2\left(\overline{M} + \overline{M}^t\right) = BB^t + I_k$ et on prends $M = \overline{M}\left(B^{-1}\right)^t$. ■

2.2 Théorie des invariants

2.2.1 Le caractère

Soit $(\mathbf{G}, +)$ un groupe additif, et $\mathbb{C}_1 = \{z \in \mathbb{C}, \mid z \mid = 1\}$ le groupe multiplicative.

Définition 2.6 • Un caractère de G est un homomorphisme $\chi : G \longrightarrow \mathbb{C}_1$.

• Soit χ un caractère de G. Si χ satisfait : $\forall g \in G; \chi(g) = 1$ alors χ est dit principal.

Théorème 2.10 *Soit χ un caractère de G alors*

$$\sum_{g \in G} \chi(g) = \begin{cases} \mid G \mid & \text{si } \chi \text{ est principal} \\ 0 & \text{si non} \end{cases} \tag{2.27}$$

Preuve : Si χ est un caractère principal on a

Pour tout $g \in G; \chi(g) = 1$ alors

$$\begin{aligned} \sum_{g \in G} \chi(g) &= \sum_{g \in G} 1 \\ &= \mid G \mid \end{aligned}$$

Si χ n'est pas principal, alors il existe $h \in G$ tel que $\chi(h) \neq 1$ et on aura

$$\begin{aligned}\chi(h)\sum_{g\in G}\chi(g) &= \sum_{g\in G}\chi(h)\chi(g)\\ &= \sum_{g\in G}\chi(h+g)\\ &= \sum_{g\in G}\chi(g)\end{aligned}$$

donc

$$(\chi(h)-1)\sum_{g\in G}\chi(g)=0$$

alors $\sum_{g\in G}\chi(g)=0.$ ■

Pour tout code linéaire C sur $\mathbb{F}_q$; et pour tout $u \in \mathbb{F}_q^n$, on définit l'application

$$\begin{aligned}\chi_u : C &\longrightarrow \mathbb{C}_1\\ v &\longmapsto \chi_u(v) = \chi(\langle u, v\rangle)\end{aligned}$$

où χ est un caractère non principal et $\langle u, v\rangle$ est le produit scalaire euclidien sur $\mathbb{F}_q^n$.

χ_u ainsi définit un caractère de C.

Théorème 2.11 *Le caractère $\chi_u : C \longrightarrow \mathbb{C}_1$ est principal si est seulement si $u \in C^\perp$. En particulier $\chi_u : \mathbb{F}_q^n \longrightarrow \mathbb{C}_1$ est principal si est seulement si $u = 0$.*

Preuve : ◁ Supposons que $u \in C^\perp$ et démontrons que χ_u est un caractère principal.

Comme $u \in C^\perp$ alors $\forall c \in C; \langle u, c\rangle = 0$

$$\chi_u(c) = \chi(\langle u, c\rangle) = \chi(0) = 1$$

donc χ_u est principal.

▷ Inversement, supposons que χ_u est un principal et démontrons que $u \in C^\perp$.

Comme χ_u est principal alors

$$\forall c \in C; \chi_u(c) = \chi(\langle u, c\rangle) = \chi(0) = 1$$

Supposons que $u \notin C^\perp$ alors $\langle u, c\rangle \in \mathbb{F}_q$, on pose $\alpha = \langle u, c\rangle$ où α parcours $\mathbb{F}_q$

donc

$$\forall \alpha \in \mathbb{F}_q; \chi(\alpha) = 1$$

alors χ est un caractère principal et ceci contredi χ n'est pas principal.

En particulier, si $C = \mathbb{F}_q^n$ alors $C^{\perp} = 0$. ■

Corollaire 2.3 Soit C un code linéaire sur $\mathbb{F}_q$, alors pour tout $u \in \mathbb{F}_q^n$

$$\sum_{c \in C} \chi_u(c) = \begin{cases} \mid C \mid & \text{si } u \in C^{\perp} \\ 0 & \text{si } u \notin C^{\perp} \end{cases} \tag{2.28}$$

Lemme 2.3 Soit $\mathbb{F}$ un anneau commutatif, et f une fonction définie sur $\mathbb{F}^n$ $(n \geq 1)$ à valeurs dans un anneau commutatif contenant $\mathbb{C}_1$.

La transformée de Hadamard $\widehat{f}$ de la fonction f est donné par

$$\forall u \in \mathbb{F}^n : \widehat{f}(u) = \sum_{v \in \mathbb{F}^n} \chi_u(v) f(v) \tag{2.29}$$

Si C est un code linéaire de longueur n sur $\mathbb{F}$ on a

$$\sum_{u \in C^{\perp}} f(u) = \frac{1}{\mid C \mid} \sum_{u \in C} \widehat{f}(u) \tag{2.30}$$

Preuve : On a

$$\begin{aligned}
\sum_{u\in C}\widehat{f}(u) &= \sum_{u\in C}\sum_{v\in\mathbb{F}^n}\chi_u(v)\,f(v)\\
&= \sum_{v\in\mathbb{F}^n}\sum_{u\in C}\chi_u(v)\,f(v)\\
&= \sum_{v\in\mathbb{F}^n}\left(\sum_{u\in C}\chi(\langle u,v\rangle)\right)f(v)\\
&= \sum_{v\in\mathbb{C}^\perp}\left(\sum_{u\in C}\chi(\langle u,v\rangle)\right)f(v)+\underbrace{\sum_{v\notin\mathbb{C}^\perp}\left(\sum_{u\in C}\chi(\langle u,v\rangle)\right)f(v)}_{\begin{array}{c}\shortparallel\\0\end{array}}\\
&= |\,C\,|\sum_{v\in\mathbb{C}^\perp}f(v)
\end{aligned}$$

alors

$$\sum_{v\in\mathbb{C}^\perp}f(v)=\tfrac{1}{|C|}\sum_{u\in C}\widehat{f}(u)$$

■

Il existe une relation entre les polynômes énumérateurs des poids de C et $C^\perp$, appelée identité de Mac Williams, elle permet d'obtenir le polynôme énumérateur des poids de $C^\perp$ à partir de celui de C.

Théorème 2.12 (Identité de Mac Williams) *Soit C un code linéaire de longueur n sur un corps $\mathbb{F}_q$, on a alors l'équation suivante :*

$$W_{C^\perp}(x,y)=\frac{1}{|\,C\,|}W_C(x+(q-1)\,y,x-y) \tag{2.31}$$

Preuve : Soit l'application f définie pour tout u de $\mathbb{F}_q^n$ par

$$f(u)=x^{n-w(u)}y^{w(u)}$$

On a alors

$$\begin{aligned}\sum_{v\in\mathbb{C}^{\perp}} f(v) &= \sum_{v\in\mathbb{C}^{\perp}} x^{n-w(u)}y^{w(u)} \\ &= W_{C^{\perp}}(x,y)\end{aligned}$$

On définit l'application δ de $\mathbb{F}_q$ dans $\{0,1\}$ telle que

$$\delta(a) = \begin{cases} 1 & \text{si } a \in \mathbb{F}_q^* \\ 0 & \text{si } a = 0 \end{cases}$$

Pour tout u de $\mathbb{F}_q^n$ on obtient que

$$\begin{aligned}\widehat{f}(u) &= \sum_{v\in\mathbb{F}_q^n} \chi(\langle u,v\rangle) f(v) \\ &= \sum_{(v_1,v_2,\ldots,v_n)\in\mathbb{F}_q^n} \chi(u_1v_1+u_2v_2+\ldots+u_nv_n)\, x^{1-\delta(v_1)}y^{\delta(v_1)} \times x^{1-\delta(v2)}y^{\delta(v_2)} \\ &\quad \times\ldots\times x^{1-\delta(v_n)}y^{\delta(v_n)} \\ &= \left(\sum_{v_1\in\mathbb{F}_q} \chi(u_1v_1)\, x^{1-\delta(v_1)}y^{\delta(v_1)}\right) \times \left(\sum_{v_2\in\mathbb{F}_q} \chi(u_2v_2)\, x^{1-\delta(v_2)}y^{\delta(v_2)}\right) \\ &\quad \times\ldots\times \left(\sum_{v_n\in\mathbb{F}_q} \chi(u_nv_n)\, x^{1-\delta(v_n)}y^{\delta(v_n)}\right) \\ &= \left(\sum_{v\in\mathbb{F}_q} \chi(u_1v)\, x^{1-\delta(v)}y^{\delta(v)}\right) \times \left(\sum_{v\in\mathbb{F}_q} \chi(u_2v)\, x^{1-\delta(v)}y^{\delta(v)}\right) \\ &\quad \times\ldots\times \left(\sum_{v\in\mathbb{F}_q} \chi(u_nv)\, x^{1-\delta(v)}y^{\delta(v)}\right) \\ &= \prod_{i=1}^{n}\left(\sum_{v\in\mathbb{F}_q} \chi(u_iv)\, x^{1-\delta(v)}y^{\delta(v)}\right)\end{aligned}$$

Si $u_i = 0$

$$\left(\sum_{v \in \mathbb{F}_q} \chi\left(u_i v\right) x^{1-\delta(v)} y^{\delta(v)} \right) = x + (q-1)\, y.$$

Si $u_i \neq 0$

$$\begin{aligned} \left(\sum_{v \in \mathbb{F}_q} \chi\left(u_i v\right) x^{1-\delta(v)} y^{\delta(v)} \right) &= x + \sum_{v \in \mathbb{F}_q^*} \chi\left(u_i v\right) x^{1-\delta(v)} y^{\delta(v)} \\ &= x + \sum_{v \in \mathbb{F}_q^*} \chi\left(u_i v\right) y \\ &= x - y \end{aligned}$$

donc

$$\widehat{f}\left(u\right) = \left(x + (q-1)\, y\right)^{n-w(u)} \left(x - y\right)^{w(u)}$$

alors

$$\begin{aligned} \sum_{u \in C} \widehat{f}\left(u\right) &= \sum_{u \in C} \left(x + (q-1)\, y\right)^{n-w(u)} \left(x - y\right)^{w(u)} \\ &\mid \quad C \mid W_{C^\perp}\left(x, y\right) = W_C\left(x + (q-1)\, y, x - y\right) \end{aligned}$$

■

Exemple 2.2 Soit $H_7 = C\left(7, 3, 4\right)$ le code de Hamming binaire de matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

et son polynôme énumérateur des poids est $W_{H_7}\left(x, y\right) = x^7 + 7x^3y^4$.

alors le polynôme énumérateur des poids de $H_7^\perp$ est

$$\begin{aligned} W_{H_7^\perp}\left(x, y\right) &= \frac{1}{2^3}\left(\left(x + y\right)^7 + 7\left(x + y\right)^3 \left(x - y\right)^4\right) \\ &= x^7 + 7x^3y^4 + 7x^4y^3 + y^7 \end{aligned}$$

Corollaire 2.4 Soit $C = C(n,k)$ un code auto- dual sur $\mathbb{F}_q$ alors on a

$$\begin{aligned} &\bullet W_C(x,y) = W_C\left(\tfrac{1}{\sqrt[2]{q}}(x+(q-1)y), \tfrac{1}{\sqrt[2]{q}}(x-y)\right) \\ &\bullet W_C(x,y) = W_C(-x,-y) \end{aligned} \tag{2.32}$$

Preuve : • Comme C est un code auto- dual donc $C = C^{\perp}$ et $k = \frac{n}{2}$, d'après le théorème de Mac Williams on a

$$\begin{aligned} W_C(x,y) &= \frac{1}{q^{\frac{n}{2}}} W_C((x+(q-1)y), x-y) \\ &= \frac{1}{\sqrt[2]{q}^n} \sum_{i=0}^{n} A_i (x+(q-1)y)^{n-i} (x-y)^i \\ &= \sum_{i=0}^{n} A_i \left(\frac{x+(q-1)y}{\sqrt[2]{q}}\right)^{n-i} \left(\frac{x-y}{\sqrt[2]{q}}\right)^i \\ &= W_C\left(\frac{1}{\sqrt[2]{q}}(x+(q-1)y), \frac{1}{\sqrt[2]{q}}(x-y)\right). \end{aligned}$$

• puisque $n = 2k$ (n pair) alors

$$\begin{aligned} W_C(x,y) &= \sum_{i=0}^{n} A_i x^{n-i} y^i \\ &= \sum_{i=0}^{n} (-1)^n A_i x^{n-i} y^i \\ &= \sum_{i=0}^{n} A_i (-x)^{n-i} (-y)^i \\ &= W_C(-x,-y) \end{aligned}$$

■

Définition 2.7 Pour tout polynôme $p(x,y)$ et pour toute matrice carrée d'ordre deux A, on définit le produit $\circ$ par

$$(A \circ p)(x,y) = p\left((x,y)A^t\right) \tag{2.33}$$

Exemple 2.3 Soit $p(x,y) = x^2 + y^2$ *et* $A = \begin{pmatrix} 1 & 1 \\ 0 & i \end{pmatrix}$

$$\begin{aligned} (A \circ p)(x,y) &= p\left((x,y)A^t\right) \\ &= p\left((x,y)\begin{pmatrix} 1 & 1 \\ 0 & i \end{pmatrix}^t\right) \\ &= p(x+y, iy) \\ &= x^2 + xy \end{aligned}$$

Définition 2.8 Un polynôme $p(x_1, x_2, ..., x_m)$ est dit invariant sous la matrice complexe A d'ordre m si

$$(A \circ p)(x_1, x_2, ..., x_m) = p(x_1, x_2, ..., x_m) \tag{2.34}$$

Corollaire 2.5 Le polynôme énumérateur d'un code auto- dual C sur $\mathbb{F}_q$ est un invariant sous les deux matrices $A = \frac{1}{\sqrt[2]{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}, -I_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

Preuve : Du corollaire précédent, on obtient

$$\begin{aligned} W_C(x,y) &= W_C\left(\frac{1}{\sqrt[2]{q}}(x+(q-1)y), \frac{1}{\sqrt[2]{q}}(x-y)\right) \\ &= W_C\left((x,y)\left(\frac{1}{\sqrt[2]{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}\right)^t\right) \\ &= \left(\frac{1}{\sqrt[2]{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix} \circ W_C\right)(x,y) \\ &= (A \circ W_C)(x,y) \end{aligned}$$

$$\begin{aligned} W_C(x,y) &= W_C(-x,-y) \\ &= W_C\left((x,y)\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^t\right) \\ &= \left(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \circ W_C\right)(x,y) \\ &= \left((-I_2) \circ W_C\right)(x,y) \end{aligned}$$

■

Théorème 2.13 [14] • *Si p est un invariant sous les matrices complexes A* et *B d'ordre m, alors p est un invariant sous tout produit de ces matrices*

• *Si p est un invariant sous les matrices inversibles $A_1, A_2, ..., A_s$ alors p est invariant sous toute matrice du groupe engendré par $A_1, A_2, ..., A_s$.*

Définition 2.9 • Soit G un groupe fini des matrices complexes carrées d'ordre m, tout polynôme de m variables p invariant sous tous les éléments de G est dit invariant du groupe G.

• L'ensemble de tous les invariants du G est une algèbre sur le corps complexe, notée par $I(G)$.

Le théorème suivant peut être utilisé pour déterminer les invariants d'un groupe.

Théorème 2.14 *Soit $G = \{A_1, A_2, ..., A_g\}$ un groupe fini de matrices carrées d'ordre m, et $p(x_1, x_2, ..., x_m)$ un polynôme.*
Alors le polynôme $\overline{p}(x_1, x_2, ..., x_m) = \frac{1}{g}\sum_{i=1}^{g} A_i \circ p(x_1, x_2, ..., x_m)$, appelé moyenne polynômiale de p, est un invariant de G.

Preuve : Pour tout $k \in \{1,2,...,g\}$ on a

$$\begin{aligned}
\left(A_k \circ \overline{p}\right)(x_1,x_2,...,x_m) &= \left(A_k \circ \frac{1}{g}\sum_{i=1}^{g}\left(A_i \circ p\right)\right)(x_1,x_2,...,x_m) \\
&= \frac{1}{g}\sum_{i=1}^{g}\left(A_k \circ \left(A_i \circ p\right)\right)(x_1,x_2,...,x_m) \\
&= \frac{1}{g}\sum_{i=1}^{g}\left(\left(A_k A_i\right) \circ p\right)(x_1,x_2,...,x_m)
\end{aligned}$$

car $\forall k \in \{1,2,...,g\}\,;\, A_k G = G$ donc

$$\begin{aligned}
\left(A_k \circ \overline{p}\right)(x_1,x_2,...,x_m) &= \frac{1}{g}\sum_{i=1}^{g}\left(A_i \circ p\right)(x_1,x_2,...,x_m) \\
&= \overline{p}\,(x_1,x_2,...,x_m)
\end{aligned}$$

■

Exemple 2.4 Soit $G = \{I_2, -I_2, A, -A\}$ où $A = \frac{1}{\sqrt[2]{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}$, $p(x,y) = x^2$ et $q(x,y) = y^2$

$$\begin{aligned}
\overline{p}\,(x,y) &= \frac{1}{4}\left[\left(I_2 \circ P\right)(x,y) + \left(\left(-I_2\right) \circ P\right)(x,y) + \left(A \circ P\right)(x,y) + \left(\left(-A\right) \circ P\right)(x,y)\right] \\
&= \frac{1}{4}\begin{pmatrix} P(x,y) + P(-x,-y) + P\left(\frac{1}{\sqrt[2]{q}}\left(x+(q-1)y\right), \frac{1}{\sqrt[2]{q}}\left(x-y\right)\right) + \\ P\left(\frac{-1}{\sqrt[2]{q}}\left(x+(q-1)y\right), \frac{-1}{\sqrt[2]{q}}\left(x-y\right)\right) \end{pmatrix} \\
&= \frac{1}{4}\left(x^2 + (-x)^2 + \left(\frac{1}{\sqrt[2]{q}}\left(x+(q-1)y\right)\right)^2 + \left(\frac{-1}{\sqrt[2]{q}}\left(x+(q-1)y\right)\right)^2\right) \\
&= \frac{1}{2q}\left((q+1)x^2 + 2(q-1)xy + (q-1)^2 y^2\right)
\end{aligned}$$

$$\begin{aligned}\overline{q}(x,y) &= \frac{1}{4}\left(y^2+(-y)^2+\left(\frac{1}{\sqrt[2]{q}}(x-y)\right)^2+\left(\frac{-1}{\sqrt[2]{q}}(x-y)\right)^2\right)\\ &= \frac{1}{2}\left(y^2+\frac{1}{q}(x-y)^2\right)\\ &= \frac{1}{2q}\left(x^2-2xy+(q-1)y^2\right)\end{aligned}$$

donc

$$\begin{aligned}\frac{1}{2}\left(\overline{p}(x,y)-(q+1)\overline{q}(x,y)\right) &= y(x-y)\\ \overline{p}(x,y)+(q-1)\overline{q}(x,y) &= x^2+(q-1)y^2\end{aligned}$$

sont des invariants de degré 2 du groupe G.

