Faculté Des Sciences Dhar El Mahraz-Fès
Département de Mathématiques
Laboratoire : LSMA
Formation doctorale en
Algèbre, Théorie des nombres et leurs applications
Du 28/11/2019 au 30/11/2019

Codes correcteurs d'erreurs

Par : Ahmed Najim

Table des matières

1 Introduction

L'orgine de la théorie des codes correcteurs est un article intitulé "A mathematical theory of communication" et publié par Claude Shannon en 1948. Dans cet article Shannon a associe à chaque canal de transmission un nombre, appelé la capacité, et montre qu'en dessous de ce nombre une communication sûre est possible.

La théorie des codes correcteurs est destinée à corriger les erreurs de transmission d'une information (plus souvent appelée message) sur un canal de communication peu fiable. Autrement dit, les données, lorsqu'elles circulent sur cette voie, sont susceptibles d'être altérées (par des phénomènes d'origines diverses : mécaniques, électriques, électromagnétiques, ...). Cette théorie a pour but la créeation de codes capables de détecter et éventuellement de corriger des erreurs survenus lors de la transmission d'un message. Cette théorie ne se limite pas qu'aux communications classiques (radio, câble coaxial, fibre optique, ...) mais également aux supports pour le stockage comme les disques compacts, la mémoire RAM et d'autres applications où la garantie de l'intégrité des données est importante.

Dans un grand nombre de cas et de situations l'intégrité absolue des données est exigée sans nouvelle demande de transmission (navette spatiale, disques durs, CD, ...). Il y a alors essentiellement deux approches possibles :
- augmenter la puissance de l'émission ;
- ajouter de la redondance à l'information.

Un code correcteur (error-correcting code ou ECC) est une technique de codage basée sur la redondance.

Le but de ce cours est d'introduire les concepts de base de l'étude des codes correcteurs d'erreurs. Ainsi, dans ce cours on présente les notions essentiels des codes correcteurs, des codes linéaires et des codes constacycliques sur un corps fini.

2 Codes et distance de Hamming

2.1 Codes correcteurs

Dans tout ce qui suit n désigne un entier naturel non nul.

Définition 2.1. *Soit F un ensemble fini. On appelle mot (de longueur n) une suite $a_1a_2...a_n$ où pour tout $i \in \{1, 2, ..., n\}$, $a_i \in F$ (F est l'alphabet).*

Définition 2.2. *Un code est un ensemble de mots construits sur un alphabet F.*

Définition 2.3. *Un codage par blocs est un code tel que tous les mots ont la même longueur, c'est donc un sous ensemble de F^n où F est l'alphabet du code.*

Remarque 2.1. *L'alphabet le plus utilisé est $\{0, 1\}$.*

Dans ce cours on ne considérera que les codes en bloc.

2.2 Distance de Hamming

Soit F un ensemble fini non vide.

Définition 2.4. *Soient $a, b \in F^n$. La distance de Hamming $d(a,b)$ entre a et b est le nombre de composantes pour lesquelles a et b diffèrent (i.e. si $a = (a_1, a_2, ..., a_n)$ et $b = (b_1, b_2, ..., b_n)$, alors $d(a,b) = Card\{i \in \{1,2,...,n\},\ tq\ a_i \neq b_i\}$).*

Exemple 2.1. *Dans $\{0,1\}^4$ on a $d(0101, 1110) = 3$.*

Proposition 2.1. *La distance de Hamming est bien une distance.*

La distance minimale d'un code C est donnée par :

$$d = min\{d(a,b);\ a, b \in C\}.$$

Le problème principal de la théorie des codes :

On suppose que F a q éléments. Un code q-aire de type $[n, M, d]$ est une partie de F^n ayant M éléments et de distance minimal égale à d.
Un bon code doit satisfaire les conditions suivantes :
1- n doit être petit (rapidité et coût de transmission).
2- M doit être grand (pour permettre une grande variété de messages).
3- d doit être grand (pour détecter et éventuellement corrigés beaucoup d'erreurs).

2.3 Stratégie de décodage

Dans le reste de cette section F dénote un alphabet fini ayant q éléments.

