REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université El Hadj Lakhdar BATNA

Faculté des sciences

Département de Mathématiques

Laboratoire des Techniques Mathématiques

MEMOIRE

En vue de l'obtention du diplôme de:

MAGISTER

Option :

MATHEMATIQUES APPLIQUEES

Présenté par :

MELAKHESSOU Ahlem

Théorie Algébrique Des Codes Convolutionnels Cycliques

Soutenue le : 14 / 12 / 2011 **Devant le jury composé de :**

Mr. Salah Eddine REBIAI	**Professeur (U. de Batna)**	**Président**
Mr. Moussa BENLAHCENE	**Chargé de cours (U. de Batna)**	**Rapporteur**
Mr. Lemnouer NOUI	**Professeur (U. de Batna)**	**Examinateur**
Mr. Douadi MIHOUBI	**Professeur (U.de M'sila)**	**Examinateur**

REMERCIEMENTS

Je tiens à remercier chaleureusement Monsieur **BEN LAHCEN MOUSSA** pour l' aide inestimable qu' il m'apporté dans la documentation nécessaire à la rédaction de cette thèse .

Je remercie également les nombreux professeur du département ma thématique ; respectivement : **SALAH EDDIN REBIAI** (professeur à l'université de Batna) Monsieur **LEMNOUAR NOUI** (professeur à l'université de Batna), Monsieur **D. MIHOUBI** (maitre de conférences Université de M'SILA) qui ont accepté d'être des membres du jury de cette thèse.

Mes remerciements aussi à tous mes professeurs qui ont contribué à ma formation.

Mes remerciements à mes parents à mon mari m'a beau coup soutenu dans la réalisation de ce projet ; sans oublier à remercier **Chatouh Karima** ; qui m'a aidé .avec ses conseils judicieux.

Mes remerciements aussi à toute ma famille, et la famille de mon mari

Table des matières

Notation

$\mathbb{F}_q$	Un corps fini à q éléments ;
$C(n,k,d)$	Code linéaire C de longueur n, de dimension k et de distance minimale d ;
G	Matrice génératrice de C ;
CC	Code convolutionnel ;
CCC	Code convolutionnel cyclique ;
$A = \mathbb{F}_q / \langle x^n - 1 \rangle$	L'anneau des polynômes modulo $x^n - 1$;
$Aut_{\mathbb{F}}(A)$	Groupe d'automorphisme de A ;
$A[z]$	Anneau des polynômes à coéfficients dans l'anneau A ;
G^t	Transposée d'une matrice G ;
Id_k	Matrice identité de rang k ;
$\deg(f(x))$	Degré de polynôme$f(x)$;
$\omega(u)$	Poids de Hamming de u ;
$A[z\ ;\sigma]$	L'ensemble $A[z]$ muni le produit $*_\sigma$;
$\operatorname{Im} G$	Image de G;

Introduction

La communication avec les sondes spatiales, à l'autre bout du système solaire, pose le problème de la fiabilité du message transmis. Une transmission sur une telle distance est obligatoirement parasitée (notamment à cause de diverses sources de perturbations électromagnétiques). Pourtant, dans ce domaine et dans bien d'autres, il est primordial que les informations collectées pas les sondes soient bien reçues. Il y a donc nécessité de "sécuriser" la transmission : c'est le rôle des codes correcteurs d'erreurs. On rajoute au message à transmettre des informations supplémentaires qui permettent de reconstituer le message au niveau du récepteur.

Le domaine d'étude des codes correcteurs a connu une évolution en définissant des classes de codes. Chaque classe possède des propriétés concernant leurs construction, par exemple les codes de Hamming, les codes BCH et les codes convolutionnels (ou convolutifs).

Les deux classes les plus importantes des codes utilisés dans la pratique, sont les codes en blocs et les codes convolutionnels.

Tandis que les deux classes jouent un rôle également important dans la pratique en matière de technologie, le code convolutionnel à été crées seulement dans les années 70 du dernier siècle.

