Université Paris 8 Vincennes - Saint Denis
Master de Mathématiques et Applications
Parcours Arithmétique, Codage et Cryptologie (ACC)

CODES OVER $\mathbb{Z}_4$

NGUYEN Doan Quan

Travail d'Étude et de Recherche
2020 - 2021

Enseignant: Martino Borello

Table de matières

1 Généralités

Un code $\mathbb{Z}_4$-linéaire de longueur n est un sous-group additif de $\mathbb{Z}_4^n$. On note aussi les éléments de $\mathbb{Z}_4$ des "vectors" même si $\mathbb{Z}_4$ n'est pas un espace vectoriel.

Exercice 1.1. *Soit $\mathcal{C}$ un code $\mathbb{Z}_4$-linéaire de longueur 4 avec 16 mots:*

$$\begin{array}{cccccccc} 0000, & 1113, & 2222, & 3331, & 0202, & 1311, & 2020, & 3133, \\ 0022, & 1131, & 2200, & 3313, & 0220, & 1333, & 2002, & 3111. \end{array}$$

(a) Montrer que tous les mots du $\mathcal{C}$ peuvent s'écrire sous forme $x\boldsymbol{c}_1 + y\boldsymbol{c}_2 + z\boldsymbol{c}_3$, avec $\boldsymbol{c}_1 = 1113$, $\boldsymbol{c}_2 = 0202$, $\boldsymbol{c}_3 = 0022$ et $x \in \mathbb{Z}_4$, $y, z \in \mathbb{Z}_2$.
(b) En déduire que $\mathcal{C}$ est un code $\mathbb{Z}_4$-linéaire

Proof. (a) On a pour $x \in \mathbb{Z}_4$ et $y, z \in \mathbb{Z}_2$

$$\begin{array}{lll} 0000 = 0.c_1 + 0.c_2 + 0.c_3 & 1113 = 1.c_1 + 0.c_2 + 0.c_3 & 2222 = 2.c_1 + 0.c_2 + 0.c_3 \\ 3331 = 3.c_1 + 0.c_2 + 0.c_3 & 0202 = 0.c_1 + 1.c_2 + 0.c_3 & 1311 = 1.c_1 + 1.c_2 + 0.c_3 \\ 2020 = 2.c_1 + 1.c_2 + 0.c_3 & 3133 = 3.c_1 + 1.c_2 + 0.c_3 & 0022 = 0.c_1 + 0.c_2 + 1.c_3 \\ 1131 = 1.c_1 + 0.c_2 + 1.c_3 & 2200 = 2.c_1 + 0.c_2 + 1.c_3 & 3313 = 3.c_1 + 0.c_2 + 1.c_3 \\ 0220 = 0.c_1 + 1.c_2 + 1.c_3 & 1333 = 1.c_1 + 1.c_2 + 1.c_3 & 2002 = 2.c_1 + 1.c_2 + 1.c_3 \\ & & 3111 = 3.c_1 + 1.c_2 + 1.c_3 \end{array}$$

(b) On a $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3$ forment une famille libre ($x\mathbf{c}_1 + y\mathbf{c}_2 + z\mathbf{c}_3 = 0 \leftrightarrow x = y = z = 0$ avec $x \in \mathbb{Z}_4$ et $y, z \in \mathbb{Z}_2$) donc $\mathcal{C}$ est un code $\mathbb{Z}_4$-linéaire. ■

On considère $\mathrm{G} = \begin{bmatrix} 1 & 1 & 1 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix}$ est une matrice génératrice de $\mathcal{C}$
Tous les mots du code $\mathcal{C}$ est écrit sous forme

$$\sum_{i=1}^{k_1} a_i c_i + \sum_{i=k_1+1}^{k_1+k_2} a_i c_i \quad avec \begin{cases} a_i \in \mathbb{Z}_4 & \text{if} \quad 1 \le i \le k_1 \\ a_i \in \mathbb{Z}_2 & \text{if} \quad k_1 + 1 \le i \le k_1 + k_2 \end{cases}$$

Le code $\mathcal{C}$ a $4^{k_1}2^{k_2}$ mots. Une matrice génératrice de $\mathcal{C}$ est la matrice $(k_1 + k_2) \times n$ sur $\mathbb{Z}_4$ dont les lignes sont des $\mathbf{c}_i$.

Défénition 1.2. *Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ sont des $\mathbb{Z}_4$-linéaires codes de longueur n.*

- *$\mathcal{C}_1$ et $\mathcal{C}_2$ sont permutation équivalence s'il existe $\mathcal{P}$ une matrice de permutation de taille n telle que $\mathcal{C}_2 = \mathcal{C}_1\mathcal{P}$.*
- *$\mathcal{C}_1$ et $\mathcal{C}_2$ sont monomialement équivalents s'il existe $\mathcal{M}$ une matrice monomialle de taille n avec les non zéros sont 1 ou 3, telle que $\mathcal{C}_2 = \mathcal{C}_1\mathcal{M}$.*

- *Le group des automorphismes de permutation $PAut(\mathcal{C})$ de $\mathcal{C}$ est le group des matrices de permutation P tel que $\mathcal{C}P = \mathcal{C}$.*
- *Le group des automorphismes monomials $MAut(\mathcal{C})$ de $\mathcal{C}$ est le group des matrices monomialles M avec les non zéros sont 1 ou 3, tel que $\mathcal{C}M = \mathcal{C}$.*□

Exercice 1.3. *Montrer que les $\mathbb{Z}_4$-linéaires codes avec matrices génératrices*

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix} et\, G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 0 & 0 & 2 \\ 0 & 2 & 0 & 2 \end{bmatrix}$$

sont monomialement équivalents.

Proof. On remarque que $G_2 = G_1\mathcal{M}$ avec $\mathcal{M} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$ est une matrice monomiale avec des coordonnées non nuls soient 1 ou 3.
Donc les codes $\mathbb{Z}_4$-linéaires avec matrices génératrices G_1 et G_2 sont monomialement équivalents. ■

Défénition 1.4. *Le code $\mathcal{C}$ a une matrice génératrice G en forme systématique si*

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

avec A, B_1, B_2 et C sont des matrices dans $\mathbb{Z}_2$, O est une matrice nulle de taille $k_2 \times k_1$. □

Théorème 1.5. *Tous les codes $\mathbb{Z}_4$-linéaires est permutation équivalence avec un code ayant une matrice génératrice en forme systématique*

On définie le produit scalaire modulo 4 sur $\mathbb{Z}_4^n$ par

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 + x_2y_2 + ... + x_ny_n \quad (mod 4)$$

avec $\mathbf{x} = x_1...x_n$ et $\mathbf{y} = y_1...y_n$.

On définie aussi le dual du code $\mathcal{C}$ est $\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{Z}_4^n | \mathbf{x} \cdot \mathbf{c} = 0, \forall \mathbf{c} \in \mathcal{C}\}$. On peut prouver facilement que $\mathbb{C}^\perp$ est aussi un code $\mathbb{Z}_4$-linéaire.

Si $\mathcal{C} \subseteq \mathcal{C}^\perp$ le code $\mathcal{C}$ est dit *auto-orthogonal*.

Si $\mathcal{C} = \mathcal{C}^\perp$, le code $\mathcal{C}$ est dit *auto-dual*.

Exercice 1.6. *$\mathcal{C}$ est un code $\mathbb{Z}_4$-linéaire. Montrer que $\mathcal{C}^\perp$ est aussi un code $\mathbb{Z}_4$-linéaire.*

Proof. Soit $x, y \in \mathcal{C}^\perp$ alors $x \cdot c = y \cdot c = 0, \forall c \in \mathcal{C}$.
Donc $(\lambda x + \mu y) \cdot c = \lambda(x \cdot c) + \mu(y \cdot c) = 0, \forall c \in \mathcal{C}$.
Ce qui implique $\lambda x + \mu y \in \mathcal{C}^\perp$ ■

Défénition 1.7. *Une matrice génératrice du code $\mathcal{C}^\perp$ est*

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

avec O est une $k_2 \times (n - k_1 - k_2)$ matrice nulle. En particulièrement, $\mathcal{C}^\perp$ a $4^{n-k_1-k_2}2^{k_2}$. □

Soit $\mathbf{x} \in \mathbb{Z}_4^n$. On suppose $n_a(\mathbf{x})$ le nombre de symbol de $\mathbf{x}$ qui est égal à a, avec $\forall a \in \mathbb{Z}_4^n$.

Défénition 1.8. *On définie le poids de Hamming est $wt_H(\boldsymbol{x}) = n_1(\boldsymbol{x}) + n_2(\boldsymbol{x}) + n_3(\boldsymbol{x})$; **le poids de Lee** est $wt_L(\boldsymbol{x}) = n_1(\boldsymbol{x}) + 2n_2(\boldsymbol{x}) + n_3(\boldsymbol{x})$; **le poids Eucli-dien** est $wt_E(\boldsymbol{x}) = n_1(\boldsymbol{x}) + 4n_2(\boldsymbol{x}) + n_3(\boldsymbol{x})$.*
La distance de Hamming, Lee et Eulidien entre $\boldsymbol{x}$ et $\boldsymbol{y}$ sont $d_H(x, y) = wt_H(x - y)$, $d_L(x, y) = wt_L(x - y)$, $d_E(x, y) = wt_E(x - y)$ respectivement. □

Théorème 1.9. *Soit $\mathcal{C}$ un code $\mathbb{Z}_4$-linéaire auto-orthogonal avec $\boldsymbol{c} \in \mathcal{C}$.*

- $wt_L(\boldsymbol{c}) \equiv 0 \bmod 2$
- $wt_E(\boldsymbol{c}) \equiv 0 \bmod 4$

Le **polynôme énumérateur des poids de Hamming** de $\mathcal{C}$ est $Ham_{\mathcal{C}}(x, y) = \sum_{\mathbf{c}\in\mathcal{C}} x^{wt_H(\mathbf{c})} y^{n-wt_H(\mathbf{c})}$; Le **polynôme énumérateur des poids de Lee** de $\mathcal{C}$ est $Lee_{\mathcal{C}}(x, y) = \sum_{\mathbf{c}\in\mathcal{C}} x^{wt_L(\mathbf{c})} y^{2n-wt_L(\mathbf{c})}$.
On obtient par conséquence

$$Ham^\perp_{\mathcal{C}}(x, y) = \frac{1}{|\mathcal{C}|} Ham_{\mathcal{C}}(y - x, y + 3x)$$

$$Lee^\perp_{\mathcal{C}}(x, y) = \frac{1}{|\mathcal{C}|} Lee_{\mathcal{C}}(y - x, y + x)$$

On note le **polynôme énumérateur des poids complet** est $cwe_{\mathcal{C}}(a, b, c, d) = \sum_{\mathbf{v}\in\mathcal{C}} a^{n_0(\mathbf{v})} b^{n_1(\mathbf{v})} c^{n_2(\mathbf{v})} d^{n_3(\mathbf{v})}$;

et le **polynôme énumérateur des poids symétrique** de $\mathcal{C}$ est $swe_{\mathcal{C}}(a, b, c) = \sum_{\mathbf{v}\in\mathcal{C}} a^{n_0(\mathbf{v})} b^{n_1(\mathbf{v})+n_3(\mathbf{v})} c^{n_2(\mathbf{v})}$

L'équation de Mac-William correspondant sont:

$$cwe_{\mathcal{C}^\perp}(a,b,c,d) = \frac{1}{\mathcal{C}} cwe_{\mathcal{C}}(a+b+c+d, a+ib-c-id,$$
$$a-b+c-d, a-ib-c+id).$$
$$swe_{\mathcal{C}^\perp}(a,b,c) = \frac{1}{\mathcal{C}} swe_{\mathcal{C}}(a+2b+c, a-c, a-2b+c).$$
$$\text{avec} \quad i = \sqrt{-1}$$

2 Codes binaires de code $\mathbb{Z}_4$-linéaire

Défénition 2.1. *On définie la notion de Fonction de Gray est* $\mathfrak{G} : \mathbb{Z}_4 \to \mathbb{F}_2^2$ *tel que*
$\mathfrak{G}(0) = 00$, $\mathfrak{G}(1) = 01$, $\mathfrak{G}(2) = 11$, $\mathfrak{G}(3) = 10$ □

Si $\mathcal{C}$ est un code $\mathbb{Z}_4$-linéaire, son image de Gray est son code binaire, noté $\mathfrak{G}(\mathcal{C})$. $\mathfrak{G}(\mathcal{C})$ est généralement non linéaire.

Remarque 2.2. $wt_L(v) = wt_H(\mathfrak{G}(v))$ *pour* $v \in \mathbb{Z}_4$

Un code $\mathcal{C}$ (dans $\mathbb{Z}_4$ ou $\mathbb{F}_4$) est distance invariante pourvu que le distribution de poids de Hamming de $\mathbf{c} + \mathcal{C}$ est invariant $\forall \mathbf{c} \in \mathcal{C}$.

Avec les codes binaires non linéaires, la distribution de la distance du code est plus significatif que la distribution de poids, puisque elle donne l'information de la capacité de corriger le code.
En rappelant que la distribution de distance de Hamming de $\mathcal{C}$ de longueur n est l'ensemble $\{B_i(\mathcal{C}) | 0 \leq i \leq n\}$ avec

$$B_i(\mathcal{C}) = \frac{1}{|\mathcal{C}|} \sum_{\mathbf{c} \in \mathcal{C}} |\{\mathbf{v} \in \mathcal{C} | d(\mathbf{v}, \mathbf{c}) = i\}|$$

avec $d(\mathbf{v}, \mathbf{c})$ est la distance de Hamming entre $\mathbf{v}$ et $\mathbf{c}$. $\{B_i(\mathcal{C}) | 0 \leq i \leq n\}$ est la moyenne de distribution de poids de $\mathbf{c}+\mathcal{C}$, $\forall \mathbf{c} \in \mathcal{C}$. Si le code est distance invariante, la distribution de distance est égale à la distribution de poids de n'importe quel ensemble $\mathbf{c} + \mathcal{C}$. Si de plus, le code contient le mot zéro, la distribution de distance est égale à la distribution de poids de $\mathcal{C}$.

On note désormais que le poids de Hamming du vecteur binaire $\boldsymbol{v}$ *est* $wt(\boldsymbol{v})$.

Théorème 2.3. *On a les assertions suivantes:*

1. *La fonction de Gray* $\mathfrak{G}$ *est la preservation de distance de* $\mathbb{Z}_4$ *avec distance de Lee à* $\mathbb{F}_2^{2n}$ *avec distance de Hamming.*
2. *Si* $\mathcal{C}$ *est un code* $\mathbb{Z}_4$*-linéaire, alors* $\mathfrak{G}(\mathcal{C})$ *est distance invariante.*

3. *Si $\mathcal{C}$ est un code $\mathbb{Z}_4$-linéaire, alors la distribution de poids de Hamming de $\mathfrak{G}(\mathcal{C})$ est égal à la distribution de poids de Lee de $\mathcal{C}$.*

Proof. On montre abord que si $a, b \in \mathbb{Z}_4$, alors $wt_L(a-b) = wt(\mathfrak{G}(a) + \mathfrak{G}(b))$. On considère:

- $a = b$, $wt_L(a-b) = 0 = wt(\mathfrak{G}(a) + \mathfrak{G}(b))$ $(\mathfrak{G}(a), \mathfrak{G}(b) \in \mathbb{Z}_2^2)$
- $a = b+1$, $wt_L(a-b) = 1 = wt(\mathfrak{G}(a)+\mathfrak{G}(b))$ $(01+00 = 01$ ou $11+01 = 10$ ou $10+11 = 01)$
- $a = b+2$, $wt_L(a-b) = 2 = wt(\mathfrak{G}(a) + \mathfrak{G}(b))$ $(wt_L(2) = 2 \times 1 = 2$; $11+00 = 11$ ou $10+01 = 11$ donc $wt(11) = 2)$.
- $a = b+3$, $wt_L(a-b) = 1 = wt(\mathfrak{G}(a) + \mathfrak{G}(b))$ $(wt_L(3) = 1$ et $wt(10+00) = wt(10) = 1)$

Comme $\mathfrak{G}(a), \mathfrak{G}(b) \in \mathbb{Z}_2$, alors $\mathfrak{G}(a) + \mathfrak{G}(b) = \mathfrak{G}(a) - \mathfrak{G}(b)$.
On note $\mathbf{v} = v_1...v_n$ et $\mathbf{w} = w_1...w_n$ sont dans $\mathbb{Z}_4^n$.
D'une part,
$d_L(\mathbf{v}, \mathbf{w}) = \sum_{i=1}^n wt_L(v_i - w_i) = \sum_{i=1}^n wt(\mathfrak{G}(v_i) - \mathfrak{G}(w_i)) = d(\mathfrak{G}(\mathbf{v}) - \mathfrak{G}(\mathbf{w}))$.

ce qui donne la première assertion.
D'autre part,
$wt_L(\mathbf{v} - \mathbf{w}) = \sum_{i=1}^n wt_L(v_i - w_i) = \sum_{i=1}^n wt(\mathfrak{G}(v_i) + \mathfrak{G}(w_i)) = wt(\mathfrak{G}(\mathbf{v}) + \mathfrak{G}(\mathbf{w}))$.

Donc la distribution de poids de Hamming de $\mathfrak{G}(\mathbf{c})+\mathfrak{G}(\mathcal{C})$ est égale à la distribution de poids de Lee de $\mathbf{c} - \mathcal{C} = \mathcal{C}$. C'est implique donc la $2^{ème}$ et $3^{ème}$ assertions. ■

On définie le produit par composant de deux vecteurs $\boldsymbol{v}$ et $\boldsymbol{w}$ dans $\mathbb{Z}_4^n$ est $\boldsymbol{v} * \boldsymbol{w}$.

Théorème 2.4. *Soit $\mathcal{C}$ un code $\mathbb{Z}_4$-linéaire. Le code binaire $\mathfrak{G}(\mathcal{C})$ est linéaire ssi pour $\boldsymbol{v}, \boldsymbol{w} \in \mathcal{C}$, $2(\boldsymbol{v} * \boldsymbol{w}) \in \mathcal{C}$.*

Proof. On peut montrer que si a et b sont dans $\mathbb{Z}_4$ alors
$\mathfrak{G}(a) + \mathfrak{G}(b) = \mathfrak{G}(a + b + 2ab)$. Alors si $\mathbf{v}$ et $\mathbf{w}$ sont dans $\mathbb{Z}_4^n$, $\mathfrak{G}(\mathbf{v}) + \mathfrak{G}(\mathbf{w}) = \mathfrak{G}(\mathbf{v} + \mathbf{w} + 2(\mathbf{v} * \mathbf{w}))$.
En particulier, si $\mathbf{v}$ et $\mathbf{w}$ sont dans $\mathcal{C}$, alors $\mathfrak{G}(\mathbf{v}) + \mathfrak{G}(\mathbf{w})$ est dans $\mathfrak{G}(\mathcal{C})$ ssi $\mathbf{v} + \mathbf{w} + 2(\mathbf{v} * \mathbf{w}) \in \mathcal{C}$. Cela implique que $2(\mathbf{v} * \mathbf{w}) \in \mathcal{C}$, car $\mathbf{v} + \mathbf{w} \in \mathcal{C}$. ■

Théorème 2.5. *On a les assertions suivantes:*

1. *Soit $\boldsymbol{u}$ et $\boldsymbol{v}$ sont dans $\mathbb{Z}_4^n$. Alors*
   $wt_E(\boldsymbol{u} + \boldsymbol{v}) \equiv wt_E(\boldsymbol{u}) + wt_E(\boldsymbol{v}) + 2(\boldsymbol{u} * \boldsymbol{v})$ (mod 8).
2. *Soit $\mathcal{C}$ un auto-orthogonal code $\mathbb{Z}_4$-linéaire dont tous les lignes $\boldsymbol{r}$ de son matrice génératrice G satisfait $wt_E(\boldsymbol{r}) \equiv 0$ (mod 8).*
   Donc $wt_E(\boldsymbol{c}) \equiv 0$ (mod 8), $\forall \boldsymbol{c} \in \mathcal{C}$.
3. *Soit $\mathcal{C}$ un code $\mathbb{Z}_4$-linéaire avec $wt_E(\boldsymbol{c}) \equiv 0$ (mod 8),$\forall \boldsymbol{c} \in \mathcal{C}$. Alors $\mathcal{C}$ est auto-orthogonal.*

***Example* 2.6.** *On définie octacode o_8 un code $\mathbb{Z}_4$-linéaire avec matrice génératrice*

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

Chaque ligne de G est orthogonale à elle-même et les lignes sont orthogonales deux par deux. Donc o_8 est auto-orthogonal, il est de type 4^4, le code est auto-dual.
D'après la théorème précédente, chaque ligne de G a le poids Euclidien égale à 8, donc tous les mots de o_8 ont le poids Euclidien est un multiple de 8, précisément égals à 8.
Le poids de Lee minimal de o_8 est 6. L'image de Gray $\mathfrak{G}(o_8)$ est un $(16, 256, 6)$ code binaire.