Soit C un code q-aire de type $[n, M, d]$. Soit b dans F^n, un mot reçu. S'il existe a dans C unique tel que a soit le mot de C le plus proche de b, on décode b par a. Si l'ensemble B des a, qui ont cette propriété, a plus d'un élément, on dit qu'on a un nœud et on décode par un élément quelconque de B.
On dit que c'est un décodage par distance minimale. Dans le cas d'un nœud, cette stratégie ne permet pas la correction de l'erreur.

Définition 2.5. *Soient C un code et t un entier ≥ 1.*
1- On dit que C corrige t erreurs si chaque fois qu'il y a k erreurs dans un mot reçu, avec $0 \leq k \leq t$, le décodage par distance minimale corrige ces erreurs.
2- On dit que C corrige exactement t erreurs s'il corrige t erreurs mais ne corrige pas $t+1$ erreurs.

Définition 2.6. *Un code C de longueur n sur l'alphabet F vérifie la condition de décodage d'ordre t si pour tout $b \in F^n$ il existe au plus un mot $a \in C$ tel que $d(a,b) \leq t$.*

Définition 2.7. *Soit a un élément de F^n. Pour un entier r strictement positif, on appelle boule de centre a et de rayon r l'ensemble*

$$B_q(a,r) = \{x \in F^n \mid d(a,x) \leq r\}.$$

Remarque 2.2. *Si un code C de longueur n sur l'alphabet F vérifie la condition de decodage d'ordre t, alors les boules fermées de centres les éléments de C et de rayon t sont deux à deux disjointes.*

Proposition 2.2. *Soit t un entier strictement positif. Si la distance minimale d d'un code C vérifie $d \geq 2t+1$, alors C corrige t erreurs.*

Preuve. Si $a \in C$ est un mot envoyé et $b \in F$ reçu, tels que $d(a,b) \leq t$. Soit $a' \in C$ tel que $a \neq a'$. Comme $d(a,a') \geq 2t+1$ et $d(b,a') \geq d(a,a') - d(a,b)$, alors $d(a',b) \geq t+1$. Donc, C peut corriger t erreurs. □

Théorème 2.1. *Tout code q-aire de type $[n,M,d]$ corrige exactement e erreurs, où e est la partie entière de $\frac{d-1}{2}$.*

Preuve. Soit C un code q-aire de type $[n,M,d]$ et soit e la partie entière de $\frac{d-1}{2}$. On a $d \geq 2e+1$ puisque $d = 2e+1$ ou $d = 2e+2$. Alors, la proposition 2.2 montre que C corrige e erreurs. Le code C ne corrige pas $e+1$ erreurs. En effet, $d = 2e+k$ avec $k \in \{1,2\}$. Soient $a, a' \in C$ tels que $d(a,a') = d = 2e+k$. On a $a_i = a'_i$, sauf aux indices $i_1, i_2, ..., i_{2e+k}$. Il existe $b \in F^n$ tel que :

$$\begin{aligned} b_i &= a_i \text{ sauf pour } i = i_1, i_2, ..., i_{e+1}, \\ b_i &= a'_i \text{ sauf pour } i = i_{e+2}, i_{e+3}, ..., i_{2e+k}. \end{aligned}$$

On suppose que a soit le mot envoyé et b soit le mot reçu. On a $d(a,b) = e+1$ et $d(a',b) = e+k-1$. Si $k = 1$, alors la stratégie de décodage commande de décoder b par a', ce qui constitue une erreur. Si $k = 2$, alors on a un nœud. □

Exercices

Exercise 2.1. *Prouver la proposition 2.1.*

Exercise 2.2. *Trouver la distance minimale du code binaire suivant :*

$$\{110001, 100111, 001111, 111011, 101000\}.$$

Exercise 2.3. *Construire un code binaire de 4 mots, de longueur 3 et de distance minimale 2.*

Exercise 2.4. *Soit t un entier strictement positif. Montrer que si la distance minimale d d'un code C vérifie $d \geq t+1$, alors C peut détecter t erreurs.*

Exercise 2.5. *Montrer que s'il existe un code q-aire de type $[n,M,d]$, alors $M \leq q^{n-d+1}$.*

3 Codes linéaires

Désormais, l'alphabet est un corps fini $\mathbb{F}_q$, à q éléments.