Les codes convolutionnels ont été utilisés dans les applications commerciales des satellites de communication, ainsi que dans les applications de satellites militaires et dans tous les standards de téléphonie mobile de deuxième génération.

L'objectif principal de ce mémoire est l'étude des codes convolutionnels qui consiste à la construction de ces codes sur différents corps finis , ces approches surtout les approches graphiques et polynômiaux, la cyclicité et la cyclicité double.

Ce travail est composé de trois chapitres structurés comme suit :

Dans le premier chapitre on donne quelque notions de base d'algèbre, ensuite on présente les notions fondamentales de la théorie des codes linéaires (la matrice génératrice, la distance minimale, la cyclicité d'un code linéaire et la représentation polynômiale).

Dans le deuxième chapitre on présente les codes convolutionnels selon les trois approches suivantes :

* L' approche de la matrice polynômiale.

* L' approche de la matrice scalaire.

* L' approche du décalage de registre .

* Les approches graphiques :

  - diagramme en arbre.

  - diagramme d'état.

  - treillis.

Le troisième chapitre consiste à la construction des codes convolutionnels $\sigma-$cycliques (codes convolutionnels cycliques au sens de Piret) et doublement cycliques. Cette construction est basée sur l'étude de l'algèbre de Piret $A[z,\sigma]$ pour certains automorphismes σ de A.

Les codes convolutionnels $\sigma-$cycliques sont caractérisés par H.GLUSING-LUERSSEN [3] comme des idéaux à gauche dans l'algèbre $A[z,\sigma]$.

Notre participation consiste à détérminer les polynômes générateurs de ces idéaux et les matrices génératrices des codes convolutionnels doublement cycliques.

Chapitre 1

Généralités sur les codes correcteurs d'erreurs

La théorie des codes est développée pour répondre au problème de la correction des erreurs introduites dans un système de transmission de l'information. À l'origine, développée par des ingénieurs en électronique, elle constitue maintenant une branche des mathématiques discrètes. Le principe de construction d'un code correcteur d'erreurs systématique consiste à ajouter aux mots constitués de m éléments d'information $a_1a_2...a_m$ où les a_i parcourent un corps fini $\mathbb{F}$, k éléments (dits de contrôle) $a_{m+1}a_{m+2}...a_{m+k}$ déterminés par le biais d'une fonction (dite fonction de codage)Ψdes m éléments d'information ; définie au préalable. La longueur d'un mot code est alors $n = m + k$. Pour vérifier qu'un mot reçu $a_1a_2...a_ma_{m+1}a_{m+2}...a_{m+k}$ appartient au code, on applique la fonction $f : \mathbb{F}^m \longrightarrow \mathbb{F}^{m+k}$ à $a_1a_2...a_m$ on obtient le bits de redondance $b_{m+1}b_{m+2}...b_{m+k}$. Ensuite on compare cette grandeur aux éléments effectivement reçus $a_{m+1}a_{m+2}...a_{m+k}$. S'il y a coïncidence entre ces grandeurs, le mot reçu est un mot code, sinon on détecte une erreur.

Nous rappelons, dans ce chapitre, quelques notions de base utiles pour l'étude des codes convolutionnels, ainsi que la cyclicité de ces codes.

1.1 Les codes linéaires

Cette famille de codes est développeé par Mac Williams et Sloane dans les années 50 [1]. Ces codes sont utilisés dans les transmissions satellitaires, téléphoniques, la sauvegarde sur disque Laser, la lutte contre le bruit, traitement de l'image et de la parole entre autres.

Définition 1

• *Soit A un ensemle fini, dit alphabet. L'ensemble des mots de longueur finie formés avec les symboles de A, muni de la loi de composition interne "concaténation" est un monoïde libre, noté $\overline{A}$. L'élément neutre de cette loi est le mot vide.*

• *Un code C sur A est un sous ensemble de $\overline{A}$. Les éléments c de C sont dits "mots codes".*

• *On dit que C est un code binaire si $A = \mathbb{F}_2 = \{0, 1\}$.*

• *Si tous les mots codes de C sont de même longueur, on dit que C est un code en bloc. Dans le cas contraire C est un code à longueur variable.*

Définition 2

Si $\mathbb{F}$ est un corp fini et C est un sous-espace vectoriel de dimension k de $\mathbb{F}^n$, alors C est dit un code linéaire de longueur n et de dimension k qu'on note $C(n, k)$.

