**REPUBLIQUE ALGERIENNNE DEMOCRATIQUE ET POPULAIRE**
**MINISTÉRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE**

**UNIVERSITÉ DE ABBAS LAGHROUR KHENCHELA**

**DÉPARTEMENT DE MATHÉMATIQUE ET INFORMATIQUE**


**MÉMOIRE**

**De fin D'étude Pour L'obtention**
**De Diplome De Master Mathématiques**

**Option :**

**Mathématique Appliquée**

# Sur la théorie des codes correcteurs d'erreurs "Application sur les codes cycliques"

**Réaliser Par :**

**Bouragaa Nawal**

**Abid Sabrina**

**Dirigé par :**

**Mr.Sahraoui Ala Eddin**

Devant la Commission d ?examen composée de :

| | | |
|---|---|---|
| M. Bahri Boubakeur | Professeur, | Examinateur |
| M. Tbessi Fouzi | Professeur, | Examinateur |
| M.Sahraoui Alaeddine | Professeur, | Directeur de mémoire |

Année universitaire 2017/2018

# *Remerciement*

***Nous remercions vivement notre encadreur, Mr Sahraoui Ala Eddine , pour nous avoir proposé ce sujet d'actualité assez passionnant ; sa patience et son organisation nous ont permis de surmonter de nombreuses difficultés liées à ce travail.***

***Nous tenons à lui exprimer nos sincères déférences pour son encadrement.***

***A monsieur le président du jury le professeur Tbessi Fouzi .***

***A messieurs le membre du jury le professeur Bahri Boubakeur.***

***Qui ont accepté d'évaluer mon travail, veillez trouver ici le témoignage de ma gratitude et de mon profond respect.***

***Merci également à tous ceux qui ont contribué à notre formation spirituelle.***

***Notre gratitude s'adresse également à tous ceux qui, de loin ou de prés, ont participé à la réalisation de ce travail.***

***Nous tenons aussi à remercier toute l'équipe pédagogique pour nous avoir transmis leur savoir tout au long de notre cycle d'étude.***

***Merci également à tous mes collègues de travail dans la direction de wilaya de la poste et des technologies de l'information et de communication qui mont soutenu avec leurs encouragements.***

# *Dédicaces*

***Je dédie ce travail à tous ceux qui m'ont apporté de l'amour et de l'affection***

***à mes parents,qui ont toujours été là pour moi et qui m'ont donnés un magnifique modèle de labeur et de persévérances.***

***Et spécialement à le personne qui encouragée mon marie Noureddine***

***Je dédie aussi à mes frère :Bachir, khamiss, Noureddine, Bilal, Abdou***

***A mes soeurs : Sabah, Nowara***

***A mon binôme Sabrina***

***A mes oncles et mes tantes .***

***A mes cousins et mes cousine***

***A tous la famille Bouragaa***

***A mes plus chére amies :Samira,Salma,Souhila, Zaineb, Khadidja, Siham, Hassina .***

***A toutes les personnes qui m'ont aidés et m'ont encouragée de prés et de loin.***

***A toute la promo de Master 2 Mathématique.***

***A mes collègues de l'université de Khenchela.***

***Nawal.B***

# *Dédicaces*

***Je dédie ce travail à tous ceux qui m'ont apporté de l'amour et de l'affection***

***à mes parents,qui ont toujours été là pour moi et qui m'ont donnés un magnifique modèle de labeur et de persévérances.***

***Je dédie aussi à mes frère :Ammar, Fateh, Yousouf, Abdou, Djamel, Doudou, Zinou .***

***A mes soeurs : Siham, Salima, Nabila, Ibtissem***

***A mon binôme Nawal***

***A mes oncles et mes tantes .***

***A mes cousins et mes cousine***

***A tous la famille***

***A mes plus chére amies :Souhila.R, Samira, Salma, Souhila, Zaineb, Khadidja, Siham, sana, Asmahan.A, Asmahan.S.***

***A toutes les personnes qui m'ont aidés et m'ont encouragée de prés et de loin.***

***A toute la promo de Master 2 Mathématique.***

***A mes collègues de l'université de Khenchela.***

***Sabrina. A***

# Notation

$p$ : un nombre premier.

$\mathbb{F}_p$ : le corps $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

$\langle ., . \rangle$ : le produit scalaire.

$\mathcal{C}[n, k, d]$ : un code de longueur $n$ , de dimension $k$ et de distance minimale $d$ .

$\mathcal{C}^{\perp}$ : le code orthogonale de $\mathcal{C}$ .

$\mathcal{H}_n(\mathbb{F}_2)$ : Code de $Hamming$ binaire.

$\mathcal{C}_n(\mathbb{F}_2)$ : Code cyclique.

$G$ : matrice génératrice .

$H$ : matrice de contrôle.

$wt(x)$ : le poids du vecteur $x$.

$d(., .)$ : distance de $Hamming$.

$d(\mathcal{C})$ : distance minimale du code $\mathcal{C}$.

$e$ : nombre d'erreur.

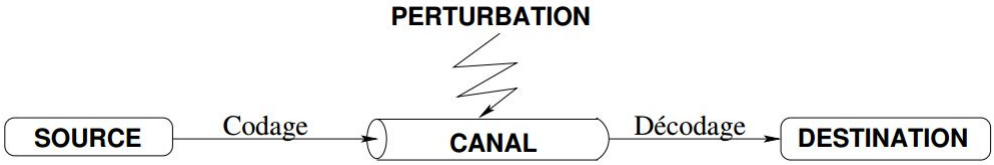
$e_{\mathcal{C}}$ : la capacité de correction.

$e_d$ : la capacité de détection.

$\mathcal{M}_n(\mathbb{K})$ : l'espace des matrices carrées.

# Introduction

La théorie des codes correcteurs d'erreurs, dont l'origine remonte à la fin des années 40, permet de transmettre de façon fiable de l'information, codée au moyen de mots binaires d'une longueur donnée, sur des lignes plus ou moins bruitées. La transmission de l'information binaire sur des lignes bruitées présentant un risque d'erreurs variable selon les cas, il s'agit de trouver un moyen de les corriger à la réception de l'information
En 1948, $ClaudeShannon$ posait la première pierre de ce qu'il a appelé une théorie mathématique de l'information, Dans les années 1940 $RichardHamming$ a reconnu que l'évolution futur d'ordinateur requis une plus grande fiabilité. En particulier la capacité à détecter et à corriger les erreurs, il a crée les codes correcteurs d'une seul erreur (les codes de $Hamming$ ) .
Voyons schématiquement le problème posé par la transmission sur un canal bruité.




L'étude de notre présent mémoire est organisée en 3 chapitres :
Le premier chapitre se consacre aux notions fondamental d'algèbre en générale, ensuite le deuxième qui décrit les codes en blocs en général et des exemples de ces codes qui existent avec leurs principes de codage et décodage, et enfin, Dans le troisième chapitre on donne une caractérisation des codes cycliques. une définition général et des exemple de ce type de code avec une application sur ce code.

# Table des matières

# Chapitre 1

# Notions fondamentales d'algèbre

## 1.1 Groupes

**Définition 1.1.1** *soit $G$ un ensemble non vide muni d'une opération $*$ :*

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (x, y) & \longmapsto & x * y \end{array}$$

*Alors, on dit que $(G\,; *)$ est un groupe si et seulement si :*
- *$*$ est associative : $(x * y\ ) * z = x * (y * z)$,pour tout $x,y,z \in G$.*
- *il existe un (unique) élément neutre $e \in G$ tel que $x * e = e * x = x$, pour tout $x \in G$.*
- *tout élément $x \in G$ a un (unique) inverse $x^{-1} \in G$ tel que $x * x^{-1} = x^{-1} * x = e$ ;*

*Un groupe $(G\,; *)$ s'appelle abélien si l'opération $*$ commutative :*

$$\forall\ x, y \in G; \quad x * y = y * x$$

.

**Exemple**
- $(\mathbb{N}\,;+\,)$ et $(\mathbb{N}\,;\,.\,)$ ne sont pas des groupes car l'opposé et l'inverse d'un nombre naturel ne sont pas des nombres naturels ;
- $(\mathbb{Z}\,;+)$, $(\mathbb{Q}\,;+)$, $(\mathbb{R}\,;+)$ et $(\mathbb{C}\,;+)$ sont des groupes abéliens avec élément neutre = zéro 0 ;
- si on note $\mathbb{Z}^* = \mathbb{Z}\diagdown\{0\}$ (et même chose pour $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$), l'ensemble $(\mathbb{Z}^*\,;\,.\,)$ n'est pas un groupe, alors que $(\mathbb{Q}^*\,;\,.\,)$,$(\mathbb{R}^*\,;\,.\,)$ et $(\mathbb{C}^*\,;\,.\,)$ sont des groupes abéliens avec élément neutre = unité 1.
- $(\mathbb{Q}\,;\,.\,)$, $(\mathbb{R}\,;\,.\,)$ et $(\mathbb{C}\,;\,.\,)$ ne sont pas des groupes car 0 n'est pas inversible.

## Propriétés immédiates

1) L'élément neutre d'un groupe est unique ;
2) Le symétrique d'un élément est unique ;
3) $\forall a; b \in G, (ab)^{-1} = b^{-1}a^{-1}$ , si la loi est multiplicative (.).

### 1.1.1 Sous-Groupes

**Définition 1.1.2** *Soit $G$ un groupe muni d'une loi de composition interne : et soit $H$ un sous ensemble non-vide de $G$. On dit que $H$ est un sous-groupe de $G$ lorsque les deux conditions suivantes sont vérifiées :*
1) *$H$ est stable pour la loi : (ce qui signifie $x.y \in H$ pour tous $x$; $y \in H$ ),*
2) *$H$ est stable par passage la l'inverse (ce qui signifie $x^{-1} \in H$ pour tout $x \in H$).*

*Dans ce cas, la restriction la $H$ de la loi . de $G$ définit une loi de composition interne dans $H$, pour laquelle $H$ est lui-même un groupe.*

### 1.1.2 Sous-groupe engendré par une partie

**Définition 1.1.3** *Soit $X$ un sous-ensemble d'un groupe $G$, l'intersection de tous les sous-groupes de $G$ contenant $X$ est un sous-groupe appelé sous-groupes engendré par $X$, on le notera $\langle X \rangle$.*

Il est clair que $\langle X \rangle$ est le plus petit sous-groupe de $G$ contenant $X$.