3.1 Définition et description

Définition 3.1. *Un code dans $\mathbb{F}_q^n$ est dit linéaire de type $[n,k]$ si c'est un sous-espace vectoriel de $\mathbb{F}_q^n$, de dimension k.*

Les codes sur $\mathbb{F}_2$ sont dits codes binaires et les codes sur $\mathbb{F}_3$ sont dits codes trinaires.

Le poids d'un mot $a = a_1a_2...a_n$ de $\mathbb{F}_q^n$ est donné par :

$$\omega(a) = Card\{i \in \{1,2,...,n\} \mid a_i \neq 0\}.$$

Le poids minimal d'un code linéaire C est donné par :

$$\omega(C) = min\{\omega(a) \mid a \in C, a \neq 0\}.$$

Théorème 3.1. *Si $a, b \in \mathbb{F}_q^n$, alors $d(a,b) = \omega(a-b)$. Si C est un code linéaire, alors sa distance minimale est égale à sont poids minimal.*

Si un code linéaire de longueur n est de dimension k et de distance minimale d, alors il est dit de type $[n,k,d]$.

Remarque 3.1. *On peut calculer la distance de Hamming entre deux mots de $\mathbb{F}_2^n$ en faisant leur somme et en comptant le nombre de 1.*

Définition 3.2. *Soient C un code linéaire de type $[n,k]$ et G une matrice $k \times n$ sur $\mathbb{F}_q$.*
1− G est une matrice génératrice de C si les vecteurs lignes de G forment une base de l'espace vectoriel C.
2− La matrice G est sous-forme standard si $G = [I_k|A]$, où I_k est la matrice unité $k \times k$ et A est une matrice $k \times (n-k)$.

Remarques 3.1. 1− *En général il y a plusieurs matrices génératricse pour un code linéaire.*
2− *Si G est une matrice génératrice d'un code C de type $[n,k]$ (sur $\mathbb{F}_q$), alors $C = \{uG \in \mathbb{F}_q^n \mid u \in \mathbb{F}_q^k\}$.*

Exemple 3.1. *Soit*

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

une matrice génératrice d'un code linéaire binaire. Les mots de ce code sont $00.G = 000$, $01.G = 101$, $10.G = 011$, $11.G = 110$.

Il est à noter que si C est un code linéaire de type $[n,k]$ sur $\mathbb{F}_q$, alors C est l'image de l'application linéaire (injective) $g : \mathbb{F}_q^k \to \mathbb{F}_q^n$ qui fait correspondre à une base de $\mathbb{F}_q^k$ une base de C. La matrice de g (dans les bases canoniques) est une matrice génératricse de C.

Maintenant, soit C est un code linéeaire de type $[n,k]$ sur $\mathbb{F}_q$. Comme C est un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension k, alors C est le noyau d'une application linéaire $h : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$. En particulier, il existe une matrice H $(n-k) \times n$ telle que $C = \{u \in \mathbb{F}_q^n \mid H^t u = 0\}$, où ${}^t u$ est le vecteur colonne tramsposé du vecteur ligne u.

Définition 3.3. *Soit C un code linéeaire de type $[n,k]$ sur $\mathbb{F}_q$. Une matrice H $(n-k) \times n$ à coefficients dans $\mathbb{F}_q$ est dite matrice de contrôle de C si $C = \{u \in \mathbb{F}_q^n \mid H^t u = 0\}$.*

Remarque 3.2. *En général il y a plusieurs matrices de contrôle pour un code linéaire.*

Dans la proposition suivante A^t désigne la matrice transposée de la matrice A.

Proposition 3.1. *Si $G = [I_k|A]$ est la matrice génératrice sous-forme standard d'un code C de type $[n, k]$, alors $H = [-A^t|I_{n-k}]$ est une matrice de contôle de C.*

Preuve. On a $HG^t = -A^t + A^t = 0$. Donc, C est inclu dans le noyau de l'application linéaire $x \mapsto Hx^t$. Comme H est de rang $n - k$, alors le noyau de cette application linéaire est de dimension k, qui est encore la dimension de C. Le résultat s'ensuit. □

3.2 Codes duaux

Le produit scalaire standard de deux vecteurs $a = a_1a_2...a_n$ et $b = b_1b_2...b_n$ de $\mathbb{F}_q^n$ est $a.b = \sum_{i=1}^{n} a_ib_i$.