Définition 2.10 Etant donné r polynômes, on dit que $f_1(x).f_2(x),...,f_r(x)$ sont algébriquement dépendants s'il existe un polynôme non nul p de r variables avec des coefficients complexes tel que :

$$p(f_1(x).f_2(x),...,f_r(x))=0$$

Si non, on dit que $f_1(x).f_2(x),...,f_r(x)$ sont algébriquements indépendants.

Définition 2.11 Soit G un groupe fini des matrices complexes d'ordre m, un ensemble $\{p_1,p_2,...,p_s\}$ des invariants de G est dit la base polynomiale de $I(G)$ si chaque invariant de G est un polynôme en $p_1,p_2,...,p_s$ c'est-à-dire l'ensemble

$$I=\left\{p_1^{i_1}p_2^{i_2}...p_s^{i_s};i_1,i_2,...,i_s\geq 0\right\}$$

engendre $I(G)$.

On utilise le lemme suivant pour montrer le théorème de Molien

Lemme 2.4 Soit $G=\{A_1,A_2,...,A_g\}$ un groupe fini des matrices complexes d'ordre m,

le nombre des invariants de G de degré 1 linéairement indépendants est

$$a_1 = \frac{1}{g}\sum_{i=1}^{g} trace\,(A_i) \tag{2.35}$$

Preuve : Soit $S = \frac{1}{g}\sum_{i=1}^{g} A_i$, soit T la matrice carrée d'orde m telle que $S' = TST^{-1}$ soit diagonale.

Posons $(y_1, y_2, .., y_m) = (x_1, x_2, ..., x_m)\,T^t$.

alors

$$\begin{aligned}
S^2 &= \frac{1}{g^2}\left(\sum_{i=1}^{g} A_i\right)\left(\sum_{j=1}^{g} Aj\right) \\
&= \frac{1}{g^2}\sum_{i=1}^{g}\sum_{j=1}^{g} A_i Aj \\
&= \frac{1}{g^2}\left\{\sum_{j=1}^{g} A_1 Aj + \sum_{j=1}^{g} A_2 Aj + ... + \sum_{j=1}^{g} A_g Aj\right\} \\
&= \frac{1}{g^2}\left\{g\sum_{k=1}^{g} A_k\right\} \\
&= S
\end{aligned}$$

$$\begin{aligned}
S'^2 &= \left(TST^{-1}\right)\left(TST^{-1}\right) \\
&= TS^2T^{-1} \\
&= TST^{-1} \\
&= S'
\end{aligned}$$

Comme S' est diagonale et $S'^2 = S'$ alors les éléments de diagonale de S' sont 0 et 1.

Supposons que $S'=\begin{pmatrix} \lambda_1 & & & & \\ & \lambda_2 & & & \\ & & . & & \\ & & & . & \\ & & & & . \\ & & & & \lambda_m \end{pmatrix}$ où $\lambda_i = 0$ ou 1 et $trace\,(S') = r$

Soit $p_i\,(y_1, y_2, ..., y_m) = y_i$ on a

$$(S' \circ p_i)\,(y_1, y_2, ..., y_m) = \begin{cases} p_i\,(y_1, y_2, ..., y_m) & \text{si } \lambda_i = 1 \\ 0 & \text{si } \lambda_i = 0 \end{cases}$$

Supposons que $\lambda_{i_1} = \lambda_{i_2} = ... = \lambda_{i_r} = 1$ où $i_k \in \{1, 2, ..., m\}, \forall k \in \{1, ..., r\}$, alors les polynômes $p_{i_1}, p_{i_2}, ..., p_{i_r}$, sont fixés par S' et tout combinaison linéaire de $p_{i_1}, p_{i_2}, ..., p_{ir}$ est certainement fixée par S', ainsi $a_1 \leq r$.

D'autre part dans le théorème 2.13 on a

$$S \circ y_i = \frac{1}{g} \sum_{i=1}^{g} A_i y_i$$

est un invariant de G pour tout i et ainsi $a_1 \geq r$.

donc $a_1 = r$.

Mais $traceS = traceS' = r$, alors $a_1 = traceS$. ■

Théorème 2.15 (Le Théorème de Molien) *Soit G un groupe fini de matrices complexes d'ordre m et soit a_k le nombre des invariants homogènes de degré k linéairement indépendants dans $I\,(G)$.*

Soit $\Phi_G\,(\lambda) = \sum_{i=0}^{\infty} a_i \lambda^i$ *alors*

$$\Phi_G\,(\lambda) = \frac{1}{\mid G \mid} \sum_{A \in G} \frac{1}{\det\,(I - \lambda A)} \tag{2.36}$$

Preuve : Considérons l'ensemble

$$P^{[d]} = \left\{ \prod_{i=1}^{m} x_i^{d_i} : \sum_{i=1}^{m} d_i = d \right\} = \left\{ p_1^d, p_2^d, ..., p_m^d, ... \right\}.$$

Soit $A_i^{[d]}$ la matrice dont les lignes sont les coefficients de

$$A_i \circ p_k^d = \sum_{j=1}^{m} \beta_{kj} p_j^d, \forall k \in \{1, 2, ..., m, ...\}$$

c-à-d la $k^{ième}$ ligne est $\beta_{k1}\beta_{k2}...\beta_{km}$.

Soit a_d le nombre des invariants linéairement indépendants de degré 1 de $G^{[d]} = \left\{ A_i^{[d]} : i \in \{1, 2, ..., g\} \right\}$,d'aprés le lemme précédent on a

$$a_d = \frac{1}{g} \sum_{i=1}^{g} trace \left(A_i^{[d]} \right)$$

Pour démontrer le théorème de Molien il suffit de démontrer que la trace de $A_i^{[d]}$ est égale au coefficient de λ^i dans l'équation suivante :

$$\frac{1}{\det (I - \lambda A_i)} = \frac{1}{\prod_{k=1}^{m} (1 - \omega_k \lambda)} \tag{2.37}$$

où $\omega_1, \omega_2, ..., \omega_m$ sont des valeurs propres de A_i, par un changement approprié des variables nous pouvons écrire

$$A_i = \begin{pmatrix} \omega_1 & & & & \\ & \omega_2 & & & \\ & & . & & \\ & & & . & \\ & & & & . \\ & & & & & \omega_m \end{pmatrix}$$

alors

$$A_i^{[d]} = \begin{pmatrix} \omega_1^d & & & & & & \\ & \omega_2^d & & & & & \\ & & . & & & & \\ & & & . & & & \\ & & & & . & & \\ & & & & & \omega_1^{d-1}\omega_2 & \\ & & & & & & . \\ & & & & & & & . \end{pmatrix}$$

et

$$trace\left(A_i^{[d]}\right) = \sum_{\substack{(i_1,i_2,\ldots,i_m)\in\{0,1,\ldots,d\}^m \\ \sum_{k=1}^{m} i_k = d}} \omega_1^{i_1}\omega_2^{i_2}\ldots\omega_m^{i_m}$$

Mais dans (2.37) on a

$$\begin{aligned} \frac{1}{\det\left(I-\lambda A_i\right)} &= \frac{1}{\prod_{k=1}^{m}\left(1-\omega_k\lambda\right)} \\ &= \prod_{k=1}^{m}\frac{1}{\left(1-\omega_k\lambda\right)} \\ &= \prod_{k=1}^{m}\sum_{i_k\geq 0}\left(\omega_k\lambda\right)^{i_k} \\ &= \sum_{j\geq 0}\sum_{\substack{i_i+i_2+\ldots+i_m=j \\ (i_i,i_2,\ldots,i_m)\in\{0,1,\ldots,j\}}}\left(\omega_1^{i_1}\omega_2^{i_2}\ldots\omega_m^{i_m}\right)\lambda^j \\ &= \sum_{j\geq 0}\left(\sum_{\substack{i_i+i_2+\ldots+i_m=j \\ (i_i,i_2,\ldots,i_m)\in\{0,1,\ldots,j\}}}\left(\omega_1^{i_1}\omega_2^{i_2}\ldots\omega_m^{i_m}\right)\right)\lambda^j \\ &= \sum_{j\geq 0}\left(trace\left(A_i^{[j]}\right)\right)\lambda^j \end{aligned}$$

■

Le théorème de Molien nous détermine les degrés des éléments d'une certaine base de

$I(G)$.

Théorème 2.16 *Soient $p_1, p_2, ..., p_s$ des polynômes de m variables avec $\deg(p_i) = \alpha_i$. si b_k est le nombre des éléments de*

$$S = \left\{ p_1^{i_1} p_2^{i_2} ... p_s^{i_s}; i_k \geq 0, \forall k \in \{1, 2, ..., s\} \right\} \tag{2.38}$$

de degré k, alors b_k est le coefficient de λ^k dans l'expression

$$\frac{1}{\prod_{k=1}^{s} (1 - \lambda^{\alpha_k})} \tag{2.39}$$

Preuve : Soit b_k le nombre des éléments de S de degré k
comme

$$\deg\left(p_1^{i_1} p_2^{i_2} ... p_s^{i_s}\right) = \alpha_1 i_1 + \alpha_2 i_2 + ... + \alpha_s i_s$$

alors b_k est le nombre des solutions de l'équation $\alpha_1 i_1 + \alpha_2 i_2 + ... + \alpha_s i_s = k$.
D'autr part

$$\begin{aligned}
\frac{1}{\prod_{i=1}^{s} (1 - \lambda^{\alpha_i})} &= \prod_{i=1}^{s} \frac{1}{(1 - \lambda^{\alpha_i})} \\
&= \prod_{i=1}^{s} \sum_{r_i \geq 0} (\lambda^{\alpha_i})^{r_i} \\
&= \sum_{k \geq 0} \sum_{r_1\alpha_1 + r_2\alpha_2 + ... + r_s\alpha_s = k} \lambda^{1\alpha_1 + r_2\alpha_2 + ... + r_s\alpha_s} \\
&= \sum_{k \geq 0} \sum_{r_1\alpha_1 + r_2\alpha_2 + ... + r_s\alpha_s = k} \lambda^k \\
&= \sum_{k \geq 0} \left(\sum_{r_1\alpha_1 + r_2\alpha_2 + ... + r_s\alpha_s = k} 1 \right) \lambda^k \\
&= \sum_{k \geq 0} b_k \lambda^k
\end{aligned}$$

■

2.2.2 Le polynôme énumérateur des poids d'un code auto- dual sur $\mathbb{F}_q$

On sait que le polynôme énumérateur d'un code auto- dual sur $\mathbb{F}_q$ est un invariant sous les deux matrices $A_1 = \frac{1}{\sqrt[2]{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}, -I_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.
Soit G le groupe engendré par $-I_2$ et A_1, dit groupe Dihedral d'ordre 4 c-à-d

$G = \{I_2. - I_2, A_1, -A_1\}$.

D'après le théorème Molien on a

$$\begin{aligned} \Phi_G(\lambda) &= \frac{1}{4} \sum_{B \in G} \frac{1}{\det(I_2 - \lambda B)} \\ &= \frac{1}{\left(1-\lambda^2\right)^2} \\ &= \frac{1}{\left(1-\lambda^2\right)\left(1-\lambda^2\right)} \end{aligned} \tag{2.40}$$

Donc il y a deux invariants homogènes de degré deux algébriquement indépendants.

Par la méthode de moyenne polynômiale on a deux invariants de degrée deux qui sont

$$\Phi_1(x,y) = x^2 + (q-1)y^2, \Phi_2(x,y) = y(x-y) \tag{2.41}$$

Reste à démontrer que les deux invariants sont algébriquement indépendants.

Supposons que les deux invariants sont algébriquement dépendants alors

$$\sum_{i,j \in I} c_{ij} \Phi_1^i \Phi_2^j = 0 \text{ et } c_{ij} \neq 0, \forall i,j \in I \subset \mathbb{N} \tag{2.42}$$

Soit $f(y)$ le coéfficient de x^m où m est le degré maximal de x dans $\sum_{i,j} c_{ij} \Phi_1^i \Phi_2^j$, alors nécessairement $f(y) = 0$.

on a

$$c_{ij}\Phi_1^i\Phi_2^j = c_{ij}\left(x^2+(q-1)\,y^2\right)^i\left(y\,(x-y)\right)^j \tag{2.43}$$

Le terme de degré maximal de x dans cette expression est

$$c_{ij}x^{2i+j}y^j \text{ où } 2i+j=m$$

donc le terme de degré maximal dans $\sum_{i,j} c_{ij}\Phi_1^i\Phi_2^j$ est $\sum_{\substack{i,j\\2i+j=m}} c_{ij}x^{2i+j}y^j$ qui est $\sum_i c_{i,m-2i}x^m y^{m-2i}$ alors $f(y)=\sum_i c_{i,m-2i}y^{m-2i}=0$, ce que implique que $c_{i,m-2i}=0$ contradiction.

En particulier, pour les codes auto- duaux binaires et ternaires on utilise les proprietés de ces codes pour déterminer le groupe G et l' algèbre $I(G)$.

D'après le théorème de Mac Williams, le polynôme énumérateur d'un code auto- dual sur $\mathbb{F}_q$ est invariant sous la matrice inversible $A=\frac{1}{\sqrt[2]{q}}\begin{pmatrix}1 & q-1\\ 1 & -1\end{pmatrix}$.

2.2.3 Le polynôme énumérateur des poids d'un code binaire auto- dual

type I

On sait que le poids de chaque mot code est pair, alors :

$$\begin{aligned} W_C(x,y) &= \sum_{\omega(c)\in C} x^{n-\omega(c)}y^{\omega(c)} \\ &= \sum_{\omega(c)\in C} x^{n-\omega(c)}(-y)^{\omega(c)} \\ &= W_C(x,-y) \\ &= \left(\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\circ W_C\right)(x,y) \end{aligned} \tag{2.44}$$

c-à-d le polynôme énumérateur est invariant sous la matrice inversible $A_1=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$.

On considère le groupe G_1 engendré par

$$A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

où $A^2 = I_2$, $A_1^2 = I_2$ et $(AA_1)^8 = I_2$ alors G_1 est le groupe de Dihedral d'ordre 16 et $G_1 = \left\{ A^i (AA_1)^j ; i \in \{0,1\} \text{ et } j \in \{0,...,7\} \right\}$

D'après le théorème de Molien on a :

$$\begin{aligned} \Phi_{G_1}(\lambda) &= \frac{1}{16} \sum_{b \in G_1} \frac{1}{\det(I_2 - \lambda B)} \\ \Phi_{G_1}(\lambda) &= \frac{1}{16} \left\{ \frac{1}{(1-\lambda^2)} + \frac{1}{1+\lambda^2} + ... \right\} \\ &= \frac{1}{(1-\lambda^2)(1-\lambda^8)} \end{aligned} \tag{2.45}$$

Alors l'algèbre $I(G_1)$ de dimension deux dont les éléments de la base polynomiale de degré deux et huit.

Sachant que $W_{i_2}(x,y) = x^2 + y^2, W_{e_8}(x,y) = x^8 + 14x^4y^4 + y^8$, sont respectivement des polynômes énumérateurs des poids de deux codes auto- duaux le code de répétition i_2 et le code de Hamming etendu e_8, alors sont des invariants de G_1.

On pose

$$\begin{aligned} \Phi_2(x,y) &= x^2 + y^2 \\ \Phi_8(x,y) &= \frac{1}{4} \left[(W_{i_2}(x,y))^4 - W_{e_8}(x,y) \right] = x^2y^2 \left(x^2 - y^2 \right)^2 \end{aligned} \tag{2.46}$$

On montre, de la même manière utilisé dans (2.41) que Φ_2 et Φ_8 sont algébriquement indèpendants, alors le polynôme énumérateur d'un code auto- dual de type I est un élément dans $I(G_1)$ engendré.par Φ_2 et Φ_8.

typeII

Dans un code auto- dual binaire de type II chaque mot code est de poids divisible par quatre alors :

$$\begin{aligned} W_C(x,y) &= \sum_{c\in C} x^{n-w(c)}y^{w(c)} \\ &= \sum_{c\in C} x^{n-w(c)}(iy)^{w(c)} \\ &= W_C(x,iy) \\ &= \left(\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \circ W_C\right)(x,y) \end{aligned} \tag{2.47}$$

c-à-d le polynôme énumérateur des poids d'un code auto- dual de type II est invariant sous la matrice inversible $A_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.