Exercice 2.7. *Dans cette exercice, on va montrer que $wt_L(o_8) = 6$. On a d'après théorème que tous les mots de o_8 ont le poids de Lee pairs; chaque ligne de son matrice génératrice a le poids de Lee 6.*

(a) Montrer qu'il n'y a pas de vecteur dans $\mathbb{Z}_4^n$ avec $wt_L = 2$ et $wt_E = 8$.

(b) Montrer que le seul vecteur dans $\mathbb{Z}_4^n$ avec $wt_L = 4$ et $wt_E = 8$ a exactement deux composants 2 et les autres sont nulles.

(c) En considérant la matrice génératrice G de o_8, montrer que o_8 n'a pas de mot de poids de Lee 4.

Proof.

(a) Soit $\mathbf{v} \in \mathbb{Z}_4^n$ avec $wt_L(\mathbf{v}) = 2$ et $wt_E(\mathbf{v}) = 8$.
Alors $wt_E(\mathbf{v}) - wt_L(\mathbf{v}) = 2n_2(\mathbf{v}) = 6$, donc $n_2(\mathbf{v}) = 3$, ce qui implique $wt_L(\mathbf{v}) \geq 6$, contradiction.
Donc il n'y a pas de vecteur dans $\mathbb{Z}_4^n$ avec $wt_L = 2$ et $wt_E = 8$.

(b) Soit $\mathbf{v} \in \mathbb{Z}_4^n$ avec $wt_L(\mathbf{v}) = 4$ et $wt_E(\mathbf{v}) = 8$.
Alors $wt_E(\mathbf{v}) - wt_L(\mathbf{v}) = 2n_2(\mathbf{v}) = 4$, donc $n_2(\mathbf{v}) = 2$. Dans ce cas là, le seul vecteur $\mathbf{v}$ qui satisfait a exactement deux composants 2 et les autres sont nulles.

(c) La matrice G de 0_8 est en forme systématique donc en considérant la combinaison de chaque pair de ses lignes dans $\mathbb{Z}_4$, on peut conclure qu'il n'y a pas de combinaison telle qu'on obtient un vecteur dans $\mathbb{Z}_4^n$ ayant deux composants 2 et les autres sont nulles. On conclut donc o_8 n'a pas de mot de poids de Lee 4. Le poids de Lee minimal de o_8 est donc égal à 6.

■

3 Codes cycliques dans $\mathbb{Z}_4$

On voit les mots du code cyclique $\mathbb{Z}_4$-linéaire $\mathbf{c} = c_0c_1...c_{n-1}$ de longueur n comme un polynôme $c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1} \in \mathbb{Z}_4[x]$. Si on considère le polynôme comme un élément du anneau quotient $\mathfrak{R}_n = \mathbb{Z}_4[x]/(x^n - 1)$, alors $xc(x)$ modulo $x^n - 1$ représente le SHIFT cyclique de $\mathbf{c}$.

En étudiant les codes cyclique dans $\mathbb{F}_q$, on trouve des polynômes générateurs et génère des idempotents de ces codes. Il est naturel de demander si un tel polynôme existe dans $\mathbb{Z}_4$. Pour ce fait, il faut étudier la factorisation de $x^n - 1$ dans $\mathbb{Z}_4$.

3.1 Factorisation de $x^n - 1$ dans $\mathbb{Z}_4$

On dit le polynôme $f(x) \in \mathbb{Z}_4$ est *irréductible* s'il y a $g(x), h(x) \in \mathbb{Z}_4[x]$ tels que $f(x) = g(x)h(x)$, alors $g(x)$ ou $h(x)$ est un unitaire.
En rappelant que dans $\mathbb{F}_q[x]$ on peut factoriser les polynômes non constants dans produit des polynômes írréductible, qui est unique par multiplication par un scalaire. Pourtant, ce n'est pas vrai en général avec des polynômes dans $\mathbb{Z}_4$.

On définit $\mu : \mathbb{Z}_4[x] \to \mathbb{F}_2[x]$ par $\mu(f(x)) = f(x) \bmod 2$. μ est déterminé par $\mu(0) = \mu(2) = 0$, $\mu(1) = \mu(3) = 1$ et $\mu(x) = x$.
μ est un homomorphisme d'anneau surjectif avec le noyau
$(2) = \{2s(x)|s(x) \in \mathbb{Z}_4[x]\}$. En particulier, c'est implique que si $f(x) \in \mathbb{F}_2[x]$, il existe $g(x) \in \mathbb{Z}_4[x]$ tel que $\mu(g(x)) = f(x)$; et deux tels $g(x)$ diffèrent par un élément $2s(x)$ pour $s(x) \in \mathbb{Z}_4[x]$. La fonction μ est appelé la *réduction homomorphisme.*

Défénition 3.1. *On définie*

- *Un polynôme $f(x) \in \mathbb{Z}_4[x]$ est dit irréductible de base si $\mu(f(x))$ est irréductible dans $\mathbb{F}_2[x]$; il est dit unitaire si son coefficient dominant est égal à 1.*
- *Un idéal $\mathcal{I}$ d'un anneau $\mathcal{R}$ est dit idéal premier si pour $ab \in \mathcal{I}$ implique soit $a \in \mathcal{I}$ ou $b^r \in \mathcal{I}$ pour r entier positif.*
- *Un polynôme $f(x) \in \mathbb{Z}_4[x]$ est primitif si l'idéal principal $(f(x)) = \{f(x)g(x)|g(x) \in \mathbb{Z}_4[x]\}$ est un idéal premier.*

Lemme 3.2. *Si $f(x) \in \mathbb{Z}_4[x]$ est un polynôme irréductible de base, alors $f(x)$ est un polynôme primitif.*

Proof. Supposons que $g(x)h(x) \in (f(x))$. Comme $\mu(f(x))$ est irréductible, $d = gcd(\mu(g(x)), \mu(f(x)))$ est soit 1 ou $\mu(f(x))$.
Si $d = 1$, il existe deux polynômes $a(x)$ et $b(x)$ dans $\mathbb{Z}_4[x]$ tels que $\mu(a(x))\mu(g(x))+\mu(ab(x))\mu(f(x)) = 1$. Comme $a(x)g(x)+b(x)f(x) = 1+2s(x)$ pour $s(x) \in \mathbb{Z}_4[x]$,

$a(x)g(x)h(x)(1+2s(x))+b(x)f(x)h(x)(1+2s(x))=h(x)(1+2s(x))^2=h(x)$.
Ça implique que $h(x)\in(f(x))$.
Supposons maintenant $d=\mu(f(x))$. Il existe alors $a(x)\in\mathbb{Z}_4[x]$ tel que $\mu(g(x))=\mu(f(x))\mu(a(x))$, implique $g(x)=f(x)a(x)+2s(x)$ pour $s(x)\in\mathbb{Z}_4[x]$. Alors $g(x)^2=(f(x)a(x))^2\in(f(x))$. Donc $f(x)$ est un polynôme primitif. ■

Défénition 3.3. *Si $\mathcal{R}\in\mathbb{Z}_4[x]$ ou $\mathbb{F}_2[x]$, $f(x)$ est premier avec $g(x)$ si $\mathcal{R}=(f(x))+(g(x))$.*

Exercice 3.4. *Soit $\mathcal{R}=\mathbb{Z}_4[x]$ ou $\mathbb{F}_2[x]$ et supposons que $f(x)$ et $g(x)$ sont polynômes dans $\mathcal{R}$. Montrer que $f(x)$ est premier avec $g(x)$ si et seulement s'il existe $a(x)$ et $b(x)$ dans $\mathcal{R}$ tel que $a(x)f(x)+b(x)g(x)=1$*

Proof. On a si $gcd(f(x),g(x))=1$ alors par algorithme d'Euclide, il existe $a(x)$ et $b(x)$ dans $\mathcal{R}$ tel que $a(x)f(x)+b(x)g(x)=1$.
Inversement, supposons qu'on a $a(x)f(x)+b(x)g(x)=1$ pour $a(x)$ et $b(x)$ dans $\mathcal{R}$ et $gcd(f(x),g(x))=d(x)$ avec $d(x)\in\mathcal{R}$. Alors $d(x)$ divise $a(x)f(x)$ et $d(x)$ divise $b(x)g(x)$, donc $d(x)$ divise $a(x)f(x)+b(x)g(x)$, implique $d(x)$ divise 1. Par conséquent $gcd(f(x),g(x))=1$. ■

Exercice 3.5. *Soit $\mathcal{R}=\mathbb{Z}_4[x]$ ou $\mathbb{F}_2[x]$. Soit $k\geq 2$. Montrer que pour $f_i(x)$ des polynômes qui sont premiers deux à deux avec $1\leq i\leq k$, alors $f_1(x)$ est premier avec $f_2(x)f_3(x)...f_k(x)$*

Proof. On a $f_1(x)$ est premier à $f_i(x)$ avec $1\leq i\leq k$. Donc il existe $a_i(x)\in\mathcal{R}$ tel que:
$a_1(x)f_1(x)+a_2(x)f_2(x)=1$
$a_1(x)f_1(x)+a_3(x)f_3(x)=1$
$a_1(x)f_1(x)+a_4(x)f_4(x)=1$
...
$a_1(x)f_1(x)+a_k(x)f_k(x)=1$
En multipliant deux premiers équations, on a $f_1(x)(a_1^2(x)+a_1(x)a_3(x)f_3(x)+a_1(x)a_2(x)f_2(x))+a_2(x)a_3(x)f_2(x)f_3(x)=1$. Donc $f_1(x)$ est premier avec $f_2(x)f_3(x)$.
En continuant par induction, on obtient le résultat. ■

Lemme 3.6. *Soient $f(x),g(x)\in\mathbb{Z}_4[x]$. $f(x)$ est premier avec $g(x)$ si et seulement si $\mu(f(x))$ est premier avec $\mu(g(x))$ dans $\mathbb{F}_2[x]$.*

Proof. Supposons que $f(x)$ est premier avec $g(x)$. Par **exercice 3.4**, il existe $a(x),b(x)\in\mathbb{Z}_4[x]$ tel que $a(x)f(x)+b(x)g(x)=1$. Alors $\mu(a(x))\mu(f(x))+\mu(b(x))\mu(g(x))=\mu(1)=1$, donc $\mu(f(x))$ est premier avec $\mu(g(x))$.
Inversement, supposons maintenant que $\mu(f(x))$ est premier avec $\mu(g(x))$. Il existe alors $a(x),b(x)\in\mathbb{Z}_4[x]$ tel que $\mu(a(x))\mu(f(x))+\mu(b(x))\mu(g(x))=1$. Comme $a(x)f(x)+b(x)g(x)=1+2s(x)$ pour $s(x)\in\mathbb{Z}_4[x]$, alors $a(x)(1+2s(x))f(x)+b(x)(1+2s(x))g(x)=(1+2s(x))^2=1$, implique $f(x)$ est premier avec $g(x)$. ■

Théorème 3.7. ***(Lemme de Hensel)*** *Soit $f(x) \in \mathbb{Z}_4[x]$. Supposons $\mu(f(x)) = h_1(x)h_2(x)...h_k(x)$ avec $h_1(x), h_2(x), ..., h_k(x)$ sont deux à deux premiers dans $\mathbb{F}_2[x]$. Alors il existe $g_1(x), g_2(x), ..., g_k(x)$ dans $\mathbb{Z}_4[x]$ tel que*

1. *$\mu(g_i(x)) = h_i(x)$ pour $1 \leq i \leq k$.*
2. *$g_1(x), g_2(x), ..., g_k(x)$ sont premiers deux à deux.*
3. *$f(x) = g_1(x)g_2(x)...g_k(x)$.*

Proof. On montre par récurrence sur k.
Suppose $k = 2$. Choisir $g_1'(x), g_2'(x) \in \mathbb{Z}_4[x]$ tel que $\mu(g_1'(x)) = h_1(x)$ et $\mu(g_2'(x)) = h_2(x)$. Alors $f(x) = g_1'(x)g_2'(x) + 2s(x)$ pour $s(x) \in \mathbb{Z}_4[x]$. Comme $h_1(x)$ est premier avec $h_2(x)$, donc $g_1'(x)$ est premier avec $g_2'(x)$ (**Lemme 2**). Alors il existe $a_i(x) \in \mathbb{Z}_4[x]$ tel que $a_1(x)g_1'(x) + a_2(x)g_2'(x) = 1$ par **exercice 3.4**. Posons $g_1(x) = g_1'(x)+2a_2(x)s(x)$ et $g_2(x) = g_2'(x)+2a_1(x)s(x)$. On a alors $\mu(g_i(x)) = \mu(g_i'(x)) = h_i(x)$, qui donne (1). Et comme $h_1(x)$ est premier avec $h_2(x)$, $\mu(g_1(x))$ est premier avec $\mu(g_2(x))$, d'où $g_1(x)$ est premier avec $g_2(x)$, qui donne (2). De plus $g_1(x)g_2(x) = g_1'(x)g_2'(x) + 2(a_1(x)g_1'(x) + a_2(x)g_2'(x))s(x) = g_1'(x)g_2'(x) + 2s(x) = f(x)$, d'où vient (3).
Supposons maintenant que $k = 3$. On a par **exercice 3.5**, $h_1(x)$ est premier avec $h_2(x)h_3(x)$. Il existe polynôme $g_1(x)$ premier avec $g_{23}(x)$ dans $\mathbb{Z}_4[x]$ tel que $\mu(g_1(x)) = h_1(x)$, $\mu(g_{23}(x)) = h_2(x)h_3(x)$, et $f(x) = g_1(x)g_{23}(x)$. Comme $h_2(x)$ est premier avec $h_3(x)$, il existe deux polynômes $g_2(x)$ et $g_3(x)$ qui sont premiers entre eux tels que $\mu(g_2(x)) = h_2(x)$, $\mu(g_3(x)) = h_3(x)$ et $g_{23}(x) = g_2(x)g_3(x)$.
Par récurrence, on déduit le théorème pour tous les k. ■

Corollaire 3.8. *Soit $f(x) \in \mathbb{Z}_4[x]$. Supposons que tous les racines de $\mu(f(x))$ sont distinctes. Alors $f(x)$ est irréductible si et seulement si $\mu(f(x))$ est irréductible.*

Proof. Si $\mu(f(x))$ est réductible, alors il factorise aux polynômes irréductibles comme tous les racines de $\mu(f(x))$ sont distinctes. Par le **lemme de Henssel**, $f(x)$ peut factorise aux polynômes irréductibles de base, qui ne sont pas unitaires (par exercice précédente), donc $f(x)$ est réductible. Supposons maintenant que $f(x) = g(x)h(x)$, avec $g(x)$ et $h(x)$ ne sont pas unitaires. Alors $\mu(f(x)) = \mu(g(x))\mu(h(x))$ avec $\mu(g(x))$ et $\mu(h(x))$ ne sont pas unitaires. ■

Défénition 3.9. *Un élément non nul a dans un anneau $\mathcal{R}$ est dit un* ***diviseur de zéro*** *s'il existe un élément non nul $b \in \mathcal{R}$ tel que $ab = 0$.*
Un ***polynôme ordinaire*** *dans $\mathbb{Z}_4[x]$ est n'importe quel polynôme non nul qui n'est pas un diviseur de zéro.*

Lemme 3.10. *Soit $f(x)$ un polynôme ordinaire dans $\mathbb{Z}_4[x]$. Il existe alors un polynôme monique $f'(x)$ et un polynôme unitaire $u(x)$ dans $\mathbb{Z}_4[x]$ tels que $\mu(f'(x)) = \mu(f(x))$ et $f'(x) = u(x)f(x)$.*

Comme $\mathbb{F}_2[x]$ est un anneau factoriel, $\mu(x^n - 1) = x^n + 1 \in \mathbb{F}_2[x]$ peut factoriser dans $h_1(x)h_2(x)...h_k(x)$ avec $h_1(x), h_2(x), ..., h_k(x)$ sont polynômes irréductibles. Dans le cas n impair, ils sont premiers deux à deux, et par le

lemme de Hensel, $x^n - 1 = g_1(x)g_2(x)...g_k(x)$ avec $g_i(x) \in \mathbb{Z}_4[x]$ qui sont polynômes irréductibles de base, deux à deux premiers, tel que $\mu(g_i(x)) = h_i(x)$. Comme les $g_i(x)$ sont polynômes irréductibles de base, par le **lemme 3.2**, ils sont polynôme primitif.
Le polynôme $x^n - 1$ n'est pas un diviseur de zéro dans $\mathbb{Z}_4[x]$ donc il est ordinaire. Par le théorème de factorisation, on peut le factoriser dans polynôme irréductible de base qui est unique par multiplication. Comme les $g_i(x)$ sont polynôme irréductible de base donc par la **corollaire 3.7**, ils sont alors irréductible. Par le **lemme 3.9**, comme les $g_i(x)$ sont ordinaire, il existe alors un polynôme monique $g_i'(x) \in \mathbb{Z}_4[x]$ tel que $\mu(g_i'(x)) = \mu(g_i(x))$ et $g_i'(x) = u_i(x)g_i(x)$ pour $u_i(x) \in \mathbb{Z}_4[x]$ un polynôme unitaire. Chaque $g_i'(x)$ est irréductible.

Théorème 3.11. *Soit n est un nombre impair. Alors* $x^n - 1 = g_1(x)g_2(x)...g_k(x)$ *avec* $g_i(x) \in \mathbb{Z}_4[x]$ *sont des uniques polynômes unitaires irréductibles (et irréductible de base) qui sont deux à deux premier dans* $\mathbb{Z}_4[x]$.
De plus, $x^n + 1 = \mu(g_1(x))\mu(g_2(x))...\mu(g_k(x))$ *est un factorisation dans polynômes irréductibles dans* $\mathbb{F}_2[x]$.

La preuve du *lemme de Hensel* nous donne un méthode pour factoriser $x^n - 1$ dans $\mathbb{Z}_4[x]$. On introduit maintenant un autre méthode s'appelant *méthode de Graeffe* qui produira un factorisation.

1. Soit $h(x)$ un facteur irréductible de $x^n + 1$ dans $\mathbb{F}_2[x]$. On écrit $h(x) = e(x) + o(x)$ avec $e(x)$ est la somme des termes de $h(x)$ avec l'exposant pair, $o(x)$ est la somme des termes de $h(x)$ avec l'exposant impair.
2. Alors $g(x)$ est le facteur irréductible de $x^n - 1$ dans $\mathbb{Z}_4[x]$ avec $\mu(g(x)) = h(x)$ et $g(x^2) = \pm(e(x)^2 - o(x)^2)$.

***Example* 3.12.** *Dans* $\mathbb{F}_2[x]$, $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$. *On applique la méthode de Graeffe à chaque facteur pour obtenir la factorisation de* $x^7 + 1$ *dans polynômes irréductibles unitaires dans* $\mathbb{Z}_4[x]$.

- *Si* $h(x) = x+1$ *alors* $e(x) = 1$, $o(x) = x$. *Donc* $g(x^2) = -(1-x^2) = x^2-1$, *d'où* $g(x) = x - 1$.
- *Si* $h(x) = x^3 + x + 1$ *alors* $e(x) = 1$, $o(x) = x^3 + x$. *Donc* $g(x^2) = x^6 + 2x^4 + x^2 - 1$, *d'où* $g(x) = x^3 + 2x^2 + x - 1$.
- *Si* $h(x) = x^3 + x^2 + 1$ *alors* $e(x) = x^2 + 1$, $o(x) = x^3$. *Donc* $g(x^2) = x^6 - x^4 - 2x^2 - 1$, *d'où* $g(x) = x^3 - x^2 - 2x - 1$.

Donc $x^7 - 1 = (x - 1)(x^3 + 2x^2 + x - 1)(x^3 - x^2 + 2x - 1)$ *est la factorisation de* $x^7 - 1$ *dans polynômes irréductibles unitaires dans* $\mathbb{Z}_4[x]$.

Remarque 3.13.

- $x^9 + 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$ *dans* $\mathbb{F}_2[x]$ *; et* $x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$ *dans* $\mathbb{Z}_4[x]$.

- $x^{15}+1=(x+1)(x^2+x+1)(x^4+x^3+1)(x^4+x+1)(x^4+x^3+x^2+x+1)$ *dans* $\mathbb{F}_2[x]$ *; et*
  $x^{15}-1=(x-1)(x^2+x+1)(x^4-x^3+2x^2+1)(x^4+2x^2-x+1)(x^4+x^3+x^2+x+1)$.