Définition 3.4. *Soit C un code linéaire de longueur n. Le code dual du C est le code*

$$C^\perp = \{a \in \mathbb{F}_q^n \mid a.b = 0,\ \forall b \in C\}.$$

Proposition 3.2. *Soit C un code linéaire de $[n, k]$. Alors, on a :*
1− $C^\perp$ est un code de type $[n, n - k]$;
2− $(C^\perp)^\perp = C$.

Théorème 3.2. *Si C est un code linéaire de type $[n, k, d]$ avec matrice de contrôle H, alors d est le nombre minimal de colonnes de H linéairement dépendantes.*

Preuve. Soit $x \in C$ de poids d. On a $x\,{}^tH = 0$. Donc, si $h_1, ..., h_n$ sont les vecteurs colonnes de H, et si $i_1, ..., i_d$ sont les indices où $x_i \neq 0$, alors $x_{i_1}h_{i_1} + ... + x_{i_d}h_{i_d} = 0$. Par conséquent, les colonnes $h_1, ..., h_n$ sont linéairement dépendantes.
Réciproquement, si $h_{i_1}, ..., h_{i_m}$ sont les m colonnes linéairement dépendantes de H. Alors, il existe $a_{i_1}, ..., a_{i_m} \in \mathbb{F}_q$ tels que $a_{i_1}h_{i_1} + ... + a_{i_m}h_{i_m} = 0$. Soit $a = a_1a_2...a_n \in \mathbb{F}_q^n$, où $a_i = a_{i_j}$ s'il existe $i_j \in \{i_1, ..., i_m\}$ tel que $i = i_j$ et $a_i = 0$ si $i \notin \{i_1, ..., i_m\}$. Alors, a vérifie la relation précédente et $\omega(a) \leq m$. Donc, $d \leq m$. □

3.3 Codes linéaires équivalents

Définition 3.5. *Soinet C et C' deux codes linéaires dans $\mathbb{F}^n$. On dit que C et C' sont équivalents si C' est l'image de C par une permutation des indices, c'est à dire, s'il existe une permuatation σ de $\{1, 2, ..., n\}$ telle que $C' = \{a_{\sigma(1)}a_{\sigma(2)}...a_{\sigma(n)} \mid a_1a_2...a_n \in C\}$.*

Remarques 3.2. *1− Si C et C' sont équivalents, alors l'ensemble des distances entre les éléments de C est identique à celui de C'. Il s'ensuit que C et C' ont la même distance minimale.*
2− La relation d'être équivalent est une relation d'équivalence.
3− A l'aide des opérations élémentaires sur les lignes et des permutations des colonnes d'une matrice génératrice d'un code linéaire, on peut réduire cette matrice à la forme standard. Le code engendré par cette matrice est équivalent au code initial.

Exercices

Exercise 3.1. *Prouver le théorème 3.1.*

Exercise 3.2. *Prouver la proposition 3.2.*

Exercise 3.3. *Prouver que si G et H sont les matrices génératrice et de contrôle, respectivement, d'un code linéaire C, alors H et G sont les matrices génératrice et de contrôle, respectivement, de $C^{\perp}$.*

Exercise 3.4. *Un code liéaire C de longueur n est dit auto-dual si $C = C^{\perp}$. Montrer que tout code auto-dual est de dimension $\frac{n}{2}$.*

Exercise 3.5. *Soit C un code linéaire binaire qui admet*

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

comme matrice génératrice. Trouver une matrice génératrice de C sous-forme standard.

4 Codes constacycliques

4.1 Codes cycliques

Définition 4.1. *Soit C un code de longueur n sur $\mathbb{F}_q$. Le code C est cyclique si :*
i) C est un code linéaire ;
ii) si $(a_1, ..., a_n) \in C$, alors $(a_n, a_1, ..., a_{n-1}) \in C$.

Il est facile de voir qu'un code linéaire de longueur n sur $\mathbb{F}_q$ est cyclique si $(a_1, ..., a_n) \in C$ implique $(a_2, a_3, ..., a_n, a_1) \in C$.