**Définition 1.1.4** *Un groupe $G$ est monogène si $G$ admet un unique générateur $a \in G$ $.i.e, G = \langle a \rangle$,*
*de plus $G$ est fini alors $G$ est cyclique.*

### 1.1.3 Homomorphismes, Isomorphismes de groupes

**Proposition 1.1.1** *Une application $f : G \longrightarrow G'$ d'un groupe $G$ dans un groupe $G'$ est un homomorphisme de groupe si :*

$$\forall\ x; y \in G; f(xy) = f(x)f(y)$$

*Un homomorphisme de groupes $f : G \longrightarrow G'$ est dit isomorphisme de groupes si $f$ est bijectif. Dans ce cas on dit que $G$ et $G'$ sont isomorphes.*
*Un isomorphisme de $G$ dans lui même est appelé automorphisme.*

## 1.2 Anneaux

**Définition 1.2.1** *soit $A$ ensemble muni de deux opérations $+ ; * : A \times A \longrightarrow A$ telles que :*
- *$(A ; +)$ est un groupe abélien, avec élément neutre noté $0 \in A$ et appelle zéro de l'anneau,*
- *$*$ est associative : $(x * y) * z = x * (y * z)$, pour tout $x ; y \in A$,*
- *l'opération $*$ est distributive par rapport la l'opération $+$ :*

– *$(x + y) * z = x *z + y * z$ pour tout $x ; y ; z \in A$.*
– *$x *(y + z) = x *y + x * z$ pour tout $x ; y ; z \in A$.*

*Un anneau $(A ; + ; *)$ s'appelle commutatif si l'opération $*$ est commutative.*
*Un anneau $(A ; + ; *)$ s'appelle unitaire si l'opération $*$ a un élément neutre noté $1 \in A$ est appelé unité de l'anneau.*

### 1.2.1 Sous-Anneaux

**Définition 1.2.2** *Soit $A$ un anneau. On appelle sous-anneau de $A$ toute partie non-vide $B$ de $A$ qui vérifie les deux conditions suivantes :*
1) *$B$ est un sous-groupe du groupe additif $A$.*
2) *$B$ est stable par la multiplication de $A$, c'est-à-dire que l'on a :*
*$xy \in B$ quels que soient $x \in B$ et $y \in B$.*

**Exemple**
Pour $\mathbb{K} = \mathbb{Z} ; \mathbb{Q} ; \mathbb{R}$et $\mathbb{C}$ : les ensembles $(\mathbb{K} ; + ; .)$ sont des anneaux commutatifs et unitaires,i.e :
- Si la loi (.) est commutatif, on dit que l'anneau est commutatif.
- Si la loi (.) possède un neutre bilatère, on dit que l'anneau est unitaire.

### 1.2.2 Idéaux

**Définition 1.2.3** *Soit $A$ un anneau et $I$ une partie de $A$. On dit que $I$ est un idéal à gauche (resp. à droite) de $A$ si :*
*a) $I$ est un sous-groupe du groupe additif $A$.*
*b) Quel que soit $a \in A$ et quel que soit $x \in I$, on a $ax \in I/(resp.xa \in I)$.*
*On dit que $I$ est un idéal bilatère ou simplement un idéal de $A$ si $I$ est à la fois un idéal à gauche et un idéal à droite de $A$.*
*Notons que dans un anneau commutatif, tous les idéaux sont bilatères.*

### Exemple

Dans tout anneau $A$, les sous-groupes triviaux $A$ et 0 sont des idéaux. Tout idéal de $A$ autre que $A$ et l'idéal nul 0 s'appelle un idéal propre de $A$.

### 1.2.3 Anneaux quotient

**Théorème 1.2.1** *Soient $A$ un anneau et $I$ un idéal bilatère de $A$.*
*Alors la relation définie par $x\mathcal{R}y \iff x - y \in I$ est une relation d'équivalence sur $A$, compatible avec les deux lois de $A$. L'ensemble quotient, noté $A/I$, muni des deux lois quotients est un anneau appelé* ***anneau-quotient*** *de $A$ par $I$.*
*Si, de plus, $A$ est commutatif, l'anneau $A/I$ est commutatif.*

### 1.2.4 Anneaux intègres

**Définition 1.2.4** *Un élément $a$ d'un anneau $A$ est un diviseur de zéro s'il est non nul et s'il existe $b \in A$ non nul tel que : $a.b = 0$*

**Définition 1.2.5** *Un anneaux $A$ est intègre ssi $A \neq \{0\}$ et si $A$ n'a pas de diviseur de zéro , autrement dit si on a :*

$$a.b = 0 \Longrightarrow (a = 0) \quad ou \quad (b = 0).$$

### 1.2.5 Homomorphismes d'anneaux

**Proposition 1.2.1** *Une application $f$ d'un anneau $A$ dans un anneau $B$ est un homomorphisme d'anneau ssi :*
1) $f(1_A) = 1_B$
2) $\forall (x, y) \in A \times A : f(x + y) = f(x) + f(y)$
3) $\forall (x, y) \in A \times A : f(x.y) = f(x).f(y)$

Si de plus$f$ est bijective, on dit que$f$ est un isomorphisme d'anneaux.

## 1.3 Corps

**Définition 1.3.1** *on appelle corps commutatif tout anneau commutatif unitaire dans lequel tout élément non-nul est inversible.*
*En notant,pour tout anneau $A$ commutatif unitaire $A^*$=$A \setminus \{0\}$*
*on a donc :($A$ corps )$\iff$ ($U(A) = A^*$ )*

### 1.3.1 Sous- Corps

**Définition 1.3.2** Soit $(K, +, .)$ est un corps, un sous-corps de $K$ est sous-anneau $F$ de $K$ tel que pour tout élément non nul $x$ de $F$, on a $x^{-1} \in F$ ;$(F, +, .)$ est un corps.

**Exemple**
- L'anneau $(\mathbb{Z},+,.)$ n'est un corps.
- Pour $\mathbb{K}=\mathbb{Q}$ ;$\mathbb{R}$ et$\mathbb{C}$ sont des corps commutatif pour les lois usuelles.
- Pour tout entier $n \geq 2$ ($\mathbb{Z}/n\mathbb{Z}$ est un corps)$\Longleftrightarrow$ ($n$ est un nombre premier).
  On note $\mathbb{F}_n = \mathbb{Z}/n\mathbb{Z}$ ; $n$ est un nombre premier.
- Tout corps fini est commutatif.

## 1.4 Espace Vectoriels

**Définition 1.4.1** On appelle espace vectoriel sur $K$, tout ensemble $E$ muni de deux loi :

1. Une loi interne appelée addition, notée + tel que $(E\,;+)$ soit un groupe abélien.
2. Une loi externe qui à tout couple $(\lambda\,;x)\in \mathrm{K}\times E$ fait correspondre un élément de $E$ noté $\lambda.x$, cette loi vérifiant les quatre propriétés suivantes :

- $\forall\ \mathrm{x}\in E$ , 1.x = x,
- $\forall$ x,y$\in E$, $\forall\lambda \in K$ ;$\lambda.(\mathrm{x+y})=\lambda.\mathrm{x}+\lambda.\mathrm{y}$,
- $\forall$ x$\in E$, $\forall\lambda,\mu \in K$,$(\lambda+\mu).\mathrm{x}=\lambda.\mathrm{x}+\mu.\mathrm{x}$,
- $\forall$ x$\in E$, $\forall\lambda,\mu \in K$,$(\lambda.\mu).\mathrm{x}=\lambda.(\mu.\mathrm{x})$,

Les éléments de $E$ s'appelle vecteurs, ceux de $k$ scalaires.

### 1.4.1 Sous-Espace Vectoriels

**Proposition 1.4.1** *une partie non vide $F$ d'un $k$-espace vectoriel $E$ est un sous-espace vectoriel de $E$ si seulement si : $\forall$ $x,y \in F$, $\forall\lambda \in k$ : $x+y \in F$ et $\lambda x \in F$.*
*Ou encore $\forall$ $x,y \in F$, $\forall\lambda,\mu \in k$ : $\lambda x+\mu y \in F$.*

**Proposition 1.4.2** *Soit $F$ une partie non vide d'un $K$-espace vectoriel $E$.*
*Les propositions suivantes sont équivalentes :*
1) *$F$ est un sous-espace vectoriel de $E$.*
2) $\forall x, y \in E, \forall\lambda, \mu \in K, \lambda x + \mu y \in F$.

**Définition 1.4.2** *On dit qu'un système fini $(x_1, x_2, ..., x_n)$ de vecteurs d'un $K$-espace vectoriel $E$ est libre si toute combinaison linéaire de $x_1, x_2, ..., x_n$ est triviale :*
*Si $\lambda_1, \lambda_2, ..., \lambda_n \in K$, tels que : $\lambda_1 x_1 + \lambda_2 x_2 + ...\lambda_n x_n = 0$, alors : $\lambda_1 = \lambda_2 = ... = \lambda_n = 0$ ;*
*On dit qu'un système fini $(x_1, x_2, ..., x_n)$ de vecteurs d'un $K$-espace vectoriel $E$ est lié s'il n'est pas libre . Ce qui revient à dire qu'il existe des scalaire $\lambda_1, \lambda_2, ..., \lambda_n$ tous non nuls tels que*

$$\lambda_1 x_1 + \lambda_2 x_2 + ...\lambda_n x_n = 0$$

**Définition 1.4.3** *On appelle espace vectoriel de dimension finie tout espace vectoriel engendré par un système fini de vecteurs. Dans le cas contraire on dit que l'espace vectoriel est de dimension infinie.*
*Un système* $(x_1, x_2, ..., x_n)$ *de vecteurs d'un* $K$*-espace vectoriel* $E$ *est dit base de* $E$
*si* $(x_1, x_2, ..., x_n)$ *est libre et générateur de* $E$*.*

### Exemples

1) Une base de $K^n$ est $(1, 0, ..., 0), (0, 1, ..., 0), ..., (0, 0, ..., 1)$ dite une base canonique.
2) Les polynômes $1, x, x^2, ..., x^n$ forment une base de l'espace vectoriel $K^n[x]$ des polynômes de degré inférieur ou égal à $n$.