Exercice 3.14.

(a) Supposons que n est impair et la factorisation de x^n+1 dans polynômes irréductibles dans $\mathbb{F}_2[x]$ est $x^n+1=(x+1)(x^{n-1}+x^{n-2}+...+x+1)$. Montrer que la factorisation de x^n-1 dans polynômes irréductibles unitaires dans $\mathbb{Z}_4[x]$ est $x^n-1=(x-1)(x^{n-1}+x^{n-2}+...+x+1)$.

(b) Montrer que pour $n=3,5,11,13$ et 19, la factorisation de x^n-1 dans $\mathbb{Z}_4[x]$ est donné par (a).

Proof.

(a) On a $(x+1)(x^{n-1}+x^{n-2}+...+x+1)=x^n+x^{n-1}+x^{n-1}+x^{n-2}+x^{n-2}+...+x^2+x+x+1=x^n+1$ dans $\mathbb{F}_2[x]$.
Aussi, $(x-1)(x^{n-1}+x^{n-2}+...+x+1)=x^n-x^{n-1}+x^{n-1}-x^{n-2}+x^{n-2}-...+x^2-x+x-1=x^n-1$ dans $\mathbb{Z}_4[x]$.

(b) $x^3+1=(x+1)(x^2+x+1)$ dans $\mathbb{F}_2[x]$; et $x^3-1=(x-1)(x^2+x+1)$ dans $\mathbb{Z}_4[x]$
$x^5+1=(x+1)(x^4+x^3+x^2+x+1)$ dans $\mathbb{F}_2[x]$; et $x^5-1=(x-1)(x^4+x^3+x^2+x+1)$ dans $\mathbb{Z}_4[x]$
$x^{11}+1=(x+1)(x^{10}+x^9+...+x+1)$ dans $\mathbb{F}_2[x]$; et $x^{11}-1=(x-1)(x^{10}+x^9+...+x+1)$ dans $\mathbb{Z}_4[x]$
$x^{13}+1=(x+1)(x^{12}+x^{11}+...+x+1)$ dans $\mathbb{F}_2[x]$; et $x^{13}-1=(x-1)(x^{12}+x^{11}+...+x+1)$ dans $\mathbb{Z}_4[x]$
$x^{19}+1=(x+1)(x^{18}+x^{17}+...+x+1)$ dans $\mathbb{F}_2[x]$; et $x^{19}-1=(x-1)(x^{18}+x^{17}+...+x+1)$ dans $\mathbb{Z}_4[x]$

■

3.2 Anneau $\mathfrak{R}_n=\mathbb{Z}_4[x]/(x^n-1)$

Afin d'étudier les code cyclique dans $\mathbb{Z}_4[x]$, on a besoin de trouver l'idéal de $\mathfrak{R}_n$. Premièrement on a besoin de connaître la structure de l'idéal de $\mathbb{Z}_4[x]/(f(x))$ avec $f(x)$ est un polynôme irréductible de base.

Exercice 3.15. *Montrer que si $\mathcal{I}$ est un idéal d'un anneau $\mathcal{R}$ et $\mathcal{I}$ contient un élément inversible, alors $\mathcal{I}=\mathcal{R}$.*

Proof. Soit $a\in\mathcal{I}$, a est inversible. Alors $1=a^{-1}a\in\mathcal{I}$. Comme $1\in\mathcal{I}$ donc pour tout $x\in\mathcal{R}$, $x=1\cdot x\in\mathcal{I}$. Alors $\mathcal{R}\subseteq\mathcal{I}$ ce qui implique $\mathcal{I}=\mathcal{R}$ ■

Lemme 3.16. *Si $f(X)$ est un polynôme irréductible de base, alors $\mathcal{R}=\mathbb{Z}_4[x]/(f(x))$ a seulement 3 idéals: $(0),(2)=2s(x)+(f(x))|s(x)\in\mathbb{Z}_4[x]$ et $(1)=\mathcal{R}$.*

Proof. Supposons $\mathcal{I}$ est un idéal non nul de $\mathcal{R}$. Soit $g(x)+(f(x)) \in \mathcal{I}$ avec $g(x) \notin (f(x))$. Comme $f(x)$ est irréductible, $\mu(f(x))$ est irréductible, $pgcd(\mu(g(x)), \mu(f(x)))$ est soit 1 ou $\mu(f(x))$. Comme on a montré dans la démonstration du **Lemme 3.2**, pour $a(x)$, $b(x)$ et $s(x)$ dans $\mathbb{Z}_4[x]$, soit $a(x)g(x) + b(x)f(x) = 1 + 2s(x)$, soit $g(x) = a(x)f(x) + 2s(x)$:
Soit $a(x)g(x) + b(x)f(x) = 1 + 2s(x)$, alors $a(x)g(x)(1 + 2s(x)) + b(x)f(x)(1 + 2s(x)) = (1 + 2s(x))^2 = 1$, implique $a(x)(1 + 2s(x)) + (f(x))$ est inverse de $g(x) + (f(x))$ qui est dans $\mathcal{R}$. Alors $\mathcal{I}$ contient un élément inversible, donc par exercice précédente, $\mathcal{I} = \mathcal{R}$.
Soit $g(x) = a(x)f(x)+2s(x)$, alors $g(x)+(f(x)) \in (2)$ et donc $\mathcal{I} \subseteq (2)$. Comme $\mathcal{I} \neq 0$, il existe $h(x) \in \mathbb{Z}_4[x]$ tel que $2h(x)+(f(x)) \in \mathcal{I}$ avec $2h(x) \notin (f(x))$. Supposons que $\mu(h(x)) \in \mu(f(x))$, alors $h(x) = a(x)f(x) + 2s(x)$ pour $a(x), s(x) \in \mathbb{Z}_4[x]$, implique $2h(x) = 2a(x)f(x) \in (f(x))$, contradiction. Donc $\mu(h(x)) \notin \mu(f(x))$ et comme $\mu(f(x))$ est irréductible, $pgcd(\mu(f(x)), \mu(h(x))) = 1$. Ça implique $a(x)h(x) + b(x)f(x) = 1 + 2s(x)$ pour $a(x), b(x), s(x) \in \mathbb{Z}_4[x]$. Alors $a(x)(2h(x))+2b(x)f(x) = 2$ donc $2+(f(x)) \in \mathcal{I}$ et donc $(2) \subseteq \mathcal{I}$. Par conséquent $\mathcal{I} = (2)$. ■

Lemme 3.17. *Soit $m(x)$ un polynôme unitaire de degré r dans $\mathbb{Z}_4[x]$. Alors $\mathbb{Z}_4[x]/(m(x))$ a 4^r éléments et tous les éléments de $\mathbb{Z}_4[x]/(m(x))$ est exprimable uniquement dans la forme $a(x) + (m(x))$ avec $a(x)$ est le polynôme zéro ou polynôme de degré inférieur à r.*

Proof. Soit $a(x) = a_d x^d + a_{d-1}x^{d-1} + ... + a_0 \in \mathbb{Z}_4[x]$. Si $d \geq r$, alors $b(x) = a(x)-a_d x^{d-r}m(x)$ a degré inférieur à d et $a(x)+(m(x)) = b(x)+(m(x))$. Par conséquent tous les éléments de $a(x) + (m(x)) \in \mathbb{Z}_4[x]/(m(x))$ ont un représentant de degré inférieur à r.
De plus, si on a $b_1(x) + (m(x)) = b_2(x) + (m(x))$ avec $b_i(x)$ sont polynômes de degré inférieur à r, alors $b_1(x) - b_2(x)$ est un multiple de $m(x)$. Comme $m(x)$ est un polynôme unitaire de degré r, si $h(x)$ est un polynôme non nul de degré s, alors $h(x)m(x)$ a polynôme de degré $r+s$, qui est supérieur égal à r. En plus, comme $b_i(x)$ sont polynômes de degré inférieur à r, $b_1(x) - b_2(x)$ est polynôme de degré inférieur à r. Ce qui implique à $b_1(x) = b_2(x)$. Donc il est nécessaire que $a(x)$ est un polynôme de degré inférieur à r. ■

Un idéal principal de $\mathfrak{R}_n$ est généré par un élément $g(x)+(x^n-1)$; pour éviter les confusions avec la notion de l'idéal dans $\mathbb{Z}_4[x]$, on note cet idéal principal $\langle g(x) \rangle$.

Lemme 3.18. *Soit n impair. Supposons que $m(x)$ est un polynôme unitaire de degré r qui est un produit des facteur irréductibles distincts de x^n-1 dans $\mathbb{Z}_4[x]$. Alors l'idéal $\langle m(x) \rangle$ de $\mathfrak{R}_n$ a 4^{n-r} éléments et tous les éléments de $\langle m(x) \rangle$ est exprimé uniquement dans la forme $m(x)a(x)$, avec $a(x)$ est un polynôme zéro ou polynôme de degré inférieur à $n - r$.*

Proof. Par le **théorème 3.10**, il existe un polynôme unitaire $h(x)$ de degré $n - r$ tel que $m(x)h(x) = x^n - 1$. Tous les éléments $(f(x))$ de $\langle m(x) \rangle$ a forme $m(x)a(x)$. On choisit $a(x)$ de degré le plus petit tel que $f(x) = m(x)a(x)$

dans $\mathfrak{R}_n$. Si $a(x) = a_d x^d + a_{d-1}x^{d-1} + ... + a_0$ avec $a_d \neq 0$ et $d \geq n - r$, alors $b(x) = a(x) - a_d x^{d-n+r} h(x)$ a degré inférieur à d. Donc $m(x)b(x) = m(x)a(x) - a_d x^{d-n+r}(x^n - 1)$ dans $\mathbb{Z}_4[x]$, implique $f(x) = m(x)a(x) = m(x)b(x)$ dans $\mathfrak{R}_n$, contradiction avec le choix de $a(x)$.
Par conséquent, tous les éléments de $\langle m(x)\rangle$ a forme $m(x)a(x)$ avec $a(x)$ de degré inférieur à $n - r$. De plus, si $m(x)a_1(x) = m(x)a_2(x)$ dans $\mathfrak{R}_n$ avec tous les $a_i(x)$ ont degré inférieur à $n - r$, alors $m(x)(a_1(x) - a_2(x))$ a degré inférieur à n dans $\mathbb{Z}_4[x]$ et aussi est un multiple de $x^n - 1$. Par le même raisonnement qu'avant $a_1(x) = a_2(x)$. ■

Théorème 3.19. *Soit n est impair et $x^n - 1 = g_1(x)g_2(x)...g_k(x)$ est un factorisation de $x^n - 1$ dans polynômes unitaires irréductibles qui sont deux à deux premiers dans $\mathbb{Z}_4[x]$. Soit $\hat{g}_i(x) = \prod_{j\neq i} g_j(x)$. Supposons que $g_i(x)$ a degré d_i. On a les assertions suivantes:*

(a) $\mathfrak{R}_n$ a 4^n éléments

(b) Si $1 \leq i \leq k$, $\mathfrak{R}_n = \langle g_i(x)\rangle \oplus \langle \hat{g}_i(x)\rangle$

(c) $\mathfrak{R}_n = \langle \hat{g}_1(x)\rangle \oplus \langle \hat{g}_2(x)\rangle \oplus ... \oplus \langle \hat{g}_k(x)\rangle$

(d) Si $1 \leq i \leq k$, $\langle \hat{g}_i(x)\rangle = \langle \hat{e}_i(x)\rangle$ avec $\langle \hat{e}_i(x)\rangle | 1 \leq i \leq k$ sont idempotents orthogonaux par paire de $\mathfrak{R}_n$, et $\sum_{i=1}^k \hat{e}_i(x) = 1$

(e) Si $1 \leq i \leq k$, $\langle \hat{g}_i(x)\rangle \approx \mathbb{Z}_4[x]/(g_i(x))$ et $\langle \hat{g}_i(x)\rangle$ a 4^{d_i} éléments

(f) Tous les idéals de $\mathfrak{R}_n$ est un somme direct de $\langle \hat{g}_i(x)\rangle$ et $\langle 2\hat{g}_i(x)\rangle$.

3.3 Générer polynômes du codes cycliques dans $\mathbb{Z}_4$

Théorème 3.20. *Soit $\mathcal{C}$ un code cyclique dans $\mathbb{Z}_4$ de longueur n impair. Alors il existe des polynômes unitaires uniques $f(x), g(x)$ et $h(x)$ tel que $x^n - 1 = f(x)g(x)h(x)$ et $\mathcal{C} = \langle f(x)g(x)\rangle \oplus \langle 2f(x)h(x)\rangle$. En plus, $\mathcal{C}$ est de type $4^{deg(h)}2^{deg(g)}$.*

Proof. Par le **théorème 3.18** $\mathcal{C}$ est un somme direct de $\langle \hat{g}_i(x)\rangle$ et $\langle 2\hat{g}_i(x)\rangle$ avec $x^n - 1 = g_1(x)g_2(x)...g_k(x)$. On va réordonner les $g_i(x)$ tel que $\mathcal{C} = \sum_{i=1}^a \langle \hat{g}_i(x)\rangle \oplus \sum_{i=a+1}^b \langle 2\hat{g}_i(x)\rangle$. Soit $f(x) = \prod_{i=b+1}^k g_i(x), g(x) = \prod_{i=a+1}^b g_i(x)$ et $h(x) = \prod_{i=1}^a g_i(x)$. Donc $x^n - 1 = f(x)g(x)h(x)$. Comme $\hat{g}_i(x)$ est un multiple de $f(x)g(x)$ avec $1 \leq i \leq a$; on a $\sum_{i=1}^a \langle \hat{g}_i(x)\rangle \subseteq \langle f(x)g(x)\rangle$. Par le **lemme 3.17**, $\langle f(x)g(x)\rangle$ est de type $4^{n-deg(fg)} = 4^{deg(h)}$, qui est aussi la taille de $\sum_{i=1}^a \langle \hat{g}_i(x)\rangle$ par **théorème 3.18**(c) et (e). Donc $\sum_{i=1}^a \langle \hat{g}_i(x)\rangle = \langle f(x)g(x)\rangle$. Par le même argument, on peut montrer que $\sum_{i=1}^a \langle 2\hat{g}_i(x)\rangle = \langle 2f(x)h(x)\rangle$. Comme tous les polynômes unitaires facteurs de $x^n - 1$ doivent factoriser dans produit des polynômes irréductibles de base qui sont le produit des uniques $g_i(x)$ par **théorème 3.10**. Comme $\langle f(x)g(x)\rangle$ est de type $4^{deg(h)}$ et $\langle 2f(x)h(x)\rangle$ est de type $2^{deg(g)}$, $\mathcal{C}$ est de type $4^{deg(h)}2^{deg(g)}$ ■

Exercice 3.21. *Soit n est impair et $m(x)$ est un produit des facteurs unitaires irréductibles de $x^n - 1$ de $\mathbb{Z}_4[x]$ de dégré r. Montrer que l'idéal $\langle 2m(x)\rangle$ de $\mathfrak{R}_n$ a 2^{n-r} et tous les éléments de $\langle 2m(x)\rangle$ est exprimé uniquement dans la forme*

$2m(x)a(x)$ *avec* $a(x)$ *de dégré inférieur à* $n-r$ *et avec les coefficients que 0 et 1.*

Proof. $m(x)$ est un produit des facteurs unitaires irréductibles de x^n-1 donc $m(x)$ est un polynôme unitaire de dégré r. Donc $2m(x)$ est un polynôme ayant les coefficients que 0 et 2. Par le même raisonnement dans **lemme 3.18**, on arrive au résultats. ■

Corollaire 3.22. *Si* $g(x)=1$, *alors* $\mathcal{C}=\langle f(x)\rangle$ *et* $\mathcal{C}$ *est de type* $4^{n-deg(f)}$;
Si $h(x)=1$, *alors* $\mathcal{C}=\langle 2f(x)\rangle$ *et* $\mathcal{C}$ *est de type* $2^{n-deg(f)}$

Corollaire 3.23. *Soit n un nombre impair. Supposons que* x^n-1 *est le produit de k polynômes irréductibles dans* $\mathbb{Z}_4[x]$. *Alors il y a* 3^k *codes cycliques de longueur n dans* $\mathbb{Z}_4[x]$.

Proof. Soit $x^n-1=g_1(x)g_2(x)...g_k(x)$ est une factorisation de x^n-1 dans polynômes unitaires irréductibles. Si $\mathcal{C}$ est un code cyclique, par **théorème 3.19**, $\mathcal{C}=\langle f(x)g(x)\rangle\oplus\langle 2f(x)h(x)\rangle$ avec $x^n-1=f(x)g(x)h(x)$. Chaque $g_i(x)$ est le facteur d'un seul de $f(x)$, $g(x)$ ou $h(x)$. Donc il y a 3^k codes cycliques de longueur n dans $\mathbb{Z}_4[x]$. ■

Example* 3.24.** *On a* $x^7-1=g_1(x)g_2(x)g_3(x)$ *avec* $g_1(x)=x-1$, $g_2(x)=x^3+2x^2+x-1$ *et* $g_3(x)=x^3-x^2+2x^2-1$ *sont des facteurs unitaires irréductibles de* x^7-1. *Par le* ***Corollaire 3.21*, il y a* $3^3=27$ *codes cycliques de longueur 7 dans* $\mathbb{Z}_4$. *Dans* ***Table 1*** *on a les polynômes générateurs des 25 non trivial codes cycliques de longueur 7. Chaque générateur est donné par produit de quelque* $g_i(x)$.
S'il y a un seul générateur a, on aura le code $\langle a(x)\rangle$*; si le générateur est* $(a,2b)$, *le code obtenu est* $\langle a(x)\rangle\oplus\langle 2b(x)\rangle$.

Si $\mathcal{C}=\langle f(x)g(x)\rangle\oplus\langle 2f(x)h(x)\rangle$, on peut écrire la matrice génératrice G de $\mathcal{C}$. Les $deg(h)$ premiers lignes de G corresponds à $x^if(x)g(x)$ pour $0\leq i\leq deg(h)-1$; les $deg(g)$ derniers lignes de G corresponds à $2x^if(x)h(x)$ pour $0\leq i\leq deg(g)-1$

Example* 3.25.** *Considérons le code numéro 22 dans* ***Table 1*.*
$g_1(x)g_3(x)=1+x+3x^2+2x^3+x^4$ *et* $2g_2(x)=2+2x+2x^3$. *Une matrice génératrice de ce code est:*

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

Code No.	Polynôme générateur	Idempotents générateurs	Type	Code dual
1	g_2g_3	$\hat{e}_1$	4	6
2	g_1g_2	$\hat{e}_3$	4^3	4
3	g_1g_3	$\hat{e}_2$	4^3	5
4	g_2	$\hat{e}_1 + \hat{e}_3$	4^4	2
5	g_3	$\hat{e}_1 + \hat{e}_2$	4^4	3
6	g_1	$\hat{e}_2 + \hat{e}_3$	4^6	1
7	$2g_2g_3$	$2\hat{e}_1$	2	25
8	$2g_1g_2$	$2\hat{e}_3$	2^3	23
9	$2g_1g_3$	$2\hat{e}_2$	2^3	24
10	$2g_2$	$2\hat{e}_1 + 2\hat{e}_3$	2^4	21
11	$2g_3$	$2\hat{e}_1 + 2\hat{e}_2$	2^4	22
12	$2g_1$	$2\hat{e}_2 + 2\hat{e}_3$	2^6	16
13	2	2	2^7	auto-dual
14	$(g_2g_3, 2g_2g_1)$	$\hat{e}_1 + 2\hat{e}_3$	$4 \cdot 2^3$	19
15	$(g_3g_2, 2g_3g_1)$	$\hat{e}_1 + 2\hat{e}_2$	$4 \cdot 2^3$	20
16	$(g_2g_3, 2g_1)$	$\hat{e}_1 + 2\hat{e}_2 + 2\hat{e}_3$	$4 \cdot 2^6$	12
17	$(g_2g_1, 2g_2g_3)$	$\hat{e}_3 + 2\hat{e}_1$	$4^3 \cdot 2$	auto-dual
18	$(g_3g_1, 2g_3g_2)$	$\hat{e}_2 + 2\hat{e}_1$	$4^3 \cdot 2$	auto-dual
19	$(g_1g_2, 2g_1g_3)$	$\hat{e}_3 + 2\hat{e}_2$	$4^3 \cdot 2^3$	14
20	$(g_1g_3, 2g_1g_2)$	$\hat{e}_2 + 2\hat{e}_3$	$4^3 \cdot 2^3$	15
21	$(g_1g_2, 2g_3)$	$\hat{e}_3 + 2\hat{e}_1 + \hat{e}_2$	$4^3 \cdot 2^4$	10
22	$(g_1g_3, 2g_2)$	$\hat{e}_2 + 2\hat{e}_1 + \hat{e}_3$	$4^3 \cdot 2^4$	11
23	$(g_2, 2g_1g_3)$	$\hat{e}_1 + \hat{e}_3 + 2\hat{e}_2$	$4^4 \cdot 2^3$	8
24	$(g_3, 2g_1g_2)$	$\hat{e}_1 + \hat{e}_2 + 2\hat{e}_3$	$4^4 \cdot 2^3$	9
25	$(g_1, 2g_2g_3)$	$\hat{e}_2 + \hat{e}_3 + 2\hat{e}_1$	$4^6 \cdot 2$	7

Table 1 *Générateur des codes cycliques de longueur 7 dans* $\mathbb{Z}_4$

Défénition 3.26. *Soit* $f(x) = a_d x^d + a_{d-1}x^{d-1} + ... + a_0 \in \mathbb{Z}_4[x]$ *avec* $a_d \neq 0$. *On définie le polynôme réciproque* $f^*(x) = \pm x^d f(x^{-1}) = \pm(a_0 x^d + a_1 x^{d-1} + ... + a_d)$.