On considère le groupe G_2 engendré par

$$A = \frac{1}{\sqrt[2]{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

où $A^2 = I_2$, $A_2^4 = I_2$, $(A_2A)^{96} = I_2$ et l'ordre de G_2 est 192, c.à.d
$G_2 = \left\{A^i (A_2A)^j ; i \in \{0,1\}, j \in \{0,...,95\}\right\}$.

D'après le théorème de Molien on a

$$\begin{aligned} \Phi_{G_2}(\lambda) &= \frac{1}{192}\sum_{b\in G_2}\frac{1}{\det(I_2 - \lambda B)} \\ &= \frac{1}{192}\left\{\frac{1}{(1-\lambda^2)} + \frac{1}{1-\lambda^2} + \frac{1}{(1-\lambda)(1-i\lambda)} + ...\right\} \\ &= \frac{1}{(1-\lambda^8)(1-\lambda^{24})} \end{aligned} \tag{2.48}$$

Alors l'algèbre $I(G_2)$ de dimension deux dont les éléments de la base polynomiale de

degré 8 et 24.

Sachant que

$$\begin{aligned} W_{e_8}(x,y) &= x^8 + 14x^4y^4 + y^8 \\ W_{g_{24}}(x,y) &= x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24} \end{aligned} \tag{2.49}$$

sont des polynômes énumérateurs des poids de deux codes auto- duaux (le code de Hamming étendu e_8 et le code de Golay g_{24} respectivement).

On pose

$$\begin{aligned} \widetilde{\Phi}_8(x,y) &= W_{e_8}(x,y) \\ \Phi_{24}(x,y) &= \frac{1}{42}\left[(W_{e_8}(x,y))^3 - W_{g_{24}}(x,y)\right] = x^4y^4\left(x^4 - y^4\right)^4 \end{aligned} \tag{2.50}$$

On montre, de la même manière utilisé dans (2.41) que $\widetilde{\Phi}_8$ et Φ_{24} sont algébriquement indépendants, alors le polynôme énumérateur des poids d'un code auto- dual de type II est un élément dans $I(G_2)$ engendré.par $\widetilde{\Phi}_8$ et Φ_{24}.

Remarque 2.4 Dans les codes de type II tous les poids des mots codes sont divisibles par quatre, ils sont divisibles par deux alors chaque élément de $I(G_2)$ est un élément de $I(G_1)$.

2.2.4 Le polynôme énumérateur des poids d'un code ternaire auto- dual

Dans un code ternaire chaque mot code est de poids divisible par trois, alors

$$\begin{aligned} W_C(x,y) &= \sum_{c\in C}^{n} x^{n-w(c)}y^{w(c)} \\ &= \sum_{c\in C}^{n} x^{n-w(c)}(\omega y)^{w(c)} \diagup \omega = e^{\frac{2\pi}{3}i} \\ &= W_C(x,\omega y) \\ &= \left(\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \circ W_C\right)(x,y) \end{aligned} \tag{2.51}$$

c-à-d le polynôme énumérateur des poids est invariant sous la matrice inversible $A_3 = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}$.

on considère le groupe G_3 engendré par

$$A = \frac{1}{\sqrt[2]{3}}\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}$$

où $A^2 = I_2, A_3^3 = I_2$ et $(AA_3)^{24} = I_2$ alors $G_3 = \left\{A^i(AA_3)^j ; i \in \{0,1\}, j \in \{0,...,23\}\right\}$ et l'ordre de G_3 est 48.

D'après le théorème de Molien on a

$$\begin{aligned} \Phi_{G_3}(\lambda) &= \frac{1}{48}\sum_{b\in G_3}\frac{1}{\det(I_2 - \lambda B)} \\ &= \frac{1}{(1-\lambda^4)(1-\lambda^{12})} \end{aligned} \tag{2.52}$$

Alors l'algèbre $I(G_3)$ de dimension deux dont les éléments de la base polynomiale de degré 4 et 12.

Sachant que

$$\begin{aligned} W_{t_4}(x,y) &= x^4 + 8xy^3 \\ W_{g_{12}}(x,y) &= x^{12} + 264x^6y^6 + 440x^3y^9 + 24y^{12} \end{aligned} \tag{2.53}$$

sont des polynômes énumérateurs des poids de deux codes auto- duaux (le tetracode t_4 et le code de golay g_{12}) alors sont des invariants de G_3, on pose

$$\begin{aligned} \Phi_4(x,y) &= W_{t_4}(x,y) \\ \Phi_{12}(x,y) &= \frac{1}{24}\left[(W_{t_4}(x,y))^3 - W_{g_{12}}(x,y)\right] = y^3\left(x^3 - y^3\right)^3 \end{aligned} \tag{2.54}$$

Donc Φ_4 et Φ_{12} sont des invariants de degré 4 et 12 et sont algébriquements indèpendants.

Alors le polynôme énumérateur des poids d'un code ternaire auto- dual est un élément dans $I(G_3)$ engendré par $\Phi_4$et Φ_{12}.

2.2.5 L' ombre d'un code

Dans cette partie, on définit un certain translaté d'un code, appelé l'ombre d'un code, et son polynôme énumérateur des poids peut être obtenu du polynôme énumérateur des poids du code par une transformation analogue à la transformé de Mac Williams.

Lemme 2.5 *Soit $C = C(n,k)$ un code binaire auto- orthogonal de type I et soit C_0 le sous ensemble des mots du code de poids divisible par quatre, alors C_0 est un sous code linéaire de C d'indice* 2.

Preuve : Soit l'application

$$\begin{aligned} \Psi : C &\longrightarrow \mathbb{F}_2 = \{0.1\} \\ u &\longmapsto \Psi(u) = \tfrac{1}{2}\omega(u) \pmod 2 \end{aligned}$$

Ψ est une application linéaire puisque

$$\begin{aligned} \Psi(u+v) &= \tfrac{1}{2}\omega(u+v) \pmod 2 \\ &= \tfrac{1}{2}\left(\omega(u) \pmod 2 + \omega(v) \pmod 2 - 2\omega(u \cap v) \pmod 2\right) \end{aligned}$$

$$
\begin{aligned}
&= \tfrac{1}{2}\omega(u) \pmod 2 + \tfrac{1}{2}\omega(v) \pmod 2 - \omega(u \cap v) \pmod 2 \\
&= \tfrac{1}{2}\omega(u) \pmod 2 + \tfrac{1}{2}\omega(v) \pmod 2 - \langle u, v\rangle \pmod 2 \\
&= \tfrac{1}{2}\omega(u) \pmod 2 + \tfrac{1}{2}\omega(v) \pmod 2 \\
&= \Psi(u) + \Psi(v)
\end{aligned}
$$

et

$$
\begin{aligned}
\ker \Psi &= \{u \in C; \Psi(u) \equiv 0 \pmod 2\} \\
&= \left\{u \in C; \tfrac{1}{2}\omega(u) \equiv 0 \pmod 2\right\} \\
&= \{u \in C; \omega(u) \equiv 0 \pmod 4\} \\
&= C_0
\end{aligned}
$$

Donc C_0 est un sous espace vectoriel de C et

$$
\begin{aligned}
\dim \ker \Psi &= \dim C - \dim \operatorname{Im} \Psi \\
&= k - 1
\end{aligned}
$$

alors

$$
[C : C_0] = \frac{\mid C \mid}{\mid C_0 \mid} = \frac{2^k}{2^{k-1}} = 2
$$

donc C_0 est un sous code linéaire de C d'indice 2. ■

Définition 2.12 L'ombre S_C d'un code binaire auto- orthogonal C est :

$$
S_C = \begin{cases} C_0^{\perp} - C^{\perp} & \text{si } C \text{ de type I} \\ C^{\perp} & \text{si } C \text{ de type II} \end{cases} \tag{2.55}
$$

et son polynôme énumérateur des poids est noté par $W_{S_C}(x, y)$.

Exemple 2.5 • Soit $C = \{0^n, 1^n\}$ le code de répétition de longueur n, où n est pair.

Si $n \equiv 0 \pmod 4$, alors le code C est de type II et dans ce cas

$$
\begin{aligned}
S_C &= C^{\perp} = \{u \in \mathbb{F}_2^n; \langle u, v\rangle \equiv 0 \pmod 2, \forall v \in C\} \\
&= \{u \in \mathbb{F}_2^n; \langle u, 1^n\rangle \equiv 0 \pmod 2\} \\
&= \{u \in \mathbb{F}_2^n; \omega(u) \equiv 0 \pmod 2\}
\end{aligned}
$$

donc S_C est l'ensemble de tous les vecteurs de $\mathbb{F}_2^n$ de poids pair.

Si $n \equiv 2 \pmod 4$, alors le code C est de type I et $C_0 = \{0^n\}$ d'où

$$\begin{aligned} S_C &= C_0^{\perp} - C^{\perp} = \mathbb{F}_2^n - \{u \in \mathbb{F}_2^n ; \omega(u) \equiv 0 \pmod 2\} \\ &= \{u \in \mathbb{F}_2^n ; \omega(u) \equiv 1 \pmod 2\} \end{aligned}$$

donc S_C est l'ensemble de tous les vecteurs de $\mathbb{F}_2^n$ de poids impair.

• Soit $C = C(2k, k)$ le code auto- dual de matrice génératrice

$$G = \begin{pmatrix} l_1 \\ l_2 \\ . \\ . \\ . \\ l_k \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & . & . & . & 0 & 0 \\ . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & 0 & 0 & . & . & . & 1 & 1 \end{pmatrix} \text{ où } G \text{ de type } k \times 2k$$

alors la matrice G_0 de type $(k-1) \times 2k$ engendre le code C_0 où

$$G_0 = \begin{pmatrix} l_1 + l_2 \\ l_2 + l_3 \\ . \\ . \\ . \\ l_{k-1} + l_k \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & . & . & . & 0 & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & 0 & 0 & . & . & . & 1 & 1 & 1 & 1 \end{pmatrix}$$

donc $C^{\perp}$est un sous code de $C_0^{\perp}$ d'indice 2 et $C_0^{\perp} = C^{\perp} \cup \left(a + C^{\perp}\right)$ tel que $a \in C_0^{\perp} \backslash C^{\perp}$.

alors $S_C = C_0^{\perp} - C^{\perp} = a + C^{\perp}$, a partir de G et G_0 on a : $a = 1010...10$.

Le théorème suivant caractérise l'ombre S_C d'un code auto- orthogonal C et son pôlynome énumérateur des poids.

Théorème 2.16 *Soient* $C = C(n, k)$ *un code binaire auto- orthogonal et* S_C *son ombre*

alors

1. $S_C = \left\{u \in \mathbb{F}_2^n; \langle u, v\rangle \equiv \frac{1}{2}\omega(v) \pmod 2, \forall v \in C\right\}$

2. S_C *est le translaté de* $C^\perp$.

3. $W_{S_C}(x,y) = \frac{1}{|C|} W_C(x+y, i(x-y))$.

Preuve : Si C est de type II

1. On a

$$\begin{aligned} S_C &= C^\perp \\ &= \{u \in \mathbb{F}_2^n; \langle u, v\rangle \equiv 0 \pmod 2, \forall v \in C\} \\ &= \left\{u \in \mathbb{F}_2^n; \langle u, v\rangle \equiv \frac{1}{2}\omega(v) \pmod 2, \forall v \in C\right\} \end{aligned}$$

2. D'une part, $S_C = C^\perp$ qu'on peut l'écrire comme le translaté de $C^\perp$ par 0.

3. D'aprés le théorème de Mac Williams on a :

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y)$$

et comme C est de type II on a :

$$W_C(x+y, x-y) = W_C(x+y, i(x-y))$$

alors

$$\begin{aligned} W_{S_C}(x,y) &= W_{C^\perp}(x,y) \\ &= \frac{1}{|C|} W_C(x+y, i(x-y)) \end{aligned}$$

Si C est de type I.

On montre que $S_C = \left\{u \in \mathbb{F}_2^n; \langle u, v\rangle \equiv \frac{1}{2}\omega(v) \pmod 2, \forall v \in C\right\}$

On a $S_C = C_0^\perp - C^\perp$ alors $\forall u \in S_C \Rightarrow u \in C_0^\perp$ et $u \notin C^\perp$

$\forall v \in C = C_0 \cup C_2$ où $C_2 = \{u \in \mathbb{F}_2^n; \omega(u) \equiv 2 \pmod 4\} = a_2 + C_0$ et $\omega(a_2) \equiv 2 \pmod 4$

On a alors $v \in C_0$ ou $v \in C_2$

Si $v \in C_2$ on a $\omega(v) \equiv 2 \pmod 4$ donc $\frac{1}{2}\omega(v) \equiv 1 \pmod 2$ et $\langle u, v\rangle \equiv 1 \pmod 2$ puis que si $\langle u, v\rangle \equiv 0 \pmod 2, \forall v \in C_2$ alors $u \in C_2^\perp$ et $u \in C_0^\perp$

alors $u \in C_2^\perp \cap C_0^\perp = (C_2 \cup C_0)^\perp = C^\perp$ contradiction car $u \notin C^\perp$.

donc $\langle u, v\rangle \equiv \frac{1}{2}\omega(v) \pmod 2$

Si $v \in C_0$ on a $\omega(v) \equiv 0 \pmod 4$ donc $\frac{1}{2}\omega(v) \equiv 0 \pmod 2$ et $\langle u, v\rangle \equiv 0 \pmod 2$

donc $S_C = \left\{u \in \mathbb{F}_2^n; \langle u, v\rangle \equiv \frac{1}{2}\omega(v) \pmod 2, \forall v \in C\right\}$

2. On a l'inclusion suivante : $C_0 \subset C \subset C^{\perp} \subset C_0^{\perp}$.

Comme C_0 est un sous code de C d'indice 2 alors $C^{\perp}$ est un sous code de $C_0^{\perp}$ d'indice 2 .

Donc $C_0^{\perp} = C^{\perp} \cup \left(a + C^{\perp}\right)$ tel que $a \in C_0^{\perp} \backslash C^{\perp}$

D'aprés (1) on a pour tout $v \in C$

$$\begin{aligned} \langle a, v \rangle &\equiv \frac{1}{2}\omega(v) \pmod 2 \\ &= \begin{cases} 0 & \text{si } v \in C_0 \\ 1 & \text{si } \forall v \in C_2 \end{cases} \end{aligned}$$

donc $S_C = C_0^{\perp} \backslash C^{\perp} = a + C^{\perp}$

alors S_C est le translaté de $C^{\perp}$

3. Soit $W_{S_C}(x,y) = \sum_{k=0}^{n} B_k x^{n-k} y^k$ où B_k est la distribution des poids de S_C, or $S_C = C_0^{\perp} - C^{\perp}$ alors

$$W_{S_C}(x,y) = W_{C_0^{\perp}}(x,y) - W_{C^{\perp}}(x,y)$$

Sachant que $W_{C_0}(x,y) = \frac{1}{2}\{W_C(x,y) + W_C(x,iy)\}$

et d'aprés le théorème de Mac Williams on a

$$\begin{aligned} W_{C_0^{\perp}}(x,y) &= \frac{1}{\mid C_0 \mid} W_{C_0}(x+y, x-y) \\ &= \frac{1}{2 \mid C_0 \mid}\{W_C(x+y, x-y) + W_C(x+y, i(x-y))\} \\ &= \frac{1}{\mid C \mid}\{W_C(x+y, x-y) + W_C(x+y, i(x-y))\} \end{aligned}$$

alors

$$\begin{aligned} W_{S_C}(x,y) &= \frac{1}{\mid C \mid}\{W_C(x+y, x-y) + W_C(x+y, i(x-y))\} \\ &\quad -\frac{1}{\mid C \mid} W_C(x+y, x-y) \\ &= \frac{1}{\mid C \mid} W_C(x+y, i(x-y)) \end{aligned}$$

■

Corollaire 2.6 Soit C un code auto- dual de type I et S_C son ombre on a les deux propriétés suivantes :

- S_C n'est pas un code linéaire.
- Si $W_C(x,y) = \sum_{j=0}^{n} A_j x^{n-j} y^j$ et $W_{S_C}(x,y) = \sum_{j=0}^{n} B_j x^{n-j} y^j$ sont respectivement les polynômes énumérateurs des poids de C et S_C alors

$$W_C(x,y) = \sum_{j=0}^{n} a_j \left(x^2+y^2\right)^{\frac{n}{2}-4j} \left[x^2y^2\left(x^2-y^2\right)^2\right]^j \tag{2.56}$$

et on déduit que

$$W_{S_C}(x,y) = \sum_{j=0}^{\left[\frac{n}{8}\right]} (-1)^j 2^{\frac{n}{2}-6j} a_j (xy)^{\frac{n}{2}-4j} \left(x^4-y^4\right)^{2j} \tag{2.57}$$

Preuve : • l'inclusion suivante étant évidante $C_0 \subset C = C^{\perp} \subset C_0^{\perp}$

et sachant que$\mid \frac{C}{C_0} \mid = 2$, il s'ensuit que $C_0^{\perp}$ est une union de deux translatés de C, ou bien de quatre translatés de C_0, donc il existe $a \in C_0^{\perp} \backslash C$ tel que

$$\begin{aligned} C_0^{\perp} &= C \cup (a+C) \\ &= C_0 \cup C_2 \cup (a+C_0) \cup (a+C_2) \\ &= C_0 \cup C_2 \cup C_1 \cup C_3 \end{aligned}$$

On déduit que

$$\begin{aligned} S_C &= a+C \\ &= C_0 \cup C_2 \cup C_1 \cup C_3 \\ &= (a+C_0) \cup (a+C_2) \\ &= C_1 \cup C_3 \end{aligned}$$

où $C_1 = a+C_0, C_3 = a+C_2 = a+a_2+C_0 = a_3+C_0$

donc l'ombre du code C est un translaté de C et une union de deux translatés de C_0, de plus

$$u+v \in \begin{cases} C_0 & \text{si } u,v \in C_1 \text{ou } u,v \in C_3 \\ C_2 & \text{si } u \in C_1 \text{et } v \in C_3 \end{cases}$$

Alors la somme de deux vecteurs de S_C n'est pas dans S_C, donc S_C n'est pas un code linéaire.