Représentation polynômiale :

Dans l'anneau quotient $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$, on note par x la classe de X. Alors, l'application

$$\begin{array}{ccc} \psi : \mathbb{F}_q^n & \longrightarrow & \frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle} \\ (a_0, a_1, ..., a_{n-1}) & \longmapsto & a_0 + a_1x + ... + a_{n-1}x^{n-1} \end{array}$$

est un isomorphisme de $\mathbb{F}_q$-espace vectoriels.

A partir de maintenant, on fait l'identification suivante :

$$c = (a_0, a_1, ..., a_{n-1}) \in \mathbb{F}_q^n \leftrightarrows c(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} \in \frac{\mathbb{F}_q[X]}{\langle X^n - 1\rangle},$$

et on parlera du mot de code (codeword) $c(x)$ comme étant le mot de code c, utilisant cette identification.
Prolangeant ceci, on interprète un code linéaire comme un sous-ensemble (sous-espace vectoriel) de $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$.

Théorème 4.1. *Un code linéaire C dans $\mathbb{F}_q^n$ est cyclique si et seulement si C est un idéal de $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$.*

Preuve. Si C est un idéal de $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$ et $c(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ est un mot de code, alors $xc(x)$ est aussi un mot de code, i.e.

$$(a_{n-1}, a_0, a_1, ..., a_{n-2}) \in C.$$

Réciproquement, si C est cyclique, alors pour tout mot de code $c(x)$ le mot $xc(x)$ est aussi dans C. Par conséquent, $x^ic(x)$ est aussi dans C pour tout i, et comme C est un code linéaire $a(x)c(x)$ est dans C pour tout $a(x)$ in $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$. Donc, C est un idéal de $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$. □

Conséquence : Rechercher tous les codes cycliques de longueur n sur $\mathbb{F}_q$ revient à rechercher tous les idéaux de $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$.

Soit ϕ le morphisme canonique de $\mathbb{F}_q[X]$ vers $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$. Soit C un idéal de $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$, non réduit à $\{0\}$, et soit I l'image réciproque de C par ϕ. Comme $\mathbb{F}_q[X]$ est un anneau principal, alors l'idéal I est principal, engendré par un polynôme qu'on choisit d'être unitaire g. Comme ϕ est surjetif, alors $C = \phi(I)$, et donc lidéal I est principal. Par conséquent, l'anneau $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$ est un anneau principal, et on voit que la factorisation de $X^n - 1$ en facteur irréductibles dans $\mathbb{F}_q[X]$ détermine tous les codes cycliques de longueur n.
D'aurtre part, comme $X^n - 1 \in I$, alors g divise $X^n - 1$, et donc il existe $h \in \mathbb{F}_q[X]$ tel que $X^n - 1 = g(X)h(X)$. Le polynôme g est appelé le polynôme générateur du code cyclique C et le polynôme h est appelé le polynôme de contrôle du code cyclique C.

Théorème 4.2. *Soit C un code cyclique de type $[n, k]$ dans $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$.*
1− Si $g = g_0 + g_1X + ... + g_rX^r$ $(r = n - k)$ est le polynôme générateur de C, alors la matrice génératrice de C est la matrice à k lignes et n colonnes suivante

$$\begin{pmatrix} g_0 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_r & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & g_0 & \cdots & g_r \end{pmatrix}.$$

2− Si h est le polynôme de contrôle de C, alors

$$C = \{a(x) \in \frac{\mathbb{F}_q[X]}{\langle X^n - 1\rangle} \mid a(x)h(x) = 0\}.$$

Preuve. 1− Il suffit de voir que $g(x), xg(x), ..., x^{k-1}g(x)$ forment une base de C.
2− Si $a(x) \in C$, alors $g(X)$ divise $a(X)$. Par suite, $g(X)h(X)$ divise $a(X)h(X)$. Ainsi $X^n - 1$ divise $a(X)h(X)$, et par conséquent $a(x)h(x) = 0$.
Réciproquement, soit $a(x) \in \frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$ tel que $a(x)h(x) = 0$. Alors, $g(X)h(X)$ $(= X^n - 1)$ divise $a(X)h(X)$. Par conséquent, $g(X)$ divise $a(X)$. Donc, $a(x) \in C$. □