Lemme 3.27. *Soit* $\boldsymbol{a} = a_0a_1...a_{n-1}$ *et* $\boldsymbol{b} = b_0b_1...b_{n-1}$ *sont des vecteurs dans* $\mathbb{Z}_4^n[x]$ *associés aux polynômes* $a(x), b(x)$. *Alors* $\boldsymbol{a}$ *est orthogonal à* $\boldsymbol{b}$ *et tous son shifts si et seulement si* $a(x)b^*(x) = 0$ *dans* $\mathfrak{R}_n$.

Si n un nombre impair et $g_i(x)$ est un facteur unitaire irréductible de $x^n - 1$ dans $\mathbb{Z}_4[x]$, alors $g_i^*(x)$ est aussi un facteur unitaire irréductible de $x^n - 1$ comme le terme constant de $g_i(x)$ est ± 1. Le polynôme réciproque $\mu(g_i^*(x))$ de $\mu(g_i(x))$ dans $\mathbb{F}_2[x]$ est un facteur irréductible de $x^n + 1$ dans $\mathbb{F}_2[x]$. Donc $g_i^*(x)$ est un facteur unitaire irréductible de base de $x^n - 1$. Par le **Théorème 3.10**, $g_i^*(x) = g_j(x)$ pour j quelconque.

Théorème 3.28. *Si* $\mathcal{C} = \langle f(x)g(x)\rangle \oplus \langle 2f(x)h(x)\rangle$ *est un code cyclique de longueur* n *dans* $\mathbb{Z}_4$ *avec* $x^n - 1 = f(x)g(x)h(x)$, *alors* $\mathcal{C}^\perp = \langle h^*(x)g^*(x)\rangle \oplus \langle 2h^*(x)f^*(x)\rangle$.

De plus, si $g(x) = 1$, $\mathcal{C} = \langle f(x) \rangle$ *et* $\mathcal{C}^\perp = \langle h^*(x) \rangle$ *; si* $h(x) = 1$, $\mathcal{C} = \langle 2f(x) \rangle$ *et* $\mathcal{C}^\perp = \langle g^*(x) \rangle \oplus \langle 2f^*(x) \rangle$.

Proof. Soit $s(x) = h^*(x)g^*(x)$, alors $s^*(x) = \pm h(x)g(x)$ et $f(x)g(x)s^*(x) = \pm(x^n - 1) \times g(x)$ dans $\mathbb{Z}_4[x]$, implique $f(x)g(x)s^*(x) = 0$ dans $\mathfrak{R}_n$. De la même manière, $2f(x)h(x)s * (x) = 0$. Donc $h^*(x)g^*(x) \in \mathcal{C}^\perp$ par **lemme 3.25**. De même, $2h^*(x)f^*(x)$ est orthogonal à $f(x)g(x)$ et ses shifts cycliques. Comme $2a(x)2b^*(x) = 0$ dans $\mathfrak{R}_n$ pour tous $a(x), b(x)$ dans $\mathbb{Z}_4$, $2h^*(x)f^*(x)$ est orthogonal à $2f(x)g(x)$ et ses shifts cycliques. Donc $2h^*(x)f^*(x) \in \mathcal{C}^\perp$. Comme $x^n - 1 = f^*(x)g^*(x)h^*(x)$, par **théorème 3.19**, $\langle h^*(x)g^*(x) \rangle + \langle 2h^*(x)f^*(x) \rangle$ est une somme direct. Donc $\langle h^*(x)g^*(x) \rangle \oplus \langle 2h^*(x)f^*(x) \rangle \subseteq \mathcal{C}^\perp$.
Comme $\mathcal{C}$ est de type $4^{deg(h)}2^{deg(g)}$, $\mathcal{C}^\perp$ est de type $4^{n-deg(h)-deg(g)}2^{deg(g)}$. Mais $\langle h^*(x)g^*(x) \rangle \oplus \langle 2h^*(x)f^*(x) \rangle \subseteq \mathcal{C}^\perp$ est de type $4^{deg(f^*)}2^{deg(g^*)} = 4^{deg(f)}2^{deg(g)}$. On obtient donc la première assertion. La deuxième assertion découle de la première, comme $g(x) = 1$ implique $g^*(x) = 1$ et $h^*(x)f^*(x) = x^n - 1$ avec $h(x) = 1$ implique $h^*(x) = 1$. ■

Example* 3.29.** *Code 14 dans* ***Table 1 *a* $f(x) = g_2(x)$, $g(x) = g_3(x)$ *et* $h(x) = g_1(x)$. *Donc son dual est* $\langle g_1^*(x)g_3^*(x) \rangle \oplus \langle 2g_1^*(x)g_2^*(x) \rangle = \langle g_1(x)g_2(x) \rangle \oplus \langle 2g_1(x)g_3(x) \rangle$, *qui est le code 19 dans la table.*
Code 22 a $f(x) = 1$, $g(x) = g_1(x)g_3(x)$ *et* $h(x) = g_2(x)$, *son dual est* $\langle g_2^*(x)g_1^*(x)g_3^*(x) \rangle \oplus \langle 2g_2^*(x) \rangle = \langle 2g_3(x) \rangle$, *qui est le code 11 dans la table.*
Code 17 a $f(x) = g_2(x)$, $g(x) = g_1(x)$ *et* $h(x) = g_3(x)$, *son dual est* $\langle g_3^*(x)g_1^*(x) \rangle \oplus \langle 2g_3^*(x)g_2^*(x) \rangle = \langle g_2(x)g_1(x) \rangle \oplus \langle 2g_2(x)g_3(x) \rangle$, *le code est auto-dual.*

3.4 Idempotents générateurs des codes cycliques dans $\mathbb{Z}_4$

Soit $\mathcal{C}$ le code cyclique non nul de longueur n impair dans $\mathbb{Z}_4$. Par le **théorème 3.19**, il existe des uniques polynômes unitaire $f(x), g(X)$ et $h(x)$ tel que $x^n - 1 = f(x)g(x)h(x)$ et $\mathcal{C} = \langle f(x)g(x) \rangle \oplus \langle 2f(x)h(x) \rangle$. Par le **théorème 3.18**(f),

Théorème 3.30. *Soit* $\mathcal{C} = \langle f(x)g(x) \rangle \oplus \langle 2f(x)h(x) \rangle$ *est un code cyclique non nul de longueur* n *impair dans* $\mathbb{Z}_4$ *avec* $x^n - 1 = f(x)g(x)h(x)$. *Pour* $e(x)$ *et* $E(X)$ *les idempotents non nuls dans* $\mathfrak{R}_n$, *on a alors:*

i. Si $g(x) = 1$, $\mathcal{C} = \langle f(x) \rangle = \langle e(x) \rangle$,

ii. Si $h(x) = 1$, $\mathcal{C} = \langle 2f(x) \rangle = \langle 2E(x) \rangle$,

iii. Si $g(X) \neq 1$ *et* $h(x) \neq 1$, $\mathcal{C} = \langle f(x)g(x) \rangle \oplus \langle 2f(x)h(x) \rangle = \langle e(x) \rangle \oplus \langle 2E(x) \rangle$

Exercice 3.31. *Soit* $I \subseteq 1, 2, ..., k$ *et* $I^c = 1, 2, ..., k \setminus I$ *est le complémentaire de I.*

1. *Montrer que* $\sum_{i \in I} \hat{e}_i(x)$ *est un idempotent dans* $\mathfrak{R}_n$.
2. *Montrer que* $\sum_{i \in I} \langle \hat{g}_i(x) \rangle = \langle \sum_{i \in I} \hat{e}_i(x) \rangle$.
3. *Montrer que* $\langle \prod_{j \in I^c} g_j(x) \rangle = \langle \sum_{i \in I} \hat{e}_i(x) \rangle$

Proof.

1. Par **théorème 3.18**(d), on a $\sum_{i\in I}\hat{e}_i(x)=1$. On le multiplie par $\sum_{i\in I}\hat{e}_i(x)$. Comme $\{\hat{e}_i(x)|1\leq i\leq k\}$ sont idempotents orthogonaux par paire, on a $\hat{e}_i(x)\hat{e}_j(x)=0$ pour $i\neq j$ et $\hat{e}_i^2(x)=\hat{e}_i(x)$. Donc $\sum_{i\in I}\hat{e}_i(x)\cdot\sum_{i\in I}\hat{e}_i(x)=\sum_{i\in I}\hat{e}_i^2(x)=\sum_{i\in I}\hat{e}_i(x)$.
2. Par **théorème 3.18**(d), $\langle\hat{g}_i(x)\rangle=\langle\hat{e}_i(x)\rangle$ donc $\sum_{i\in I}\langle\hat{g}_i(x)\rangle=\sum_{i\in I}\langle\hat{e}_i(x)\rangle=\langle\sum_{i\in I}\hat{e}_i(x)\rangle$
3. Par le même raisonnement du Proof de **théorème 3.18**, si $x^n-1=g_1(x)g_2(x)...g_m(x)$ avec $f(x)=\prod_{i=b+1}^{m}g_i(x)$, $h(x)=\prod_{i=k+1}^{b}g_i(x)$ et $g(x)=\prod_{i=1}^{k}g_i(x)$ alors $\sum_{i\in I}\langle\hat{g}_i(x)\rangle=\langle\prod_{j\in I^c}g_j(x)\rangle$. Par le point (2) avant, on obtient $\langle\prod_{j\in I^c}g_j(x)\rangle=\langle\sum_{i\in I}\hat{e}_i(x)\rangle$.

■

Défénition 3.32. ***Un multiplicateur*** μ_a *sur* $\{0,1,...,n-1\}$ *définie par* $i\mu_a\equiv ia \bmod n$ *est une permutation des coordonnées* $\{0,1,...,n-1\}$ *d'un code cyclique de longueur* n *avec* $gcd(a,n)=1$.

On peut appliquer le multiplicateur dans code $\mathbb{Z}_4$ linéaire. Pour codes cycliques dans $\mathbb{F}_q$, $f(x)\mu_a\equiv f(x^a) \bmod x^n-1$ pour $f(x)\in\mathfrak{R}_n$. Aussi, $(f(x)g(x))\mu_a=(f(x)\mu_a)(g(x)\mu_a)$ pour $f(x),g(x)\in\mathfrak{R}_n$, implique si $e(x)$ est un idempotent dans $\mathfrak{R}_n$ alors $e(x)\mu_a$ l'est aussi.

Lemme 3.33.

i. Soit $\mathcal{C}=\langle e(x)\rangle$ *est un code cyclique* $\mathbb{Z}_4$*-linéaire avec idempotent générateur* $e(x)$*. Alors l'idempotent générateur de* $\mathcal{C}^\perp$ *est* $1-e(x)\mu_{-1}$.

ii. Pour $i=1$ *ou* 2*, soit* $\mathcal{C}_i=\langle e_i(x)\rangle$ *est codes cycliques* $\mathbb{Z}_4$*-linéaires avec idempotents générateurs* $e_i(x)$*. Alors l'idempotent générateur de* $\mathcal{C}_1\cap\mathcal{C}_2$ *est* $e_1(x)e_2(x)$ *et l'idempotent générateur de* $\mathcal{C}_1+\mathcal{C}_2$ *est* $e_1(x)+e_2(x)-e_1(x)e_2(x)$.

Proof. Comme $e(x)(1-e(x))=0$ dans $\mathfrak{R}_n$, $e(x)$ est orthogonal au polynôme réciproque de $1-e(x)$ et tous son shifts (**lemme 3.25**) ; mais ce ne sont que des multiples scalaires des shifts cycliques de $1-e(x)\mu_{-1}$. Donc $1-e(x)\mu_{-1}\in\mathcal{C}^\perp$. Par **théorème 3.19**, si $g(x)=1$, $\mathcal{C}$ a un polynôme générateur $f(x)$. De plus par **théorème 3.26**, $\mathcal{C}^\perp$ a un polynôme générateur $h^*(x)$; pourtant, $1-e(x)$ est l'idempotent générateur de $\langle h(x)\rangle$ par **théorème 3.18**. Donc $1-e(x)\mu_{-1}$ est l'idempotent générateur de $\langle h^*(x)\rangle=\mathcal{C}^\perp$.
On a $e_1(x)e_2(x)\in\mathcal{C}_1\cap\mathcal{C}_2$. Donc $\langle e_1(x)e_2(x)\rangle\subseteq\mathcal{C}_1\cap\mathcal{C}_2$. Si $c(x)\in\mathcal{C}_1\cap\mathcal{C}_2$ alors $c(x)=s(x)e_1(x)$ et $c(x)e_2(x)=c(x)$ (par **exercice 3.32**(a)) ; donc $c(x)=c(x)e_2(x)=s(x)e_1(x)e_2(x)\in\langle e_1(x)e_2(x)\rangle$. Donc $\mathcal{C}_1\cap\mathcal{C}_2=\langle e_1(x)e_2(x)\rangle$. Ensuite, si $c(x)=c_1(x)+c_2(x)$ avec $c_i(x)\in\mathcal{C}_i$ pour $i=1$ ou 2, alors par **exercice 3.32**(a) $c(x)(e_1(x)+e_2(x)-e_1(x)e_2(x))=c_1(x)+c_1(x)e_2(x)-c_1(x)e_2(x)+c_2(x)e_1(x)+c_2(x)-c_2(x)e_1(x)=c_1(x)+c_2(x)=c(x)$. Comme $e_1(x)+e_2(x)-e_1(x)e_2(x)\in\mathcal{C}_1+\mathcal{C}_2$, alors $\mathcal{C}_1+\mathcal{C}_2=\langle e_1(x)+e_2(x)-e_1(x)e_2(x)\rangle$ par **exercice 3.32**(b). ■

Exercice 3.34. *Soit $\mathcal{C}$ un code cyclique dans $\mathbb{F}_q$ ou $\mathbb{Z}_4$.*

(a) Soit $e(x)$ l'idempotent générateur de $\mathcal{C}$, montrer que $c(x) \in \mathcal{C}$ si et seulement si $c(x)e(x) = c(x)$.

(b) Montrer que si $e(x) \in \mathcal{C}$ et $c(x)e(x) = c(x)$ pour tout $c(x) \in \mathcal{C}$, alors $e(x)$ est l'idempotent générateur de $\mathcal{C}$.

Proof.

(a) Si $c(x) \in \mathcal{C}$, comme $\mathcal{C} = \langle e(x) \rangle$, $c(x) = s(x)e(x)$. Donc $c(x)e(x) = s(x)e^2(x) = s(x)e(x) = c(x)$. Inversement, on a $c(x) = c(x)e(x) \in \langle e(x) \rangle = \mathcal{C}$.

(b) Comme $e(x) \in \mathcal{C}$ donc $\langle e(x) \rangle \subseteq \mathcal{C}$. Pour $c(x) \in \mathcal{C}$, $c(x) = c(x)e(x) \in \langle e(x) \rangle$ donc $\mathcal{C} \subseteq \langle e(x) \rangle$. Alors $\mathcal{C} = \langle e(x) \rangle$.

■

Un autre façon pour construire le "idempotent générateur" de $\mathcal{C}$ est à partir de l'idempotent primitif.

Théorème 3.35. *Soit n un nombre impair et $g_1(x)g_2(x)...g_k(x)$ est la factorisation de $x^n - 1$ dans polynômes irréductibles dans $\mathbb{Z}_4[x]$. Soit $\hat{g}_i(x) = \prod_{j \neq i} g_j(x)$ et $\langle \hat{g}_i(x) \rangle = \langle \hat{e}_i(x) \rangle$ avec $\hat{e}_i(x)$ est un idempotent de $\mathfrak{R}_n$. Soit $\mathcal{C} = \langle f(x)g(x) \rangle \oplus \langle 2f(x)h(x) \rangle$ avec $f(x)g(x)h(x) = x^n - 1$. Supposons que $f(x)g(x) = \prod_{i \in I} g_i(x)$ et $f(x)h(x) = \prod_{j \in J} g_j(x)$ avec I et J des sous-groups de $\{1, 2, ..., k\}$. Alors:*

i. $I^c \cap J^c = \varnothing$ avec I^c et J^c sont des complémentaires de I et J respectivement dans $\{1, 2, ..., k\}$

ii. $\mathcal{C} = \langle e(x) + 2E(x) \rangle$ avec $e(x) = \sum_{i \in I^c} \hat{e}_i(x)$ et $E(x) = \sum_{j \in J^c} \hat{e}_j(x)$.

Il y a un méthode pour construire idempotent, y compris l'idempotent primitif, dans $\mathfrak{R}_n$. Le méthode commence par l'idempotent binaire de $\mathcal{R}_n$.

Théorème 3.36. *Soit $\langle b(x) \rangle = \langle \mu(f(x)) \rangle$ avec $f(x)g(x) = x^n - 1$ dans $\mathbb{Z}_4[x]$, $b(x)$ est un idempotent binaire dans $\mathcal{R} = \mathbb{F}_2[x]/(x^n + 1)$ et n est impair. Soit $e(x) = b^2(x)$ avec $b^2(x)$ est calculé dans $\mathbb{Z}_4[x]$. Alors $e(x)$ est l'idempotent générateur de $\langle f(x) \rangle$.*

Proof. Comme $b^2(x) = b(x)$ dans $\mathcal{R}_n$, $\mu(e(x)) = \mu(b^2(x)) = b(x) + \mu(a(x)(x^n - 1))$ pour $a(x) \in \mathbb{Z}_4[x]$, implique $e(x) = b(x) + a(x)(x^n - 1) + 2s(x)$ pour $s(x) \in \mathbb{Z}_4[x]$. Alors $e^2(x) = b^2(x) + d(x)(x^n - 1)$ dans $\mathbb{Z}_4[x]$ d'où $e^2(x) = e(x)$ dans $\mathfrak{R}_n$. Donc $e(x)$ est un idempotent dans $\mathfrak{R}_n$.
On a $1+b(x)$ est l'idempotent générateur dans $\mathcal{R}_n$ de $\langle \mu(g(x)) \rangle$. Donc $1+b(x) = r(x)g(x)+2s(x)$ pour $r(x), s(x)$ dans $\mathbb{Z}_4[x]$. Donc $b(x) = 1+r(x)g(x)+2(1+s(x))$; en élévant à carré, on obtient $e(x) = b^2(x) = 1 + t(x)g(x)$ pour $t(x) \in \mathbb{Z}_4[x]$. Alors $e(x)f(x) = f(x) + t(x)(x^n - 1)$ dans $\mathbb{Z}_4[x]$, implique $f(X) \in \langle e(x) \rangle$ dans

$\mathfrak{R}$ d'où $f(x) \subseteq \langle e(x) \rangle$.
Comme $e(x) = b^2(x)$, $\mu(e(x)) = \mu(b^2(x)) \in \langle \mu(f(x)) \rangle$ dans $\mathcal{R}_n$. Alors $e(x) = u(x)f(x) + 2v(x)$ dans $\mathbb{Z}_4[x]$, $e^2(x) = u^2(x)f^2(x)$, implique $e^2(x) \in \langle f(x) \rangle$ dans $\mathfrak{R}_n$. Comme $e(x)$ est un idempotent dans $\mathfrak{R}_n$, $e(x) \in \langle f(x) \rangle$ d'où $\langle e(x) \rangle \subseteq \langle f(x) \rangle$. Alors $\langle e(x) \rangle = \langle f(x) \rangle$ et $e(x) = b^2(x)$ est l'idempotent générateur de $\langle f(x) \rangle$. ■