**Définition 1.4.4** *Soient* $E$*,* $E'$ *deux espaces vectoriels sur* $K$ *et* $f$ *une application de* $E$ *dans* $E'$*. On dit que* $f$ *est linéaire, si :*
$1) f(v + w) = f(v) + f(w);\ \forall v, w \in E,$
$2) f(\lambda v) = \lambda f(v),\ \forall v \in E, \forall \lambda \in K.$

**Remarque 1.4.1** *Pour toute application linéaire* $f$*, on a* $f(0) = 0$ *puis-que* $f$ *est un homomorphisme de groupes.*

## 1.5 Matrices associées aux application linéaires

Soient $\mathbb{E}$ et $\mathbb{E}'$ deux espaces vectoriels sur $\mathbb{K}$, de dimension $n$ et $p$ respectivement et
$f : \mathbb{E} \longrightarrow \mathbb{E}'$ une application linéaires. Choisissons $\{(e_1, e_2, ..., e_n)\}$ une base de $\mathbb{E}$ et $\{(e'_1, e'_2, ..., e'_p)\}$ une base de $\mathbb{E}'$, les images par $f$ des vecteurs $e_1, e_2, ..., e_n$ se décomposent sur la base $(e'_1, e'_2, ..., e'_n)$ :
$f(e_1) = a_{11}e'_1 + a_{21}e'_2 + ... + a_{p1}e'_p,$
$f(e_2) = a_{12}e'_1 + a_{22}e'_2 + ... + a_{p2}e'_p,$
.....
$f(e_n) = a_{1n}e'_1 + a_{2n}e'_2 + ... + a_{pn}e'_p.$

**Définition 1.5.1** *On appelle matrice de $f$ dans les bases $(e_1, e_2, ..., e_n)$, $(e'_1, e'_2, ..., e'_n)$ la matrice notée $M(f)$ dont les colonnes sont les composantes des vecteurs $f(e_1), f(e_2), ..., f(e_n)$ dans la base $(e'_1, e'_2, ..., e'_p)$*

$$M(f) = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{p1} & a_{p2} & ... & a_{pn} \end{pmatrix}$$

Il est claire que la matrice associée à $f$ dépend du choix des bases de $\mathbb{E}$ et $\mathbb{E}'$.

## Exemples

1) Soit $\mathbb{E}$ un espace vectoriel de dimension $n$ finie et $id_{\mathbb{E}} : \mathbb{E} \longrightarrow \mathbb{E}$ l'application qui associe $x$ à $x$ ,on considère une base $\{(e_i, i = 1, ..., n)\}$ de $\mathbb{E}$.
On a :

$$M(id_{\mathbb{K}}) = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & 1 \end{pmatrix} = I_n$$

Cette matrice est dite la matrice d'unité de $\mathcal{M}_n(\mathbb{K})$ l'espace des matrices carrées.

**Définition 1.5.2** *Une matrice carrée est une matrice dont le nombre de lignes est égal au nombre de colonnes. Ce nombre s'appelle l'ordre de la matrice.*
*Notons $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices carrée d'ordre $n$ à coefficients dans $\mathbb{K}$*

### 1.5.1 Rappels sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Soit $p$ un nombre premier. Nous savons que l'anneau $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo $p$ dans ce cas est un corps. C'est-à-dire que tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible.
Si on décrit les classes de $\mathbb{Z}/p\mathbb{Z}$ par leur représentant appartenant à l'intervalle d'entiers :

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, ..., p-1\}.$$

Alors on voit que tout élément non nul $a \in \mathbb{F}_p$ vérifie $a^{p-1} \equiv 1[p]$

### 1.5.2 Le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$

#### Les éléments générateurs

Nous avons vu que lorsque $p$ est premier, le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ est égal à $\mathbb{Z}/p\mathbb{Z} - \{0\}$, ce groupe est cyclique, plus précisément .

**Théorème 1.5.1** *Soit $p$ un nombre premier. Alors, le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ est cyclique. c'est-à-dire ce groupe peut être engendré par un élément générateur " dit aussi élément primitif" il existe un élément $\alpha$ tel que :*

$$\mathbb{Z}/p\mathbb{Z}^* = \{1, \alpha, \alpha^2, ..., \alpha^{p-2}\}.$$

### 1.5.3 Polynôme Irréductible

Soit $\mathbb{F}_p[x]$ l'ensemble des polynômes en $x$ à coefficient dans $\mathbb{F}_p$, un polynôme $g(x)$ de $\mathbb{F}_p[x]$ est dit irréductible sur $\mathbb{F}_p$, s'il ne se décompose pas en un produit de polynômes non triviaux, c'est-à-dire polynômes de degrés strictement positifs de $\mathbb{F}_p[x]$.

#### Exemples

Le polynôme $p(x) = 1 + x + x^2$ est irréductible sur $\mathbb{F}_2$.
Le polynôme $f(x) = x + x^3$ n'est pas irréductible sur $\mathbb{F}_2$ car $f(x) = x(1 + x^2)$.

### 1.5.4 Période d'un polynôme

Tout polynôme à une période, est la période d'un polynôme irréductible de degré $n$ est $2^m - 1$.
Tout polynôme irréductible sur $\mathbb{F}_2$ de degré $m$ divise $x^l + 1$ avec $l = 2^m - 1$.

#### Exemple

$x^3 + x + 1$ divise $x^7 + 1$ on effet, $2^3 - 1 = 7$, $x^7 + 1 = (x^4 + x^2 + x + 1)(x^3 + x + 1)$.

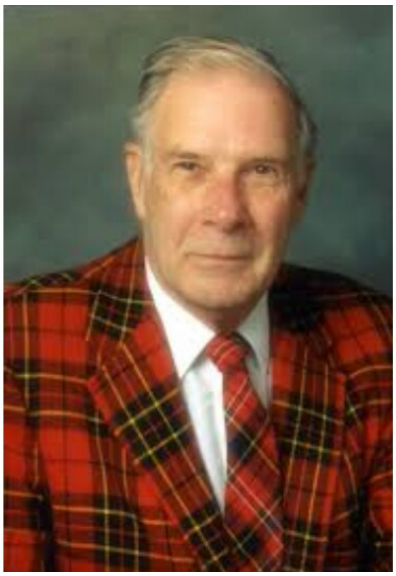
### 1.5.5 Polynôme primitif

Un polynôme $p(x)$ de degré $m$ est dit primitif si le plus petit entier $n$ pour que $g(x)$ divise $x^n + 1$ est $n = 2^m - 1$.

# Chapitre 2

# Codes,codes linéaires, codes de *Hamming*

$RichardWesleyHamming$, né le 11 février 1915 à Chicago (Illinois) et décédé le 7 janvier 1998 à Monterey (Californie) est un mathématicien célèbre à qui on doit les codes de$Hamming$ et la distance de $Hamming$. Il reçut le Prix Turing en 1968.



Dans ce chapitre, nous allons étudier les codes linéaires sur un corps fini $\mathbb{F}_q$. Même si l'on ne s'intéresse ultérieurement qu'aux codes binaires, il est nécessaire de considérer dans certaines constructions des codes sur des corps finis plus généraux.

## 2.1 Code en blocs ; distance de *Hamming*

En général un mot code est $x = (x_1, ..., x_n) \in \mathcal{A}^n$ de longueur $n$ ou $\mathcal{A}$ est un ensemble appelé alphabet
l'ensemble des mot de de code forment le code $\mathcal{C}$
pour $x \in \mathcal{C}$, si le vecteur transmit $x'$ on dit qu'il y a erreur, pour corriger l'erreur ou on cherche un élément dans $\mathcal{C}$ qui soit le plus proche de $x' \notin \mathcal{C}$, pour cela on doit faire intervenir de distance

### exemple

le code$ISBN$ 'International Standard $BookNumber$, ce code est utilise pour le catalogue des livre dans ce cas le mot de code est de longueur 10
$x = (x_1, x_2, ..., x_{10})$ ou $x_i \in 0, 1, 2, ..., 9, x$ telle que $x = 10$ à condition : $\sum_{k=1}^{10} kx_k \equiv 0[11]$
$ISBN$ : 0-387-54894-7 "Introduction to codage theory de H.var.limit"
$(0\times1)+(3\times2)+(8\times3)+(7\times4)+(5\times5)+(4\times6)+(8\times7)+(9\times8)+(4\times9)+(7\times10) = 341 \equiv 0[11]$

**Définition 2.1.1** *soit$\mathcal{A}$ un ensemble fini et n un entier naturel $n \neq 0$ ; un code en bloc est une partie $\mathcal{C}$ de $\mathcal{A}^n$ ; $\mathcal{A}$ est appelé alphabet de $\mathcal{C}$, tout élément de $\mathcal{C}$est dit mot de code*
*un code $\mathcal{C}$ est linéaire si $\mathcal{A} = \{0; 1\}$*

## 2.2 Distance et poids de*Hamming*

**Définition 2.2.1** *Soit $x = (x_1, x_2, ..., x_n) \in \mathcal{A}^n$, le poids de Hamming de $x$, noté $wt(x)$ est égal au nombre de coordonnées non nulles de $x$.*

$$wt(x) = card\{i : 1 \leq i \leq n / x_i \neq 0\}$$

On définit une application :

$$\begin{array}{rcl} d : \mathcal{A}^n \times \mathcal{A}^n & \longrightarrow & \mathbb{R}_+ \\ (x, y) & \longmapsto & d(x, y) \end{array}$$

$d(x, y) = card\{i : / x_i \neq y_i\}$ est le nombre d'indice pour lequel les composantes de $x$ et $y$ sont distinctes.
Cette distance vérifie les propriétés usuelles des distances :
Symétrie : $d(x, y) = d(y, x)$
Positivité : $d(x, y) \geq 0$
$d(x, y) = 0 \Leftrightarrow x = y$
Inégalité triangulaire : $d(x, y) \leq d(x, z) + d(z, y)$
Cet distance est appelée la distance de $Hamming$.
alors :

$$d(x, y) = wt(x - y) = card\{i : 1 \leq i \leq n / x_i \neq y_i\}$$

Le support d'un élément $x \in \mathcal{A}^n$ est l'ensemble des indices $i$ tels que $x_i \neq 0$.
Le poids de $x$ est donc le cardinal de son support, il faut remarquer que la distance de *Hamming* est une vrai distance au sens métrique du terme.
La boule de centre $x$ et de rayon $r$ est par définition l'ensemble :

$$B(x,r) = \{y : y \in \mathcal{A}^n / d(x,y) \leq r\}$$

On peut remarquer que : $y \in B(x,r) \Longleftrightarrow y - x \in B(0,r)$.