Théorème 4.3. *Soit C un code cyclique de type $[n, k]$ dans $\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}$. Si $h = h_0+h_1X+...+h_kX^k$ est le polynôme de contrôle de C, alors*

1− *la matrice de contrôle de C est la matrice à $n-k$ lignes et n colonnes suivante*

$$\begin{pmatrix} h_k & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_k & \cdots & h_0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & h_k & \cdots & h_0 \end{pmatrix};$$

2− *le code dual $C^\perp$ est cyclique engendré par le poynôme $h_0^{-1}x^k h(\frac{1}{x})$.*

Preuve. 1− Soit $a(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} \in C$. Comme $a(x)h(x) = 0$, d'après le théorème 4.2, alors $H^t(a_0, a_1, ..., a_{n-1}) = 0$. Soit $C' = \{u \in I\!F_q^n \mid H^t u = 0\}$. On a $C \subseteq C'$. Comme $h_{n-r} \neq 0$, les lignes de H sont linéairement indépendantes, et donc H est de rang $n-k$. Donc, $dim\, C' = k = dim\, C$ (puisque C' est le noyau de l'application linéaire définie par H). D'où $C' = C$. Par définition, la matrice H est une matrice de contrôle de C.
2− $h_0^{-1}X^k h(\frac{1}{X})$ est unitaire et divise $X^n - 1$. En efft, comme $h(X)g(X) = X^n - 1$, alors $X^k h(\frac{1}{X}X^{n-k}g(\frac{1}{X}) = 1 - X^n$. D'après le théorème 4.2, le code engendré par le polynôme $h_0^{-1}x^k h(\frac{1}{x}) = h_0^{-1}(h_0x^k + h_1x^{k-1} + ... + h_k)$ est celui qui admet la matrice H comme matrice génératrice. D'après l'exercice 3.3, le code engendré par H est $C^\perp$. Donc, $h_0^{-1}x^k h(\frac{1}{x})$ engendre $C^\perp$. □

4.2 Décomposition de $X^n - 1$ sur $\mathbb{F}_q$

Dans cette section on suppose que n et q sont premiers entre eux.

Soit r un entier avec $0 \leq r \leq n-1$. La q-classe cyclotomique de r modulo n est déninie par :

$$C_r = \{r.q^j \pmod n \mid j = 0, 1, ...\}.$$

Il est à noter que $C_r = \{r, r.q, ..., , r.q^e\}$, où e est le plus petit entier positif tel que $rq^e \equiv r \pmod n$. Les q-classes cyclotomiques modulo n font une partition de l'ensemble des entiers $\{0, 1, 2, ..., n-1\}$. Un sous-ensemble $\{r_1, r_2, ..., r_\rho\}$ de $\{0, 1, ..., n-1\}$ est appelé ensemble complet des représentants de toutes les q-classes cyclotomiques modulo n si $C_{r_1}, C_{r_2}, ..., C_{r_\rho}$ sont distictes et

$$\bigcup_{i=1}^{\rho} C_{r_i} = \{0, 1, ..., n-1\}.$$

Soit t le plus petit entier non nul tel que n divise $q^t - 1$. L'entier t est l'ordre multiplicatif de q modulo n noté par $ord_n(q)$. Alors, $X^n - 1$ divise $X^{q^t} - 1$ et donc les racines de $X^n - 1$ sont dans $\mathbb{F}_{q^t}$.

Théorème 4.4. *Soit $t = ord_n(q)$. Soit η une racine primitive $n^{ième}$ de l'unité dans $\mathbb{F}_{q^t}$.*
1− *Pour chaque r avec $0 \leq r \leq n-1$, le polynôme minimal de η^r sur $\mathbb{F}_q$ est*

$$M_{\eta^r}(X) = \prod_{i \in C_r} (X - \eta^i);$$

où C_r est la q-classe cyclotomique de r modulo n.
2− *Si $\{r_1, r_2, ..., r_\rho\}$ est un ensemble complet des représentants de toutes les q-classes cyclotomiques modulo n, alors la factorisation de $X^n - 1$ en facteurs irréductibles dans $\mathbb{F}_q[X]$ est donnée par*

$$X^n - 1 = M_{\eta^{r_1}}(X) M_{\eta^{r_2}}(X) ... M_{\eta^{r_\rho}}(X).$$

4.3 Codes constacycliques

Définition 4.2. *Soit λ un élément non nul de $\mathbb{F}_q$. Un code C de longueur n sur $\mathbb{F}_q$ est dit λ-constacyclique si :*

i) C est un code linéaire ;

ii) si $(a_1, ..., a_n) \in C$, alors $(\lambda a_n, a_1, ..., a_{n-1}) \in C$.