Example* 3.37.** *On a dans* $\mathbb{Z}_4[x]$ $x^7 - 1 = g_1(x)g_2(x)g_3(x)$ *avec* $g_1(x) = x - 1$, $g_2(x) = x^3 + 2x^2 + x - 1$ *et* $g_3(x) = x^3 - x^2 + 2x - 1$. *D'abord* $\mu(\overline{g}_i(x)) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, *alors* $b_1(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ *est l'idempotent générateur de* $\mu(\overline{g}_i(x))$ [1]. *De même raisonnement,* $\mu(\overline{g}_2(x)) = x^4 + x^2 + x + 1$ *et* $b_2(x) = x^4 + x^2 + x + 1$, $\mu(\overline{g}_3(x)) = x^4 + x^3 + x^2 + 1$ *et* $b_3(x) = x^4 + x^3 + x^2 + 1$. *Par* ***théorème 3.36*,*

$$\begin{aligned} \overline{e}_1(x) &= -x^6 - x^5 - x^4 - x^3 - x^2 - x - 1 \\ \overline{e}_2(x) &= 2x^6 + 2x^5 - x^4 + 2x^3 - x^2 - x - 1 \\ \overline{e}_3(x) &= -x^6 - x^5 + 2x^4 - x^3 + 2x^2 + 2x - 1 \end{aligned}$$

Par ***théorème 3.30*** *et résultat d'exercice* [2]*, chaque code cyclique a un idempotent générateur* $e(x) + 2E(x)$. *Dans* ***Table 1****, on a l'idempotent générateur des 25 codes cycliques non trivial de longueur 7 dans* $\mathbb{Z}_4[x]$. *L'idempotent* $e(x)$ *et* $E(x)$ *chacun est la somme des quelque* $\overline{e}_1(x)$, $\overline{e}_2(x)$, $\overline{e}_3(x)$.
Code 4 est $\langle g_2(x) \rangle$*; donc* $f(x)g(x) = g_2(x)$ *et* $f(x)h(x) = x^n - 1$ *implique* $e(x) = \overline{e}_1(x) + \overline{e}_3(x)$ *et* $2E(x) = 0$ *par* ***théorème 3.35****.*
Code 12 est $\langle 2g_1(x) \rangle$*, alors* $f(x)g(x) = x^n - 1$ *et* $f(x)h(x) = g_1(x)$*, implique* $e(x) = 0$ *et* $2E(x) = 2\overline{e}_2(x) + 2\overline{e}_3(x)$
Code 20 est $\langle g_1(x)g_3(x) \rangle + \langle 2g_1(x)g_2(x) \rangle$ *alors* $f(x)g(x) = g_1(x)g_3(x)$ *et* $f(x)h(x) = g_1(x)g_2(x)$ *implique* $e(x) = \overline{e}_2(x)$ *et* $2E(x) = 2\overline{e}_3(x)$*. Code 20 est un idéal généré par* $\overline{e}_2(x) + 2\overline{e}_3(x)$
Code 21 est $\langle g_1(x)g_2(x) \rangle + \langle 2g_3(x) \rangle$*, alors* $f(x)g(x) = g_1(x)g_2(x)$ *et* $f(x)h(x) = g_3(x)$ *implique* $e(x) = \overline{e}_3(x)$ *et* $2E(x) = 2\overline{e}_1(x) + 2\overline{e}_2(x)$*. Code 21 est un idéal généré par* $2\overline{e}_1(x) + 2\overline{e}_2(x)$

4 Codes résidus quadratiques sur $\mathbb{Z}_4$

Tout au long de cette section, p est un nombre premier avec $p \equiv \pm 1 \bmod 8$. Soit $\mathcal{Q}_p$ le group des résidus quadratiques non nuls modulo p ; $\mathcal{N}_p$ le group des non-résidus quadratiques modulo p.

Lemme 4.1. *r est défini par $p = 8r \pm 1$. Soit $k \in \mathbb{F}_p$ avec $k \neq 0$. Soit $N_{\mathcal{Q}_p}(k)$ est le nombre des couples non ordonnés $\{\{i, j\} | i + j = k, i \neq j, i, j \in \mathcal{Q}_p\}$. $N_{\mathcal{N}_p(k)}$*

[1] Exemple 4.3.4 dans document
[2] Soit $\mathcal{C} = \langle e(x) \rangle \oplus \langle 2E(x) \rangle$ avec $e(x)$ et $E(x)$ des idempotents, montrer que $\mathcal{C} = \langle e(x) + 2E(x) \rangle$

est défini de manière analogue. Alors $N_{\mathcal{Q}_p}(k) = r - 1$ *si* $k \in \mathcal{Q}_p$ *et* $N_{\mathcal{Q}_p}(k) = r$ *si* $k \in \mathcal{N}_p$ *;* $N_{\mathcal{N}_p}(k) = r - 1$ *si* $k \in \mathcal{N}_p$ *et* $N_{\mathcal{N}_p}(k) = r$ *si* $k \in \mathcal{Q}_p$.

Proof. Calculer $N_{\mathcal{Q}_p}(k)$: le nombre de couples $(x, y) \in \mathbb{F}_p^2$ avec $x^2 + y^2 = k$ est $8r$. En définissant $\{i, j\} = \{x^2 + y^2\}$ avec $i, j \in \mathcal{Q}_p, i + j = k$, on arrive aux solutions de l'équation précédente. Il y a 3 possibilités:

(a) $x = 0$ ou $y = 0$

(b) $x \neq 0$ et $y \neq 0$ avec $x = \pm y$

(c) $x \neq 0$ et $y \neq 0$ avec $x \neq \pm y$

Les solutions de l'équation $x^2+y^2 = k$ dans la forme (a) ou (b) sont les solutions de $i + j = k$ avec $i = 0$, $j = 0$ ou $i = j$ et donc elles n'appartiennent pas à $N_{\mathcal{Q}_p}(k)$. Quand $k \in \mathcal{N}_p$, (a) n'arrive pas ; (b) n'arrive non plus car $x^2 + y^2 = k$ et $x = \pm y$ implique $2x^2 = k$, donc $2 \in \mathcal{N}_p$, contradiction. Alors, toutes les solutions de $x^2 + y^2 = k$ si $k \in \mathcal{N}_p$ sont dans la forme (c).
Quand $k \in \mathcal{Q}_p$, il y a 4 solutions dans la form (a), qui sont $(\pm\gamma, 0)$ et $(0, \pm\gamma)$ avec $\pm\gamma$ sont 2 solutions de $z^2 = k$; il y a 4 solutions dans la form (b) qui sont $(\pm\gamma, \pm\gamma)$ avec $\pm\gamma$ sont 2 solutions de $2z^2 = k$, $2 \in \mathcal{Q}_p$. Donc les $8r-8$ solutions restants sont dans la forme (c). Dans le cas (c) avec $k \in \mathcal{Q}_p$ ou $k \in \mathcal{N}_p$, chaque couple de solution dans les 8 couples de solutions de l'équation dans le groupe $(\pm x, \pm y)$ et $(\pm y, \pm x)$ est la solution de $i + j = k$ qui appartient à $N_{\mathcal{Q}_p}(k)$. Par conséquent, $N_{\mathcal{Q}_p}(k) = r - 1$ si $k \in \mathcal{Q}_p$ et $N_{\mathcal{Q}_p}(k) = r$ si $k \in \mathcal{N}_p$.

Soit $\alpha \in \mathcal{N}_p$. Alors $i + j = k$ si et seulement si $i\alpha + j\alpha = k\alpha$. Donc $N_{\mathcal{N}_p}(k) = N_{\mathcal{Q}_p}(k\alpha)$. Par conséquent, $N_{\mathcal{N}_p}(k) = r-1$ si $k \in \mathcal{N}_p$; et $N_{\mathcal{N}_p}(k) = r$ si $k \in \mathcal{Q}_p$. ■

Soit $Q(x) = \sum_{i\in\mathcal{Q}_p} x^i$ et $N(x) = \sum_{i\in\mathcal{N}_p} x^i$. Notons que 1, $Q(x)$ et $N(x)$ sont idempotents dans $\mathcal{R}_p = \mathbb{F}_2[x]/(x^p + 1)$. Une combinaison de ces idempotents est idempotents dans $\mathfrak{R}_p$, qui définira les Codes résidus $\mathbb{Z}_4$-quadratiques. Un multiple d'un vecteur 1 est aussi un idempotent ; soit $\overline{j}(x) = p\sum_{i=0}^{p-1} x^i$. En particulière $\overline{j}(x) = 3\sum_{i=0}^{p-1} x^i$ si $p \equiv -1 \bmod 8$ et $\overline{j}(x) = p\sum_{i=0}^{p-1} x^i$ si
$p \equiv 1 \bmod 8$

Lemme 4.2. *r est défini par* $p = 8r \pm 1$. *Si r est impair, alors* $Q(x) + 2N(x)$, $N(x) + 2Q(x)$, $1 - Q(x) + 2N(x)$ *et* $1 - N(x) + 2Q(x)$ *sont des idempotents dans* $\mathfrak{R}_p$. *Si r est pair, alors* $-Q(x)$, $-N(x)$, $1 + Q(x)$ *et* $1 + N(x)$ *sont des idempotents dans* $\mathfrak{R}_p$. *De plus, si r est pair ou impair,* $\overline{j}(x)$ *est un idempotent de* $\mathfrak{R}_p$.

Proof. On va montrer le cas si r est impair. Dans $\mathfrak{R}_p$, par **Lemme 4.1**:

$$\begin{aligned} Q(x)^2 =& (\sum_{i\in\mathcal{Q}_p} x^i)^2 = \sum_{i\in\mathcal{Q}_p} x^2 i \quad + \sum_{i\neq j, i,j\in\mathcal{Q}_p} x^{i+j} \\ =& Q(x) + 2[(r-1)Q(x) + rN(x)] = Q(x) + 2N(x) \end{aligned}$$

comme r est impair et $2 \in \mathcal{Q}_p$. De même,

$$\begin{aligned} N(x)^2 =&(\sum_{i\in\mathcal{N}_p} x^i)^2 = \sum_{i\in\mathcal{N}_p} x^2 i \quad + \sum_{i\neq j, i,j\in\mathcal{N}_p} x^{i+j} \\ &= N(x) + 2[(r-1)N(x) + rQ(x)] = N(x) + 2Q(x) \end{aligned}$$

Alors $(Q(x)+2N(x))^2 = Q(x)^2 = Q(x)+2N(x)$; $(N(x)+2Q(x))^2 = N(x)^2 = N(x)+2Q(x)$; $(1-Q(x)+2N(x))^2 = (1-Q(x))^2 = 1-2Q(x)+Q(x)^2 = 1-Q(x)+2N(x)$; et $(1-N(x)+2Q(x))^2 = (1-N(x))^2 = 1-2N(x)+N(x)^2 = 1-N(x)+2Q(x)$.
Et $\overline{j}(x)^2 = p^2 \sum_{i=0}^{p-1} x^i \sum_{j=0}^{p-1} x^j = p^2(p\sum_{i=0}^{p-1} x^i) = \overline{j}(x)$ comme $p^2 \equiv 1 \bmod 8$. ■

4.1 Codes résidus $\mathbb{Z}_4$-quadratique: $p \equiv -1 \bmod 8$

On regard d'abord le cas que $p \equiv -1 \bmod 8$. Soit $p+1 = 8r$.
Soit r est impair, on définie $\mathcal{D}_1 = \langle Q(x) + 2N(x)\rangle$, $\mathcal{D}_2 = \langle N(x) + 2Q(x)\rangle$, $\mathcal{C}_1 = \langle 1 - N(x) + 2Q(x)\rangle$, $\mathcal{C}_2 = \langle 1 - Q(x) + 2N(x)\rangle$.
Soit r est pair, on définie $\mathcal{D}_1 = \langle -Q(x)\rangle$, $\mathcal{D}_2 = \langle -N(x)\rangle$, $\mathcal{C}_1 = \langle 1 + N(x)\rangle$, $\mathcal{C}_2 = \langle 1 + Q(x)\rangle$.
Ces codes sont dits *Codes résidus $\mathbb{Z}_4$-quadratique* quand $p \equiv -1 \bmod 8$.

Théorème 4.3. *Soit $p \equiv -1 \bmod 8$. Les Codes résidus $\mathbb{Z}_4$-quadratique satisfont:*

i. $\mathcal{D}_i\mu_a = \mathcal{D}_i$ *et* $\mathcal{C}_i\mu_a = \mathcal{C}_i$ *pour* $a \in \mathcal{Q}_p$ *;* $\mathcal{D}_1\mu_a = \mathcal{D}_2$ *et* $\mathcal{C}_1\mu_a = \mathcal{C}_2$ *pour* $a \in \mathcal{N}_p$ *; en particulière,* $\mathcal{D}_1$ *et* $\mathcal{D}_2$ *sont équivalents,* $\mathcal{C}_1$ *et* $\mathcal{C}_1$ *sont aussi.*

ii. $\mathcal{D}_1 \cap \mathcal{D}_2 = \langle \overline{j}(x)\rangle$ *et* $\mathcal{D}_1 + \mathcal{D}_2 = \mathfrak{R}_p$

iii. $\mathcal{C}_1 \cap \mathcal{C}_2 = \{0\}$ *et* $\mathcal{C}_1 + \mathcal{C}_2 = \langle \overline{j}(x)\rangle^{\perp}$.

iv. $\mathcal{D}_1$ *et* $\mathcal{D}_2$ *sont de type* $4^{(p+1)/2}$ *;* $\mathcal{C}_1$ *et* $\mathcal{C}_2$ *sont de type* $4^{(p-1)/2}$

v. $\mathcal{D}_i = \mathcal{C}_i + \langle \overline{j}(x)\rangle$ *pour* $i = 1$ *et* 2

vi. $\mathcal{C}_1$ *et* $\mathcal{C}_2$ *sont auto-orthogonals et* $\mathcal{C}_i^{\perp} = \mathcal{D}_i$ *pour* $i = 1$ *et* 2.

Proof. Supposons que $p+1 = 8r$. On va montrer le cas si r est impair.

Pour (i), si $a \in \mathcal{N}_p$, alors $(Q(x)+2N(x))\mu_a = N(x)+2Q(x)$. On en déduit que $\mathcal{D}_1\mu_a = \mathcal{D}_2$. De même, si $a \in \mathcal{E}_p$, alors $(Q(x)+2N(x))\mu_a = Q(x)+2N(x)$ et $(N(x)+2Q(x))\mu_a = N(x)+2Q(x)$, implique $\mathcal{D}_i\mu_a = \mathcal{D}_i$

Comme $p \equiv -1 \bmod 8$, $\overline{j}(x) = 3\sum_{i=0}^{p-1} x^i = 3 + 3Q(x) + 3N(x)$. Donc $(Q(x)+2N(x))(N(x)+2Q(x)) = (Q(x)+2N(x))(\overline{j}(x)+1-(Q(x)+2N(x))) = (Q(x)+2N(x))\overline{j}(x)+Q(x)+2N(x)-(Q(x)+2N(x))^2 = (Q(x)+2N(x))\overline{j}(x) = 3((p-1)/2)\sum_{i=0}^{p-1} s^i + 3(p-1)\sum_{i=1}^{p-1} x^i = (3/2)(p-1)\overline{j}(x) = (12r-3)\overline{j}(x) = \overline{j}(x)$.

Par **lemme 3.31**, $\mathcal{D}_1 \cap \mathcal{D}_2 = \langle \overline{j}(x) \rangle$.
Par le même raisonnement, $\mathcal{D}_1 + \mathcal{D}_2$ a idempotent générateur $Q(x) + 2N(x) + N(x) + 2Q(x) - (Q(x) + 2N(x))(N(x) + 2Q(x)) = 3Q(x) + 3N(x) - \overline{j}(x) = 1$. Par conséquent $\mathcal{D}_1 + \mathcal{D}_2 = \mathfrak{R}_p$.

Comme $(Q(x)+2N(x))(N(x)+2Q(x)) = \overline{j}(x)$, on a $(1-N(x)+2Q(x)) \times (1-Q(x)+2N(x)) = 1 - N(x) + 2Q(x) - Q(x) + 2N(x) + (N(x) + 2Q(x))(Q(x) + 2N(x)) = 1 + N(x) + Q(X) + \overline{j}(x) = 0$ qui montre $\mathcal{C}_1 \cap \mathcal{C}_2 = \{0\}$. Comme $(1 - N(x) + 2Q(X))(1 - Q(x) + 2N(X)) = 0$, $\mathcal{C}_1 + \mathcal{C}_2$ a idempotent générateur $1-N(x)+2Q(x)+1-Q(x)+2N(x) = 2+N(x)+Q(x) = 1-\overline{j}(x) = 1-\overline{j}(x)\mu_{-1}$ avec $\overline{j}(x)\mu_{-1} = \overline{j}(x)$. Par **lemme 3.31**, $\mathcal{C}_1 + \mathcal{C}_2 = \langle \overline{j}(x) \rangle^{\perp}$.

On observe que $|\mathcal{D}_1 + \mathcal{D}_2| = |\mathcal{D}_1||\mathcal{D}_2|/|\mathcal{D}_1 \cap \mathcal{D}_2|$. Par (i), $|\mathcal{D}_1| = |\mathcal{D}_2|$ et par (ii), $|\mathcal{D}_1 + \mathcal{D}_2| = 4^p$ et $|\mathcal{D}_1 \cap \mathcal{D}_2| = 4$. Donc $\mathcal{D}_1$ et $\mathcal{D}_2$ a size $4^{(p+1)/2}$; il est aussi leur type comme chacun a un idempotent générateur.

Par (ii), $\overline{j}(x) \in \mathcal{D}_2$ implique $(N(x)+2Q(x))\overline{j}(x) = \overline{j}(x)$ comme $N(x)+2Q(x)$ est un multiple d'identité de $\mathcal{D}_2$. Par **lemme 3.31**, l'idempotent générateur de $\mathcal{C}_1 + \langle \overline{j}(x) \rangle$ est $1 - N(x) + 2Q(x) + \overline{j}(x) - (1 - N(x) + 2Q(x))\overline{j}(x) = 1 - N(x) + 2Q(x) + \overline{j}(x) - (\overline{j}(x) - \overline{j}(x)) = Q(x) + 2N(x)$, qui montre que $\mathcal{C}_1 + \langle \overline{j}(x) \rangle = \mathcal{D}_1$. De même, $\mathcal{C}_2 + \langle \overline{j}(x) \rangle = \mathcal{D}_2$.

Par **lemme 3.31**, l'idempotent générateur de $\mathcal{C}^{\perp}$ est $1 - (1 - N(x) + 2Q(x))\mu_{-1} = N(x)\mu_{-1}+2Q(x)\mu_{-1}$. On a $-1 \in \mathcal{N}_p$ comme $p \equiv -1 \bmod 8$. Donc $N(x)\mu_{-1} = Q(x)$ et $Q(x)\mu_{-1} = N(x)$. Par conséquent l'idempotent générateur de $\mathcal{C}^{\perp}$ est $Q(x) + 2N(x)$, qui vérifie $\mathcal{C}_1^{\perp} = \mathcal{D}_1$. De même façon $\mathcal{C}_2^{\perp} = \mathcal{D}_2$. Alors il implique que $\mathcal{C}_i$ est auto-orthogonal comme $\mathcal{C}_i \subseteq \mathcal{D}_i$ par (v). ■

***Example* 4.4.** *Il y a 4 codes cycliques de longueur 7 dans $\mathbb{Z}_4$ donnés dans la **table 1** sont codes résidus quadratiques. Dans ce cas, $p = 7$ et $r = 1$. On a $\overline{e}_1(x) = \overline{j}(x)$, $\overline{e}_2(x) = 1 - Q(x) + 2N(x)$ et $\overline{e}_3(x) = 1 - N(x) + 2Q(x)$. Donc $\mathcal{D}_1$ est le code 4, $\mathcal{D}_2$ est le code 5, $\mathcal{C}_1$ est le code 2 et $\mathcal{C}_2$ est le code 3.*

4.2 Codes résidus $\mathbb{Z}_4$-quadratique: $p \equiv 1 \bmod 8$

Quand $p \equiv 1 \bmod 8$, on juste inverse le rôle de $\mathcal{C}_i$ et $\mathcal{D}_i$ du code défini dans le cas $p \equiv -1 \bmod 8$. Soit $p - 1 = 8r$.
Soit r est impair, on définie $\mathcal{D}_1 = \langle 1 - N(x) + 2Q(x) \rangle$, $\mathcal{D}_2 = \langle 1 - Q(x) + 2N(x) \rangle$, $\mathcal{C}_1 = \langle Q(x) + 2N(x) \rangle$, $\mathcal{C}_2 = \langle N(x) + 2Q(x) \rangle$.
Soit r est pair, on définie $\mathcal{D}_1 = \langle 1 + N(x) \rangle$, $\mathcal{D}_2 = \langle 1 + Q(x) \rangle$, $\mathcal{C}_1 = \langle -Q(x) \rangle$, $\mathcal{C}_2 = \langle -N(x) \rangle$.
Ces codes sont dits *Codes résidus $\mathbb{Z}_4$-quadratique* quand $p \equiv 1 \bmod 8$.