## exemple

$x = (a,b,b)\,; y = (a,c,d)$ alors $d\,(x,y) = 2$

**Proposition 2.2.1** *d est une distance appelé distance de Hamming*

## preuve

on a $d$ donnée par :

$$d(x,y) = card\{i/x_i \neq y_i\}$$

soit $x, y \in \mathcal{A}^n$ telle que :$x = (x,x,...,x), y = (y,y,...,y)$
1) $d(x;y) = 0$ car : $card\{i/x_i \neq x_i\} = 0$

2)

$$\begin{array}{rcl} d(x;y) & = & d(y;x) \\ & = & card\{i/x_i \neq y_i\} \\ & = & card\{i/y_i \neq x_i\} \end{array}$$

3) soit $x, y, z \in \mathcal{A}^n$

$$\begin{array}{rcl} & A & = & \{i/x_i = y_i\} \\ \text{posons :} & B & = & \{i/y_i = z_i\} \\ & C & = & \{i/x_i = z_i\} \end{array}$$

On va démontrer l'inégalité triangulaire suivant :

$$d(x;z) \leq d(x;y) + d(y;z)$$

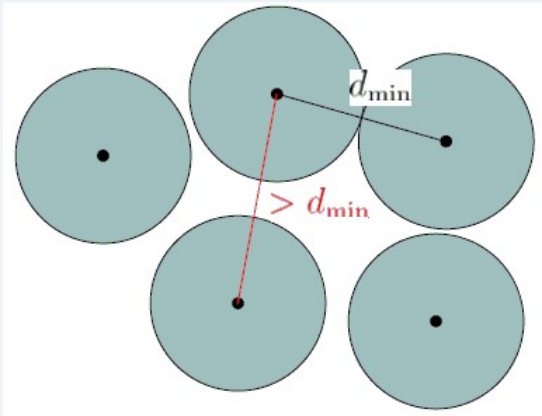
On a :

$$\begin{array}{rcl} A \cap B \subset C & \Longrightarrow & C^c \subset (A \cap B)^c \\ \overline{C} \subset \overline{A} \cup \overline{B} & \Longrightarrow & card(\overline{C}) \leq card(\overline{A}) + card(\overline{B}) \\ & \Longrightarrow & d(x;z) \leq d(x;\,) + d(y;z) \end{array}$$

donc $d$ est une distance de *hamming*

**Définition 2.2.2** *Soit $\mathcal{C} \subset \mathcal{A}^n$ un code en bloc et "d" la distance de Hamming, on appelé distance minimale de $\mathcal{C}$ le nombre :*

$$d(\mathcal{C}) = min\{d(x,y)/x \neq y; x, y \in \mathcal{C}\}$$




### exemple

soit $\mathcal{C} = \{a, b, c\}$, tel que : $a = (0,1,1,1,0)$ ,$b = (1,0,1,0,1)$, $c = (1,1,0,1,1)$
$d(a,b) = 4$
$d(a,c) = 3$
$d(b,c) = 3$
donc $d(\mathcal{C}) = 3$

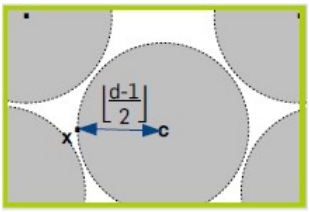
## 2.3 Décodage et correction

supposons que $x = (x_1, x_2, ..., x_n) \in \mathcal{C}$ est transmis en $x' = (x'_1, x'_2, ..., x'_n)$ ;$x'$ doit appartenir à C ; sinon il y a au moins un erreur, $d(x, x')$ représente le nombre d'erreurs.
pour retrouver le mot initial $x$ ; on cherche un mot de $\mathcal{C}$ le plus proche de $x'$

### exemple

$\mathcal{C} = \{a, b, c\}$ ; $oua = (01110)$ , $b = (10101)$ , $c = (11011)$,
si $x' = (10011)$ est le vecteur transmis
ou calcule $d(x', a)$ ; $d(x', b)$ ; $d(x', c)$
$\mathcal{C}$ est le plus proche de $x'$, donc $x'$ est décodé par $c$

**Proposition 2.3.1** *Notons* $e = [\frac{d-1}{2}]$, *les boules* $B(x,e)$ *avec* $x \in \mathcal{C}$ *sont deux à deux disjointes, et* $e$ *est la valeur maximale du rayon pour cette propriété.*
*On dit que* $\mathcal{C}$ *détecte* $d-1$ *erreurs et corrige* $e = [\frac{d-1}{2}]$




**Proposition 2.3.2** *soit* $\mathcal{C}$ *un code de longueur* $n$ *sur l'alphabet* $A$ .
*on dit que* $\mathcal{C}$ *corrige* $e$ *erreurs ,si pour tout* $x \in A^n$ *,il existe au plus un mot* $c$ *de* $\mathcal{C}$ *tel que* $d(x,c) \leq e$
*on dit que* $\mathcal{C}$ *est de capacité* $e$, *si* $\mathcal{C}$ *corrige* $e$ *erreurs et ne corrige pas* $e+1$ *erreurs*

**Proposition 2.3.3** $\mathcal{C}$*corrige* $e$ *erreurs* $\Longleftrightarrow \forall c, c' \in \mathcal{C}, c \neq c'$ ,

$$B(c,e) \cap B(c',e) = \varnothing$$

*tel que* $B(x,r) = \{y \in A^n / d(x,y) \leq r\}$ *,est appelée la boule de centre* $x$ *est de rayon* $r$

## preuve

si $\mathcal{C}$ ne corrige pas $e$ erreurs ;alors $\exists x \in A^n; \exists c, c' \in \mathcal{C}; c \neq c'$
$d(x,c) \leq e; d(x,c') \leq e \Longleftrightarrow$ donc $B(c,e) \cap B(c',e) \neq \varnothing$

**Proposition 2.3.4** *soit* $\mathcal{C}$ *un code de longueur* $n$ *et de distance minimale* $d$ *; alors :*

$$e = \left[\frac{d-1}{2}\right]$$

## preuve

$x \in A^n$ supposons qu'il existe $c, c' \in \mathcal{C}$ tel que :

$$d(x,c) \leq eetd(x,c') \leq e$$
$$d(c,c') \leq d(x,c) + d(x,c') \leq 2e \leq d$$

ce qui signifie contradiction car $d(c,c') \geq d$, il reste à montre que $\mathcal{C}$ ne corrige pas $e+1$ erreurs
soient $x = (x_1, x_2, ..., x_n) \in C, y = (y_1, y_2, ..., y_n) \in \mathcal{C}$ tel que $d(x,y) = d$
on peut supposer $x_1 \neq y_1, x_2 \neq y_2, ..., x_d \neq y_d$ et $x_i = y_i$ pour $i \geq d$
on pose $z = (z_1, z_2, ..., z_n)$ tel que $z = (y_1, .., y_e + 1, x_e + 2, ..., x_d, x_d + 1, ...x_n)$
$d(x,z) = e+1, d(z,y) = n - (e+1) \leq e+1 \Rightarrow z \in B(x,e+1) \cap B(y,e+1)$ donc $C$ ne corrige pas $e+1$ erreurs

### Remarque

si le nombre d'erreurs est inférieur à $e$ alors $\mathcal{C}$ corrige les erreurs
si le nombre d'erreurs dépasse $e$; $\mathcal{C}$ ne peut pas corrige les erreurs, car il peut exister plusieurs élément de $\mathcal{C}$ proches de $x$ vecteurs reçu

### Isométrie

**Définition 2.3.1** *soit $(A^n, d)$ un espace de Hamming ,une isométrie de Hamming est une application :*

$$f : A^n \longrightarrow A^n$$

*tel que :* $\forall (x, y) \in A^n, d(f(x), f(y)) = d(x, y)$

### exemple

soit $\sigma$ une permutation de $\sigma_n$ :
$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$
soit $f : A^n \to A^n$ définie par $f(x_1, ..., x_n) = \left(x_{\sigma(1)}, ..., x_{\sigma(n)}\right)$ alors $f$ est une isométrie

## 2.4 Code équivalents

Deux codes $\mathcal{C}, \mathcal{C}' \subset A^n$, sont dit équivalents,s'il existe $f$ une isométrie de $A^n$,
tel que $\mathcal{C}' = f(\mathcal{C})$

### Remarque

les propriétés métriques sont conservées par équivalence ,donc deux codes équivalents ont même distance minimale don même capacité de correction

## 2.5 Code linéaire

soit $K$ un corps fini à$q$ élément ,donc $K = \mathbb{F}_q$ est commutatif

**Définition 2.5.1** *Soit $K$ un corps fini et soit $n > 0$. Le $K$-espace vectoriel $K^n$ est muni de la métrique de Hamming. Un code linéaire est un $K$-sous-espace de $K^n$. Ses paramètres sont : sa longueur $n$, sa dimension , sa distance minimale . Ces deux derniers paramètres sont notés généralement $k$ et $d$. On dit que le code $\mathcal{C}$ est un code $[n, k, d]$ ;alors $\mathcal{C}$ est de cardinal $q^k$ ; $|K| = q$*

## exemple

1. $K = \mathbb{F} = \{0; 1\}$
   $\mathcal{C} = \{(x_1, x_2, x_3) \in K^3 / x_1 + x_2 + x_3 = 0\} \Rightarrow x_3 = x_1 + x_2$ donc $(x_1, x_2, x_1 + x_2) = x_1(1, 0, 1) + x_2(0, 1, 1) \Rightarrow \mathcal{C} = \{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$
   $\mathcal{C}$ est $[3, 2, 2]$
2. $K^n; \{0\}$ sont codes linéaires triviaux
   $V = \langle (1, ..., 1) \rangle = \{(a, ..., a); a \in K\}$ code répétition $V = [n, 1, n]$ code linéaire .