Soit λ un élément non nul de $\mathbb{F}_q$. Si $\lambda = 1$, les codes λ-constacycliques sont les codes cycliques. Si $\lambda = -1$, les codes λ-constacycliques sont appelés codes négacycliques. Comme pour les codes cycliques un code λ-constacyclique peut être vu comme un idéal $\langle g(x) \rangle$ dans l'anneau $\frac{\mathbb{F}_q[X]}{\langle X^n - \lambda \rangle}$, où le polynôme générateur $g(X)$ est l'unique polynôme unitaire de degré minimal dans le code et divisant $X^n - \lambda$.

Remarque 4.1. *Si la caractéristique du corps est 2, alors les codes négacycliques ne sont autre que les codes cycliques.*

Voici un exemple qui montre que les deux anneaux $\frac{\mathbb{F}_q[X]}{\langle X^n - 1 \rangle}$ et $\frac{\mathbb{F}_q[X]}{\langle X^n + 1 \rangle}$ ne sont pas toujours isomorphes.

Exemple 4.1. *L'anneau $\frac{\mathbb{F}_3[X]}{\langle X^2 + 1 \rangle}$ est intègtre (i.e. un corps), alors que l'anneau $\frac{\mathbb{F}_q[X]}{\langle X^2 - 1 \rangle}$ n'est pas intègre. Donc, ces deux anneaux ne sont pas isomorphes.*

Proposition 4.1. *Si n est impair, alors*

$$\begin{array}{rccc} \varphi : & \frac{\mathbb{F}_q[X]}{\langle X^n - 1 \rangle} & \longrightarrow & \frac{\mathbb{F}_q[X]}{\langle X^n + 1 \rangle} \\ & f(x) & \longmapsto & f(-x) \end{array}$$

est un isomorphisme d'anneaux.

Preuve. Pour deux polynôme $f(X), g(X) \in \mathbb{F}_q[X]$, $f(X) \equiv g(X) \pmod{X^n - 1}$ si et seulement si il existe $h(X) \in \mathbb{F}_q[X]$ tel que $f(X) - g(X) = h(X)(X^n - 1)$. Or

$$\begin{array}{rcl} f(X) - g(X) = h(X)(X^n - 1) & \Leftrightarrow & f(-X) - g(-X) = h(X)((-X)^n - 1) \\ & \Leftrightarrow & f(-X) - g(-X) = -h(X)(X^n + 1). \end{array}$$

Donc, φ est bien défini et il est facile de voir qu'il est bejictif, et de vérifier que c'est un homomorphisme d'anneaux. □

Exercices

Exercise 4.1. *Montrer que $X^n - 1$ n'a pas de racines multiples dans $\mathbb{F}_q$ si et seulement si n et q sont premiers entre eux.*

Exercise 4.2. *Déterminer le plus petit code cyclique binaire de longueur 7 qui contient le mot 0011101.*

Exercise 4.3. *Trouver tous les codes cycliques trinaires de longueur 4.*

Exercise 4.4. *Soit $g(X) = (X-1)^6$ le polynôme générateur d'un codes cycliques trinaires de longueur 9.*
1− *Déterminer la dimension de C.*
2− *Déterminer le nombre de mots de C.*

Exercise 4.5. *Soit λ un élément non nul de $\mathbb{F}_q$. Montre que le code dual d'un code λ-constacyclique est un code λ^{-1}-constacyclique.*

Annexe :

Beaucoup de travaux sur les codes λ-constacycliques ont été faits. Dans le tableau suivant on cite quelques uns. Dans ce tableau on indique les noms des auteurs, leurs cotributions et l'année de publication du travail fait.