Théorème 4.5. *Soit $p \equiv 1 \bmod 8$. Les Codes résidus $\mathbb{Z}_4$-quadratique satisfont:*

i. $\mathcal{D}_i\mu_a = \mathcal{D}_i$ et $\mathcal{C}_i\mu_a = \mathcal{C}_i$ pour $a \in \mathcal{Q}_p$; $\mathcal{D}_1\mu_a = \mathcal{D}_2$ et $\mathcal{C}_1\mu_a = \mathcal{C}_2$ pour $a \in \mathcal{N}_p$; en particulière, $\mathcal{D}_1$ et $\mathcal{D}_2$ sont équivalents, $\mathcal{C}_1$ et $\mathcal{C}_1$ sont aussi.

ii. $\mathcal{D}_1 \cap \mathcal{D}_2 = \langle \bar{j}(x) \rangle$ *et* $\mathcal{D}_1 + \mathcal{D}_2 = \mathfrak{R}_p$

iii. $\mathcal{C}_1 \cap \mathcal{C}_2 = \{0\}$ *et* $\mathcal{C}_1 + \mathcal{C}_2 = \langle \bar{j}(x) \rangle^{\perp}$.

iv. $\mathcal{D}_1$ *et* $\mathcal{D}_2$ *sont de type* $4^{(p+1)/2}$ *;* $\mathcal{C}_1$ *et* $\mathcal{C}_2$ *sont de type* $4^{(p-1)/2}$

v. $\mathcal{D}_i = \mathcal{C}_i + \langle \bar{j}(x) \rangle$ *pour* $i = 1$ *et* 2

vi. $\mathcal{C}_1^{\perp} = \mathcal{D}_2$ *et* $\mathcal{C}_2^{\perp} = \mathcal{D}_1$

4.3 Codes résidus $\mathbb{Z}_4$-quadratique étendus

Soit $\mathcal{D}_1$ et $\mathcal{D}_2$ sont des codes résidus quadratiques de longueur $p \equiv \pm 1 \bmod 8$ définis dans les dernières parties. On va définir 2 extensions de $\mathcal{D}_i$:

$$\widehat{\mathcal{D}}_i = \{c_\infty c_0 ... c_{p-1} | c_0 ... c_{p-1} \in \mathcal{D}_i, c_\infty + c_0 + ... + c_{p-1} \equiv 0 \bmod 4\}$$

$$\widetilde{\mathcal{D}}_i = \{c_\infty c_0 ... c_{p-1} | c_0 ... c_{p-1} \in \mathcal{D}_i, -c_\infty + c_0 + ... + c_{p-1} \equiv 0 \bmod 4\}$$

$\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ sont des *Codes résidus $\mathbb{Z}_4$-quadratique étendus* de longueur $p+1$. Notons que $\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ sont équivalents par la fonction qui multiplie par 3 le coordonné étendu. Si $\mathbf{c}_i$ est un mot du code $\mathcal{D}_i$, alors $\widehat{\mathbf{c}}_i$ et $\widetilde{\mathbf{c}}_i$ sont les mots étendus des $\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ respectivement.

Théorème 4.6. *Soit G_i la matrice génératrice de $\mathcal{C}_i$ codes résidus $\mathbb{Z}_4$-quadratique. Alors les matrices génératrices $\widehat{G}_i$ et $\widetilde{G}_i$ de $\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ respectivement sont:*

i. Si $p \equiv -1 \bmod 8$,

$$\widehat{G}_i = \begin{bmatrix} 3 & 3 & \dots & 3 \\ 0 & & & \\ \vdots & & G_i & \\ 0 & & & \end{bmatrix} \quad et \quad \widetilde{G}_i = \begin{bmatrix} 1 & 3 & \dots & 3 \\ 0 & & & \\ \vdots & & G_i & \\ 0 & & & \end{bmatrix}$$

ii. Si $p \equiv 1 \bmod 8$,

$$\widehat{G}_i = \begin{bmatrix} 3 & 1 & \dots & 1 \\ 0 & & & \\ \vdots & & G_i & \\ 0 & & & \end{bmatrix} \quad et \quad \widetilde{G}_i = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 0 & & & \\ \vdots & & G_i & \\ 0 & & & \end{bmatrix}$$

Théorème 4.7. *Soit $\mathcal{D}_i$ les codes résidus $\mathbb{Z}_4$-quadratique de longueur p. On a les suivants:*

i. Si $p \equiv -1 \bmod 8$, *alors $\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ sont auto-dual. De plus, tous les mots des $\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ ont le poids Euclidien est un multiple de 8.*

ii. Si $p \equiv 1 \bmod 8$, *alors* $\widehat{\mathcal{D}}_1^{\perp} = \widetilde{\mathcal{D}}_2$ *et* $\widehat{\mathcal{D}}_2^{\perp} = \widetilde{\mathcal{D}}_1$

Proof. Soit $p \equiv -1 \bmod 8$, par le **théorème 4.3**(vi), $\mathcal{C}_i^{\perp} = \mathcal{D}_i$. Donc comme le coordonné étendu de n'importe quel vecteur de $\mathcal{C}_i$ est 0, les mots étendus de $\mathcal{C}_i$ sont orthogonaux aux tous les mots dans $\widehat{\mathcal{D}}_i$ ou $\widetilde{\mathcal{D}}_i$. Comme le produit interne de $\widehat{\overline{j}}(x)$ est $3^2(p+1) \equiv 0 \bmod 4$ et de $\widetilde{\overline{j}}(x)$ est $1^2 + 3^2 p \equiv 0 \bmod 4$, $\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ sont auto-orthogonaux par **théorème 4.3**(v). Par **théorème 4.3**(iv), $\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ a $4^{(p+1)/2}$ mots, implique $\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ sont auto-duaux. De plus, on a les lignes des matrices génératrices de $\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ sont les extensions de $\overline{j}(x)$ et les shifts cycliques de l'idempotent générateur de $\mathcal{C}_i$. Mais les lignes des matrices génératrices de $\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ ont le poids Euclidien est un multiple de 8, donc tous les mots de $\widehat{\mathcal{D}}_i$ et $\widetilde{\mathcal{D}}_i$ ont le poids Euclidien est un multiple de 8, par **théorème 2.5**.

Supposons $p \equiv 1 \bmod 8$. Par **théorème 4.5**(vi), $\mathcal{C}_1^{\perp} = \mathcal{D}_2$ et $\mathcal{C}_2^{\perp} = \mathcal{D}_1$. Comme le coordonné étendu de n'importe quel vecteur de $\mathcal{C}_i$ est 0, les mots étendus de $\mathcal{C}_i$ sont orthogonaux aux tous les mots dans $\widehat{\mathcal{D}}_j$ ou $\widetilde{\mathcal{D}}_j$ avec $j \neq i$. Comme le produit interne de $\widehat{\overline{j}}(x)$ est $3 + p \equiv 0 \bmod 4$, $\widehat{\mathcal{D}}_j^{\perp} \subseteq \widetilde{\mathcal{D}}_i^{\perp}$ avec $j \neq i$ ■

***Example* 4.8.** *Par **théorème 4.7**, les codes résidus quadratiques étendus $\widehat{\mathcal{D}}_1$ ou $\widehat{\mathcal{D}}_2$ de longueur $p + 1 = 24$ sont les codes auto-duaux avec tous les mots du codes ont le poids Euclidien un multiple de 8. Si $\mathcal{C}$ est l'un de ces codes, l'énumérateur des poids symétrique est:*

$$\begin{aligned} swe_{\mathcal{C}}(a,b,c) =& a^2 4 + c^2 4 + 759(a^8 c^{16} + a^{16} c^8) + 2576 a^1 2 c^{12} \\ &+ 12144(a^2 b^8 c^{14} + a^{14} b^8 c2) + 170016(a^4 b^8 c^{12} + a^{12} b^8 c^4) \\ &+ 765072(a^6 b^8 c^{10} + a^{10} b^8 c6) + 1214400 a^8 b^8 c^8 \\ &+ 61824(a b^{12} c^{11} + a^1 1 b^1 2c) + 1133440(a^3 b^{12} c^9 + a^9 b^{12} c^3) \\ &+ 4080384(a^5 b^{12} c^7 + a^7 b^{12} c^5) + 24288(b^{16} c^8 + a^8 b^{16}) \\ &+ 680064(a^2 b^{16} c^6 + a^6 b^{12} c^2) + 1700160 a^4 b^{16} c^4 + 4096 b^2 4 \end{aligned}$$

Donc $\mathcal{C}$ a poids de Hamming minimum 8, le poids de Lee minimum 12 et le poids d'Euclidien minimum 16.

5 Codes auto-duaux dans $\mathbb{Z}_4$

Par **théorème 1.9**, le poids Euclidien de tous les mots d'un code auto-orthogonal est un multiple de 4. Par le **théorème 2.5**, si le poids Euclidien de tous les mots du code est un multiple de 8, alors le code est auto-orthogonal.

Défénition 5.1. *Un code $\mathbb{Z}_4$-linéaire auto-dual est de **Type II** si le poids Euclidien de tous les mots du code est un multiple de 8;*
*Un code $\mathbb{Z}_4$-linéaire auto-dual est de **Type I** s'il y a les mots du code avec le poids Euclidien n'est pas un multiple de 8.*

On va voir que les code de Type II existe pour les code de longueur $n \equiv 0 \bmod 8$. Ils contiennent un mot de code avec tous coordonnés ± 1. Par example,

par **théorème 4.7**, les codes résidus $\mathbb{Z}_4$-quadratiques de longueur $p+1$ avec $p \equiv -1 \bmod 8$ est de Type II.

Théorème 5.2. *Soit $\mathcal{C}$ est un code auto-dual sur $\mathbb{Z}_4$ de longueur n. On a les suivants:*

i. Si $\mathcal{C}$ est de Type II, alors le poids Euclidien minimum de $\mathcal{C}$ est au plus $8\lfloor n/24 \rfloor + 8$.

ii. Si $\mathcal{C}$ est de Type I, alors le poids Euclidien minimum de $\mathcal{C}$ est au plus $8\lfloor n/24 \rfloor + 8$, sauf si $n \equiv 23 \bmod 24$ la borne est $8\lfloor n/24 \rfloor + 12$. Si on a égalité dans la deuxième borne, alors $\mathcal{C}$ est obtenu par raccourcir [3] un code de Type II de longueur $n+1$.

Les codes satisfont ces bornes sont appelées *Euclidien extremum.*

***Example* 5.3.** *Par **Example 4.8**, les codes résidus $\mathbb{Z}_4$-quadratiques étendus de longueur 24 est de Type II avec le poids Euclidien minimum 16. Ce sont les codes Euclidien extremum.*

Défénition 5.4. *Soit $\mathcal{C}$ est un code $\mathbb{Z}_4$-linéaire de longueur n. Il y a deux codes linéaire binaire de longueur n associé à $\mathcal{C}$. Le **code résidu** $Res(\mathcal{C})$ est $\mu(\mathcal{C})$. Le **code torsion** $Tor(\mathcal{C})$ est $\{\boldsymbol{b} \in \mathbb{F}_2^n | 2\boldsymbol{b} \in \mathcal{C}\}$. Les vecteurs dans $Tor(\mathcal{C})$ sont obtenus à partir des vecteurs dans $\mathcal{C}$ avec tous les composants 0 ou 2 en divisant ces composants en deux.*

Si $\mathcal{C}$ a une matrice génératrice G dans la forme systématique, alors $Res(\mathcal{C})$ et $Tor(\mathcal{C})$ ont matrices génératrices:

$$G_{Res} = \begin{bmatrix} I_{k_1} & A & B_1 \end{bmatrix} \quad et \quad G_{Tor} = \begin{bmatrix} I_{k_1} & A & B_1 \\ O & I_{k_2} & C \end{bmatrix}$$

Alors $Res(\mathcal{C}) \subseteq Tor(\mathcal{C})$.

Théorème 5.5. *Si $\mathcal{C}$ est un code $\mathbb{Z}_4$ linéaire auto-dual, alors $Res(\mathcal{C})$ est "doubly-even" est $Res(\mathcal{C}) = Tor(\mathcal{C})^{\perp}$.*

Proof. Supposons que $\mathcal{C}$ a matrice génératrice G. On note un des premiers k_1 lignes de G par $\mathbf{r} = (\mathbf{i}, \mathbf{a}, \mathbf{b}_1 + 2\mathbf{b}_2)$, avec $\mathbf{i}$, $\mathbf{a}$, $\mathbf{b}_1$ et $\mathbf{b}_2$ sont lignes de I_{k_1}, A, B_1 et B_2 respectivement. Donc $0 \equiv \mathbf{r} \cdot \mathbf{r} \equiv \mathbf{i} \cdot \mathbf{i} + \mathbf{a} \cdot \mathbf{a} + \mathbf{b}_1 \cdot \mathbf{b}_1 \bmod 4$, implique que les lignes de G_{Res} sont "doubly-even", donc sont auto-orthogonaux. Si $\mathbf{r}' = (\mathbf{i}', \mathbf{a}', \mathbf{b}_1' + 2\mathbf{b}_2')$ est l'autre premier k_1 lignes, alors

$$\mathbf{r} \cdot \mathbf{r}' \equiv \mathbf{i} \cdot \mathbf{i}' + \mathbf{a} \cdot \mathbf{a}' + \mathbf{b}_1 \cdot \mathbf{b}_1' + 2(\mathbf{b}_2 \cdot \mathbf{b}_1' + \mathbf{b}_1 \cdot \mathbf{b}_2') \bmod 4 \tag{1}$$

[3] Raccourcir un code $\mathbb{Z}_4$ linéaire à un coordonné donné est fait par suivant: S'il y a les mots du code qui contiennent toutes les valeurs de $\mathbb{Z}_4$ dans ce coordonné, on choisit les mots avec 0 ou 2 dans cette position et on supprime la coordonné pour obtenir un mot pour court ; Si tous les mots du code donnent 0 ou 2 à ce coordonné, on choisit les mots avec seulement 0 dans cette position et on supprime la coordonné. Dans chaque cas, le code raccourci est linéaire avec deux fois moins des mots du code que l'avant. De plus, si le code original est auto-dual, le code raccourci l'est aussi.

Si $\mathbf{s} = (\mathbf{0}, 2\mathbf{i}', 2\mathbf{c})$ est l'un des k_2 derniers lignes de G, par la même notation, alors

$$\mathbf{r} \cdot \mathbf{s} \equiv 2\mathbf{a} \cdot \mathbf{i}' + 2\mathbf{b}_1 \cdot \mathbf{c} \bmod 4 \tag{2}$$

Comme $\mathbf{r} \cdot \mathbf{r}' \equiv \mathbf{r} \cdot \mathbf{s} \equiv 0 \bmod 4$, (1) et (2) implique que les lignes de G_{Res} sont orthogonaux aux lignes de G_{Tor} en tant que des vecteurs binaires. Donc $Res(\mathcal{C}) \subseteq Tor(\mathcal{C})^{\perp}$; comme $\mathcal{C}$ est auto-dual, $2k_1+k_2 = n$, implique que $Res(\mathcal{C}) = Tor(\mathcal{C})^{\perp}$.En particulier, $Res(\mathcal{C})$ est auto-orthogonal, et comme il a une matrice génératrice avec des lignes "doubly-even", $Res(\mathcal{C})$ est "doubly-even". ■

Corollaire 5.6. *Soit $\mathcal{C}$ est un code de Type II de longueur n. Donc $Tor(\mathcal{C})$ est un code binaire pair, $Res(\mathcal{C})$ contient le vecteur binaire avec 1 partout, $\mathcal{C}$ contient un mot de code avec des entrées sont ± 1, et $n \equiv 0 \bmod 8$.*

Proof. Soit $\mathbf{c} \in Tor(\mathcal{C})$. Alors $2\mathbf{c} \in \mathcal{C}$; comme $wt_E(2\mathbf{c}) \equiv 0 \bmod 8$, $\mathbf{c}$ est un vecteur binaire de poids pair. Par conséquent $Tor(\mathcal{C})$ est un code binaire pair. Donc $Res(\mathcal{C})$ contient le vecteur binaire avec 1 partout comme $Res(\mathcal{C}) = Tor(\mathcal{C})^{\perp}$ dans le **théorème 5.5**. Tous les vecteur $\mathbf{v} \in \mathcal{C}$ avec $\mu(\mathbf{v}) = 1$ n'ont pas d'entrées 0 ou 2; au moins un de ces $\mathbf{v}$ existe. Donc $0 \equiv wt_E(\mathbf{v}) \equiv n \bmod 8$. ■

On va maintenant étudier à partir un code binaire "doubly-even" arbitraire comment construire un code $\mathbb{Z}4$-linéaire auto-dual avec ce code binaire comme son code résidu.

Corollaire 5.7. *Soit $\mathcal{C}$ est un code $\mathbb{Z}4$-linéaire auto-dual avec avec matrice génératrice dans la forme systématique. Donc $\mathcal{C}$ a une matrice génératrice de forme:*

$$G' = \begin{bmatrix} F & I_k + 2B \\ 2H & O \end{bmatrix},$$

où B, F et H sont matrices binaires. De plus, matrices génératrices de $Res(\mathcal{C})$ et $Tor(\mathcal{C})$ sont

$$G'_{Res} = \begin{bmatrix} F & I_k \end{bmatrix} \quad et \quad G'_{Tor} = \begin{bmatrix} F & I_k \\ H & O \end{bmatrix}$$

Proof. Soit $k = k_1$ où $\mathcal{C}$ est de type $4^{k_1}2^{k_2}$. Comme $\mathcal{C}$ est auto-dual, $k_2 = n-2k$. On montre d'abord que $\mathcal{C}$ a matrice génératrice sous la forme
$G" = \begin{bmatrix} D & E & I_k + 2B \\ O & 2I_{n-2k} & 2C \end{bmatrix}$,
avec B, C, D et E sont matrices binaires. On commence par la matrice génératrice en forme systématique G défini dans **définition 1.4**, remplace le premier $k = k_1$ lignes par $\begin{bmatrix} D & E & I_k + 2B \end{bmatrix}$. Par **Théorème 5.5**, les k coordonnées les plus à droite de $Res(\mathcal{C})$ sont les positions d'information, et les $n-k$ coordonnées les plus à gauche de $Tor(\mathcal{C})$ sont les positions d'information. Donc pour la matrice G_{Res}, B_1 a le rang binaire k donc a un matrice inverse binaire D. D'où les premières k lignes de G peut être remplacé par

$D\begin{bmatrix} I_k & A & B_1+2B_2 \end{bmatrix} = \begin{bmatrix} D & E+2E_1 & I_k+2B_3 \end{bmatrix}$ avec $DA = 2E + 2E_1$ et $D(B_1 + 2B_2) = I_k + 2B_3$. En ajoutant $E_1\begin{bmatrix} O & 2I_{n-2k} & 2C \end{bmatrix}$ à cela donne G". Ajouter ensuite $2C\begin{bmatrix} D & E & I_k+2B \end{bmatrix}$ aux $n-2k$ derniers lignes de G" pour obtenir G'. ■

5.1 Formule de masse

Soit $\mathcal{C}$ un code $\mathbb{Z}_4$ linéaire auto-dual de type $4^k 2^{n-2k}$ avec $0 \leq k \leq \lfloor n/2 \rfloor$. Par **Théorème 5.5**, $Res(\mathcal{C})$ est un $[n, k]$ code binaire auto-orthogonal doubly-even, et on peut appliquer une matrice de permutation P à $\mathcal{C}$ de sorte que la matrice génératrice G' de $\mathcal{C}P$ est donnée en **Corollaire 5.7**. Inversement, si on commence par un $[n, k]$ code binaire auto-orthogonal doubly-even avec matrice génératrice $[FIk]$ qui génère $Res(\mathcal{C})P$, il faut pouvoir trouver la matrice binaire B pour produire les premières k lignes de G'. Alors que la sous-matrice H dans G' n'est pas unique, elle est uniquement déterminée par $Res(\mathcal{C})^{\perp} = Tor(\mathcal{C})$. Cela produit une matrice génératrice pour $\mathcal{C}P$ et à partir de là on peut produire $\mathcal{C}$. Donc pour compter le nombre total de codes $\mathcal{C}$ avec un code résiduel donné, il suffit de compter le nombre de choix pour B.