• Comme W_C est un élément de $I(G_1)$, on a :

$$\begin{aligned} W_C(x,y) &= \sum_{2i+8j=n} \alpha_{ij} \left(x^2+y^2\right)^i \left(x^2y^2\left(x^2-y^2\right)^2\right)^j \\ &= \sum_{0\le j\le \left[\frac{n}{8}\right]} \alpha_{\left(\frac{n}{2}-4j\right)j} \left(x^2+y^2\right)^{\frac{n}{2}-4j} \left(x^2y^2\left(x^2-y^2\right)^2\right)^j \\ &= \sum_{0\le j\le \left[\frac{n}{8}\right]} a_j \left(x^2+y^2\right)^{\frac{n}{2}-4j} \left(x^2y^2\left(x^2-y^2\right)^2\right)^j \end{aligned}$$

Pour le polynôme énumérateur de l'ombre on a

$$\begin{aligned} W_{S_C}(x,y) &= \frac{1}{|C|} W_C(x+y, i(x-y)) \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{j=0}^{\left[\frac{n}{8}\right]} a_j \left((x+y)^2+(i(x-y))^2\right)^{\frac{n}{2}-4j} \\ &\quad \times \left((x+y)^2(i(x-y))^2\left((x+y)^2-(i(x-y))^2\right)^2\right)^j \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{j=0}^{\left[\frac{n}{8}\right]} a_j (4xy)^{\frac{n}{2}-4j} \left(-2^2\left(x^2-y^2\right)^2\left(x^2+y^2\right)^2\right)^j \\ &= \sum_{j=0}^{\left[\frac{n}{8}\right]} (-1)^j a_j 2^{\frac{n}{2}-6j} (xy)^{\frac{n}{2}-4j} \left(x^4-y^4\right)^{2j} \end{aligned}$$

■

Remarque 2.5 Si C est un code de type II, alors $C_2 = \phi$ et $S_C = C = C_0$ par conséquent, la construction de l'ombre est interessante seulement dans le cas des codes de type I.

Chapitre 3

Classification des codes auto- duaux

Après l'étude les codes auto- duaux et leurs polynômes énumérateurs des poids, nous allons maintenant étudier la méthode de collage comme une technique dans la classification les codes auto- duaux.

En général on constate qu'il y a beaucoup de codes avec basse distance minimale et seulement quelques-uns avec grande distance minimale, la méthode de collage est bonne pour trouver tous les codes de basse distance minimale.

Dans ce chapitre on classifie les codes binaires jusqu'à la longueur 22, et jusqu'à la longueur 20 pour les codes ternaires.

3.1 Construction des codes auto- duaux par la méthode de collage

La méthode de collage consiste à construire des codes de longueurs données à partir des codes de longueurs plus petites.

Dans notre présentation, nous utilisons des codes auto- orthogonaux ou auto- duaux pour construire des codes auto- duaux de longueur plus grande, et à distance minimale supérieure ou égale aux distances minimales des codes utilisés.

3.1.1 Codes décomposables

Soint $C_1 = C(n_1, k_1, d_1), C_2 = C(n_2, k_2, d_2), ..., C_t = C(n_t, k_t, d_t)$ des codes de matrices génératrices $G_1, G_2, ..G_t$ respectivement.

Soit C un code de matrice génératrice suivante

$$\begin{pmatrix} G_1 & & & 0 \\ & G_2 & & \\ & & \ddots & \\ 0 & & & G_t \end{pmatrix}$$

alors $C = C(n, k, d)$ où $n = n_1 + ... + n_t$, $k = k_1 + k_2 + ... + k_t$, $d = \min\{d_1, ..., d_t\}$.

Nous disons que le code C est décomposable et on écrit $C = C_1C_2...C_t$ ou

$C = C_1 \oplus C_2 \oplus ... \oplus C_t$

Proposition 3.1 Soit $C = C_1C_2...C_t$ un code décomposable alors

• $W_C(x, y) = \prod_{i=1}^{t} W_{C_i}(x, y)$.

• Si les codes $C_1, C_2, ..., C_t$ sont des codes auto- duaux alors C est un code auto- dual.

Preuve : • *S*ans perdre de généralité, on démontre la relation pour $t = 2$ alors

$$C = C_1C_2 \ et \ G = \left(\begin{array}{c|c} G_1 & 0 \\ \hline 0 & G_2 \end{array}\right)$$

D'une part on a :

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

où $A_i = \sum_{i_1+i_2=i} A^1_{i_1} A^2_{i_2}$ et $A^k_{i_k}$ le nombre des mots du code de poids i_k dans C_k .

D'autre part on a

$$\begin{aligned} W_{C_1}(x,y)\, W_{C_2}(x,y) &= \left(\sum_{l=0}^{n_1} A_l^1 x^{n_1-l} y^l\right)\left(\sum_{k=0}^{n_2} A_k^2 x^{n_2-k} y^k\right) \\ &= \sum_{l=0}^{n_1}\sum_{k=0}^{n_2} A_l^1 A_k^2 x^{n_1+n_2-(l+k)} y_k^{l+k} \\ &= \sum_{i=0}^{n=n_1+n_2}\left(\sum_{l+k=i} A_l^1 A_k^2\right) x^{n-i} y^i \\ &= \sum_{i=0}^{n} A_i x^{n-i} y^i \end{aligned}$$

d'ou

$$W_C(x,y) = W_{C_1}(x,y)\, W_{C_2}(x,y)$$

• Si les codes $C_1, C_2, ..., C_t$ sont des codes auto- duaux, dans ce cas on obtient :

$$\begin{aligned} k &= \frac{n_1}{2} + \frac{n_2}{2} + ... + \frac{n_t}{2} \\ &= \frac{n}{2} \end{aligned}$$

et toutes les lignes dans G sont orthogonales, alors le code C est auto- dual. ■

3.1.2 Codes indécomposables

Soient $C_1 = C(n_1, k_1, d_1), C_2 = C(n_2, k_2, d_2), ..., C_t = C(n_t, k_t, d_t)$ des codes de matrices génératrices $G_1, G_2, ..., G_t$ respectivement.

Soit C un code de matrice génératrice ayant la forme suivante :

$$\left(\begin{array}{ccc} G_1 & & 0 \\ & G_2 & \\ & \ddots & \\ 0 & & G_t \\ \hline & X & \end{array}\right)$$

où X est une matrice de type $l \times (n_1 + ... + n_t)$, avec $1 \leq l \leq \sum_{i=1}^{t} (n_i - k_i)$
alors $C = C(n, k, d)$ et $n = n_1 + ... + n_t$, $k = k_1 + .. + k_t + l$, $d \leq \min(d_1, ..., d_t,)$.

Nous disons que le code C est indécomposable et on note par $C = (C_1 C_2 ... C_t)^+$.

L'usage d'une telle méthode pour construire des codes auto- duaux d'une certaine longueur est basée sur le choix des composantes C_i auto-orthogonales de telle sorte que les composantes contiennent les vecteurs de poids minimal du code à construire.

En effet, soit $C = C\left(n, \frac{n}{2}, d\right)$ un code auto- dual, le polynôme énumérateur des poids un élément de $I(G)$, détermine le nombre de vecteurs de poids minimal.

On choisit les composantes parmi les codes d_4, e_7, e_8, d_{2k} (pour les codes binaires) et $e_3, t_4, g_8, g_9, g_{10}, g_{11}, \gamma_{11}, p_{12}, p_{13}, \eta_{14}, h_{15}, h_{16}$ (pour les codes ternaires) [13], [16].

Le choix de composantes $C_i = C(n_i, k_i, d_i)$ détermine la longueur n et les lignes de X ainsi que leur nombre.

Le choix de la matrice X est conditionné par l'orthogonalité de ses lignes et l'orthogonalité de leurs projections sur chaque composante C_i i e

si $X = \begin{pmatrix} X^1 \\ X^2 \\ \vdots \\ X^l \end{pmatrix}$ où $X^j = X_1^j X_2^j ... X_t^j$ avec $X_i^j \in C_i^{\perp}$ et $\langle X^j, X^k \rangle = 0$.

Soit C_i une composante quelconque du code auto- dual indécomposable C et

$$s_i = \frac{\mid C_i^{\perp} \mid}{\mid C_i \mid}$$

alors

$$C_i^{\perp} = \bigcup_{j=0}^{s_i - 1} \left(a_j^i + C_i\right)$$

les X_i^j sont choisis dans $\left\{a_0^i = 0, a_1^i, ..., a_{s_i-1}^i\right\}$.

3.1.3 Autres codes indécomposables

Soint des codes $C_1 = C(n_1, k_1, d_1), C_2 = C(n_2, k_2, d_2), ..., C_t = C(n_t, k_t, d_t)$ de matrices génératrices $G_1, G_2, ..., G_t$ respectivement.

On considère les codes $\widetilde{C_1}, \widetilde{C_2}, ..., \widetilde{C_t}$ de matrices génératrice $\widetilde{G_1}, \widetilde{G_2}, ..., \widetilde{G_t}$ définies par :

$$\widetilde{G_i} = (G_i \parallel 0_{\alpha_i})$$

Considérons le code $\widetilde{C}$ de matrice génératrice

$$\left(\begin{array}{ccc} \widetilde{G_1} & & 0 \\ & \widetilde{G_2} & \\ & \ddots & \\ 0 & & \widetilde{G_t} \\ \hline & \widetilde{X} & \end{array}\right)$$

où $\widetilde{X}$ est une matricede type $l \times \left(\sum_{i=1}^{t}(n_i + \alpha_i)\right)$.

alors le code $\widetilde{C} = C\left(\widetilde{n}, \widetilde{k}, \widetilde{d}\right)$ tel que

$\widetilde{n} = \sum_{i=1}^{t}(n_i + \alpha_i) = \sum_{i=1}^{t} n_i + \sum_{i=1}^{t} \alpha_i = n + \alpha$

$\widetilde{k} = \left(\sum_{i=1}^{t} k_i\right) + \alpha = k + \alpha$, $\widetilde{d} \leq \min(d_1, d_2, ..., d_t)$

Le code $\widetilde{C} = C\left(\widetilde{n}, \widetilde{k}, \widetilde{d}\right)$ est équivalent à un code de matrice génératrice

$$G = \left(\begin{array}{ccc|c} G_1 & & 0 & \\ & G_2 & & 0_\alpha \\ & \ddots & & \\ 0 & & G_t & \\ \hline & X & & X_\alpha \end{array}\right)$$

on note $f_\alpha = \begin{pmatrix} 0_\alpha \\ X_\alpha \end{pmatrix}$

3.2 Classification des codes auto- duaux binaires

Pour les codes binaires auto- duaux il y a deux types de codes, les codes de type I et de type II. Les codes de type I sont de longueur pair et tous les mots code sont de poids divisibles par deux, mais les codes de type II sont de longueur multiple de huit et tous les poids du mots code sont divisibles par quatre. Dans cette partie nous donnons une classification des codes auto- duaux binaires de longueur inférieure ou égale à 22.

3.2.1 Les codes auto- duaux de distance minimale deux

Les codes auto- duaux de longueur n et de distance minimale égale à deux peuvent être obtenu a partir des codes auto- duaux de longueur $n-2$ et le code auto- dual i_2.

Théorème 3.1 *Soit $C = C(2k, k)$ un code auto- dual de distance minimale 2, alors $C = i_2 \oplus \overline{C}$ où $\overline{C} = C(2k-2, k-1)$ est un code auto- dual de distance minimale $d \geq 2$.*

Preuve : Comme C est de distance minimale 2 alors il existe un mot code de poids deux, supposons que $U_1 = 110...0 \in \mathbb{F}_2^{2k}$

Soit G une matrice génératrice de C telle que

$$G = \begin{pmatrix} U_1 \\ U_2 \\ . \\ . \\ . \\ U_k \end{pmatrix}$$

Comme C est un code auto-dual alors la première et la deuxième composante dans

$U_2, ..., U_k$ sont tous des 0 ou des 1 c-à-d

$$G \sim \left(\begin{array}{c|c} 11 & 0^{2k-2} \\ \hline 00 & \acute{U}_1 \\ . & . \\ . & . \\ . & . \\ 00 & \acute{U}_k \end{array}\right)$$

où $00\acute{U_i} = \begin{cases} U_i + U_1 & \text{Si la première et la deuxième composante dans } U_i \text{ est 1} \\ U_i & \text{Si la première et la deuxième composante dans } U_i \text{ est 0} \end{cases}$

On pose $\overline{G} = \begin{pmatrix} \acute{U}_2 \\ . \\ . \\ . \\ \acute{U}_k \end{pmatrix}$ de type $(2k-2)\times(k-1)$ et toutes les lignes de $\overline{G}$ sont orthogonales, alors $\overline{G}$ *définit un code auto- dual* $\overline{C} = C\left(2k-2, k-1\right)$. ■

Proposition 3.2 Si $C = C\left(2k, k\right)$ est un code auto- dual qui contient r mots du code de poids deux alors C est équivalent à un code auto- dual $i_2^r \oplus \overline{C}$ où $\overline{C} = C\left(2(k-r), k-r, d \geq 4\right)$ est un code auto- dual de distance minimale supérieure ou égale à quatre.

preuve : par récurrence sur r.

Théorème 3.2 Soient $C_1 = C\left(2k, k, 2\right), C_2 = C\left(2k, k, 2\right)$ deux codes auto- duaux où $C_1 = i_2 \oplus \overline{C_1}, C_2 = i_2 \oplus \overline{C_2}$ et $\overline{C_1}$, $\overline{C_2}$ sont des codes de type $C\left(2k-2, k-1, d \geq 4\right)$ alors $C_1 \sim C_2 \iff \overline{C_1} \sim \overline{C_2}$.

preuve : Supposons que $\overline{C_1}, \overline{C_2}$ sont des codes équivalents alors

$\exists \overline{\delta} \in S_{2k-2}$, $\forall \overline{c_1} \in \overline{C_1}$; $\delta\left(\overline{c_1}\right) \in \overline{C_2}$ et $\exists \delta_2 \in S_2$, $\forall u \in i_2$; $\delta_2\left(u\right) \in i_2$

donc $\exists \delta = \delta_2 \overline{\delta} \in S_{2k}$, $\forall c = u\overline{c_1} \in C_1$; $\delta\left(c\right) = \delta_2\left(u\right) \overline{\delta}\left(\overline{c_1}\right)$

on a $\delta\left(c\right) = \delta_2\left(u\right) \overline{\delta}\left(\overline{c_1}\right) \in i_2 \oplus \overline{C_2} = C_2$

alors C_1 et C_2 sont des codes équivalents.

Supposons que C_1 et C_2 sont des codes équivalents alors

$\exists \delta \in S_{2k}$, $\forall c_1 \in C_1$; $\delta(c_1) \in C_2$

comme $C_1 = i_2 \oplus \overline{C_1}$ et contient un seul mot code de poids deux alors

$\exists \delta_2 \in S_2$, $\forall u \in i_{2;}$ $\delta_2(u) \in i_2$ tel que $\delta = \delta_2 \overline{\delta}$ où $\overline{\delta} \in S_{2k-2}$ et

$\delta(c) = \delta_2(u)\,\overline{\delta}(\overline{c_1}) \in C_2 = i_2 \oplus \overline{C}$ alors $\overline{\delta}(\overline{c_1}) \in \overline{C_2}$

donc $\overline{C_1}$ et $\overline{C_2}$ sont des codes équivalents. ■

Proposition 3.3 Soient $C_1 = C(2k, k, 2)$, $C_2 = C(2k, k, 2)$ des codes auto- duaux où $C_1 = i_2^r \oplus \overline{C_1}$, $C_2 = i_2^r \oplus \overline{C_2}$ et $\overline{C_1}$, $\overline{C_2}$ sont des codes de type $C(2k - 2r, k - r, d \geq 4)$ alors $C_1 \sim C_2 \iff \overline{C_1} \sim \overline{C_2}$.

Preuve : la même démonstration que dans la proposition précédente.

Les deux propositions de ci dessus montrer que le nombre des codes auto- duaux inéquivalents $C = C(2k, k, 2)$ égal au nombre de codes auto- duaux inéquivalents $\overline{C} = C(2k - 2, k - 1, d)$ où $d \geq 2$.