### 2.5.1 Poids de *Hamming*

**Définition 2.5.2** *soit $x = (x_1, ..., x_n) \in K^n$ ;on appelle poids de $x$,le nombre*

$$wt(x) = card\{i / x_i \neq 0\} \Longrightarrow wt(x) = d(x, 0)$$

*on déduit :*

- $d(x, y) = wt(x - y)$
- $wt(x) = 0 \Leftrightarrow x = 0$
- $wt(\lambda x) = wt(x), \lambda \in K - \{0\}$
- $wt(x + y) \leq wt(x) + wt(y)$

**Proposition 2.5.1** *La distance minimale d'un code linéaire $\mathcal{C}$ est égale au plus petit poids non nul de ce code :*

$$d(\mathcal{C}) = min\{wt(x) / x \in \mathcal{C} - \{0\}\}$$

## preuve

posons $d = d(\mathcal{C}) \leq d(x, y); \forall x \neq y \in \mathcal{C}$,

$$\alpha = min\{wt(x); x \neq 0\} \Rightarrow \alpha = min\{d(x, 0) \neq 0\}$$

alors

$$d \leq d(x, 0) \Rightarrow d \leq \alpha \tag{1}$$

$wt(x) = d(x, 0), wt(x - y) = d(x, y)$

$$\alpha \leq wt(x - y) \Rightarrow \alpha \leq d(x, y), \forall x, y \in \mathcal{C} \Rightarrow \alpha \leq d \tag{2}$$

donc, de (1) et (2) on a : $d = \alpha$

## 2.6 Matrice génératrice , de contrôle de parité

On a deux façons de représenter un code linéaire à l'aide des matrices. Soit en utilisant un homomorphisme dont le code est l'espace vectoriel image , on obtient ainsi la notion de matrice génératrice.
Soit on introduit un homomorphisme dont le code est le noyau , on aura ainsi la notion de matrice contrôle.

### Matrice génératrice

Pour connaitre le code en tant que sous espace , il suffit de lui déterminer une base, celle ci est le plus souvent représentée sous la forme d'une matrice $k \times n$ sur $\mathbb{K}$, la matrice génératrice du code , dont les lignes sont les vecteurs de cette base.
Pour former un mot de code, on calcule le produit d'un vecteur-ligne $(u_1, ..., u_k)$ et de la matrice génératrice :

$$(u_1, ..., u_k) \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ & & \cdots & \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix} = (x_1, ..., x_k)$$

### Propriétés

Soit $\mathcal{C}$ un code linéaire sur un corps $\mathbb{K}$.
1/ On dit qu'une matrice est une matrice génératrice de $\mathcal{C}$ si et seulement si elle est matrice $k \times n$ sur $\mathbb{K}$ , avec $k \leqslant n$ dont le rang est $k$.
2/ Un code possède plusieurs matrices génératrices.
3/ Les mots de $\mathcal{C}$ sont tout les combinaisons linéaires des lignes d'une matrice génératrice. Si $G$ est une matrice génératrice de $\mathcal{C}[n, k, d]$ sur $\mathbb{K}$ , alors :
4/ les matrices génératrices de $\mathcal{C}$ sont de la forme $A \times G$, où $A$ est une matrice carré inversible $k \times k$ sur $\mathbb{K}$.
5/ si $c_1, c_2, ..., c_n$ sont les vecteurs colonnes de $G$ les mots du code $\mathcal{C}$ sont tous sous la forme :

$$m_u = (\langle c_1, u\rangle, \langle c_2, u\rangle, ..., \langle c_n, u\rangle),$$

avec $u \in \mathbb{K}^k$ et $\langle ., .\rangle$ désigne le produit scalaire usuel de $\mathbb{K}^k$

**Remarque 2.6.1** *Soit $\mathcal{C}$ un code linéaire $[n, k, d]$ , l'encodage se fait en multipliant le mot source par la matrice génératrice du code*

**Définition 2.6.1** *Une matrice génératrice d'un code $\mathcal{C}$ est normalisée ou canonique si la matrice formée par les k première colonnes est la matrice d'unité : $G = [I_k|A]$.*
*Si un code est définit par une matrice génératrice normalisée , on dit que ce code est systématique*

**Remarque 2.6.2** *Tout code linéaire est équivalent à un code linéaire systématique.*

### Code dual et matrice de contrôle

Une autre manière pour définir un code linéaire est de donner une application linéaire dont il est le noyau.
On obtient ainsi une matrice $H$ telle que :

$$\mathcal{C} = \{(x_1, ..., x_n); H \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0\}.$$

Le code dual du code $\mathcal{C}$ est son espace orthogonal , on désigne par $\langle ., . \rangle$ le produit scalaire usuel : $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$.
Le code dual du code $\mathcal{C}$ est son espace orthogonal :

$$\mathcal{C}^{\perp} = \{y : y \in \mathbb{K}^n / \forall x \in \mathcal{C}, \langle x, y \rangle\}$$

Une matrice de contrôle de parité de $\mathcal{C}$ est une matrice $(n-k) \times n$ génératrice de $\mathcal{C}^{\perp}$ .

### Remarque

1/ Le dual de $\mathcal{C}^{\perp}$ est $\mathcal{C}$ lui même ; $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$
2/ Un code est dit auto dual s'il est égal à son dual c-à-d : $\mathcal{C}^{\perp} = \mathcal{C}$

**Proposition 2.6.1** *Soit $\mathcal{C}$ un code linéaire de matrice génératrice $G$, supposons que $G$ soit de la forme dite canonique ou systématique $G = [I_k|A]$, alors une matrice de contrôle de parité est $H = [-A^t|I_{n-k}]$.*

### Conséquences

$G$ est une matrice génératrice de $\mathcal{C}$ alors :
1/ si $H$ une matrice de contrôle de parité de $\mathcal{C}$ , alors : $G^t H = 0$.
2/ $c_1, ..., c_n$ colonnes de $H$, alors : $H \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 c_1 + .... + x_n c_n = 0$
Donc $C$ contient un mot de poids au plus $d$,*ssi* 'l existe une combinaison linéaire à coefficients non-nulles de $d$ colonnes de $H$ qui est elle même nulle.
3/ Ainsi, un code $\mathcal{C}$ est de poids $d$ si et seulement si, il existe $d$ colonnes de sa matrice de contrôle de parité linéairement dépendante, tandis que $d-1$ colonnes quelconques sont indépendantes.

## 2.7 Les codes de *Hamming*

Dans ce paragraphe ,on construit une famille des codes qui ont pour propriété de corriger une erreur.
On travaille dans $\mathbb{F}_2^k$.

**Définition 2.7.1** *Le code de Hamming est un code linéaire défini par sa matrice de contrôle de parité dont les colonnes sont tous les vecteurs de* $\mathbb{F}_2^k - \{0\}$.
*donc on peux définir le code de Hamming de longueur* $2^k - 1$ *par une matrice de contrôle dont les colonnes sont les vecteurs de* $\mathbb{F}_2^k - \{0\}$ *ordonnés par l'ordre lexicographique*

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

*alors :*
$H \in \mathcal{M}_{k\times(2^k-1)}$.

**Exemple** :
pour $k = 3$, on obtient pour matrice de contrôle :

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \text{ donc } H' = \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right)$$

Alors la matrice génératrice est :

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

Alors $\mathcal{C} = [7, 4, 3]$ donc $\mathcal{C}^\perp = [7, 3, 4]$ . Le code $\mathcal{C}$ est :

$$\begin{array}{rlll} \mathcal{C} = & \{(0000000); & (1000011); & (0100101); \\ & (0001111); & (0011001); & (0010011); \\ & (0010110); & (0110011); & (0110111) \\ & (0101111); & (1000011); & (1011010) \\ & (1110000); & (1001100); & (1100110); (1111111)\} \end{array}$$

**Proposition 2.7.1** *Pour tout $k \geq 3$ , le code de Hamming est de distance minimale égale à 3.*
*Par conséquent il est capable de corriger une seule erreur.*

**Preuve:** Supposons $x, y$ deux mots dans code binaire de $Hamming$ , soit $H$ sa matrice de contrôle, comme $\mathcal{C}$ est un code linéaire alors $x - y \in \mathcal{C}$.
Supposons que $d(x, y) = 1$, alors $x - y$ est un vecteur de la base canonique donc $H(x - y)$ est un colonne de $H$ , comme$x - y \neq 0$ car tous les colonnes de $H$ sont non nulle , mais $x - y \in C$ , alors $H(x - y) = 0$ contradiction.
Supposons que $d(x, y) = 2$, alors $H(x - y) = 0$ si et seulement s'il existe deux colonnes de $H$ qui sont linéairement dépendants.
Ce n'est pas le cas d'où $d(x, y) \geqslant 3$, pour tous les mots de code $x, y$.
Tout matrice de contrôle d'un code binaire de $Hamming$ aura trois colonnes qui sont linéairement dépendante , donc en fait des mots de code sont de distance 3 □

### Conséquence

Le code binaire de $Hamming$ est capable de corriger une seul erreur.

## 2.8 Code équidistant

**Définition 2.8.1** *Un code $\mathcal{C}$ à poids fixe, est un code dont ses mots non nulle ont le même poids :*

$$\forall x \neq y \in \mathcal{C}, x \neq 0, y \neq 0; wt(x) = wt(y).$$

**Définition 2.8.2** *Un code $\mathcal{C}$ équidistant , c'est un code où la distance entre deux mots différent est fixe :*

$$\forall x \neq y \in \mathcal{C}, d(x, y) = fixe.$$

**Proposition 2.8.1** *Soit $\mathcal{C}$ un code linéaire , alors : $\mathcal{C}$ est équidistant si et seulement si $\mathcal{C}$ est à poids fixe.*

**Preuve:** : Soit $\mathcal{C}$ un code linéaire équidistant donc $d(x, y) = cst$ alors :
pour $y = 0$ , $d(x, 0) = cst$ , donc $wt(x) = cst$ donc $\mathcal{C}$ est à poids fixe.
La réciproque :
Soit $\mathcal{C}$ un code linéaire à poids fixe alors :
$\forall x, y \in \mathcal{C}, d(x, y) = wt(x - y)$,
posons $z = x - y \in \mathcal{C}$ donc $wt(z) = cst = d(x, y)$.
Alors : $\mathcal{C}$ est un code à poids fixe.