Commençant par une matrice génératrice $\begin{bmatrix} F & Ik \end{bmatrix}$, qui génère un $[n, k]$ code binaire auto-orthogonal doubly-even $\mathcal{C}_1$, choisit H pour que

$$\begin{bmatrix} F & I_k \\ H & O \end{bmatrix}$$

génère $\mathcal{C}_2 = \mathcal{C}_1^{\perp}$. On montre maintenant qu'il y a $2^{k(k+1)/2}$ choix qui donne les codes auto-dual $\mathbb{Z}_4$-linéaires avec matrices génératrices sous la forme $\mathcal{G}'$ donné en **Corollaire 5.7**. Comme le produit interne modulo 4 des vecteurs dont les composantes ne sont que 0 et 2 est toujours 0, le produit interne de deux des $n-2k$ dernières lignes de G' est égal à 0. Quel que soit le choix de B, le produit interne modulo 4 d'une des k premières lignes de G' avec l'une des $n-2k$ dernières lignes de G' est est également toujours 0 comme $\mathcal{C}_1^{\perp} = \mathcal{C}_2$. En outre, le produit interne modulo 4 d'une des k premières lignes de G' avec lui-même vaut 0 quel que soit le choix de B car $\mathcal{C}_1$ est doubly-even. Soit $B = [b_{i,j}]$ avec $1 \leq i \leq k$, $1 \leq j \leq k$.Choisit les entrées de B sur ou au-dessus de la diagonale (c'est $b_{i,j}$, avec $1 \leq i \leq j \leq k$) arbitrairement; remarquez qu'on choisit librement $k(k+1)/2$ entrées. On doit seulement on assurer que le produit intérieur de la ligne i et de la ligne j de G', avec $1 \leq i \leq j \leq k$, vaut 0 modulo 4. Mais ce produit interne modulo 4 est

$$\mathbf{f}_i \cdot \mathbf{f}_j + 2(b_{i,j} + b_{j,i}), \tag{3}$$

où $\mathbf{f}_i$ et $\mathbf{f}_j$ sont les lignes i et j de F. Comme $\mathcal{C}_1$ est auto-orthogonal, $\mathbf{f}_i \cdot \mathbf{f}_j \equiv 0 \bmod 2$, implique qu'on peut résoudre (3) pour la valeur binaire $b_{i,j}$ uniquement pour que le produit intérieur souhaité soit 0 modulo 4. Cela prouve le résultat suivant, montré pour la première fois dans.

Théorème 5.8. *Pour $0 \leq k \leq \lfloor n/2 \rfloor$, il y a $v_{n,k}2^{k(k+1)/2}$ codes auto-duaux sur $\mathbb{Z}_4$ de longueur n et de type $4^k 2^{n-2k}$, où $v_{n,k}$ est le nombre de $[n,k]$ code binaire auto-orthogonal doubly-even. Le nombre total des codes auto-duaux sur $\mathbb{Z}_4$ de longueur n est*

$$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} v_{n,k}2^{k(k+1)/2}.$$

Théorème 5.9. *Si $n \equiv 0 \bmod 8$, il y a $\mu_{n,k}2^{1+k(k-1)/20}$ Type II codes sur $\mathbb{Z}_4$ de longueur n et type $4^k 2^{n-2k}$ pour $0 \leq k \leq n/2$, où $\mu_{n,k}$ est le nombre de $[n,k]$ code binaire auto-orthogonal doubly-even contenant **1**.Le nombre total de $\mathbb{Z}_4$ de longueur n est*

$$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \mu_{n,k}2^{1+k(k-1)/2}$$

Notez que dans la preuve du théorème 9.12.5, on a donné une relation de récurrence pour $\mu_{n.k}$, à savoir
$\mu_{n,1} = 1$ et

$$\mu_{n,k+1} = \frac{2^{n-2k-1} + 2^{n/2-k-1} - 1}{2k-1}\mu_{n,k}$$

pour $k \geq 1$.

5.2 Codes cyclique auto-duaux

On a observé à de nombreuses reprises l'existence de codes cycliques auto-duaux sur $\mathbb{Z}$.Le **théorème 3.19** donne une paire de polynômes générateurs pour les codes cycliques.

Théorème 5.10. *Soit $\mathcal{C} = \langle f(x)g(x)\rangle \oplus \langle 2f(x)h(x)\rangle$ est un code cyclique sur $\mathbb{Z}_4$ de longueur impaire n, où $f(x)$, $g(x)$ et $h(x)$ sont des polynômes unitaire tel que $x^n - 1 = f(x)g(x)h(x)$. Alors $\mathcal{C}$ est auto-dual si et seulement si $f(x) = h^*(x)$ et $g(x) = g^*(x)$.*

Proof. On remarque d'abord que le terme constant de tout facteur irréductible de x^{n-1} n'est égal ni à 0 ni à 2. En particulier, par définition, $f^*(x)$, $g^*(x)$ et $h^*(x)$ sont tous unitaire et $f^*(x)g^*(x)h^*(x) = x^n - 1$.

Suppose que $f(x) = h^*(x)$ et $g(x) = g^*(x)$. Par **théorème 3.26**, $\mathcal{C}^\perp = \langle h^*(x)g^*(x)\rangle \oplus \langle 2h^*(x)f^*(x) = \langle f(x)g(x)\rangle \oplus \langle 2f(x)h(x)\rangle = \mathcal{C}$ et $\mathcal{C}$ est auto-dual.

Supposons que $\mathcal{C}$ est auto-dual. Puisque $\mathcal{C} = l'angle f(x)g(x)\rangle \oplus \langle 2f(x)h(x)\rangle$ et $\mathcal{C}^\perp = \langle h^*(x)g^*(x)\rangle \oplus \langle 2h^*(x)f^*(x)$ et ces décompositions sont uniques, on a

$f(x)g(x) = h^*(x)g^*(x), et$

$f(x)h(x) = h^*(x)f^*(x)$.

De (12.18), $x^n-1 = f(x)g(x)h(x) = h^*(x)g^*(x)h(x)$. Comme $f^*(x)g^*(x)h^*(x) = x^n - 1$, on a $h^*(x)g^*(x)h(x) = h^*(x)g^*(x)f^*(x) = x^n - 1$. Par la factorisation unique de $x^n - 1$ en polynômes unitaires irréductibles, $f^*(x) = h(x)$. De même $x^n - 1 = f(x)h(x)g(x) = h^*(x)f^*(x)g(x)$, implique que $g(x)^*_g(x)$ ■

5.3 Les codes en treillis auto-duaux sur $\mathbb{Z}_4$

Une méthode pour construire des treillis à partir de codes binaires est appelée *Construction A*. Il existe un analogue méthode dans $\mathbb{Z}_4$ appelé *Construction* A_4, commençant par un code $\mathcal{C}$ $\mathbb{Z}_4$-linéaire de longueur n. *Construction* A_4 produit un treillis $\Lambda_4(\mathcal{C})$, qui est l'ensemble de tous les $\mathbf{x}$ dans $\mathbb{R}^n$ obtenu à partir d'un mot du code dans $\mathcal{C}$ en considérant les mots du code comme un vecteur entier avec 0, 1, 2 et 3, ajouter des multiples de 4 à tous les composants et diviser le vecteur résultant par 2. En particulier,

$$\Lambda_4(\mathcal{C}) = \{\mathbf{x} \in \mathbb{R}^n | 2\mathbf{x} \bmod 4 \in \mathcal{C}\}$$

Si la matrice génératrice G de $\mathcal{C}$ est écrite dans la forme systématique alors la matrice génératrice M pour $\Lambda_4(\mathcal{C})$ est

$$M = \frac{1}{2}\begin{bmatrix} I_{k_1} & A & B_1 + 2B_2 \\ O & I_{k_2} & 2C \\ O & O & 4I_{n-k_1-k_2} \end{bmatrix}$$

Théorème 5.11. *Soit $\mathcal{C}$ est un code $\mathbb{Z}_4$-linéaire de longueur n avec poids d'Euclidien minimal d_E. On a les suivants:*

i. *Si $d_E \leq 16$,la norme minimale μ de $\Lambda_4(\mathcal{C})$ est $\mu = d_E/4$; si $d_E > 16$, $\mu = 4$.*

ii. $det\Lambda_4(\mathcal{C}) = 4^{n-2k_1-k_2}$.

iii. $\Lambda_4(\mathcal{C}^\perp)$=$\Lambda_4(\mathcal{C})^*$.

iv. *$\Lambda_4(\mathcal{C})$ est intégrale si et seulement si $\mathcal{C}$ est auto-orthogonal.*

v. *$\Lambda_4(\mathcal{C})$ est de Type I si et seulement si $\mathcal{C}$ est de Type I.*

vi. *$\Lambda_4(\mathcal{C})$ est de Type II si et seulement si $\mathcal{C}$ est de Type II.*

***Example* 5.12.** *D'après **l'exemple 2.6**, l'octacode o_8 est un code de type II avec un poids Euclidien minimum de 8. D'après le **théorème 5.11**, $\Lambda_4(o_8)$ est un treillis de type II dans $\mathbb{R}^8$ avec une norme minimale 2. Il s'agit d'un treillis de Gosset E_8, dont nous rappelons qu'il s'agit de l'unique treillis de type II dans $\mathbb{R}^8$. E_8 a précisément 240 points de treillis de norme minimale 2. L'énumérateur de poids symétrisé de o_8 est*

$$swe_{o_8}(a, b, c) = a^8 + 16b^8 + c^8 + 14a^4c^4 + 112a^3b^4c + 112ab^4c^3.$$

Pour les mots du code de o_8 avec le poids Euclidien 8 il y a 16 mots avec tous les composants sont ± 1, 112 mots avec quatre composants sont ± 1 et un composant égal 2. Pour les premiers 16 mots, il y aura 16 points de treillis de forme $1/2(\pm 1^8)$ qui donne un vecteur avec 8 entrées égaux à $\pm 1/2$. Après, il y aura 112 points de treillis de forme $1/2(0^3, \pm 1^4, 2)$; pour chacun des 112 points, quatre peuvent être enlevé de composant qui est égal à 2, donner 112 points de treillis de forme $1/2(0^3, \pm 1^4, -2)$.

6 Anneaux de Galois

Soit $f(x)$ un polynôme unitaire irréductible de base de dégré r. Par le **lemme 3.15**, **lemme 3.16**, $\mathbb{Z}_4[x]/(f(x)$ est un anneau avec 4^r éléments et un seul idéal non trivial. Cet anneau est appellé *Anneaux de Galois*. Tous les anneaux de Galois de même ordre sont isomorphes, et on note un anneau de Galois d'ordre 4^r par $GR(4^r)$. Comme pour les corps finis, $GR(4^r)$ est un anneau de charactéristique 4 contient un sous anneau $\mathbb{Z}_4$

Théorème 6.1. *Un anneaux de Galois $\mathcal{R} = GR(4^r)$ contient un élément ξ d'ordre $2^r - 1$. Tous les éléments $c \in \mathcal{R}$ peuvent être s'écrit sous forme unique $c = a + 2b$ avec a, b sont les éléments de $\mathcal{T}(\mathcal{R}) = \{0, 1, \xi, \xi^2, ..., \xi^{2^r-2}\}$*

L'élément ξ est dit un ***élément primitive*** ; l'expression $c = a + 2b$ avec a et b dans $\mathcal{T}(\mathcal{R})$ est s'appelé une ***une réprésentation 2-adique*** de c. Un seul idéal non trivial (2) est $2\mathcal{R} = \{2t | t \in \mathcal{T}(\mathcal{R})\}$; les éléments de $2\mathcal{R}$ consistent de 0 et tous les diviseurs de zéro dans $\mathcal{R}$. Les éléments inversibles de $\mathcal{R}$ sont les éléments de $\mathcal{R} \setminus 2\mathcal{R}$.

Soit $f(x)$ un polynôme unitaire irréductible de base de dégré r dans $\mathbb{Z}_4[x]$, $\mu(f(x))$ est un polynôme irréductible de dégré r dans $\mathbb{F}_2[x]$. Une réduction homomorphisme $\mu : \mathbb{Z}_4[x] \to \mathbb{F}_2[x]$ qui induit un homomorphisme $\overline{\mu}$ de $\mathbb{Z}_4[x]/(f(x))$ à $\mathbb{F}_2[x]/(\mu(f(x))$ donné par $\overline{\mu}(a(x) + (f(x))) = \mu(a(x)) + (\mu(f(x)))$ avec noyau (2). Donc si $\mathcal{R}$ est un anneau de Galois sur $\mathbb{Z}_4[x]/(f(x))$, l'anneau quotient $\mathcal{R}/2\mathcal{R}$ est isomorphisme à $\mathbb{F}_{2^r}$ avec l'élément primitif $\xi \in \mathcal{R}$ arrive à un élément primitif de $\mathbb{F}_{2^r}$.

Soit p un nombre premier et $q = p^r$. On rappele que le groupe automorphisme du corps finis $\mathbb{F}_q$, appellé le groupe de Galois $Gal(\mathbb{F}_q)$ de $\mathbb{F}_q$, est un code cyclique d'ordre r généré par automorphisme de Frobenius $\sigma_p : \mathbb{F}_q \to \mathbb{F}_q$ avec $\sigma_p(\alpha) = \alpha^p$.
Pour le groupe d'automorphisme $GR(4^r)$, on a une structure similaire, noté $Gal(GR(4^r))$, est s'appellé *Le groupe de Galois* de $GR(4^r)$. Ce groupe est cyclique d'ordre r généré par *Automorphisme Frobenius* $v_2 = GR(4^r) \to GR(4^r)$, v_2 défini par $v_2(c) = a^2 + 2b^2$, avec $a + 2b$ est la réprésentation 2-adique de c. Les éléments de $\mathbb{F}_q$ fixé par σ_p est aussi l'élément de sous corps primitif $\mathbb{F}_q$. De même raison, les éléments de $GR(4^r)$ fixé par v_2 est aussi l'élément de sous

anneau $\mathbb{Z}_4$.

Soit $n = 2^r - 1$. Il existe un polynôme irréductible $f_2(x) \in \mathbb{F}_2[x]$ de dégré r ayant une racine dans $\mathbb{F}_{2^r}$ d'ordre n ; rappelons qu'il est polynôme primitif dans $\mathbb{F}_2[x]$. Par **le méthode de Graeffe**, on peut trouver un polynôme unitaire irréductible de base $f(x) \in \mathbb{Z}_4[x]$ tel que $\mu(f(x)) = f_2(x)$, $f(x)$ est le polynôme primitif de $\mathbb{Z}_4[x]$. Dans anneau de Galois $GR(4^r) = \mathbb{Z}_4[x]/(f(x))$, soit $\xi = x + (f(x))$. Alors $f(\xi) = 0$ et ξ est l'élément primtif de $GR(4^r)$.

Tous les éléments de $c \in GR(4^r)$ peuvent être exprimé dans la forme "multiplicatif" $c = a + 2b$; ou dans la forme additive $c = \sum_{i=0}^{r-1} c_i \xi^i$, avec $c_i \in \mathbb{Z}_4$

Défénition 6.2. *Soit σ_2 l'automorphisme Frobenius de $\mathbb{F}_{2^r}$. La fonction trace $Tr_r : \mathbb{F}_{2^r} \to \mathbb{F}_2$ est défini par*

$$Tr_r(\alpha) = \sum_{i=0}^{r-1} \alpha^{2^i} = \sum_{i=0}^{r-1} \sigma_2^i(\alpha) \qquad pour\ \alpha \in \mathbb{F}_{2^r}$$

*On défini **fonction trace relative** $TR_r : GR(4^r) \to \mathbb{Z}_4$ est défini par*

$$TR_r(\alpha) = \sum_{i=0}^{r-1} v_2^i(\alpha) \quad pour\ \alpha \in GR(4^r)$$

7 Codes Kerdock

On va définir le code Kerdock binaire de longueur 2^{r+1} comme l'image de Gray du code étendu d'un code cyclique $\mathbb{Z}_4$-linéaire de longueur $n = 2^r - 1$. Soit $H(x)$ le polynôme primitif irréductible de base de dégré r. Soit $f(x)$ le polynôme réciproque de $(x^n - 1)/((x - 1)H(x))$. On a $f(x)$ est un facteur de $x^n - 1$. On définie $K(x + 1)$ est un code cyclique de longueur $2^r - 1$ dans $\mathbb{Z}_4$ généré par $f(x)$. Par **corollaire 3.20**, $K(x+1)$ est un code cyclique de longueur $n = 2^r - 1$ de type $4^{n-deg(f)} = 4^{r+1}$. Soit $\widehat{K}(r + 1)$ est le code cyclique étendu obtenu par ajouter un bit' de contrôle à $K(r + 1)$. Il est un code de longueur 2^r et de type 4^{r+1}.

Défénition 7.1. *Le code Kerdock $\mathcal{K}(v + 1)$ est l'image de Gray $\mathfrak{G}(\widehat{K}(r + 1))$ de $\widehat{K}(r + 1)$. Alors $\mathcal{K}(v + 1)$ est un code de longueur 2^{r+1} avec 4^{r+1} mots de code.*

***Example* 7.2.** *Si $n = 2^3 - 1$, on écrit $H(x) = x^3 + 2x^2 + x - 1$. Dans ce cas, $f^*(x) = (x^7 - 1)/((x - 1)H(x)) = x^3 - x^2 + 2x - 1$ et $f(x) = x^3 + 2x^2 + x + 1$.*

On note dans cette section l'anneau de Galois $GR(4^r) = \mathbb{Z}_4[x]/(H(x))$. Soit ξ est la racine primitive de $H(x)$ dans $GR(4^r)$.

Lemme 7.3. *Soir $r \geq 2$, on a les suivants:*

i. Un polynôme $c(x) \in \mathfrak{R}_n$ est dans $K(r+1)$ si et seulement si $(x-1)H(x)c^*(x) = 0 \in \mathfrak{R}_n$

ii. Matrice génératrice G_{r+1} et $\widehat{G}_{r+1}$ pour $K(r+1)$ et $\widehat{K}(r+1)$ respectivement sont

$$G_{r+1} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \xi & \xi^2 & \dots & \xi^{n-1} \end{bmatrix}, \quad \widehat{G}_{r+1} = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \xi & \xi^2 & \dots & \xi^{n-1} \end{bmatrix}$$

On peut remplacer chaque ξ^i par la vecteur colonne $\begin{bmatrix} b_{i,0} & b_{i,1} & \dots & b_{i,r-1} \end{bmatrix}^\top$, avec $\xi^i = \sum_{j=0}^{r-1} b_{i,j}\xi^j$.

Proof. Comme $\mathfrak{R}_n = \langle (x-1)H(x) \rangle \oplus \langle f^*(x) \rangle$ par **théorème 3.18**, $(x-1)H(x)c^*(x) = 0$ dans $\mathfrak{R}_n$ si et seulement si $c^*(x) \in \langle f^*(x) \rangle$ si et seulement si $c(x) = f(x)s(x)$ pour $s(x) \in \mathfrak{R}_n$.

Pour (ii), on note la matrice obtenue de $\begin{bmatrix} 1 & \xi & \xi^2 & \dots & \xi^{r-1} \end{bmatrix}$ par remplacer les ξ^i avec le coefficient de $c = \sum_{i=0}^{r-1} c_i \xi^i$ est une matrice $r \times r$. Alors les $r+1$ lignes de $\widehat{G}_{r+1}$ génèrent un code de type 4^{r+1} ; Si on peut montrer le bit de parité de $\mathbf{r}_1 = \begin{bmatrix} 1 & 1 & \dots & 1 \end{bmatrix}$ est 1 et le bit de parité de $\mathbf{r}_2 = \begin{bmatrix} 1 & \xi & \xi^2 & \dots & \xi^{n-1} \end{bmatrix}$ est 0. Comme $\mathbf{r}_1$ a $2^r - 1$ nombre 1 et $2^r - 1 \equiv 3 \bmod 4$ pour $r \geq 2$, donc le bit de parité de $\mathbf{r}_1$ est 1. Le bit de parité de $\mathbf{r}_2$ est $-\sum_{i=0}^{n-1} \xi^i = -(\xi^n - 1)/(\xi - 1) = 0$ comme $\xi^n = 1$.