1.1.1 Codage en bloc linéaire

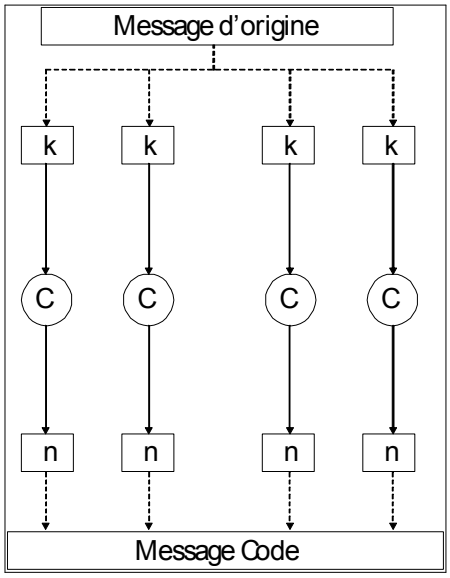
Nous allons considérer dans la suite que $\mathbb{F}$ est un corps fini, et $V = \mathbb{F}^n$ l'espace vectoriel de dimension n sur $\mathbb{F}$.

Le codage en bloc consiste à découper le message à transmettre (un paquet de bits de $\mathbb{F}$) en blocs ayant tous une certaine longueur k fixée à l'avance. Puis en lui joignant $n-k$ bits supplémentaires appelés bits de contrôle, ou bits de parité. Le bloc obtenu est dit mot code.

Le nombre n s'appelle la longueur du code.

Si les bits de contôle sont placés à la fin de chaque bloc ; le codage est dit systématique.

La figure suivante représente le codage en bloc :



Remarque 3

Le codage en bloc linéaire peut être représenter par une application linéaire

$$\phi : \mathbb{F}^k \longrightarrow \mathbb{F}^n$$
$$u \longmapsto \phi(u) = c$$

où $u = (u_0, u_1, ..., u_{k-1})$ *représente les* k *symboles d'information et* $c = (c_0, c_1, ..., c_{n-1})$ *le mot code qui lui est associé.*

1.1.2 La matrice génératrice d'un code linéaire

Etant donné un code linéaire $C(n,k)$ sur le corps $\mathbb{F}$. Soient $g_1, g_2, .., g_k$ une base de $C(n,k)$. Alors tout élément c de $C(n,k)$ est de la forme $c = u_1.g_1 + u_2.g_2 + ... + u_k.g_k$.

En posant $G = \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix}$ on obtient $c = u \cdot G$ où $u = (u_1, u_2, ..., u_k)$.

Proposition 4

Soit $C(n,k)$ un code linéaire dont $\{g_1, g_2, ..., g_k\}$ est une base de $C(n,k)$, alors tout élément de $C(n,k)$ s'écrit sous la forme

$$C = \left\{c : c = u \cdot G, u \in \mathbb{F}^k\right\} \tag{1.1}$$

où

$$G = \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix}$$

est une matrice de type $k \times n$.

Définition 5

Une matrice génératrice d'un code linéaire $C(n,k)$, notée G, est une matrice d'ordre k dont les vecteur lignes forment une base de $C(n,k)$.

Notons qu'il existe autant de matrices génératrices pour un code linéaire que de bases du sous espace $C(n,k)$.

L'encodage de $C(n,k)$ associé à $G = \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix}$ est l'aplication linéaire

$$\phi : \mathbb{F}^k \longrightarrow C(n,k) \subset \mathbb{F}^n$$

dont la matrice associée, relativement à la base canonique de $\mathbb{F}^k$ et la base $\{g_1, g_2, ..., g_k\}$ de $C(n,k)$, est la transposée de G. Tout message $u = (u_1, ..., u_k) \in \mathbb{F}^k$ est codé par

$$\phi(u) = G^t . \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix}$$

L'application $\phi : \mathbb{F}^k \longrightarrow C(n,k)$ est bijective car la matrice G est de rang maximum k.