□

**Remarque 2.8.1** *La proposition* (2.8.1) *est vrai seulement pour les codes linéaire. Voici un contre exemple :*

$$\mathcal{C} = \{x = (110100); y = (001011); z = (111000)\}$$

$\mathcal{C}$ *est un code non linéaire de poids fixe* $wt(x) = wt(y) = wt(z) = 3$ *mais :* $d(x, y) = 6, d(y, z) = 4$

L'inégalité triangulaire $wt(u + v) \leq wt(u) + wt(v)$ détient , mais comme l'exemple suivant montre qu'il est trop faible pour raconter toute l'histoire .

| $v$ | 0 | $v_1$ | $v_2$ | $v_3$ | $v_1 + v_2$ | $v_1 + v_3$ | $v_2 + v_3$ | $v_1 + v_2 + v_3$ |
|---|---|---|---|---|---|---|---|---|
| $wt(v)$ | 0 | 1 | 1 | 1 | 2 | 2 | 2 | 1 |

## 2.8.1 Décodage par syndrome

Soit $\mathcal{C}$ un code linéaire $[n, k, d]$ sur $\mathbb{K}$ , Soit $H$ une matrice de contrôle de $\mathcal{C}$.

**Définition 2.8.3** *Pour* $x \in \mathbb{K}^n$ , $x \in \mathcal{C} \Longleftrightarrow xH^T = 0$
$xH^T$ *est appelé Syndrome de* $x$ .
*On défini une relation d'équivalence dans* $\mathbb{K}^n$ *par :* $x\mathcal{R}y \Longleftrightarrow (x - y)H^T = 0$ ;
*alors :*

$$\begin{array}{rcl} xH^T = yH^T & \Longleftrightarrow & (x - y)H^T = 0 \\ x\mathcal{R}y & \Longleftrightarrow & x - y \in C. \end{array}$$

*L'ensemble des classes est* $\dfrac{\mathbb{K}^n}{C} = \{x + c | x \in \mathbb{K}\}$ , *alors :* $|\dfrac{\mathbb{K}^n}{C}| = \dfrac{|\mathbb{K}^n|}{|C|} = \dfrac{q^n}{q^k} = q^{n-k} = m.$
*Soit* $u$ *un représentons de la classe* $\bar{x} = x + c$ *de poids minimum ,* $u$ *est appelé le leader de* $\bar{x}$.
*Soit* $\{u_1, u_2, ..., u_m\}$ *l'ensemble des leaders dans* $\mathbb{K}^n$.

### Principe de décodage par syndrome

1/ On détermine les leaders $u_1, u_2, ..., u_m$ .
2/ On construit le tableau standard :

| *leader* | $u_1 = 0$ | $u_2$ | ..... | $u_m$ |
|---|---|---|---|---|
| *syndrome* | $S(u_1) = u_1H^T$ | $S(u_2) = u_2H^T$ | ..... | $S(u_m) = u_mH^T$ |

3/ Soit $y \in \mathbb{K}^n$ le message reçu , $y$ affecte au moins de $e$ erreurs.
4/ On calcule $S(y) = yH^T$.
5/ On cherche $u_i$ un leader d'une classe de même syndrome que $y$.
6/ On décode le mot reçu pour $x = y - u_i$.

**Exemple**

Soit $\mathcal{C}$ un code de longueur 6 de matrice génératrice
$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ ; alors $H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$ ,
$d = 3$ ; alors $e = 1$

| *leader* | 0 | $e_1$ | $e_2$ | $e_3$ | $e_4$ | $e_5$ | $e_6$ | $e_4 + e_5$ |
|---|---|---|---|---|---|---|---|---|
| *syndrome* | (000) | (101) | (111) | (011) | (100) | (010) | (001) | (110) |

Soit $y(011111)$ un mot reçu

$$S(y) = yH^T = (011111) \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (011),$$

$x = y - u_i$ alors $x = (011111) - (001000) = (010111)$

**Cas où il y a au plus d'une erreur**

Soit $C$ le mot envoyé et $x$ le mot reçu, $d(x, c) =$ nombre d'erreurs.
$x - c = \lambda e_i$, $e_i$ étant un élément de la base canonique.
$(x - c)H^T = xH^T - cH^T = xH^T = \lambda e_i H^T$ car $c \in C$.
alors :

$$\lambda e_i H^T = \lambda c_i$$

tel que : $c_i$ est la $i$ ème colonne dans $H$, donc l'erreur est commise dans la $i$ ème colonne

## Exemple sur code de *Hamming*

Soit le code binaire de *Hamming* , $\mathcal{C}[7, 4, 3]$.
Soit $v = (1001) \in \mathbb{F}_2^4$, soit $G$ une matrice génératrice de ce code tel que :

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right),$$

donc $vG = c \in C$ ,alors :

$$vG = (1001) \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) = (1001100).$$

La matrice de contrôle $H$ qui convient à $G$ est

$$H = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Sachant que le mot reçu est $x = (0001100)$, alors on obtient le mot envoyée comme ci dessus :

$$xH^T = (0001100)\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (011)$$

,
donc c'est la 1 ère colonne de la matrice de contrôle $H$ , alors l'erreur est commise à la première position .
Donc le message envoyé est $c = (1001)$

### 2.8.2 Les codes "Maximum Distance Séparable" ($MDS$)

Soit $\mathcal{C}$ un code linéaire $[n, k, d]$ (i.e. de longueur $n$, de dimension $k$ et de distance minimale $d$) sur un corps fini $K$. Soient $H$ sa matrice de contrôle et $G$ sa matrice génératrice. Alors le rang de $H$ est égal à $n - k$ . Donc il y a au plus $n - k$ colonnes dans $H$ linéairement indépendantes. Il existe donc dans C des mots de poids $n - k + 1$. On obtient :
d $\leq n - k + 1$ . Cette relation entre les paramètres du code $\mathcal{C}$ est la borne de Singleton.

**Définition 2.8.4** *Le code $\mathcal{C}$ est dit "maximum distance séparable" est un code $MDS$ si et seulement si $d = n - k + 1$ ; i.e. sa matrice de contrôle est de rang $d - 1$ (ou encore sa matrice génératrice est de rang $n - d + 1$).*
*Il est dit $MDS$ trivial lorsque $k = 1$ ou $k \geq n - 1$.*

***Exemple***
*On peut aisément construire un code $MDS$ trivial binaire de type $[n, n-1, 2]$ . Nous donnons ci-après un exemple de matrice génératrice pour $n = 6$ ; la généralisation, pour toute longueur, est évidente. Le code de matrice génératrice*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$ *est $MDS$ trivial.*

*Citons les propriétés immédiates de ces codes :*
1) $\mathcal{C}$ *est* $MDS$ *si et seulement si chaque ensemble de* $n-k$ *colonnes de sa matrice de parité* $H$ *est de rang* $n-k$ *;*
2) *Si* $\mathcal{C}$ *est* $MDS$*, alors* $\mathcal{C}^{\perp}$ *l'est aussi ;*
3) $\mathcal{C}$ *est* $MDS$ *si et seulement si chaque ensemble de* $k$ *colonnes de sa matrice génératrice* $G$ *est de rang* $k$*.*

*On a certaines informations sur les codes* $MDS$ *; ainsi ils constituent une classe de codes dont on connait la distribution des poids.*

# Chapitre 3

# les codes cycliques

**Définition 3.0.5** *soit $k$ un corps commutatif fini ,un code linéaire $\mathcal{C}$ de longueur $n$ est dit cyclique si :*

$$(x_1; x_2; ...; x_n) \in \mathcal{C} \Longrightarrow (x_n; x_1; ...; x_{n-1}) \in \mathcal{C}$$

## Remarque

soit $P$ la matrice de permutation correspondante au cycle $(1; 2; ...; n)$ alors :

$$P = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & ... & 1 \\ 1 & 0 & 0 & ... & 0 \end{pmatrix}$$

donc

$$x = (x_1; ...; x_n).P = (x_1; ...; x_n) \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & ... & 1 \\ 1 & 0 & 0 & ... & 0 \end{pmatrix} = (x_n, x_1, ..., x_{n-1})$$

$$\mathcal{C} \text{ cyclique} \Longleftrightarrow x \in \mathcal{C} \Longrightarrow x.P \in \mathcal{C}$$

**Proposition 3.0.2** *soit $\mathcal{C}$ un code linéaire de matrice génératrice $G$ et de matrice de contrôle $H$ ,alors :*

$$\mathcal{C} \text{ est cyclique} \Longleftrightarrow GP^tH = 0$$

## 3.1 Polynôme générateur et polynôme de contrôle

soit $\mathcal{C}$ un code cyclique de longueur $n$ et de dimension $m$ sur $k$
alors il existe un polynôme unitaire unique $g$ de $K[x]$ de degré $n-m$ divisant $x^n-1$
telle que : $\mathcal{C}$ est l'idéal de $\frac{K[X]}{\langle x^n-1\rangle}$ engendré par $\overline{g(x)}$
donc les éléments de $\mathcal{C}$ sont des multiples de $g(x) mod[x^n-1]$
le polynôme $g$ est dit : " polynôme générateur de $\mathcal{C}$ "
Le polynôme $h(x)$ telle que $g(x)h(x) = x^n - 1$ est appelé le polynôme de contrôle $\mathcal{C}$.

### Réciproquement

Tout polynôme $g$ de dégrée $n-m$ ,divisant $x^n-1$ est un polynôme générateur d'un code cyclique de longueur $n$ est de dimension $m$

### lemme 1

Chaque élément de $R_n$ est représente par une seule polynôme de dégrée $< n$
pour prouver le lemme, on utilise le fait suivant :
**Fait ( division avec le reste )**
pour tout $f(x) \in \mathbb{F}_q[x]$, $g(x) \in \mathbb{F}_q[x]\backslash\{0\}$, il existe unique $Q(x), r(x) \in \mathbb{F}_q[x]$ tel que :
$f(x) = g(x)Q(x) + r(x)$ et $deg(r(x)) < deg(g(x))$ (peut être $r(x) = 0$)
Dans ce cas, le polynôme $Q(x)$ est le quotient, et $r(x)$ le reste, de $f(x)$ lorsqu'il est divisé par $g(x)$.
peur trouver Le quotient et le reste, en utilisant l'algorithme de "longue division de polynômes". Exemple de division longue : diviser $x^5+1$ par $x^2+x+1$ dans $\mathbb{F}_2[x]$, trouver :

$$\begin{array}{r|l} x^5+1 & \underline{x^2+x+1} \\ \underline{x^5+x^4+x^3} & x^3+x^2+1 \\ x^4+x^3+1 & \\ \underline{x^4+x^3+x^2} & \\ x^2+1 & \\ \underline{x^2+x+1} & \\ x & \end{array}$$

Donc $x^5+1 = (x^2+x+1)Q(x) + r(x)$ dans $\mathbb{F}_2[x]$, avec $Q(x) = x^3+x^2+1$ et $r(x) = x$ .
cet exemple montre une longue division de polynômes sur $\mathbb{F}_2$. ( Division par un binaire fixe polynomial est largement implémenté dans les circuits électroniques au niveau matériel, au moyen de registres à décalage . Nous verrons bientôt pourquoi de telles implémentations sont nécessaires).