Exemple 3.1 Pour $n = 16$

Chaque code auto- dual de distance minimale 2 est équivalent au code $i_2 \oplus C_{14}$. Donc le nombre des codes auto- duaux inéquivalents $C = C(16, 8, 2)$ est égal au nombre de codes auto- duaux inéquivalents $C(14, 7, d)$ où $d = 2, 4$.

Remarque 3.1 Tous les codes auto- duaux de distance minimale 2 et de longueur $n \geq 4$ sont des codes décomposables.

3.2.2 Les codes auto- duaux de distance minimale supérieure ou égale à quatre

Pour tous les codes auto- duaux binaires dont la distance minimale est quatre, on utilise les codes auto- orthogonaux suivants comme des composantes dans la méthode de collage.

• $d_4 = C(4, 1, 4)$ de matrice génératrice $\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$ et le nombre des mots code de poids quatre est égal à un, et les trois vecteurs de collage non nuls sont :

$a = 1010$, $b = 0011$, $c = 1001$.

• $d_{2k} = C(2k, k-1, 4)$ de matrice génératrice

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & . & . & . & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & . & . & . & 0 & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & . & . & . & 1 & 1 & 1 & 1 \end{pmatrix}$$

Ce code contient $(k-1)+(k-2)+...+1 = \frac{(k-1)k}{2}$ mots code de poids quatre et les trois vecteurs de colles non nuls sont : $a = 1010...10$, $b = 0000...11$, $c = 1010...01$.

• $e_7 = C(7, 3, 4)$ le code de Hamming de matrice génératrice

$$\left(\begin{array}{c||cccc} & 0 & 1 & 1 & 1 \\ I_3 & 1 & 0 & 1 & 1 \\ & 1 & 1 & 0 & 1 \end{array}\right)$$

et le nombre des mots du codes de poids quatre est égal à 7, et un seul vecteur de collage qui est $d = 1111111$.

• $e_8 = C(8, 4, 4)$ le code de Hamming étendu auto- dual de matrice génératrice

$$\left(\begin{array}{c||cccc} & 0 & 1 & 1 & 1 \\ I_4 & 1 & 0 & 1 & 1 \\ & 1 & 1 & 0 & 1 \\ & 1 & 1 & 1 & 0 \end{array}\right) \tag{3.1}$$

et le nombre des mots codes de poids quatre est égal à 14, ce code est utilisé pour les codes décomposables.

• La composante f_n n'est pas un code auto- orthogonal, mais on l'utilise pour compléter la longueur.

D'après les propriétés précédentes, on peut procéder à la construction des codes auto-duaux $C\left(n, \frac{n}{2}\right)$, de distance minimale quatre en quatre étapes :

1/ Par le corollaire 2.6, on détermine les polynômes qui possèdent les mêmes propriétés que le polynôme énumérateur des poids d'un code auto- dual.

2/ On détermine A_4 le nombre des mots code de poids minimal quatre.

3/ On détermine les composantes $C_1, C_2, ..., C_t$ telles que le code auto- orthogonal $C_1 \oplus C_2 \oplus ... \oplus C_t$ contient A_4 mots code de poids quatre.

4/ S'il existe une matrice X dans la méthode de collage, alors le code $C = (C_1 C_2 ... C_t)^+$ est auto- dual de distance minimale quatre, si non on ne peut construire un code auto- dual par des composantes $C_1, C_2, ..., C_t$.

Construction des codes auto- duaux binaires de distance minimale supérieure ou égale à quatre

Dans le Théorème 2.4 les codes auto- duaux de distance minimale quatre existent pour $n \geq 8$

n = 8

Dans l'algèbre $I(G_1)$ les polynômes de degré 8 ayant les mêmes propriétés que le polynôme énumérateur des poids d'un code auto- dual sont :

$$\begin{aligned} W_C(x,y) &= \left(x^2+y^2\right)^4 + a_1\left(x^2y^2\left(x^2-y^2\right)^2\right) \\ &= x^8 + (a_1+4)\,x^6y^2 + (-2a_1+6)\,x^4y^4 + (a_1+4)\,x^2y^6 + y^8 \end{aligned}$$

Pour les codes de distance minimale différente de deux on a : $a_1 = -4$ donc

$$W_C(x,y) = x^8 + 14x^4y^4 + y^8 = S_C(x,y)$$

le code auto- dual correspondant W_C est le code de Hamming étendu e_8 de type II de matrice génératrice standard

$$\left(\begin{array}{c|cccc} & 0 & 1 & 1 & 1 \\ I_4 & 1 & 0 & 1 & 1 \\ & 1 & 1 & 0 & 1 \\ & 1 & 1 & 1 & 0 \end{array}\right)$$

n = 10

On a les polynômes de degré 10 qui sont :

$$\begin{aligned} W_C(x,y) &= \left(x^2+y^2\right)^5 + a_1\left(x^2+y^2\right)\left(x^2y^2\left(x^2-y^2\right)^2\right) \\ &= x^{10} + (5+a_1)\,x^8y^2 + (10-a_1)\,x^6y^4 + (10-a_1)\,x^4y^6 \\ &\quad + (5+a_1)\,x^2y^8 + y^{10} \end{aligned}$$

$$\begin{aligned} W_{S_C}(x,y) &= \sum_{i=0}^{1}(-1)^i\,a_i 2^{5-6i}\,(xy)^{5-4i}\left(x^4-y^4\right)^{2i} \\ &= 2^5\,(xy)^5 - \frac{a_1}{2}\,(xy)\left(x^4-y^4\right)^2 \end{aligned}$$

Pour les codes de distance minimale différente de deux on a : $a_1 = -5$ donc

$$\begin{aligned} W_C(x,y) &= x^{10} + 15x^6y^4 + 15x^4y^6 + y^{10} \\ W_{S_C}(x,y) &= \frac{5}{2}x^9y + 27x^5y^5 + \frac{5}{2}xy^9 \end{aligned}$$

alors pour $n = 10$ il n'existe aucun code auto- dual de distance minimale 4.

n = 12

On a les polynômes de degré 12 qui sont :

$$\begin{aligned} W_C(x,y) &= \left(x^2+y^2\right)^6 + a_1\left(x^2+y^2\right)^2\left(x^2y^2\left(x^2-y^2\right)^2\right) \\ &= x^{12} + (6+a_1)\,x^{10}y^2 + 15x^8y^4 + (20-2a_1)\,x^6y^6 + 15x^4y^8 \\ &\quad + (6+a_1)\,x^2y^{10} + y^{12} \end{aligned}$$

$$\begin{aligned} W_{S_C}(x,y) &= \sum_{i=0}^{1}(-1)^i\,a_i 2^{6-6i}\,(xy)^{6-4i}\left(x^4-y^4\right)^{2i} \\ &= 2^6\,(xy)^6 - a_1\,(xy)^2\left(x^4-y^4\right)^2 \end{aligned}$$

Pour les codes de distance minimale différente de deux on a : $a_1 = -6$ donc

$$\begin{aligned} W_C(x,y) &= x^{12} + 15x^8y^4 + 32x^6y^6 + 15x^4y^8 + y^{12} \\ W_{S_C}(x,y) &= 6x^{10}y^2 + 52x^6y^6 + 6x^2y^{10} \end{aligned}$$

le code auto- dual correspondant a W_C et S_C est $(d_{12})^+$, et le vecteur de collage est $a = 101010101010$, ce code est équivalent au code sous forme systématique

$$\left(\begin{array}{c||cccccc} & 0 & 1 & 1 & 1 & 1 & 1 \\ & 1 & 0 & 1 & 1 & 1 & 1 \\ I_6 & 1 & 1 & 0 & 1 & 1 & 1 \\ & 1 & 1 & 1 & 0 & 1 & 1 \\ & 1 & 1 & 1 & 1 & 0 & 1 \\ & 1 & 1 & 1 & 1 & 1 & 0 \end{array}\right)$$

n = 14

$$\begin{aligned} W_C(x,y) &= \left(x^2+y^2\right)^7 + a_1\left(x^2+y^2\right)^3\left(x^2y^2\left(x^2-y^2\right)^2\right) \\ &= x^{14} + (7+a_1)\,x^{12}y^2 + y^{14} + (21+a_1)\,x^{10}y^4 + (35-2a_1)\,x^8y^6 \\ &\quad + (35-2a_1)\,x^8y^6 + ... \end{aligned}$$

$$\begin{aligned} W_{S_C}(x,y) &= \sum_{i=0}^{1}(-1)^i\,a_i 2^{7-6i}\,(xy)^{7-4i}\left(x^4-y^4\right)^{2i} \\ &= 2^7\,(xy)^7 - 2a_1\,(xy)^3\left(x^4-y^4\right)^2 \end{aligned}$$

Pour les codes de distance minimale différente de deux on a : $a_1 = -7$ donc

$$\begin{aligned} W_C(x,y) &= x^{14} + 14x^{10}y^4 + 49x^8y^6 + 49x^8y^6 + ... \\ W_{S_C}(x,y) &= 14x^{11}y^3 + 100x^7y^7 + 14x^3y^{11} \end{aligned}$$

le code auto- dual correspondant a W_C et W_{S_C} est $(e_7^2)^+$ et le vecteur de collage est dd, ce code est équivalent au code systématique

$$\left(\begin{array}{c||ccccccc} & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ I_7 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ & 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{array}\right)$$

n = 16

Pour les codes auto- duaux décomposables on déduit un seul code auto- dual de type II de distance minimale quatre qui est le code $e_8^2 = e_8 \oplus e_8$, de polynôme enumérateur des

poids est

$$\begin{aligned} W_C(x,y) &= \left(x^8+14x^4y^4+y^8\right)^2 \\ &= x^{16}+28x^{12}y^4+198x^8y^8+28x^4y^{12}+y^{16} \end{aligned}$$

ce code est équivalent au code systématique

$$\left(\begin{array}{c||cccccccc} & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ I_8 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right)$$

Pour les codes indécomposables on a :

$$\begin{aligned} W_C(x,y) &= \left(x^2+y^2\right)^8 + a_1\left(x^2+y^2\right)^4\left(x^2y^2\left(x^2-y^2\right)^2\right) + a_2\left(x^2y^2\left(x^2-y^2\right)^2\right)^2 \\ W_{S_C}(x,y) &= \sum_{i=0}^{2}(-1)^i a_i 2^{8-6i}(xy)^{8-4i}\left(x^4-y^4\right)^{2i} \end{aligned}$$

Pour les codes de distance minimale différente de deux on a : $a_1=-8$ donc

$$\begin{aligned} W_C(x,y) &= x^{16}+(12+a_2)x^{12}y^4+(64-4a_2)x^{10}y^6+(102+6a_2)x^8y^8+... \\ W_{S_C}(x,y) &= \frac{a_2}{16}x^{16}+\left(32-\frac{a_2}{4}\right)x^{12}y^4+\left(192+\frac{3a_2}{8}\right)x^8y^8+... \end{aligned}$$

Dans W_C on a $-12 \leq a_2 \leq 16$, et dans W_{S_C} la condition sur a_2 est positive et multiple de 16 alors $a_2 \in \{0,16\}$.

Si $a_2 = 0$ on a :

$$\begin{aligned} W_C(x,y) &= x^{16} + 12x^{12}y^4 + 64x^{10}y^6 + 102x^8y^8 + ... \\ W_{S_C}(x,y) &= 32x^{12}y^4 + 192x^8y^8 + 32x^4y^{12} \end{aligned}$$

le code auto- dual de type I correspondant à W_C et W_{S_C} est $(d_8^2)^+$, et les deux vecteurs de collage sont : $X_1 = ab, X_2 = ba$..ce code est équivalent au code systématique

$$\left(\begin{array}{c||cccccccc} & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ I_8 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

Si $a_2 = 16$ on a :

$$W_C(x,y) = W_{S_C}(x,y) = x^{16} + 28x^{12}y^4 + 198x^8y^8 + 28x^4y^{12} + y^{16}$$

le code auto-dual de type II correspondant W_C est $(d_{16})^+$, et le vecteur de collage est :

$a = 1010...10$ ce code est équivalent au code systématique

$$\left(\begin{array}{c|c} & 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\ & 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1 \\ & 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1 \\ I_8 & 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1 \\ & 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1 \\ & 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1 \\ & 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1 \\ & 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0 \end{array}\right)$$

Remarque 3.2 Les deux codes e_8^2, $(d_{16})^+$ sont des codes auto- duaux de type II qui possèdent le même polynôme énumérateur des poids mais sont inéquivalents puisque l'ordre de groupe d'automorphismes de e_8^2 est différent à celui de $(d_{16})^+$.([3])

n = 18

Il n'existe pas des codes auto- duaux décomposables de distance minimale quatre.
Pour les codes indécomposables on a :

$$\begin{aligned} W_C(x,y) &= \left(x^2+y^2\right)^9 + a_1\left(x^2+y^2\right)^5\left(x^2y^2\left(x^2-y^2\right)^2\right) + a_2\left(x^2+y^2\right) \\ &\quad \times\left(x^2y^2\left(x^2-y^2\right)^2\right)^2 \\ W_{S_C}(x,y) &= \sum_{i=0}^{2}(-1)^i a_i 2^{9-6i}(xy)^{9-4i}\left(x^4-y^4\right)^{2i} \\ &= 2^9x^9y^9 - 2^3a_1(xy)^5\left(x^4-y^4\right)^2 + 2^{-3}a_2xy\left(x^4-y^4\right)^4 \end{aligned}$$

Pour les codes de distance minimale différente de deux on a : $a_1 = -9$ donc

$$\begin{aligned} W_C(x,y) &= x^{18} + (9+a_2)x^{14}y^4 + (75-3a_2)x^{12}y^6 + (171+2a_2)x^{10}y^8 + ... \\ W_{S_C}(x,y) &= \frac{a_2}{8}x^{17}y + \left(72-\frac{a_2}{2}\right)x^{13}y^5 + \left(368+\frac{3a_2}{4}\right)x^9y^9 + ... \end{aligned}$$

Dans W_C on a $-9 \leq a_2 \leq 25$ et dans W_{S_C} la condition sur a_2 est positive et multiple de 8 alors $a_2 \in \{0, 8, 16, 24\}$

Si $a_2 = 0$ alors $A_4 = 9$

Le code auto- dual ayant 9 mots code de poids quatre est $(d_6^3)^+$ et les trois vecteurs de collage sont : $X_1 = abc, X_2 = cab, X_3 = bbb$, ce code est équivalent au code systématique

$$\left(\begin{array}{c||ccccccccc} & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ I_9 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{array}\right)$$

On a les composantes $(d_8 d_6 f_4)$, $(e_7 d_4^2 f_3)$ qui contiennent 9 mots codes de poids quatre, mais il n'existe pas une matrice X dans la méthode de collage c-à-d on ne peut pas construire des codes auto- duaux à partir de ces composantes.

Si $a_2 = 8$ alors $A_4 = 17$

le code auto- dual correspondant est $(d_{10} e_7 f_1)^+$, et les deux vecteurs de collage sont :

$X_1 = a0^71, X_2 = cd0$, ce code est équivalent au code systématique

$$\left(\begin{array}{c|c} & 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0 \\ & 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0 \\ & 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0 \\ & 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0 \\ I_9 & 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1 \\ & 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1 \\ & 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1 \\ & 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0 \\ & 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 0 \end{array}\right)$$

Si $a_2 \in \{16, 24\}$ ce que implique que le nombre des mots code de poids quatre $A_4 \in \{25, 33\}$, dans ce cas il n'existe pas des composantes qui contiennent ce nombre c-à-d on ne peut pas construire des codes auto- duaux qui possèdent 25 et 33 mots code de poids quatre.

n = 20

Pour les codes décomposables on déduit un code auto- dual de distance minimale quatre qui est $e_8 \oplus (d_{12})^+$, de polynôme énumérateur des poids

$$\begin{aligned} W_{e_8 \oplus (d_{12})^+}(x, y) &= \left(x^8 + 14x^4y^4 + y^8\right)\left(x^{12} + 15x^8y^4 + 32x^6y^6 + 15x^4y^8 + y^{12}\right) \\ &= x^{20} + 29x^{16}y^4 + 32x^{14}y^6 + 226x^{12}y^8 + 448x^{10}y^{10} + 226x^8y^{12} \\ &\quad + 32x^6y^{14} + 29x^4y^{16} + y^{20} \end{aligned}$$

ce code est équivalent au code systématique

$$\left(\begin{array}{c|c} & \begin{array}{cccccccccc} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{array} \\ I_{10} & \end{array}\right)$$

Pour les codes indécomposables on a :

$$\begin{aligned} W_C(x,y) &= \left(x^2+y^2\right)^{10} + a_1\left(x^2+y^2\right)^6\left(x^2y^2\left(x^2-y^2\right)^2\right) + a_2\left(x^2+y^2\right)^2 \\ &\quad \times\left(x^2y^2\left(x^2-y^2\right)^2\right)^2 \end{aligned}$$

$$\begin{aligned} W_{S_C}(x,y) &= \sum_{i=0}^{2}(-1)^i a_i 2^{10-6i}(xy)^{10-4i}\left(x^4-y^4\right)^{2i} \\ &= 2^{10}x^{10}y^{10} - 2^4 a_1(xy)^6\left(x^4-y^4\right)^2 + 2^{-2}a_2x^2y^2\left(x^4-y^4\right)^4 \end{aligned}$$

Pour les codes de distance minimale différente de deux on a : $a_1 = -10$ donc

$$\begin{aligned} W_C(x,y) &= x^{20} + (5+a_2)x^{16}y^4 + (80-2a_2)x^{14}y^6 + (250-a_2)x^{12}y^8 \\ &\quad + (352+4a_2)x^{10}y^{10} + ... \end{aligned}$$

$$W_{S_C}(x,y) = \frac{a_2}{4}x^{18}y^2 + (180-a_2)x^{14}y^6 + \left(704+\frac{3a_2}{2}\right)x^{10}y^{10} + ...$$

Dans W_C on a $-5 \leq a_2 \leq 40$ et dans S_C la condition sur a_2 est positive et multiple de 4 alors

$$a_2 \in \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40\}$$

Si $a_2 = 0$ alors $A_4 = 5$

le code auto-dual ayant cinq mots code de poids quatre est $(d_4^5)^+$ et les cinq vecteurs de collage sont : $X_1 = 00aba$, $X_2 = a00ab$, $X_3 = ba00a$, $X_4 = aba00$, $X_5 = 0aba0$, ce code est équivalent au code systématique

$$\left(\begin{array}{c|c} & 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0 \\ & 0\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 1 \\ & 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ & 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0 \\ & 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 0 \\ I_{10} & 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0 \\ & 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0 \\ & 0\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1 \\ & 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0 \\ & 0\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1 \end{array}\right)$$

On ne peut pas construire des codes auto- duaux à partir des composantes $(d_6 d_4^2 f_6)$ puisque il n'existe pas une matrice X dans la méthode de collage.
Si $a_2 = 4$ alors $A_4 = 9$

le code auto- dual ayant 9 mots code de poids quatre est $(d_6^3 f_2)^+$ et les quatre vecteurs de collage sont : $X_1 = aaa10$, $X_2 = ccc01$, $X_3 = abc00$, $X_4 = cab00$, ce code est équivalent

au code systématique

$$\left(\begin{array}{c|c} & \begin{array}{cccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{array} \\ I_{10} & \end{array}\right)$$

Pour les composantes $(d_8 d_6 f_6)$ il n'existe pas de code auto- dual de distance minimale quatre.