Auteurs	Contributions	Année
Dinh [4]	Constacyclic codes of length $2p^s$ over $\mathbb{F}_q$	2012
Bakshi [1]	Constacyclic codes of length $2^t p^s$ over $\mathbb{F}_q$	2012
Dinh [5]	Constacyclic codes of length $3p^s$ over $\mathbb{F}_q$	2013
Dinh [6]	Constacyclic codes of length $4p^s$ over $\mathbb{F}_q$	2013
Dinh [7]	Cyclic and negacyclic codes of length $6p^s$ over $\mathbb{F}_q$	2014
Chen et al. [2]	Constacyclic codes of length lp^s over $\mathbb{F}_q$	2014
Chen et al. [3]	Constacyclic codes of length $2l^m p^n$ over $\mathbb{F}_q$	2015
Sharma and Rani [16]	Constacyclic codes of length $4l^m p^n$ over $\mathbb{F}_q$	2016
Liu et al. [11]	Constacyclic codes of length $3\ell p^s$ over $\mathbb{F}_q$	2016
Tong [17]	Constacyclic codes of length $kl^a p^b$ over $\mathbb{F}_q$, where $(ord_k q, l) = 1$	2016
Rani [14]	Cyclic and negacyclic codes of length $8\ell^m p^n$ over $\mathbb{F}_q$	2017
Rani [15]	Constacyclic codes of length $8\ell^m p^n$ over $\mathbb{F}_q$	2018
Dinh and Rani [8]	Constacyclic codes of length $2^{\mathfrak{K}}\ell^m p^n$ over $\mathbb{F}_q$	2019

Bibliographie

[1] G.K. Bakshi, A class of constacyclic codes over a finite field, Finite Fields Appl. 18 (2012) 362–377.

[2] B. Chen, H.Q. Dinh, H. Liu, Repeated-root constacyclic codes of length lp^s and their duals, Discrete Appl. Math. 177 (2014) 60–70.

[3] B. Chen, H.Q. Dinh, H. Liu, Repeated-root constacyclic codes of length $2l^m p^n$, Finite Fields Appl. 33 (2015) 137–159.

[4] H.Q. Dinh, Repeated-root constacyclic codes of length $2p^s$, Finite Fields Appl. 18 (2012) 133–143.

[5] H.Q. Dinh, Structure of repeated-root constacyclic codes of length $3p^s$ and their duals, Discrete Math. 313 (2013) 983–991.

[6] H.Q. Dinh, On repeated-root constacyclic codes of length $4p^s$, AsianEur. J Math, vol. 6, no. 2, 1350020, 2013.

[7] H.Q. Dinh, Structure of repeated-root cyclic and negacyclic codes of length $6p^s$ and their duals, AMS Contemp. Math. 609 (2014) 69–87.

[8] H. Q. Dinh and S. Rani, Structure of some classes of repeated-root constacyclic codes of length $2^{\mathfrak{K}}\ell^m p^n$, Discrete Math. 342 (2019) https ://doi.org/10.1016/j.disc.2019.111609.

[9] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[10] J. H. van Lint, Introduction to coding theory, 2nd edition, Graduate Texts in Math. 86, Springer-Verlag, Berlin-Heidelberg-New York, 1992.

[11] L. Liu, L. Q. Li, X. S. Kai and S. X. Zhu, Repeated-root constacyclic codes of length $3\ell p^s$ and their dual codes, Finite Fields Appl., 42 (2016), 269-295.

[12] T. K. Moon, Error correction coding, mathematical methods and algorithms, Wiley-Interscience, 2005.

[13] M. Purser, Introduction to error-correcting codes, Artech House, 1995.

[14] S. Rani, On cyclic and negacyclic codes of length $8\ell^m p^n$ over finite field, Asian-Eur. J. Math. (2017) http ://dx.doi.org/10.1142/S1793557118500717.

[15] S. Rani, Structure of repeated-root constacyclic codes of length $8\ell^m p^n$, Asian-Eur. J. Math. (2018) http ://dx.doi.org/10.1142/S1793557119500505.

[16] A. Sharma, S. Rani, Repeated-root constacyclic codes of length $4l^m p^n$, Finite Fields Appl. 40 (2016) 163–200.

[17] H. Tong, Repeated-root constacyclic codes of length $kl^a p^b$ over a finite field, Finite Fields Appl. 41 (2016) 159–173.