1.1.3 La matrice de contrôle

Etant donné le code linéaire $C = C(n,k)$ de matrice génératrice G .

Considérons l'orthogonal (suivant le produit scalaire usuel sur $\mathbb{F}^n$) de C :

$$C^{\perp} = \left\{ v \in V : v^t c = 0 : \forall c \in C \right\}$$

Lemme 6

Soit $C = C(n,k)$

•$C^{\perp} = C(n, n-k)$ *(dit code dual de* C*).*

•*Si* H *est une matrice génératrice de* $C^{\perp}$ *alors*

$$C = \left\{ c \in V : H^t c = 0 \right\}$$

•*Pour toutes matrices génératrices* G *et* H *de* C *et* $C^{\perp}$ *respectivement, on a* $H^t.G = 0$.

Preuve

Le sous espace orthogonal de l'espace ligne de la matrice H, qu'on appèlle l'espace nul de la matrice H est exactement le code C.

En d'autre terme, on peut écrire :

$$C = \left\{ c \in V : H^t c = 0 \right\}$$

Il est clair qu'on a la relation suivante :

$$H^t G = 0$$

La matrice H est appelée la matrice de contrôle du code C. ■

1.1.4 La distance minimale d'un code linéaire

Soit $C = C(n,k)$ un code linéaire sur $\mathbb{F}$.

Définition 7

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

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

Définition 8

On appelle distance minimale d'un code linéaire $C = C(n,k)$, *notée* d, *la plus petite distance de Hamming entre deux mots codes différents*

$$d = \min_{\substack{u \neq v \\ u,v \in C}} d(u,v) \tag{1.2}$$

et on note $C = C(n,k,d)$.

Théorème 9

Un code $C = C(n,k,d)$ *peut corige au moins* $\left[\frac{d-1}{2}\right]$ *erreurs par mot.*

1.2 Codes classiques

1.2.1 Les codes de Hamming

Les codes de Hamming sont des codes linéaires. Ils sont caractérisés par l'aisance de codage et de décodage. Ils ont été introduits par Golay en 1949, et par Hamming en 1950.[1]

Nous donnons une présentation succinte, dans ce qui suit, les codes de Hamming binaires (tous les résultats sont généralisables au cas des corps finis quelconques).

Définition 10

Le code de Hamming à m bits de contrôle, noté $Ham(m)$ est le code linéaire de longueur $n = 2^m - 1$, dont la matrice de contrôle $H_m = (h_1, h_2, \ldots, h_n)$ est caractérisée par :

"le $i^{ième}$ vecteur colonne h_i est la représentation binaire de l'entier naturel i dans $\mathbb{F}_2$ ".

Autrement dit $Ham(m)$ est un $C(2^m - 1, 2^m - m - 1)$ et avec :

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

Exemple 11

Pour $m = 3$, on obtient comme matrice de contrôle

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Proposition 12

Pour tout $m \geq 3$, $Ham\,(m)$ est de distance minimale égale à 3. Par conséquent il est capable de corriger une seule erreur.

1.2.2 Les codes cycliques

La propriété cyclique de ce genre de codes permet une notation polynômiale particulièrement pratique rendant leur implémentation physique facile et réalisable en utilisant les circuits électroniques.

Définition 13

Soit C un sous espace de $\mathbb{F}^n$. On dit que C est cyclique si C satisfait :

$u_1 = \{c_0, c_1, ..., c_{n-1}\} \in C \Longrightarrow u_2 = \{c_{n-1}, c_0, c_1, ..., c_{n-2}\} \in C.$

Proposition 14 [3]

Soit C un sous espace de $\mathbb{F}^n$. C est cyclique si et seulement si

$$CS \subseteq C \text{ où } S = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{pmatrix} \text{ de type } n \times n \tag{1.3}$$

Représentation polynômiale des codes cycliques

Soit $\mathbb{F}[x]$ l'anneau unitaire des polynômes sur le corps $\mathbb{F}$. $\mathbb{F}[x]$ possède une structure d'espace vectoriel sur $\mathbb{F}$ ayant $\{1, x, x^2, ...\}$ comme base.