Si $a_2 = 8$ alors $A_4 = 13$

le code auto- dual ayant 13 mots code de poids quatre est $(d_8^2 d_4)^+$ et les trois vecteurs de collage sont : $X_1 = aba$, $X_2 = baa$, $X_3 = bbc$.ce code est équivalent au code systématique

$$\left(\begin{array}{c|c} & \begin{array}{cccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{array} \\ I_{10} & \end{array}\right)$$

Pour les composantes $d_8 d_6 f_6$ il n'existe pas un code-auto dual de distance minimale est quatre.

Si $a_2 = 12$ alors $A_4 = 17$

le code auto- dual ayant 17 mots code de poids quatre est $(e_7^2 d_6)^+$ et les deux vecteurs de collage sont : $X_1 = d0a$, $X_2 = ddb$, ce code est équivalent au code systématique

$$\left(\begin{array}{c|c} & 1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0 \\ & 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0 \\ & 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0 \\ & 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0 \\ & 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0 \\ I_{10} & 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0 \\ & 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1 \\ & 1\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0 \\ & 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1 \\ & 1\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1 \end{array} \right)$$

Pour les composantes $d_{12} d_4^2$, $d_{10} e_7 f_3$ il n'existe pas des codes auto- duaux de distance minimale quatre.

Si $a_2 = 16$ alors $A_4 = 21$

le code auto- dual ayant 21 mots code de poids quatre est $(d_{12} d_8)^+$ et les deux vecteurs

de collage sont : $X_1 = ab$, $X_2 = ba$..ce code est équivalent au code systématique

$$\left(\begin{array}{c|c} & 1\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0 \\ & 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0 \\ & 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 0 \\ & 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0 \\ & 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0 \\ I_{10} & 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1 \\ & 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0 \\ & 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0 \\ & 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1 \\ & 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1 \end{array}\right)$$

Pour la composante $(d_{14}f_6)$ il n'existe pas un code auto- dual de distance minimale quatre.

Si $a_2 \in \{20, 24, 28, 32, 36\}$, alors $A_4 \in \{25, 29, 33, 37, 41\}$

Il n'existe pas des composantes qui contiennent ce nombre de mots code de poids quatre c-à-d on ne peut pas construire des codes auto- duaux.

Si $a_2 = 40$ alors $A_4 = 45$

le code auto- dual ayant 45 mots code de poids quatre est $(d_{20})^+$ et le vecteur de collage

est : $a = 1010...10$, ce code est équivalent au code systématique

$$\left(\begin{array}{c|c} & 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\ & 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\ & 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\ & 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1 \\ & 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1 \\ I_{10} & 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1 \\ & 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1 \\ & 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1 \\ & 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1 \\ & 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0 \end{array}\right)$$

n = 22

Pour les codes auto- duaux décomposables on déduit un seul code auto- dual de distance minimale quatre qui est $e_8 \oplus (e_7^2)^+$, de polynôme énumérateur des poids est :

$$\begin{aligned} W_{e_8 \oplus \left(e_7^2\right)^+}(x,y) &= \left(x^8 + 14x^4y^4 + y^8\right) \times \left(\begin{array}{c} x^{14} + 14x^{10}y^4 + 49x^8y^6 \\ +49x^8y^6 + 14x^4y^{10} + y^{14} \end{array}\right) \\ &= x^{22} + 28x^{18}y^4 + 49x^{16}y^6 + 246x^{14}y^8 + 700x^{12}y^{10} + ... \end{aligned}$$

ce code est équivalent au code systématique

$$\left(\begin{array}{c|c} & \begin{array}{ccccccccccc} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{array} \\ I_{11} & \end{array}\right)$$

Pour les codes indécomposables on a :

$$\begin{aligned} W_C(x,y) &= \left(x^2+y^2\right)^{11} + a_1\left(x^2+y^2\right)^7\left(x^2y^2\left(x^2-y^2\right)^2\right) + a_2\left(x^2+y^2\right)^3 \\ &\quad \times\left(x^2y^2\left(x^2-y^2\right)^2\right)^2 \end{aligned}$$

$$\begin{aligned} W_{S_C}(x,y) &= \sum_{i=0}^{2}(-1)^i a_i 2^{11-6i}(xy)^{11-4i}\left(x^4-y^4\right)^{2i} \\ &= 2^{11}x^{11}y^{11} - 2^5 a_1(xy)^7\left(x^4-y^4\right)^2 + 2^{-1}a_2x^3y^3\left(x^4-y^4\right)^4 \end{aligned}$$

Pour les codes de distance minimale différente de deux on a : $a_1 = -11$ donc

$$\begin{aligned} W_C(x,y) &= x^{22} + a_2x^{18}y^4 + (77-a_2)x^{16}y^6 + (330-3a_2)x^{14}y^8 \\ &\quad + (616+3a_2)x^{12}y^{10} + ... \\ W_{S_C}(x,y) &= \frac{a_2}{2}x^{19}y^3 + (352-2a_2)x^{15}y^7 + (1344+3a_2)x^{11}y^{11} + ... \end{aligned}$$

Comme $W_{S_C}(x,y) = W^{(1)}(x,y) + W^{(3)}(x,y)$ et $W^{(1)}(x,y) = W^{(3)}(x,y)$ (voir théorème 5 [3]), alors $W_{S_C}(x,y) = 2W^{(1)}(x,y)$ c-à-d les coefficients dans W_{S_C} sont pairs, donc la condition sur a_2 à partir de W_C, W_{S_C} est : $0 \leq a_2 \leq 77$ et $\frac{a_2}{2}$ divisible par deux (a_2 est divisible par quatre) alors

$$a_2 \in \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76\}$$

Si $a_2 = A_4 = 0$

Il y a un seul code auto- dual de distance minimale 6, appelé le code de Golay tronqué g_{22} obtenue du code de Golay g_{24} et défini par :

$g_{22} = \{u \in \mathbb{F}_2^{22}; 00u \in g_{24}$ où $11u \in g_{24}\}$, alors ce code est de matrice génératrice

$$G_{g_{22}} = \begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} \tag{3.2}$$

Si $a_2 = A_4 = 4$

Le code auto- dual est $(d_4^4 f_6)^+$, avec les sept vecteurs de collage sont :

$X_1 = 0abc101110$, $X_2 = 0cab011110$, $X_3 = 00aa011011$, $X_4 = 0b0b011101$,

$X_5 = 0cc0010111, X_6 = aaaa000000$, $X_7 = bbbb0000000$.ce code est équivalent au code

systématique

$$\left(\begin{array}{c|c} & \begin{array}{cccccccccc} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{array} \\ I_{11} & \end{array}\right)$$

et il n'existe pas un code auto- dual pour la composante $(d_4 d_6 f_{12})$.

Si $a_2 = A_4 = 8$

Le code auto-dual est $(d_6^2 d_4^2 f_2)^+$, avec les cinq vecteurs de collage sont :

$X_1 = a0a010$, $X_2 = 00bb11$, $X_3 = aab000$, $X_4 = b0ca00$, $X_5 = 0bac00$, ce code est

équivalent au code systématique

$$\left(\begin{array}{c|c} & 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0 \\ & 0\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0 \\ & 0\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0 \\ & 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 0 \\ & 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1 \\ I_{11} & 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ & 1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ & 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0 \\ & 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0 \\ & 1\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1 \\ & 1\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1 \end{array}\right)$$

et il n'existe pas de codes auto- duaux par les deux composantes $(e_7 d_4 f_{11})$, $(d_8 d_4^2 f_6)$.

Si $a_2 = A_4 = 12$

Le code auto- dual est $(d_8 d_6^2 f_2)^+$, avec les quatre vecteurs de collage sont :

$X_1 = ba010$, $X_2 = a0011$, $X_3 = abb00$, $X_4 = 0cc00$, ce code est équivalent au code

systématique

$$\left(\begin{array}{c|c} & 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0 \\ & 0\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0 \\ & 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ & 1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ & 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0 \\ I_{11} & 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 0 \\ & 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1 \\ & 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0 \\ & 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0 \\ & 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1 \\ & 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1 \end{array}\right)$$

et il n'existe pas de codes auto- duaux par des composantes $(d_{10}d_4^2f_4)$, $(d_8^2f_6)$, $(e_7d_6d_4^2f_1)$.

Si $a_2 = A_4 = 16$

les deux codes auto- duaux sont $(d_{10}d_6^2)^+$ et $(d_8e_7d_6f_1)^+$, avec les trois vecteurs de collage sont : $X_1 = a0c$, $X_2 = 0aa$, $X_3 = bbb$ et $X_1 = 0db1$, $X_2 = b0a1$, $X_3 = a0b0$, ces codes sont équivalents respectivement les codes systématiques

$$\left(\begin{array}{c|c} & 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ & 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ & 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ & 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0 \\ & 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 0 \\ I_{11} & 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1 \\ & 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0 \\ & 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1 \\ & 1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1 \\ & 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1 \\ & 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1 \end{array}\right) \text{ et } \left(\begin{array}{c|c} & 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1 \\ & 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1 \\ & 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1 \\ & 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1 \\ & 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0 \\ I_{11} & 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1 \\ & 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1 \\ & 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 0 \\ & 1\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0 \\ & 1\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0 \\ & 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 1 \end{array}\right)$$

et il n'existe pas des codes auto- duaux à partir des composantes $(d_{16}d_4f_2)$, $(d_{10}d_8d_4)$, $(e_7^2d_4^2)$.

Si $a_2 = A_4 = 20$

Le code auto- dual est $(d_{10}^2f_2)^+$, où les trois vecteurs de collage sont : $X_1 = a010$, $X_2 = 0a01$, $X_3 = cc00$, ce code est équivalent au code systématique

$$\left(\begin{array}{c||cccccccccc} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ I_{11} & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

et il n'existe pas un code auto- dual par des composantes $(e_7^2d_8)$.

Si $a_2 \in \{24, 32, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76\}$

Dans ce cas il n'existe pas des codes auto- duaux puisque il n'existe pas des composantes qui contiennent ce nombre des mots code de poids quatre.

Si $a_2 = A_4 = 28$

Le code auto- dual est $(d_{14}e_7f_1)^+$, avec les deux vecteurs de collage sont :

$X_1 = a01$, $X_2 = bd1$,ce code est équivalent au code systématique

$$\left(\begin{array}{c|c} & \begin{array}{cccccccccc} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \\ I_{11} & \end{array}\right)$$

Et il n'existe pas un code auto- dual par des composantes $(d_{16}f_6)$.

Si $a_2 = A_4 = 36$

Dans ce cas il n'existe pas un code auto- dual par des composantes $(d_{18}f_4)$.

Le tableau suivant montre la classification de tous les codes binaires auto- duaux inéquivalents pour $n = 2, ..., 22$ et l'ordre de groupe d'automorphismes [15] pour vérifier

le nombre total des codes auto- duaux avec l'usage de la formule de masse.

n	d	le code auto- dual	les vecteurs de colle	de type	$\mid Aut\,(C)\mid$	le nombre des codes auto- duaux inéquivanents
2	2	i_2	_	(I)	2	1
4	2	i_2^2	_	(I)	8	1
6	2	i_2^3	_	(I)	48	1
8	2	i_2^4	_	(I)	384	2
	4	e_8	_	(II)	1344	
10	2	i_2^5	_	(I)	3840	2
		$i_2 e_8$	_		2688	
12	2	i_2^6	_	(I)	46080	3
		$i_2^2 e_8$	_		10752	
	4	$(d_{12})^+$	a		23040	
14	2	i_2^7	_	(I)	645120	4
		$i_2^3 e_8$	_		64512	
		$i_2\,(d_{12})^+$	_		46080	
	4	$(e_7^2)^+$	dd		56448	
16	2	i_2^8	_	(I)	10321920	7
		$i_2^4 e_8$	_		516096	
		$i_2^2\,(d_{12})^+$	_		184320	
		$i_2\,(e_7^2)^+$	_		112896	
	4	$(d_8^2)^+$	ab, ba		3612672	
		$(d_{16})^+$	a	(II)	5160960	
		e_8^2	_		73728	
		i_2^9	_		185794560	

18	2	$i_2^5 e_8$	_	(I)	5160960	9
		$i_2^2 \left(d_{12}\right)^+$	_		1105920	
		$i_2^2 \left(e_7^2\right)^+$	_		451584	
		$i_2 \left(d_8^2\right)^+$	_		7225344	
		$i_2 \left(d_{16}\right)^+$	_		10321920	
		$i_2 e_8^2$	_		147456	
	4	$\left(d_{10} e_7 f_1\right)^+$	$a01, cd0$		322560	
		$\left(d_6^3\right)^+$	abc, cab, bbb		82944	
20	2	i_2^{10}	_	(I)	3715891200	16
		$i_2^6 e_8$	_		61931520	
		$i_2^3 \left(d_{12}\right)^+$	_		8847360	
		$i_2^3 \left(e_7^2\right)^+$	_		2709504	
		$i_2^2 \left(d_8^2\right)^+$	_		28901376	
		$i_2^2 \left(d_{16}\right)^+$	_		41287680	
		$i_2^2 e_8^2$	_		589824	
		$i_2 \left(d_{10} e_7 f_1\right)^+$	_		645120	
		$i_2 \left(d_6^3\right)^+$	_		165888	
	4	$\left(d_4^5\right)^+$	$00aba, a00ab, ba00a, aba00, 0aba0$		122880	
		$\left(d_6^3 f_2\right)^+$	$aaa10, ccc01, abc00, cab00$		82944	
		$\left(e_7^2 d_6\right)^+$	$d0a, ddb$		1354752	
		$\left(d_8^2 d_4\right)^+$	$aba, b0a, bbb$		294912	
		$\left(d_{12} d_8\right)^+$	ab, ba		4423680	
		$\left(d_{20}\right)^+$	a		1857945600	
		$e_8 \left(d_{12}\right)^+$	_		30965760	
		i_2^{11}	_		81749606400	
		$i_2^7 e_8$	_		867041280	
		$i_2^4 \left(d_{12}\right)^+$	_		88473600	
		$i_2^4 \left(e_7^2\right)^+$	_		21676032	

22	2	$i_2^3\,(d_8^2)^+$	_	(I)	173408256	25
		$i_2^3\,(d_{16})^+$	_		247726080	
		$i_2^3 e_8^2$	_		3538944	
		$i_2^2\,(d_{10}e_7f_1)^+$	_		2580480	
		$i_2^2\,(d_6^3)^+$	_		663552	
		$i_2\,(d_4^5)^+$	_		245760	
		$i_2\,(d_6^3 f_2)^+$	_		165888	
		$i_2\,(e_7^2 d_6)^+$	_		2709504	
		$i_2\,(d_8^2 d_4)^+$	_		589824	
		$i_2\,(d_{12}d_8)^+$	–		8847360	
	2	$i_2\,(d_{20})^+$	_		3715891200	
		$i_2 e_8\,(d_{12})^+$	–		61931520	
	4	$e_8\,(e_7^2)^+$	–		75866112	
		$(d_4^4 f_6)^+$	$0abc101110, 0cab011110, 00aa011011$ $0b0b011101, 0cc0010111, aaaa000000$ $bbbb000000$		36864	
		$(d_6^2 d_4^2 f_2)^+$	$a0a010, 00bb11, aab000, b0ca00, 0bac00$		36864	
		$(d_8 d_6^2 f_2)^+$	$ba010, a0011, abb00, 0cc00$		221184	
		$(d_8 e_7 d_6 f_1)^+$	$0db1, b0a1, a0b0$		774144	
		$(d_{10}d_6^2)^+$	$a0c, 0aa, bbb$		2211840	
		$(d_{10}^2 f_2)^+$	$a010, 0a01, cc00$		7372800	
		$(d_{14}e_7f_1)^+$	$a01, bd1$		54190080	
	6	(g_{22})	(3.2)		887040	

3.3 Classification des codes auto- duaux ternaires

Les codes auto- duaux sur $\mathbb{F}_3$ sont uniquement définis pour des longueurs multiples de quatre, ils ont été classifiés jusqu'à la longueur 20, les codes extrémaux sont aussi connus pour la longueur 24 [5], mais dans cette partie on arrête dans la classification les codes auto- duaux ternaires à $n = 20$ puisque à partir de cette valeur, le nombre des codes inéquivalents devient grand, par exemple pour $n = 24$ le nombre des codes inéquivalents est 59 [5].