**preuve de lemme**
Prenons un élément de $\mathcal{R}_n$, représenté par un polynôme $f(x)$. Alors le même élément de$\mathcal{R}_n$ est également représenté par le polynômer$(x) = f(x) - Q(x)(x^n - 1)$ où $r(x)$ est fourni par Long Division de sorte que $deg(r(x)) < n$.
Par conséquent. tout élément de $\mathcal{R}_n$ =$\mathbb{F}_q[x]$ $/(x^n - 1)$ est représenté par un polynôme de degré $< n$.
Deux polynômes $r_1 = r_2$ de degré$< n$ ne peuvent pas représenter le même élément de $mathcalR_n$
$deg(r1 - r2) < n$ signifie que $r_1 - r_2$ ne peut pas être un multiple du polynôme $x^n - 1$

## Lemme (*Prange*, 1957)

Codes cycliques $\mathcal{C} \subseteq F_q^n$ sont les idéaux de l'anneau $R_n$ .
**Preuve**
Soit $\mathcal{C} \subseteq F_q^n$ est un code cyclique. Par définition, $\mathcal{C}$ est linéaire, donc est un sous-groupe additif de $R_n$.
De plus, $xC \subseteq C$ parce que $\mathcal{C}$ est fermé sous le décalage cyclique. Itérer, nous obtenir $x^2\mathcal{C} = x(x\mathcal{C}) \subseteq x\mathcal{C} \subseteq \mathcal{C}, x^3\mathcal{C} \subseteq \mathcal{C}, ...x^{n-1}\mathcal{C} \subseteq \mathcal{C}$. Depuis $1, x, ..., x^{n-1}$ base de $R_n$ , cela montre que $R_n\mathcal{C} \subseteq \mathcal{C}$ d'où $\mathcal{C}$ est un idéal. Pour classer les codes cycliques dans $F_q^n$ , nous devons classer les idéaux de $R_n$ . Ceci est fait avec le aide du suivant.

**Théorème 3.1.1** ***(structure des idéaux de*** $R_n$***)***
*Si C est un idéal de$R_n$, alors il existe un unique polynôme unitaire $g(x)$ telles que$\mathcal{C}$ est représenté par l'ensemble des multiples de $g(x)$ de degré inférieur à $n$ , D'où $\mathcal{C} = gR_n$.*
*Le polynôme g(x) est un diviseur de $x^n - 1$ dans $\mathbb{F}_q[x]$, tel que $\mathbb{F}_q[x]$.*

## preuve

(*Existence de* $g(x)$), soit $g(x) \in \mathbb{F}_q[x]$ est un polynôme non nul de degré inférieur qui représente un élément de $\mathcal{C}$. Faire $g(x)$ unitaire en le divisant par son coefficient.
Tous les multiples de $g(x)$ représentent les éléments de $\mathcal{C}$ ; car $\mathcal{C}$ est un idéal. Réciproquement, si f(x) représente un élément de $\mathcal{C}$, on écrit $r(x) = f(x) - g(x)Q(x)$ où $deg\, r(x) < deg\, g(x)$. De sorte que $r(x)$ représente également un élément de $\mathcal{C}$. Mais $g(x)$ a degré inférieur parmi les polynômes non nuls avec cette propriété, d'où $r(x) = 0$ et $f(x) = g(x)Q(x)$.
Nous avons prouvé que tous les polynômes qui représentent les éléments de $\mathcal{C}$ sont des multiples de $g(x)$.
On a deux conclusions :
$x^n - 1$ est un multiple de $g(x)$. Deuxièmement, par le Lemme 1 chaque élément de $\mathcal{C}$ est représenté par un multiple de $g(x)$ de degré<n.
Unicité de g(x) : soit un autre polynôme $g_1(x)$ avec ces propriétés doit être un multiple de $g(x)$ et $g(x)$ doit être un multiple de $g_1(x)$, donc, les deux polynômes sont unitaires,
alors $g_1(x) = g(x)$.

### Remarque

pour déterminer les codes cycliques de longueur $n$ ;il suffit de déterminer les polynômes de degré $n-m$ divisant $x^n-1$

$$dim\mathcal{C} = n - deg(g) = n - (n-m) = m$$

**Proposition 3.1.1** *soit $\mathcal{C}$ un code cyclique de longueur $n$ et de dimension $m$ et de polynôme générateur $g$ ;on pose $h = \frac{x^n-1}{g}$ de degré $m$,alors*

$$b \in \mathcal{C} \Longleftrightarrow b.h \equiv 0[x^n-1]$$

*$h$ est appelé polynôme de contrôle de $\mathcal{C}$*

## 3.2 matrice génératrice et matrice de contrôle pour un code cyclique

**Définition 3.2.1** *soit $\mathcal{C}$ un code cyclique de longueur $n$ est de dimension $m$ sur $k$ ;*
$g(x) = g_0 + g_1x + ... + g_{n-m}x^{n-m}$ *, son polynôme générateur*
$h(x) = h_0 + h_1x + ... + h_mx^m$ *, son polynôme de contrôle*

*alors une matrice génératrice de $\mathcal{C}$ est donnée*

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-m} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & & g_{n-m} & \cdots & 0 \\ \vdots & & & \ddots & \vdots & & \vdots \\ 0 & & \cdots & g_0 & g_1 & \cdots & g_{n-m} \end{pmatrix} \in \mathcal{M}_{m\times n},$$

*une matrice de contrôle de $\mathcal{C}$ est donnée pas :*

$$H = \begin{pmatrix} h_m & h_{m-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_m & \cdots & & h_0 & \cdots & 0 \\ \vdots & & & \ddots & \vdots & & \vdots \\ 0 & & \cdots & h_m & h_{m-1} & \cdots & h_0 \end{pmatrix} \in \mathcal{M}_{n-m\times n},$$

**Exemple**
rappellent que le code $E_3$ ; telle que $E_3 = \{000; 110; 011; 101\} \subseteq \mathbb{F}_2^3$ considérée comme un idéal de $R_3$, est représentée par le code polynômes $0, 1+x, x+x^2 = x(1+x)$ et $1+x^2 = (1+x)^2$, de degré $< 3$. Le polynôme de code unitaire degré inférieur est $1+x$. Observer que tous les polynômes de code sont des multiples de $1+x$ qui est donc le polynôme générateur du code cyclique $E_3$ .

## Exemple

Utilisent le théorème (3.1.1) et le théorème (3.2.1) pour trouver tous les codes binaires cycliques de longueur 3.
**Solution** : Les polynômes générateurs sont facteurs unitaire de $x^n - 1$ dans $\mathbb{F}_p[x]$ Le premier pas est de factoriser $x^n - 1$ dans **polynômes unitaire irréductibles** dans $\mathbb{F}_p[x]$ Un polynôme est irréductible s'il ne peut être écrit comme un produit de deux polynômes de degré positif.
Notez que le polynôme $x^n - 1$ est ne pas irréductible dans $\mathbb{F}_p[x]$, pour tous $n; p > 1$ .
Effectivement,$x^n - 1 = (x - 1)(x^{n-1} + ... + x + 1)$.
Nous travaillons sur le corps $\mathbb{F}_2$ et observez :

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

Le polynôme $x - 1 = x + 1$ est irréductible, car il est de degré 1.
Pouvons-nous factoriser le polynôme$x^2 + x + 1$ dans$\mathbb{F}_2[x]$?
Si nous pouvions, nous aurions un factorisation $(x + a)(x + b)$.
Mais alors $ab = 1$ ce qui signifie $a = b = 1$ dans $\mathbb{F}_2$.
Notez que $(x + 1)^2 = x^2 + 1$ dans $\mathbb{F}_2[x]$ Nous avons montré que $x^2 + x + 1$ est irréductible dans $\mathbb{F}[x]$ Donc, les facteurs unitaire possibles de $x^3 - 1$ dans $\mathbb{F}_2[x]$ sont :

$$1; 1 + x; 1 + x + x^2; 1 + x^3$$

Nous pouvons maintenant lister tous les codes cycliques $\mathbb{F}_2^3$ comme idéaux de $R_3$ généré par chacun des ci-dessus polynômes.
Pour chaque code, nous donnons une matrice de générateur $G$, indiquer la distance minimale ré et un nom bien connu du code, et souligner son double code (qui est aussi cyclique).

• $g(x) = 1$,

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

ce qui correspond à la code binaire trivial de longueur 3 :
$\{000, 100, 010, 001, 110, 101, 011, 111\} = \mathbb{F}_2^3$ avec $d = 1$.
Le dual de code de $\mathbb{F}_2^3$ est le code zéro (voir ci-dessous)
• $g(x) = 1 + x$,

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

c'est $\{000, 110, 011, 101\}$=$E_3$ ce qui correspond à la code binaire trivial de longueur 3 :qui a $d = 2$. Le dual de $E_3$ est $\mathcal{C}[3, 2]$ (voir ci-dessous).
• $g(x) = 1 + x + x^2$,

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

c'est $\{000, 111\} = \mathcal{C}[3, 2]$, le code de répétition de longueur 3 avec $d = 3$.
Ce code est $(E_3)^{\perp}$.

• $g(x) = 1 + x^3$, Théorème (3.2.1) renvoie la matrice $G$ avec $k = 3 - 3 = 0$ rangées, $G = [\,]$
Le seul code de dimension 0 est le code zéro, $\{000\}$. C'est un code inutile, mais formellement c'est un code linéaire et cyclique, donc nous devons l'autoriser pour des raisons de cohérence.
La distance minimale du code zéro est indéfinie. Ce code est $(\mathbb{F}_2^3)^{\perp}$
Fin de l'exemple.