On considère le sous espace

$$\begin{aligned} A &= \{f \in \mathbb{F}[x] : \deg(f) \prec n\} \\ &= \left\{a_0 + a_1 x + ... + a_{n-1} x^{n-1} : a_i \in \mathbb{F}; 0 \leq i \leq n-1\right\} \end{aligned} \tag{1.4}$$

Proposition 15

les espaces vectoriels $\mathbb{F}^n$ *et* A *sont isomorphes.*

Preuve

On considère l'application

$$\begin{aligned} P &: \mathbb{F}^n \longrightarrow A \\ v &= (a_0, a_1, ..., a_{n-1}) \mapsto P(v) = \sum_{i=0}^{n-1} a_i x^i \end{aligned}$$

P est linéaire du fait que :

$$\begin{aligned} P(\alpha v + \beta u) &= \sum_{i=0}^{n-1} (\alpha a_i + \beta b_i) x^i \\ &= \sum_{i=0}^{n-1} \alpha a_i x^i + \sum_{i=0}^{n-1} \beta b_i x^i \\ &= \alpha \sum_{i=0}^{n-1} a_i x^i + \beta \sum_{i=0}^{n-1} b_i x^i \\ &= \alpha P(v) + \beta P(u) \end{aligned}$$

Soient u et v dans $\mathbb{F}^n$ tels que $P(u) = P(v)$.

Alors $0 = P(u) - P(v) = \sum_{i=0}^{n-1} (a_i - b_i) x^i$.D'où $u = v$.

Si $\mathbb{F} = \mathbb{F}_q$ pour un certain q et comme $\mid \mathbb{F}_q^n \mid = \mid A \mid = q^n$ alors P est un isomorphisme d'espaces vectoriels. ■

Considérons l'anneau quotient

$$\mathbb{F}[x] \diagup \langle x^n - 1 \rangle = \left\{ a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{F}; 0 \leq i \leq n-1 \right\}$$

où

$$\begin{aligned}
\alpha &= [x] \equiv x[x^n - 1] \\
\alpha^2 &= \left[x^2\right] \equiv x^2[x^n - 1] \\
&\vdots \\
\alpha^{n-1} &= \left[x^{n-1}\right] \equiv x^{n-1}[x^n - 1] \\
\alpha^n &\equiv 1[x^n - 1]
\end{aligned}$$

Alors on peut représenter $\mathbb{F}[x] \diagup \langle x^n - 1 \rangle$ sous la forme :

$$\mathbb{F}[x] \diagup \langle x^n - 1 \rangle = \left\{ v_0 + v_1 x + ... + v_{n-1} x^{n-1},\ v_i \in \mathbb{F} \right\} \tag{1.5}$$

D'où l'isomorphie de A et $\mathbb{F}[x] \diagup \langle x^n - 1 \rangle$.

Proposition 16

Soit $C \subset \mathbb{F}^n$ un code linéaire. Alors

$$C \text{ cyclique} \iff [c \in P(C) \Longrightarrow xc \in P(C)]$$

Preuve

•Soit

$$\begin{aligned}
v = (a_0, a_1, ..., a_{n-1}) \in C \ &\Longrightarrow P(v) = a_0 + a_1 x + ... + a_{n-1} x^{n-1} \\
&\Longrightarrow xP(v) = (a_0 x + a_1 x^2 + ... + a_{n-1} x^n) \\
&\equiv (a_0 x + a_1 x^2 + ... + a_{n-1})\,[x^n - 1] \\
&= a_{n-1} + a_0 x + a_1 x^2 + ... + a_{n-2} x^{n-1}
\end{aligned}$$

Si C est cyclique alors $(a_{n-1}, a_0, ..., a_{n-2}) \in C$. Donc $xP(v) \in P(C)$.