Les codes auto- orthogonaux (auto- duaux) utilisés comme des composantes dans la méthode de collage sont

• $e_3 = [3, 1, 3]$ code de matrice génératrice (111) et les vecteurs de colle sont $-a, +a$ tel que $a = 120$, ce code contient deux mots code de poids trois.

• $t_4 = [4, 2, 3]$ le petit code auto- dual de matrice génératrice

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

ce code contient huit mots code de poids trois.

• $g_{12} = [12, 6, 6]$ le code de Golay auto- dual de matrice génératrice

$$\begin{pmatrix} 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 \end{pmatrix}$$

• $\gamma_{11} = [11, 4, 6]$ le code auto- orthogonal de matrice génératrice

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 1 & 2 \end{pmatrix}$$

et les vecteurs de collage sont l'espace engendré par la matrice

$$\begin{pmatrix} r \\ s \\ t \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

• $g_{11} = [11, 5, 6]$ le code auto- orthogonal qui contient des vecteurs c tels que $0c \in g_{12}$, alors ce code de matrice génératrice

$$\begin{pmatrix} 1 & 1 & 2 & 1 & 0 & 1 & 2 & 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 2 & 1 & 2 & 1 & 1 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 & 2 & 0 & 2 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 2 & 1 \end{pmatrix}$$

et les vecteurs de colle sont choissis comme suit :

si $1u \in g_{12}$ avec $\omega(u) = 5$ alors $+u, -u$ sont des vecteurs de collage où $u = 00000112102$.

• $g_{10} = [10, 4, 6]$ le code auto- orthogonal qui contient des vecteurs c tels que $00c \in g_{12}$, alors g_{10} de matrice génératrice

$$\begin{pmatrix} 1 & 1 & 2 & 1 & 2 & 1 & 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 2 & 0 & 2 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 2 & 1 \end{pmatrix}$$

si x, y choissis comme suit : $11x \in g_{12}, 12y \in g_{12}$ alors $x = 1210200000, y = 1002110000$ donc les vecteurs de collage sont l'espace engendré par x et y.

• $g_9 = [9, 3, 6]$ de matrice génératrice

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 \end{pmatrix}$$

et les vecteurs de collage sont l'espace engendré par la matrice

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 \end{pmatrix}$$

• $g_8 = [8, 2, 5]$ le code auto- orthogonal de matrice génératrice

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 & 1 & 2 & 1 \end{pmatrix}$$

et les vecteurs de collage sont l'espace engendré par la matrice

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \end{pmatrix}$$

Les codes auto- orthogonaux $g_{11}, \gamma_{11}, g_{10}, g_9, g_8$ sont des sous codes de code de Golay g_{12}.

• $p_{13} = [13, 6, 6]$ code auto- orthogonal de matrice génératrice

$$\left(\begin{array}{c|ccccccc} & 2 & 2 & 1 & 2 & 0 & 0 & 1 \\ & 1 & 0 & 1 & 2 & 2 & 0 & 2 \\ I_6 & 2 & 0 & 1 & 0 & 2 & 2 & 1 \\ & 1 & 0 & 2 & 2 & 0 & 2 & 1 \\ & 1 & 2 & 2 & 0 & 2 & 0 & 1 \\ & 1 & 2 & 1 & 0 & 0 & 2 & 2 \end{array}\right)$$

et les deux vecteurs de collage sont t_0, $-t_0$ où $t_0 = 1101000001000$.

• $p_{12} = [12, 5, 6]$ code auto- orthogonal qui contient des vecteurs c tels que $c0 \in p_{13}$, alors ce code de matrice génératrice

$$\left(\begin{array}{c|ccccccc} & 1 & 0 & 1 & 2 & 2 & 0 & 2 \\ & 2 & 0 & 1 & 0 & 2 & 2 & 1 \\ I_5 & 1 & 0 & 2 & 2 & 0 & 2 & 1 \\ & 1 & 2 & 2 & 0 & 2 & 0 & 1 \\ & 1 & 2 & 1 & 0 & 0 & 2 & 2 \end{array}\right)$$

et les vecteurs de collage sont l'espace engendré par $t_0^{'}$, $t_3^{'}$ où $t_0 = t_0^{'}0$, $t_3 = t_3^{'}1$ et $t_3 = 0011010000010$.

• $h_{16} = [16, 8, 6]$ est l'unique code auto- dual de matrice génératrice $(I_8 \| H_8)$ où H_8 est la matrice de Hadamard d'ordre 8 dont les coefficients sont 1 ou -1, qui vérifie l'égalité $HH^t = 8I_8$ alors on trouve la matrice H_8 comme suite :

$$H_8 = \left(\begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 \\ 1 & 2 & 2 & 1 & 1 & 2 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\ 1 & 2 & 1 & 2 & 2 & 1 & 2 & 1 \\ 1 & 1 & 2 & 2 & 2 & 2 & 1 & 1 \\ 1 & 2 & 2 & 1 & 2 & 1 & 1 & 2 \end{array}\right)$$

• $h_{15} = [15, 7, 6]$ code auto- orthogonal qui contient des vecteurs c tels que $c0 \in h_{16}$, alors ce code de matrice génératrice

$$\left(\begin{array}{c|cccccccc} & 1 & 2 & 0 & 0 & 2 & 0 & 2 & 2 \\ & 2 & 0 & 0 & 2 & 1 & 2 & 1 & 0 \\ & 2 & 0 & 2 & 0 & 1 & 2 & 0 & 1 \\ I_7 & 1 & 2 & 1 & 1 & 2 & 0 & 0 & 0 \\ & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 1 \\ & 1 & 2 & 1 & 0 & 0 & 1 & 2 & 0 \\ & 1 & 2 & 0 & 1 & 0 & 1 & 0 & 2 \end{array}\right)$$

si u un vecteur de poids cinq est choissi comme suit $1u \in h_{16}$ alors les deux vecteurs de collage sont u, $-u$ alors $u = 000000120020220$.

• $h_{14} = [14, 6, 6]$ le code auto- orthogonal est obtenu en supprimant deux composantes de même côté de h_{16} alors ce code de matrice génératrice

$$\left(\begin{array}{c|c} & 1\ 1\ 2\ 2\ 1\ 1\ 2\ 2 \\ & 1\ 2\ 2\ 1\ 1\ 2\ 2\ 1 \\ & 1\ 1\ 1\ 1\ 2\ 2\ 2\ 2 \\ I_6 & 1\ 2\ 1\ 2\ 2\ 1\ 2\ 1 \\ & 1\ 1\ 2\ 2\ 2\ 2\ 1\ 1 \\ & 1\ 2\ 2\ 1\ 2\ 1\ 1\ 2 \end{array}\right)$$

si x et y deux vecteurs choissi comme suit : $11x \in h_{16}$ et $12y \in h_{16}$, alors des veteurs de collage sont l'espace engendré par x et y.

• $\eta_{14} = [14, 6, 6]$ le code auto- orthogonal obtenue par supprimer une composante de chaque coté de h_{16}, et le même vecteurs de colle de h_{14}.

Construction des codes auto- duaux ternaires

D'après la théorie des invariants on a le polynôme énumérateur des poids d'un code ternaire auto- dual est un élément dans $I(G_3)$ engendré par $\Phi_4(x, y) = x^4 + 8xy^3$ et $\Phi_{12}(x, y) = y^3(x^3 - y^3)^3$ et la condition sur n est divisible par quatre.

n = 4

On a :

$$W_C(x, y) = x^4 + 8xy^3$$

Le code auto- dual associé au polynôme énumérateur des poids est t_4 de matrice génératrice

$$G_{t_4} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}$$

n = 8

Le seul code auto- dual décomposable est t_4^2, de polynôme énumérateur des poids :

$$\begin{aligned} W_{t_4^2}(x,y) &= \left(x^4+8xy^3\right)^2 \\ &= x^8+16x^5y^3+64x^2y^6 \end{aligned}$$

n = 12

Pour les codes décomposables on a un seul code décomposable est t_4^3, de polynôme énumérateur des poids :

$$\begin{aligned} W_{t_4^3}(x,y) &= \left(x^4+8xy^3\right)^3 \\ &= x^{12}+24x^9y^3+192x^6y^6+512x^3y^9 \end{aligned}$$

Pour les codes indécomposables on a :

$$\begin{aligned} W_C(x,y) &= \left(x^4+8xy^3\right)^3+a_1\left(y^3\left(x^3-y^3\right)^3\right) \\ &= x^{12}+(24+a_1)x^9y^3+(192-3a_1)x^6y^6+(512+3a_1)x^3y^9-a_1y^{12} \end{aligned}$$

donc $-24 \leq a_1 \leq -2$ et a_1 est pair alors

$a_1 \in \{-24,-22,-20,-18,-16,-14,-12,-10,-8,-6,-4,-2\}$.

Si $a_1 = -24$ alors $A_3 = 0$

Le code auto- dual est le code de Golay g_{12} de matrice génératrice (2.10).

Si $a_1 \in \{-22,-20,-18\}$ alors $A_3 \in \{2,4,6\}$

Il n'existe pas des codes auto- duaux à partir des composantes $(e_3f_9)^+$, $(e_3^2f_6)^+$, $(e_3^3f_3)^+$ qui contiennent ce nombre des mots code de poids trois.

Si $a_1 = -16$ alors $A_3 = 8$

Le code auto- dual est $(e_3^4)^+$, où les deux vecteurs de colle sont : $X_1 = aaa0$, $X_2 = 0\overline{a}aa$

Si $a_1 \in \{-14,-12,-10,-8,-6,-4,-2\}$ alors $A_3 \in \{10,12,14,16,18,20,22\}$

Il n'existe pas des composantes qui contiennent ce nombre des mots codes de poids trois.

n = 16

On a trois codes décomposables :

Le premier code est t_4^4, de polynôme énumérateur des poids :

$$\begin{aligned} W_{t_4^3}(x,y) &= \left(x^4+8xy^3\right)^4 \\ &= x^{16}+32x^{13}y^3+384x^{10}y^6+2048x^7y^9+4096x^4y^{12} \end{aligned}$$

Le deuxième code est $t_4 \oplus g_{12}$, de polynôme énumérateur des poids :

$$\begin{aligned} W_{t_4\oplus g_{12}}(x,y) &= \left(x^4+8xy^3\right)\left(x^{12}+264x^6y^6+440x^3y^9+24y^{12}\right) \\ &= x^{16}+8x^{13}y^3+264x^{10}y^6+2552x^7y^9+3544x^4y^{12}+192xy^{15} \end{aligned}$$

Le troisième code est $t_4 \oplus (e_3^4)^+$, de polynôme énumérateur des poids :

$$\begin{aligned} W_{t_4\oplus\left(e_3^4\right)^+}(x,y) &= \left(x^4+8xy^3\right)\left(x^{12}+8x^9y^3+240x^6y^6+464x^3y^9+16y^{12}\right) \\ &= x^{16}+16x^{13}y^3+304x^{10}y^6+2384x^7y^9+3728x^4y^{12}+128xy^{15} \end{aligned}$$

Pour les codes indécomposables on a :

$$\begin{aligned} W_C(x,y) &= \left(x^4+8xy^3\right)^4+a_1\left(x^4+8xy^3\right)\left(y^3\left(x^3-y^3\right)^3\right) \\ &= x^{16}+(32+a_1)x^{13}y^3+(384+5a_1)x^{10}y^6+(2048-21a_1)x^7y^9 \\ &\quad +(4096+23a_1)x^4y^{12}-8a_1xy^{15} \end{aligned}$$

alors $-32 \leq a_1 \leq 0$ et a_1 est pair donc $a_1 \in \{-32,-30,...,-4,-2,0\}$

Pour les codes indécomposables.

Si $a_1 = -32$ alors $A_3 = 0$.

Le code auto- dual est h_{16} de distance minimale 6 de matrice génératrice $[I_8 \parallel H_8]$.

Si $a_1 = -30$ alors $A_3 = 2$.

Le code auto- dual est $(e_3p_{13})^+$, où le vecteur de colle est $X_1 = at_0$.

Si $a_1 = -28$ alors $A_3 = 4$.

Le code auto- dual est $(e_3^2 g_{10})^+$, où les deux vecteurs de colle sont : $X_1 = a0x$, $X_2 = 0ay$.

Si $a_1 = -26$ alors $A_3 = 6$.

La composante qui contiennent six nombres des mots code de poids trois est e_3^3 mais il n'existe pas le composant f_7 tel que $(e_3^3 f_7)^+$ un code auto- dual.

Si $a_1 = -24$ alors $A_3 = 8$.

le code auto- dual est $(e_3^4 f_4)^+$, où les quatres vecteurs de colle sont : $X_1 = a0002111$, $X_2 = 0a001211$, $X_3 = 00a01121$, $X_4 = 000a1112$.

Si $a_1 \in \{-22, -20, -18, ..., -2, 0\}$ alors $A_3 \in \{10, 12, 14, ..., 30, 32\}$.

Il n'existe pas de composantes qui contiennent ce nombre des mots code de poids trois.

n = 20

On a sept codes décomposables :

Le premièr code est t_4^5, de polynôme énumérateur des poids :

$$\begin{aligned} W_{t_4^5}(x,y) &= \left(x^4 + 8xy^3\right)^5 \\ &= x^{20} + 40x^{17}y^3 + 640x^{14}y^6 + 5120x^{11}y^9 + 20\,480x^8y^{12} + 32\,768x^5y^{15} \end{aligned}$$

Le deuxième code est $t_4^2 \oplus g_{12}$, de polynôme énumérateur des poids

$$\begin{aligned} W_{t_4^2 \oplus g_{12}}(x,y) &= \left(x^4 + 8xy^3\right)^2 \left(x^{12} + 264x^6y^6 + 440x^3y^9 + 24y^{12}\right) \\ &= x^{20} + 16x^{17}y^3 + 328x^{14}y^6 + 4664x^{11}y^9 + 23\,960x^8y^{12} + 28\,544x^5y^{15} \\ &\quad + 1536x^2y^{18} \end{aligned}$$

Le troisième code est $t_4^2 \oplus (e_3^4)^+$, de polynôme énumérateur des poids :

$$\begin{aligned} W_{t_4^2 \oplus \left(e_3^4\right)^+}(x,y) &= \left(x^4 + 8xy^3\right)^2 \left(x^{12} + 8x^9y^3 + 240x^6y^6 + 464x^3y^9 + 16y^{12}\right) \\ &= x^{20} + 24x^{17}y^3 + 432x^{14}y^6 + 4816x^{11}y^9 + 22\,800x^8y^{12} + 29\,952x^5y^{15} \\ &\quad + 1024x^2y^{18} \end{aligned}$$

Le quatrième code est $t_4 \oplus h_{16}$, de polynôme énumérateur des poids :

$$\begin{aligned} W_{t_4 \oplus h_{16}}(x,y) &= \left(x^4 + 8xy^3\right)\left(x^{16} + 224x^{10}y^6 + 2720x^7y^9 + 3360x^4y^{12} + 256xy^{15}\right) \\ &= x^{20} + 8x^{17}y^3 + 224x^{14}y^6 + 4512x^{11}y^9 + 25\,120x^8y^{12} \\ &\quad +27\,136x^5y^{15} + 2048x^2y^{18} \end{aligned}$$

Le cinqième code est $t_4 \oplus (e_3p_{13})^+$, de polynôme énumérateur des poids :

$$\begin{aligned} W_{t_4 \oplus (e_3p_{13})^+}(x,y) &= \left(x^4 + 8xy^3\right)\left(\begin{array}{c} x^{16} + 2x^{13}y^3 + 234x^{10}y^6 + 2678x^7y^9 \\ +3406x^4y^{12} + 240xy^{15} \end{array}\right) \\ &= x^{20} + 10x^{17}y^3 + 250x^{14}y^6 + 4550x^{11}y^9 + 24\,830x^8y^{12} + \\ &\quad 27\,488x^5y^{15} + 1920x^2y^{18} \end{aligned}$$

Le sixième code est $t_4 \oplus (e_3^2g_{10})^+$, de polynôme énumérateur des poids :

$$\begin{aligned} W_{t_4 \oplus \left(e_3^2g_{10}\right)^+}(x,y) &= \left(x^4 + 8xy^3\right)\left(\begin{array}{c} x^{16} + 4x^{13}y^3 + 244x^{10}y^6 + 2636x^7y^9 + 3452x^4y^{12} \\ +224xy^{15} \end{array}\right) \\ &= x^{20} + 12x^{17}y^3 + 276x^{14}y^6 + 4588x^{11}y^9 + 24\,540x^8y^{12} + 27\,840x^5y^{15} \\ &\quad +1792x^2y^{18} \end{aligned}$$

Le septième code est $t_4 \oplus (e_3^4f_4)^+$, de polynôme énumérateur des poids :

$$\begin{aligned} W_{t_4 \oplus \left(e_3^4f_4\right)^+}(x,y) &= \left(x^4 + 8xy^3\right)\left(\begin{array}{c} x^{16} + 8x^{13}y^3 + 264x^{10}y^6 + 2552x^7y^9 + 3544x^4y^{12} \\ +192xy^{15} \end{array}\right) \\ &= x^{20} + 16x^{17}y^3 + 328x^{14}y^6 + 4664x^{11}y^9 + 23\,960x^8y^{12} + 28544x^5y^{15} \\ &\quad +1536x^2y^{18} \end{aligned}$$

Pour les codes auto- duaux indécomposables on a :

$$\begin{aligned} W_C(x,y) &= \left(x^4+8xy^3\right)^5 + a_1\left(x^4+8xy^3\right)^2\left(y^3\left(x^3-y^3\right)^3\right) \\ &= x^{20} + (40+a_1)\,x^{17}y^3 + (640+13a_1)\,x^{14}y^6 + (5120+19a_1)\,x^{11}y^9 \\ &\quad + (20\,480-145a_1)\,x^8y^{12} + (32\,768+176a_1)\,x^5y^{15} - 64a_1x^2y^{18} \end{aligned}$$

On a : $-40 \leq a_1 \leq 0$ et a_1 est pair, alors $a_1 \in \{-40,-38,...,-2,0\}$

Si $a_1 = -40$ alors $A_3 = 0$.