## Application

on va déterminer tous les codes cyclique de longueur 7 sur $\mathbb{F}_2$
$x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$

1) $g(x) = x + 1$

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

$\mathcal{C}_1 = [7; 6]$

$h(x) = \frac{x^7-1}{x+1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
alors $H = (1111111)$
$H$ admet 2 colonne liée et toute famille a une colonne libre donc $d = 2$

$$\mathcal{C}_1 = [7; 6; 2]$$

2) $g(x) = 1$

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \vdots & & & \ddots & & & \vdots \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = I_7$$

$\mathcal{C} = \{x.G; x \in \mathbb{F}_2^7\} = \mathbb{F}_2^7$

$h(x) = x^7 - 1$ ; alors $H = 7 \times 0 \Rightarrow d = 1$

$$\mathcal{C}_2 = [7; 7; 1]$$

3) $g(x) = x^7 - 1$ alors $G = 0$
alors $\mathcal{C}_3 = 0$

$$\mathcal{C}_3 = [7; 0]\,; H = I_7$$

4) $g(x) = x^3 + x^2 + 1$

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

$h(x) = (x+1)(x^3 + x^2 + 1)$
$\quad = x^4 + x^2 + x + x^3 + x + 1$
$\quad = x^4 + x^2 + x^3 + 1$

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

$c_1 + c_2 + c_6 = 0$

$d \leqslant 3$ chaque famille de deux colonne est libre alors $d = 3$

$$\mathcal{C}_4 = [7; 4; 3]$$

5) $g(x) = x^3 + x + 1$
$h(x) = (x+1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$

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

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

$c_2 + c_6 + c_7 = 0$

$d \leqslant 3$ chaque famille de deux colonne est libre alors$d = 3$

$$\mathcal{C}_5 = [7; 4; 3]$$

6) $g(x) = (x+1)(x^3+x^2+1) = x^4+x^2+x+1$

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

$h(x) = x^3+x+1$

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

$c_1 + c_2 + c_4 + c_7 = 0$ donc
$d \leqslant 4$ chaque famille de 3 colonne est libre

$$\mathcal{C}_6 = [7; 3; 4]$$

7) $g(x) = (x+1)(x^3+x+1) = x^4+x^3+x^2+1$ alors

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

$h(x) = x^3+x^2+1$

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

$c_1 + c_4 + c_6 + c_7 = 0$ , donc
$d \leqslant 4$ chaque famille de 3 colonne est libre $\Rightarrow$ d=4

$$\mathcal{C}_7 = [7; 3; 4]$$

8) $g(x) = (x^3 + x^2 + 1)(x^3 + x + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
alors $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$
h(x)= x+1

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix};$$

$c_1 + c_2 + ... + c_7 = 0$ donc $d \leqslant 7$

$$\mathcal{C}_8 = [7; 1; 7]$$

## Remarques

1) L'orthogonal des codes précédents :
$dim\mathcal{C} + dim\mathcal{C}^{\perp} = dimE = n$

| $\mathcal{C}$ | $\mathcal{C}_1$ | $\mathcal{C}_2$ | $\mathcal{C}_3$ | $\mathcal{C}_4$ | $\mathcal{C}_5$ | $\mathcal{C}_6$ | $\mathcal{C}_7$ | $\mathcal{C}_8$ |
|---|---|---|---|---|---|---|---|---|
| $\mathcal{C}^{\perp}$ | $\mathcal{C}_8$ | $\mathcal{C}_3$ | $\mathcal{C}_2$ | $\mathcal{C}_7$ | $\mathcal{C}_6$ | $\mathcal{C}_5$ | $\mathcal{C}_4$ | $\mathcal{C}_1$ |
| $d$ | 1 | 2 | $\nearrow$ | 3 | 3 | 4 | 4 | 7 |

comme $d(\mathcal{C}_4) = d(\mathcal{C}_5) = 3$ alors $\mathcal{C}_4$ ou $\mathcal{C}_5$ le code de $Hamming$ de longueur 7

$$H_{\mathcal{C}_4} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$H_{\mathcal{C}_5} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \Longrightarrow P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 5 & 6 & 3 & 2 & 7 \end{pmatrix}$$

$\mathcal{C}_4$ et $\mathcal{C}_5$ sont équivalents
2) $\mathcal{C}_1$ : n-k+1 = 7-6+1 = 2 = d alors $\mathcal{C}_1$ est un M.D.S code
$\mathcal{C}_2$ : n-k+1 = 7-7+1 = 1 = d alors $\mathcal{C}_2$ est un M.D.S code
$\mathcal{C}_8$ : n-k+1 = 7-1+1 = 7 = d alors $\mathcal{C}_8$ est un M.D.S code

# Bibliographie


[1] Serir Khadidja, Application des codes correcteurs d'erreurs *ReedMuller* , université Aboo Bakr Belkaid.Tlemcen ; 2011 .

[2] Claude Cartel, cours de code correcteurs d'erreurs ( et fonction boolément) , D.E.A de Mathématique et Informatique de Bamako ; 2007 .

[3] Jean-Guillaume Dumas, Jean-Louis Roch,Éric Tannier, Sébastien Varrette, Théorie des codes Compression , cryptage , correction , *Dunod*, Paris ; 2007, 2013.

[4] Sahraoui Alaeddine, Les codes Simplexe , Université *Laarbi Ben M'hidi Oum El BOUAGHI* ; 2013.

[5] B. Rouzeyre, Codes détecteurs et correcteurs .

[6] Structures algébriques : groupes , anneaux et corps , Maths *PCSI*.

[7] Pierre *Abbrugiati*, Introduction aux codes correcteurs d'erreurs , 23 janvier 2006.

[8] Licence Math-Info 1 ère année, Résume sur les structures algébriques des ensembles avec opérations Groupes , Université Claude Bernard Lyon 1 ; Printemps 2012.

[9] François Dumas, ALGÈBRE : GROUPES ET ANNEAUX 1 , Université Blaise Pascal U.F.R. Sciences et Technologies ; 2007-2008.

[10] Marc Chaumont, Codes Correcteurs d'erreurs Cours 1 + Introduction + Codes linéaires en bloc ; Novembre 12, 2008

[11] Yuri Bazlov ,MATH32032 Coding Theory - 2017/18 Semester 2 ,Manchester University

[12] ADEL ALAMADHI , HOUDA SBOUI, PATRICK SOLÉ , AND OLFA YEMEN ,CYCLIC CODES OVER M 2 ($\mathbb{F}_2$ ) , Arxiv , 31/01/2012

[13] Nuh Aydin, An Introduction to Cording Theory via Hamming Codes :A Computational Science Model, Kenyon College, aydinn@Kenyon.edu, 8 -2007

[14] N.HADI-SAID,A.ALI- PACHA, M'HAMED et A.BELGHORAF, Méthodes de Détermination des Polynôme Primitifs, Sept 2009

# Résumé

Les télécommunications sont devenues indispensables dans notre vie quotidienne, cet échange numérique d'informations se fait par le biais de canaux de communication comme le câble, la fibre optique, le wifi, les satellites ...etc.

Ces canaux ne sont pas tous fiable 100%. la théorie des codes correcteurs d'erreurs s'est développée pour répondre à ce genre de problème.

Le principe des codes correcteurs d'erreurs est de rajouter une information supplémentaire redondante de manière à détecter et éventuellement corriger de possibles erreurs de transmission.

La genèse de ces codes consiste à effectuer deux opérations à savoir le codage et le décodage. La première consiste en l'adjonction des bits de redondance, tandis que la deuxième essayera de détecter et corriger les erreurs en passant par plusieurs étapes.

La théorie des codes correcteurs ne se limite pas qu'aux communications classiques ( radio, télévision, etc.) mais également aux supports pour le stockage comme disque compact, Pour le code cyclique défini sur $\mathbb{F}_{64}$ est plus largement utilisé pour les CD ROM.

Notre travail est seulement une entrée sur le code cyclique qui est un cas particulier de code quasi-cyclique, cette recherche de congé aux personnes intéressée dans ce domaine.

# Abstract

Telecommunications have become indispensable in our daily life, this digital exchange of information is done through communication channels such as cable, optical fiber, wireless, satellites...

These channels are not all reliable 100%. the theory of error correcting codes was developed to meet this kind of problem.

The principle of error-correcting codes is to add additional redundant information to detect and correct any possible transmission errors.

The genesis of these codes is to perform two operations : the encoding and decoding. The first is the addition of redundant bits, while the second will attempt to detect and correct errors through several stages.

The coding theory is not confined only to traditional communications ( radio, television, etc...) but also for storage media like compact disks, for cyclic code set to $\mathbb{F}_{64}$ is most widely used for the CD ROM.

Our work is only one entry on cyclic code which is a special case of codes almost cyclical this search for leave to people intersted in this area.

# ملخص

اصبحت الاتصَالَات السلكية و اللَاسلكية لَا غنَى عنهَا في حيَاتنَا اليومية، و يَتِم هَذَا التبَادل الرقمي لِلمعلومَات من خلَال قنوَات الَاتصَال مثل الكَابل و الَاليَاف البَصرية الويفي و الَاقمَار الَاصطنَاعية.
هذه القنوَات ليست دقيقة 100% .
و بَالتَالي نظرية الترميز المصحِحة لِلَاخطَاء اكتشفت لتصحيح مثل هذه المشَاكل، حيث ترتكز علَى اضَافة معلومَات إِلَى المعلومة الأصلية المرَاد إِرسَالهَا بهدف تعيِين موَاقع الأخطَاء و تصحيحهَا ، تطبيق هذه النظرية يتضمن القيَام بعمليتين أسَاسيتين الأولَى تسمَى بَالترميز أي اضَافة معلومة مرَاقبة في اخر المعلومة الأصلية و الثَانية تسمَى بفك الترميز و التي تمكنَنَا من اكتشَاف الأخطَاء و تصحيحهَا مرورَا بعدة مرَاحل .
اذن لَا يقتصر استعمَالهَا علَى الَاتصَالَات الكلَاسيكية فقط ( مذيَاع ، تلفَاز ) بل ايضَا علَى أجهزة التخزين مثل اقرَاص المضغوطة و التي يستعمل من أجلهَا الترميز الدوري المعرف علَى $\mathbb{F}_{64}$ مثلمَا رأينَا مدخل الَى هذه الترميزَات الدورية و التي هي حَالة خَاصة من الترميزَات الشبه دورية حيث تقدر الِازَاحة بدرجة وَاحدة ، و بهذَا نترك البحث لِلمهتمين في هذَا المجَال .