•Inversement

Pour

$$\begin{aligned} v = (a_0, a_1, ..., a_{n-1}) \in C \Longrightarrow P(v) &= a_0 + a_1 x + ... + a_{n-1} x^{n-1} \in A \\ &\Longrightarrow xP(v)\left[x^n - 1\right] \in A \\ &\Longrightarrow a_0 x + a_1 x^2 + ... + a_{n-1} \in A \\ &\Longrightarrow a_{n-1} + a_0 x + a_1 x^2 + ... + a_{n-2} x^{n-1} \in A \\ &\Longrightarrow (a_{n-1}, a_0, ..., a_{n-2}) \in C \end{aligned}$$

Alors C est cyclique. ■

Lemme 17

Soit $I \subset A$. Si I est idéal de A alors I satisfait :

$$c \in I \Longrightarrow xc \in I$$

Proposition 18 [1]

Le sous espace vectoriel C de $\mathbb{F}[x] \diagup \langle x^n - 1 \rangle$ est un code cyclique si et seulement si $P(C)$ est un idéal de A.

Preuve

Suposons que C est cyclique et prouvons qu'il est un idéal de $\mathbb{F}[x] \diagup \langle x^n - 1 \rangle$.

Si $c \in P(C)$ alors on a :

$$xc \in P(C)$$

Et par induction sur i on trouve :

$$\forall i : 0 \leq i \leq n-1 : x^i c \in P(C)$$

Par linéarité on peut écrire :

$$v(x)\, c(x) \in P(C)$$

pour tout polynôme $v(x)$ de $\mathbb{F}[x] \diagup \langle x^n - 1 \rangle$, ce qui montre que C est un idéal.

Réciproquement, supposons que C est un idéal dans $\mathbb{F}[x] \diagup \langle x^n - 1 \rangle$. Si $c(x) \in P(C)$ alors $xc(x) \in P(C)$ et d'après proposition 1.4 C est cyclique. ■

Proposition 19

Tout idéal de $\mathbb{F}[x] \diagup \langle x^n - 1 \rangle$ est engendré par un diviseur de $x^n - 1$.

Remarque 20

Tout diviseur $g(x)$ de degré m, $m \prec n$, de $x^n - 1$ on peut lui associer un code cyclique de longueur n et de dimension $n - m$ dont la matrice génératrice est donnée par :

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-m-1}g(x) \end{pmatrix}$$

$$= \begin{pmatrix} g_0 & g_1 & \cdots & g_{m-1} & g_m & 0 & \cdots & \cdots & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_{m-1} & g_m & \cdots & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_{m-2} & g_{m-1} & g_m & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_{m-1} & g_m \end{pmatrix}$$

où : $g(x) = g_0 + g_1 x + \cdots + g_{m-1}x^{m-1} + g_m x^m$.

1.2.3 Les codes BCH

Parmi les codes linéaires cycliques connus, les codes BCH$(1959 - 1960)$. Ces codes présentent une grande capacité de correction, pour des erreurs indépendantes.

Considérons un corps fini $\mathbb{F}$.

Définition 21

Soient r un entier positif et $\alpha \in \mathbb{F} = \mathbb{F}_{q=p^m}$ une racine $n-$ième de l'unité où p est l'ordre multiplication de q modulo n.

Un code BCH sur $\mathbb{F}_q$ de longueur n et de distance minimale $2 \leq d \leq n$ est un code cyclique dont le polynôme générateur $g(x)$ admet la suite :

$$\alpha_r, \alpha_{r+1}, \ldots, \alpha_{r+d-2}$$

de $d-1$puissances consécutives de α comme racines c-à-d

$$g(x) = \prod_{i=r}^{r+d-2} (x - \alpha_i)$$

Si $p_i(x)$ est le polynôme minimale de α^i sur $\mathbb{F}$, donc le polynôme générateur $g(x)$ du code BCH est :

$$g(x) = ppcm\left(p_r(x), p_{r+1}(x), ..., p_{r+d-2}(x)\right)$$

Théorème 22

Avec les données précédentes on a : $d_{\min} \geq d$(où $d_{\min}$ est la distance minimal de C).