On a six codes auto- duaux inéquivalents de distance minimale six :

Le code $(f_2^{10})^+$ de matrice génératrice

$$\begin{pmatrix} 1&1&1&1&1&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&1&2&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&2&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&2&0&0 \\ 1&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 1&1&2&2&0&0&0&0&0&0&1&2&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&2&2&0&0&0&0&0&0&1&2&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&2&2&0&0&0&0&0&0&1&2 \\ 0&0&1&2&0&0&0&0&0&0&0&0&1&1&2&2&0&0&0&0 \\ 0&0&0&0&0&0&1&2&0&0&0&0&0&0&0&0&1&1&2&2 \end{pmatrix} \tag{3.3}$$

Le code $(f_4^4 f_2^2)^+$ de matrice génératrice

$$\begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 2 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 1 & 0
\end{pmatrix} \tag{3.4}$$

Le code $(f_4^5)^+$ de matrice génératrice

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 2 & 0 & 0 \\
1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
2 & 2 & 1 & 1 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 2 & 1 & 1 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 1 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 1 & 0 & 0 & 1 & 2 \\
0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 1
\end{pmatrix} \tag{3.5}$$

Le code $(f_5^4)^+$ de matrice génératrice

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0
\end{pmatrix} \tag{3.6}$$

Le code $(g_9^2 f_2)^+$,où les quatres vecteurs de colle sont : $X_1 = 1^3 0^6 1^3 0^8$,
$X_2 = 0^2 10^2 20^2 20^2 20^2 10^2 10^2$, $X_3 = 0^3 120210^{10} 1^2$, $X_4 = 0^{12} 12021012$.

Le code $(g_{10}^2)^+$, où les deux vecteurs de colle sont : $X_1 = x\,(x+y)$, $X_2 = (2x+y)\,x$.

Si $a_1 = -38$ alors $A_3 = 2$

On a deux codes auto- duaux inéquivalents :

le premier code est $(e_3 g_9 g_8)^+$, où les quatres vecteurs de colle sont : $X_1 = 0^3 1^3 0^6 102^2 0^4$,
$X_2 = 0^3 101^2 0^2 10^4 20^3 10$, $X_3 = 0^3 1020^4 12010^3 10^2$, $X_4 = 120^{10} 10^2 120^2 2$.

le deuxième code est $(e_3 f_8 f_4^2 f_1)^+$ de matrice génératrice

$$\begin{pmatrix}
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 0 \\
1 & 2 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} \tag{3.7}$$

Si $a_1 = -36$ alors $A_3 = 4$.

On a quatre codes auto- duaux inéquivalents :

le premier code est $(e_3^2 \eta_{14})^+$, où les deux vecteurs de colle sont :$X_1 = a0x$, $X_2 = 0ay$.

le deuxième code est $(e_3^2 h_{14})^+$, où les deux vecteurs de colle sont :$X_1 = a0x$, $X_2 = 0ay$.

le troisième code est $(e_3^2 p_{12} f2)^+$, où les trois vecteurs de colle sont :$X_1 = 00t_0'12$, $X_2 = a0t_3'01$, $X_3 = aa011$

le quatrième code est $(e_3^2 g_{10} f_4)^+$, où les quatres vecteurs de colle sont : $X_1 = 00x1200$, $X_2 = 00y0012$, $X_3 = a001111$, $X_4 = 0a02211$.

Si $a_1 = -34$ alors $A_3 = 6$

On a deux codes auto- duaux inéquivalents :

le premier code est $(e_3^2 g_{11})^+$, où les deux vecteurs de colle sont : $X_1 = aaa0$, $X_2 = 0a\bar{a}u$.

le deuxième code est $(e_3^2 \gamma_{11})^+$, où les trois vecteurs de colle sont : $X_1 = a00r$, $X_2 = 0a0s$, $X_3 = 0aat$.

Si $a_1 = -32$ alors $A_3 = 8$

On a un seul code auto- dual est $(e_3^4 g_8)^+$, où les quatres vecteurs de colle sont :

$X_1 = aa0010002000$, $X_2 = a\overline{a}0001000200$, $X_3 = 00aa00100020$, $X_4 = 000a\overline{a}00010002$

Si $a_1 = -30$ alors $A_3 = 10$

On a un seul code auto- dual est $(e_3^5 f_5)^+$, où les quatres vecteurs de colle sont :

$X_1 = 0aaaa10000$, $X_2 = a0aaa01000$, $X_3 = aa0aa00100$, $X_4 = aaa0a00010$, $X_5 = aaaa000001$.

Si $a_1 = -28$ alors $A_3 = 12$

On a un seul code auto- dual est $(e_3^6 f_2)^+$, où les quatres vecteurs de colle sont :

$X_1 = aaa00000$, $X_2 = 000aaa00$, $X_3 = 0a\overline{a}00011$, $X_4 = 0000a\overline{a}12$.

Si $a_1 \in \{-26, -24, -22, ..., 0\}$ alors $A_3 \in \{14, 16, 18, ..., 40\}$ il n'existe pas des composantes qui contiennent ce nombre des mots code de poids trois.

Le tableau suivant montre la classification de tous les codes ternaires auto- duaux inéquivalents pour $n = 4, ..., 20$ et l'ordre de groupe d'automorphismes pour vérifier le

nombre total des codes auto- duaux avec l'usage de la formule de masse.

n	d	le code	les vectedurs de colle	$\mid Aut\,(C)\mid$	le nombre des codes auto-duaux inéquivalents
4	3	t_4	(2.9)	48	1
8	3	t_4^2	–	4608	1
12	3	t_4^3	–	663552	3
		$(e_3^4)^+$	$aaa0, 0\overline{a}aa$	62208	
	6	g_{12}	(2.10)	190080	
16	3	t_4^4	_	127 401 984	7
		$t_4\,(e_3^4)^+$	_	2985 984	
		$t_4 g_{12}$	_	9123 840	
		$(e_3^4 f_4)^+$	$a0002111, 0a001211,$ $00a01121, 000a1112$	248 832	
		$(e_3^2 g_{10})^+$	$a0x, 0ay$	103 680	
		$(e_3 p_{13})^+$	at_0	67 392	
	6	h_{16}	$[I_8 \parallel H_8]$	43 008	
		t_4^5	_	30 576 476 160	
		$t_4^2\,(e_3^4)^+$	_	286 654 464	
		$t_4^2 g_{12}$	_	875 888 640	
		$t_4\,(e_3^4 f_4)^+$	_	11 943 936	
		$t_4\,(e_3^2 g_{10})^+$	_	4976 640	
		$t_4\,(e_3 p_{13})^+$	_	3234 816	
		$t_4 h_{16}$	_	2064 384	

20	3	$(e_3^6 f_2)^+$	$aaa00000,\ 000aaa00$ $0a\overline{a}00011,\ 0000a\overline{a}12$	13 436 928	
		$(e_3^5 f_5)^+$	$0aaaa10000, a0aaa01000, aa0aa00100$ $aaaa000001,\ aaa0a00010$	1866 240	
		$(e_3^4 g_8)^+$	$a^2 0^2 10^3 20^3, a\overline{a}0^3 10^3 20^2$ $0^2 a^2 0^2 10^3 20, 0^2 a\overline{a}0^3 10^3 2$	331 776	
		$(e_3^3 g_{11})^+$	$aaa0, 0a\overline{a}u$	20 528 640	
		$(e_3^3 \gamma_{11})^+$	$a00r, 0a0s, 0aat$	62 208	
		$(e_3^3 p_{12} f_2)^+$	$00t_0'12, a0t_0'01, aa011$	62 208	
		$(e_3^2 g_{10} f_4)^+$	$00x1200, 00y0012, a001111, 0a02211$	414 720	
		$(e_3^2 h_{14})^+$	$a0x, 0ay$	27 648	
		$(e_3^2 \eta_{14})^+$	$a0x, 0ay$	24 192	
		$(e_3 f_8 f_4^2 f_1)^+$	(3.7)	2304	
		$(e_3 g_9 g_8)^+$	$0^3 1^3 0^6 102^2 0^4, 0^3 1020^4 12010^3 10^2$ $0^3 101^2 0^2 10^4 20^3 10, 120^{10} 10^2 120^2 2$	6912	
	6	$(f_2^{10})^+$	(3.3)	3840	24
		$(f_4^4 f_2^2)^+$	(3.4)	512	
		$(f_4^5)^+$	(3.5)	10 240	
		$(f_5^4)^+$	(3.6)	1920	
		$(g_9^2 f_2)^+$	$1^3 0^6 1^3 0^8, 0^2 10^2 20^2 20^2 20^2 10^2 10^2$ $0^3 120210^{10} 1^2, 0^{12} 12021012$	10 368	
		$(g_{10}^2)^+$	$x\,(x+y)\,, (2x+y)\,x$	2073 600	

Conclusion

Dans notre travail, nous avons proposé une classification exhaustive des codes auto-duaux binaires de longueurs $n = 2, ..., 22$ et ternaires de longueurs $n = 4, ..., 20$.

Une classification qui donne pour chaque longueur la distance minimale, le type de code, une matrice génératrice, ainsi que le groupe d'automorphismes et par conséquent le nombre de codes équivalents et inéquivalents.

Dans la construction de ses codes, on a utilisé la méthode de collage (gluing method).

On a confirmé que les codes auto- duaux binaires de distance minimale deux sont des codes décomposables pour tout longueur n (avec i_2 comme une composante et un code auto- dual de longueur $n-2$), et pour les codes ternaires dont la distance minimale est égale à trois (distance minimale possible d'un code auto- dual ternaire) on a trouvé des codes décomposables avec t_4 comme une composante, et des codes indécomposables avec e_3 comme une composante.

À partir des éléments de l'algèbre $I(G)$ (où chaque élément est un polynôme énumérateurs des poids éventuel d'un certain code auto- dual on a pu déterminer les éléments de degré inférieur ou égal à 22 pour le cas binaire et de degré inférieur ou égal à 20 pour le cas ternaire. Pour le cas binaire (par exemple) la forme générale d'un élément de degré 24 dans $I(G_1)$ est

$$\begin{aligned} W_C(x,y) &= \left(x^2+y^2\right)^{12} + a_1\left(x^2+y^2\right)^8\left(x^2y^2\left(x^2-y^2\right)^2\right) + a_2\left(x^2+y^2\right)^4 \\ &\quad \times\left(x^2y^2\left(x^2-y^2\right)^2\right)^2 + a_3\left(x^2y^2\left(x^2-y^2\right)^2\right)^3 \\ &= x^{24} + (-6+a_2)\,x^{20}y^4 + (64+a_3)\,x^{18}y^6 + (399-4a_2-6a_3)\,x^{16}y^8 \\ &\quad + (960+15a_3)\,x^{14}y^{10} + (1260+6a_2-20a_3)\,x^{12}y^{12} + ... \end{aligned}$$

Le nombre de polynômes énumérateurs eventueles est égal au nombre de solutions du

système linéaire :

$$\begin{cases} a_2 \geq 6 \\ a_3 \geq -64 \\ 399 - 4a_2 - 6a_3 \geq 0 \\ 1260 + 6a_2 - 20a_3 \geq 0 \end{cases}$$

Existe-t-il des conditions supplémentaires (et avec quel moyen peut- on déterminer ces conditions) pour confirmer qu'un tel élément est un polynôme énumérateur du code auto-dual de longueur $n = 24$.

Peut être avec une méthode calculatoire (programation) on peut désigner les solutions valables pour déterminer ces codes pour n pair quelconque.

Bibliographie

[1] E. R. BERLEKAMP, F. J. MAC WILLIAMS et N. J. A. SLOANE, *Gleason's theorem on self-dual codes*, IEEE Transactions on Information Theory **18** (1972), 409-414.

[2] R. T. BILOUS, G. H. J. VAN REES, *An enumeration of binary self- dual codes of length 32,* Designs, Codes and cryptography, (2002), 61- 86.

[3] J. H. CONWAY, N. J. A. SLOANE, *A new upper bound on the minimal distance of self- dual codes*, IEEE Transactions on Information Theory **36** (1990), 1319- 1333.

[4] J. H. CONWAY, N. J. A. SLOANE, *Self- dual codes over the integers modulo 4*, Journal of Combinatorial Theory **A 62** (1993), 30- 45.

[5] J. S. LEON, V. PLESS et N. J. A. SLOANE, *On ternary self- dual codes of length 24*, IEEE Transactions on Information Theory **27** (1981), 1976- 1980.

[6] R. LIDL, G. PILZ, Applied abstract algebra, Springer- Verlag, New York, Berlin, Heidelberg, 1997.

[7] F. J. MAC WILLIAMS, C. L. MALLOWS et N. J. A. SLOANE, *Generalizations of Gleason's theorem on wieght enumerators of self- dual codes*, IEEE Transactions on Information Theory **18** (1972), 794- 805.

[8] F. J. MAC WILLIAMS, N. J. A. SLOANE, *The theory of error- correcting codes*, North- Holland, Amsterdam, 1986.

[9] C. L. MALLOWS, N. J. A. SLOANE, *An upper bound for self- dual codes*, Information and conrol **22** (1973), 188- 200.

[10] G. NEBE, E. M. RIAINS, N. J. A. SLOANE, Self- dual codes and invariants, Springer- Verelag, Berlin, Heidelberg 2006.

[11] S. NEDELOAIA, *Etude énumérateurs des poids des codes linéaires utilisant des formes décomposées des matrices génératrices*, Thése de doctorat, Université de Limoges 2005.

[12] A. OTMANI, *Code cortex et construction de code auto- duaux optimaux*, Thèse de doctorat, Université de Limoges, 2002.

[13] E. M. RAINS et N. J. A. SLOANE, *Self- dual codes in* HANDBOOK OF CODING THEORY,V. Pless and W. C. Huffman éd, Elsevier, Amsterdam, 1998.

[14] S. ROMAN, Coding and information theory, Springer- Verlag, New York, Berlin, Heidelberg, 1992.

[15] V.PLESS, *A classification of self- orthogonal codes over GF(2)*, Discrete Mathematics **3** (1972), 209- 246.

[16] V. PLESS, N. J. A. SLOANE et H. WARD, *Ternary self- dual codes of minimum weight 6 and the classification of self- dual codes of length 20*, IEEE Transactions on Information Theory **26** (1980), 305- 316.

[17] A. POLI, L. I. HUGUET, Codes correcteurs. Théorie et applications, Masson, Paris, 1988.

[18] N. J. A. SLOANE, *Error- correcting codes and invariant theory : New applications of a nineteenth.century technique*, Amer. Math. Monthly **84** (1977), 82- 107.

Résumé

Dans un code linéaire les paramètres suivants : longueur, dimension, distance minimale jouent un rôle fondamental dans sa détermination. Dans ce mémoire nous étudions d'une part une classe de codes correcteurs d'erreurs appelés codes auto- duaux, et leurs paramètres, aussi leurs polynôme énumérateurs des poids comme invariant du groupe détermine à partir de l'identité de Mac Williams et les propriétés de ses codes.

D'autre part on donne une classification exhaustive des codes auto- duaux inéquivalents pour les longueurs inférieure ou égale à 22 et une construction de ces codes en utilisant la méthode de collage, dans le cas binaire et ternaire.

Mots clés : code linéaire, code auto- dual, polynôme énumérateurs des poids, théorie des invariants, l'ombre du code, code sur $\mathbb{Z}_4$

Abstract

In linear code, the following parameters : length, minimal distance, dimension, play a fundamental role in its determination. In this thesis, we study a class of correctors codes called self dual codes and their polynomials weights enumerators like invariant of a group determined by the identity of Mac Williams and the properties of these codes.

In addition, one gives a classification of the self- dual codes in equivalents by length up 22 and a construction of codes by using the Gluing method in the binary and ternary case.

Key words : linear code, self dual codes, weight enumerators, invariant theory, Shadow code, code over $\mathbb{Z}_4$.