Il suffit de montrer que $c(x) \in K(r+1)$ avec $c(x)$ le polynôme associé à $\mathbf{r}_1$ et $\mathbf{r}_2$. Pour $\mathbf{r}_1$, soit $c(x) = \sum_{i=0}^{n-1} x^i$. Comme $(x-1)c^*(x) = (x-1)\sum_{i=0}^{n-1} x^i = x^n - 1$ dans $\mathbb{Z}_4[x]$, $(x-1)H(x)c^*(x) = 0$ dans $\mathfrak{R}_n$, donc $c(x) \in K(r+1)$ par (i). Pour $\mathbf{r}_2$ il y a r mots du code possible. Soit $\sum_{i=0}^{n-1} \xi^i x^i$, donc les coefficients de $c(x)$ est dans $GR(4^r)$. Par (i), on a besoin juste de montrer que $H(x)c^*(x) = 0$ avec les coefficients de $c(x)$ est dans $GR(4^r)$. Alors $c^*(x) = \xi \sum_{i=0}^{n-1} \xi^{n-1-i} x^i$ ($c^*(x)$ est unitaire). Soit $H(x) = \sum_{i=0}^{n-1} H_i x^i$. Le coefficient de x^k pour $0 \geq k \geq n-1$ dans $H(x)c^*(x)$ est

$$\xi \sum_{i+j \equiv k \bmod n} H_i \xi^{n-1-j} = \xi \sum_{i=0}^{n-1} H_i \xi^{n-1-k+i} = \xi^{n-k} \sum_{i=0}^{n-1} H_i \xi^i$$

comme $\xi^n = 1$. On a $\xi^{n-k} H(\xi) = 0$ comme ξ est la racine de $H(x)$. Donc $(x-1)H(x)c^*(x) = 0$ ■

***Example* 7.4.** *Par le **lemme 7.3** , la matrice génératrice de $\widehat{K}(4)$ est*

$$\widehat{G}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 3 & 3 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 3 & 1 & 1 \end{bmatrix}$$

On va maintenant lister tous les mots du code de $K(r+1)$ et $\widehat{K}(r+1)$. Soit $\mathbf{1}_n$ est un vecteur de longueur n avec toutes entrées sont 1.

Lemme 7.5. *Soit $r \geq 2$ et $n = 2^r - 1$. Alors $\boldsymbol{c} \in K(r+1)$ si et seulement s'il existe $\lambda \in \mathcal{R} = GR(4^r)$ et $\epsilon \in \mathbb{Z}_4$ tel que*

$$\boldsymbol{c} = (TR_r(\lambda), TR_r(\lambda\xi), TR_r(\lambda\xi^2), ..., TR_r(\lambda\xi^{n-1})) + \epsilon \boldsymbol{1}_n \tag{4}$$

Le bit de parité de $\boldsymbol{c}$ est ϵ

Proof. $\sum_{i=0}^{n-1}(TR_r(\lambda\xi^i)+\epsilon) = TR_r(\lambda\sum_{i=0}^{n-1}\xi^i)+(2^r-1)\epsilon = TR_r(\lambda(\epsilon^n-1)/(\epsilon-1)) + (2^r-1)\epsilon = TR_r(0) + (2^r-1)\epsilon = (2^r-1)\epsilon \equiv 3 \bmod 4$. Alors le bit de parité est ϵ.

Soit $\mathcal{C} = \{(TR_r(\lambda), TR_r(\lambda\xi), TR_r(\lambda\xi^2), ..., TR_r(\lambda\xi^{n-1}))+\epsilon\mathbf{1}_n | \lambda \in GR(4^r), \epsilon \in \mathbb{Z}_4\}$. On doit montrer que $\mathcal{C}$ a 4^{r+1} mots ; il est clair si on montre $TR_r(\lambda\xi^i)+\epsilon = TR_r(\lambda_1\xi^i) + \epsilon_1$ pour $0 \geq i \geq n-1$, implique $\lambda = \lambda_1$ et $\epsilon = \epsilon_1$. Comme le bit de parité de $\mathbf{c}$ est ϵ, alors $\epsilon = \epsilon_1$. Alors $TR_r(\zeta\xi^i) = 0$ pour $0 \geq i \geq n-1$ avec $\zeta = \lambda - \lambda_1$. On doit montrer que $\zeta = 0$. Comme $TR_r(\zeta\xi^i) = 0$, $TR_r(\zeta(2\xi^i)) = 0$ et donc $TR_r(\zeta s) = 0$ pour tout $s \in \mathcal{R}$. Donc TR_r est 0 sur l'idéal (ζ). Comme TR_r est surjectif, il existe $\alpha \in \mathcal{R}$ tel que $TR_r(\alpha) = 1$ et donc $TR_r(2\alpha) = 2$. Par **lemme 3.15** (ζ) doit être l'idéal nul, donc $\zeta = 0$.

On va montrer que si $\mathbf{c}$ est en forme (3), alors $\mathbf{c} \in K(r+1)$. Comme $\mathbf{1}_n \in K(r+1)$, on doit montrer que $\mathbf{c} \in K(r+1)$ quand $\epsilon = 0$. ■

Lemme 7.6. *Soit $\mathcal{R} = GR(4^r)$ a un élément primitif ξ. Soit $n = 2^r - 1$. Supposons que $\lambda \in \mathcal{R}$ mais $\lambda \notin 2\mathcal{R}$. Alors tous les éléments de $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$ avec $\mathcal{S}_1 = \{\lambda(\xi^j - \xi^k) | 0 \geq j \geq n-1, 0 \geq k \geq n-1, j \neq k\}$ et $\mathcal{S}_2 = \{\pm\lambda\xi^j | 0 \geq j \geq n-1\}$ sont distinctes et ils sont les éléments de $\mathcal{R} \setminus 2\mathcal{R}$.*

Proof. On a le groupe des éléments inversible de $\mathcal{R}$ est $\mathcal{R} \setminus 2\mathcal{R}$. On doit montrer que $\mathcal{S}$ est inversible et distinct car $\mathcal{R} \setminus 2\mathcal{R}$ a $4^r - 2^r$ éléments et, si le

Comme λ est inversible, les éléments de $\mathcal{S}_2$ sont inversible. Donc les éléments de $\mathcal{S}_2$ sont distincts comme $-\xi^j = \xi^j + 2\xi^j$ est différent à ξ^k pour n'importe j et k.

Pour montrer que $\mathcal{S}_1$ est inversible, il suffit de montrer que $\xi^j - \xi^k$ est inversible pour $j \neq k$. Si il n'est pas inversible, $\xi^j - \xi^k \in 2\mathcal{R}$. Rappelons que la réduction homomorphisme modulo 2 $\overline{\mu} : \mathcal{R} \to \mathbb{F}_{2^r} = \mathcal{R}/2\mathcal{R}$ envoie l'élément primitif ξ de $\mathcal{R}$ dans $\overline{\mu}(\xi) = \theta$ de $\mathbb{F}_{2^r}$. Comme $\overline{\mu}(\xi)^j + \overline{\mu}(\xi)^k = 0$, implique $\theta^j + \theta^k = 0$. Mais $\theta^j \neq \theta^k$ pour $j \neq k$ et $0 \geq j, k \geq n-1$. Donc les éléments de $\mathcal{S}_1$ sont inversibles. On va montrer que les éléments de $\mathcal{S}_1$ sont distincts. Supposons que $\xi^j - \xi^k = \xi^l - \xi^m$ avec $j \neq k$ et $l \neq m$; alors

$$1 + \xi^a = \xi^b + \xi^c \tag{5}$$

avec $m - j \equiv a \bmod n$, $l - j \equiv b \bmod n$ et $k - j \equiv c \bmod n$. Alors $(1+\xi^a)^2 - v_2(1+\xi^a) = (\xi^b + \xi^c)^2 - v_2(\xi^b + \xi^c)$, implique que $1 + \xi^{2a} + 2\xi^a - v_2(1) -$

$v_2(\xi^a) = \xi^{2b} + \xi^{2c} + 2\xi^{b+c} - v_2(\xi^b) - v_2(\xi^c)$ avec v_2 est automorphisme Frobenius. Donc $2\xi^a = 2\xi^{b+c}$ et donc $a \equiv b + c \bmod n$. Alors si $x = \theta^a$, $y = \theta^b$ et $z = \theta^c$ alors $x = yz$. En applicant $\overline{\mu}$ sur (4), on a $1 + x = y + z$. Donc $0 = 1 + yz + y + z = (1 + y)(1 + z)$ qui est dans $\mathbb{F}_{2^r}$, implique $y = 1$ ou $z = 1$. Alors $b \equiv 0 \bmod n$ ou $c \equiv 0 \bmod n$. Donc $l = j$ ou $k = j$ (impossible), implique $k = m$. Donc les éléments de $\mathcal{S}_1$ sont distincts.

On doit montrer au final que les éléments de $\mathcal{S}_1 \cup \mathcal{S}_2$ sont distincts. Supposons que $\xi^j - \xi^k = \pm\xi^m$. En factoriser un puissance de ξ, on obtient $1 + \xi^a = \xi^b$. Alors $(1 + \xi^a)^2 - v_2(1 + \xi^a) = \xi^{2b} - v_2(\xi^b)$, qui donne $1 + 2\xi^a + \xi^{2a} - (1 + \xi^a) = xi^{2b} - \xi^{2b} = 0$. Donc $2\xi^a = 0$ contradiction. ■

On va définir la distribution de poids de Lee de $\overline{K}(r + 1)$, qui est aussi a distribution de poids de Hamming du code Kerdock binaire $\mathcal{K}(r+1) = \mathfrak{G}(\overline{K}(r+1))$ par **théorème 2.3**.

Théorème 7.7. *Soit $r \geq 3$ r impair. Soit A_i le nombre de vecteurs dans $\overline{K}(r + 1)$ de poids de Lee 1. Alors*

$$A_i = \begin{cases} 1 & si \quad i = 0, \\ 2^{r+1}(2^r - 1) & si \quad i = 2^r - 2^{(r-1)/2}, \\ 2^{r+1} - 2 & si \quad i = 2^r, \\ 2^{r+1}(2^r - 1) & si \quad i = 2^r + 2^{(r-1)/2}, \\ 1 & si \quad i = 2^{r+1}, \\ 0 & sinon \end{cases}$$

C'est aussi le poids de Hamming du code Kerdock $\mathcal{K}(r + 1)$

Proof. Soit $\mathcal{R} = GR(4^r)$ et $\mathbf{v}_\lambda = \{(TR_r(\lambda), TR_r(\lambda\xi), TR_r(\lambda\xi^2), ..., TR_r(\lambda\xi^{n-1}))$ avec $n = 2^r - 1$. Par **lemme 7.5**, les vecteurs dans $\overline{K}(r + 1)$ a la forme $(0, \mathbf{v}_\lambda + \epsilon\mathbf{1}_{n+1}$ pour $\lambda \in \mathcal{R}$ et $\epsilon \in \mathbb{Z}_4$. On calcule le poids de Lee en considérant 3 cas:
Cas I: $\lambda = 0$
$\mathbf{v}_\lambda$ est un vecteur nul, et $(0,\mathbf{v}_\lambda) + \epsilon\mathbf{1}_{n+1} = \epsilon\mathbf{1}_{n+1}$ a poids de Lee 0 is $\epsilon = 0$, $n + 1 = 2^r$ si $\epsilon = 1$ ou 3, et $2(n + 1) = 2^{r+1}$ si $\epsilon = 2$. On obtiendra un vecteur de poids de Lee 0, deux vecteurs de poids de Lee 2^r et un vecteur de poids de Lee 2^{r+1}
Cas II: $\lambda \in 2\mathcal{R}$ avec $\lambda \neq 0$
Donc $\lambda = 2\xi^i$ pour $0 \geq i \geq n - 1$. Donc le groupe des composants de $\mathbf{v}_\lambda$ $\{TR_r(2\xi^j)|0 \geq i \geq n - 1\}$ est toujours indépendent de i. Mais il y a 2^{r-1} valeurs sont 2 et l'autre $2^{r-1} - 1$ sont 0. Donc tout vecteur $(0, \mathbf{v}_j) + \epsilon\mathbf{1}_{n+1}$ a soit 2^{r-1} valeurs 2 et 2^{r-1} valeurs 0 quand $\epsilon = 0$ ou 2; ou soit 2^{r-1} valeurs 1 et 2^{r-1} valeurs 3 quand $\epsilon = 1$ ou 3. Dans tous les cas, le poids Lee de ces vecteurs est 2^r. Il y a $4n = 2^{r+2} - 4$ vecteurs.
Cas III:$\lambda \in \mathcal{R}$ avec $\lambda \neq 2\mathcal{R}$

Soit $\mathcal{R}^{\#} = \mathcal{R} \setminus 2\mathcal{R}$. Pour $j \in \mathbb{Z}_4$, $n_j = n_j(\mathbf{v}_\lambda)$ est le nombre des composants de $\mathbf{v}_\lambda$ égaux à j. Soit $i = \sqrt{-1}$. On définie:

$$S = \sum_{j=0}^{n-1} i^{TR_r(\lambda\xi^i)} = n_0 - n_2 + i(n_1 - n_3) \tag{6}$$

Si $\overline{S}$ le conjugué de S. Alors:

$$\begin{aligned} S\overline{S} &= \sum_{j=0}^{n-1} i^{TR_r(\lambda(\xi^j - \xi^j))} + \sum_{j \neq k} i^{TR_r(\lambda(\xi^j - \xi^k))} \\ &= 2^r - 1 + \sum_{a \in \mathcal{R}^{\#}} i^{TR_r(a)} - \sum_{j=0}^{n-1} i^{TR_r(\lambda\xi^i)} - \sum_{j=0}^{n-1} i^{TR_r(-\lambda\xi^i)} \\ &= 2^r - 1 + \sum_{a \in \mathcal{R}^{\#}} i^{TR_r(a)} - S - \overline{S}. \end{aligned} \tag{7}$$

Mais $\sum_{a \in \mathcal{R}} i^{TR_r(a)} = \sum_{a \in \mathcal{R}} i^{TR_r(a)} - \sum_{a \in 2\mathcal{R}} i^{TR_r(a)} = 0$. Donc on aura $(S+1)(\overline{S}+1) = 2^r$, donc

$$(n_0 - n_2 + 1)^2 + (n_1 - n_3)^2 = 2^r$$

par (5). En calculant les solutions de l'équation $x^2 + y^2 = 2^r$ (**exercice 7.8**), on a $x = \delta_1 2^{(r-1)/2}$, $y = \delta_2 2^{(r-1)/2}$ avec δ_1 et δ_2 sont ± 1. Par (6), on obtient:

$$n_0 - n_2 = -1 + \delta_1 2^{(r-1)/2} \qquad n_1 - n_3 = \delta_2 2^{(r-1)/2}$$

Pourtant $2\mathbf{v}_\lambda = \mathbf{v}_{2\lambda}$ est un vecteur dans le cas II, alors:

$$n_0 + n_2 = 2^{r-1} - 1 \qquad n_1 + n_3 = 2^{r-1}$$

En solvant le système de 4 équations ci-dessus:

$$n_0 = 2^{r-2} + \delta_1 2^{(r-3)/2} - 1 \tag{8}$$

$$n_1 = 2^{r-2} + \delta_2 2^{(r-3)/2} \tag{9}$$

$$n_2 = 2^{r-2} - \delta_1 2^{(r-3)/2} \tag{10}$$

$$n_3 = 2^{r-2} + \delta_2 2^{(r-3)/2} \tag{11}$$

On obtient:

$\epsilon \setminus j$	0	1	2	3	Poids Lee
0	$n_0 + 1$	n_1	n_2	n_3	$2^r - \delta_1 2^{(r-1)/2}$
1	n_3	$n_0 + 1$	n_1	n_2	$2^r + \delta_2 2^{(r-1)/2}$
2	n_2	n_3	$n_0 + 1$	n_1	$2^r + \delta_1 2^{(r-1)/2}$
3	n_1	n_2	n_3	$n_0 + 1$	$2^r - \delta_2 2^{(r-1)/2}$

La dernière colonne est obtenu par $wt_L((0, \mathbf{v}_\lambda) + \epsilon\mathbf{1}_{n+1}) = n_1((0, \mathbf{v}_\lambda) + \epsilon\mathbf{1}_{n+1}) + 2n_2((0, \mathbf{v}_\lambda) + \epsilon\mathbf{1}_{n+1}) + n_3((0, \mathbf{v}_\lambda) + \epsilon\mathbf{1}_{n+1})$ en utilisant (8), (9), (10), (11).
Donc il y a $2(4^r - 2^r) = 2^{r+1}(2^r - 1)$ mots du code de poids Lee $2^r - 2^{(r-1)/2}$ et $2(4^r - 2^r) = 2^{r+1}(2^r - 1)$ mots du code de poids Lee $2^r + 2^{(r-1)/2}$ ■

Exercice 7.8. *Soit $r \geq 3$ impair. Soit x et y sont les solutions entiers de $x^2 + y^2 = 2^r$. On a les suivants:*

i. Montrer que x et y sont pairs

ii. Montrer que x et y sont les solutions entiers de $x^2+y^2 = 2^r$ si et seulement si x_1 et y_1 sont les solutions entiers de $x_1^2 + y_1^2 = 2^{r-2}$ avec $x_1 = \frac{x}{2}$ et $y_1 = \frac{y}{2}$

iii. Montrer que les solutions uniques de $x^2 + y^2 = 2^r$ sont $x = \pm 2^{(r-1)/2}$ et $y = \pm 2^{(r-1)/2}$.

Proof.

i. Supposons que x et y sont impair. Posons $x = 2a + 1$ et $y = 2b + 1$ avec $a, b \in \mathbb{Z}$. Alors on a $(2a + 1)^2 + (2b + 1)^2 = 4(a^2 + a + b^2 + b) + 2 = 2(2(a^2 + a + b^2 + b) + 1) = 2^r$. Donc $2(a^2 + a + b^2 + b) + 1 = 2^{r-1}$, contradiction.
Supposons maintenant que x ou y est impair (le rôle de x et y sont équivalents). Posons $x = 2a + 1$ et $y = 2b$, alors on a $(2a + 1)^2 + 4b^2 = 4(a^2 + a + b^2) + 1 = 2^r$, contradiction
Donc x et y sont pairs.

ii. Posons $x = 2x_1$ et $y = 2y_1$. Comme x et y sont les solutions de $x^2 + y^2 = 2^r$, alors $(2x_1)^2 + (2y_1)^2 = 2^r$, implique $x_1^2 + y_1^2 = 2^{r-2}$.
Inversement, supposons que x_1 et y_1 sont les solutions entiers de $x_1^2+y_1^2 = 2^{r-2}$ avec $x_1 = \frac{x}{2}$ et $y_1 = \frac{y}{2}$. Alors on a $(\frac{x}{2})^2 + (\frac{y}{2})^2 = 2^{r-2}$, implique $\frac{x^2}{4} + \frac{y^2}{4} = \frac{2^r}{4}$ donc $x^2 + y^2 = 2^r$.

iii. Comme l'équation est symétrique, le rôle de x et y sont équivalents, on peut supposer que $x = y$. On obtient $2x^2 = 2^r$ implique $x^2 = 2^{r-1}$. Donc $x = \pm 2^{(r-1)/2}$, d'où $y = \pm 2^{(r-1)/2}$.

■

8 Codes Preparata

Les codes Preparata binaires sont les codes non linéaires avec distance invariant de longueur 2^{r+1} et distance minimale 6. Ils sont sous groupes des codes Hamming étendus.

Théorème 8.1. *Soit $r \geq 3$ impair. Alors $P(r + 1)$ et $\mathcal{P}(r + 1)$ sont les codes avec distances invariants. L'énumérateur de poids de Lee de $P(r + 1)$, qui est*

aussi l'énumérateur de poids de Hamming de $\mathcal{P}(r+1)$ est:

$$\begin{aligned} Lee_{P(r+1)}(x,y) =& \frac{1}{4^{r+1}}[(y-x)^{2^{r+1}} + (y+x)^{2^{r+1}} \\ &+ 2^{r+1}(2^r-1)(y-x)^{2^r-2^{(r-1)/2}}(y+x)^{2^r+2^{(r-1)/2}} \\ &+ 2^{r+1}(2^r-1)(y-x)^{2^r+2^{(r-1)/2}}(y+x)^{2^r-2^{(r-1)/2}} \\ &+ (2^{r+2}-2)(y-x)^{2^r}(y+x)^{2^r}]. \end{aligned}$$

Si $B_j(r+1)$ est le nombre de mot de code dans $P(r+1)$ de poids de Lee j, qui est aussi e nombre de mot de code dans $\mathcal{P}(r+1)$ de poids de Hamming j, alors

$$\begin{aligned} B_j(r+1) =& \frac{1}{4^{r+1}}[K_j^{2^{r+1},2}(0) + 2^{r+1}(2^r-1)K_j^{2^{r+1},2}(2^r-2^{(r-1)/2}) \\ &+ (2^{r+2}-2)K_j^{2^{r+1},2}(2^r) + 2^{r+1}(2^r-1)K_j^{2^{r+1},2}(2^r+2^{(r-1)/2}) \\ &+ K_j^{2^{r+1},2}(2^{r+1})]. \end{aligned}$$

avec $K_j^{2^{r+1},2}$ est le polynôme Krawtchouck. De plus, la distance minimum de $\mathcal{P}(r+1)$ est 6 et $B_j(r+1) = 0$ si j est impair.

References

[1] Huffman, W. Cary, and Vera Pless. *Fundamentals of error-correcting codes. Chapter 12.* Cambridge university press, 2010.