Définition 23

Si C est un code BCH de distance désignée d et $m = 1\,(n = q-1)$. Alors le code C est dit code Reed Solomon et en particulier

$$g(x) = \prod_{i-1}^{d-1} \left(x - \alpha^i\right)$$

1.2.4 Les codes de Reed-Solomon

Les codes de Reed-Solomon sont souvent présentés comme un cas particulier des codes BCH à coefficient dans $\mathbb{F}_q$, de lonqueur $n = q-1$ et de distance minimale la plus large possible. Ces codes ont été introduit en 1952 par Buch.

Définition 24

Soit α un élément primitif dans $\mathbb{F}_q$. Un code de Reed-Solomon, est un code BCH au sens strict sur $\mathbb{F}_q$ de longueur $n = q - 1$ et son polynôme générateur admet comme racines :

$$\alpha, \alpha^2, ..., \alpha^{d-1}$$

Et comme le polynôme minimum de α^j dans $\mathbb{F}_q$ est $x - \alpha^j$ alors :

$$g(x) = (x - \alpha)\left(x - \alpha^2\right)...\left(x - \alpha^{d-1}\right).$$

1.2.5 Les codes de Goppa

En 1970, Goppa a décrit de manière différente une sous classe de codes linéaires, non nécessairement cycliques, qui présente des propriétés très importantes.

Définition 25

Soit$g(x)$ un polynôme dans $\mathbb{F}_{q^m}[x]$ de degré t, $1 \leq t \leq n$, et soit $L = \{\gamma_0, \gamma_1, ..., \gamma_n\}$, un ensemble de t éléments distincts de $\mathbb{F}_{q^m}$ tels que $g(\gamma_i) \neq 0$ pour $1 \leq i \leq n$.

Un code de Goppa, noté $\Gamma(L, g)$, associé a $g(x)$ dit polynôme de Goppa, est l'ensemble des vecteurs $c = (c_0, c_1, ..., c_{n-1})$ de $\mathbb{F}_q^n$ qui vérifient la relation suivante dant l'anneau des polynômes à coefficients dans $\mathbb{F}_{q^m}$, $\left(\mathbb{F}_{q^m}[x]\right)$:

$$\sum_{i=0}^{n-1} c_i g(\gamma_i)^{-1} \frac{g(x) - g(\gamma_i)}{x - \gamma_i} = 0$$

Remarque 26

Si on pose : $g(x) = x^{d-1}$ et $L = \{\alpha^{-1} : 1 \leq i \leq n\}$, où α est la racine $n^{ième}$ de l'unité dans $\mathbb{F}_{q^m}$, alors $\Gamma(L, g)$ est le code BCH au sens strict défini sur $\mathbb{F}_q$, de longueur n est de distance apparente d.

Lemme 27

Soit $\Gamma(L, g)$ un code de Goppa sur $\mathbb{F}_{q,}$ tel que $L = \{\gamma_0, \gamma_1, ..., \gamma_n\} \subseteq \mathbb{F}_{q,^m}$.

$(c_0, c_1, ..., c_{n-1}) \in \Gamma(L, g)$ *est un mot code si selement si on a :*

$$\sum_{i=0}^{n-1} \frac{c_i}{x - \gamma_i} \equiv 0.$$

Chapitre 2

Codes convolutionnels

Les codes convolutionnels constituent l'une des principales familles de codes correcteurs. De même que les code en blocs, les codes convolutionnels peuvent être utilisés soit à la détection des erreurs soit à leur correction. Dans la majorité des cas, la répétition des messages où l'on a décelé des erreurs se faisant par blocs, l'utilisation des codes en blocs est recommandée à la détection des erreurs seulement.

Ce chapitre est composé de trois sections. Dans la première on donne quelques définitions des modules (module à gauche, module à droite, sous-module). Dans la deuxième on présente les codes convolutionnels par les trois approches (l'approche de la matrice polynômiale, l'approche de la matrice scalaire, l'approche de décalage de registre), et on utilise aussi les trois représentations graphiques de ces codes de type diagramme en arbre, diagramme d'état et treillis.

2.1 Module sur un anneau

2.1.1 Module

Définition 28

On appelle module à gauche(resp. à droite) sur l'anneau $\mathbb{F}$ *ou encore* $\mathbb{F}$*-module à gauche(resp à droite), l'objet* $(V, +, \times)$ *formé d'un ensemble* V*, une loi de composition*

interne

$$\begin{array}{rcl} + & : & V \times V \longrightarrow V \\ (x,y) & \longmapsto & x+y \end{array}$$

et une loi de composition externe

$$\begin{array}{rcl} \mathbb{F} \times V & \longrightarrow & V \ (resp.V \ \times \mathbb{F} \longrightarrow V \ ) \\ (\lambda, x) & \longmapsto & \lambda x \ (resp \ (x,\lambda) \longmapsto x\lambda) \end{array}$$

que vérifient les conditions suivantes :

1. $(V,+)$ *est un groupe commutatif.*
2. $\forall \lambda, \mu \in \mathbb{F}, \forall x \in V;\ \lambda(\mu x) = (\lambda\mu)\, x \ (resp.\,(x\lambda)\,\mu = x\,(\lambda\mu))$.
3. $\forall x \in V; 1.x = x \ (resp.x.1 = x)$.
4. $\forall \lambda, \mu \in \mathbb{F}, \forall x \in V;\ (\lambda+\mu)\, x = \lambda x + \mu x \ (resp.x\,(\lambda+\mu) = x\lambda + x\mu)$.
5. $\forall \lambda \in \mathbb{F}, \forall x, y \in V;\ \lambda(x+y) = \lambda x + \lambda y \ (resp\,(x+y)\,\lambda = x\lambda + y\lambda)$.

Remarque 29

1. *Si V est un $\mathbb{F}$-module à gauche et à droite on dit que V est un $\mathbb{F}$-module.*
2. *Lorsque l'anneau $\mathbb{F}$ est un corps, V est un espace vectoriel sur $\mathbb{F}$.*

Exemple 30

Pour tout anneau $\mathbb{F}$ et tout entier $n \geq 1$, soit l'ensemble

$$\mathbb{F}^n = \mathbb{F} \times \mathbb{F} \times \cdots \times \mathbb{F} (n \ facteur)$$

en posant par définition

$$\left(\xi_1, \xi_2, \cdots, \xi_n\right) + \left(\eta_1, \eta_2, \cdots, \eta_n\right) = \left(\xi_1 + \eta_1, \xi_2 + \eta_2, \cdots, \xi_n + \eta_n\right)$$

$$\lambda \cdot \left(\xi_1, \xi_2, \cdots, \xi_n\right) = \left(\lambda\xi_1, \lambda\xi_2, \cdots, \lambda\xi_n\right)$$

$\mathbb{F}^n$ *est un module à gauche sur* $\mathbb{F}$.

On peut vérifier aussi que $\mathbb{F}^n$ *comme un* $\mathbb{F}$*-module à droite ; il suffit pour cela de définir l'addition dans* $\mathbb{F}^n$ *comme ci-dessus, et de poser*

$$\left(\xi_1, \xi_2, \cdots, \xi_n\right) \cdot \lambda = \left(\xi_1\lambda, \xi_2\lambda, \cdots, \xi_n\lambda\right)$$

Exemple 31

Pour tout anneau $\mathbb{F}[z]$ *et tout entier* $n \geq 1$*, soit l'ensemble*

$$\mathbb{F}[z]^n = \mathbb{F}[z] \times \mathbb{F}[z] \times \cdots \times \mathbb{F}[z] \,(n \text{ facteur})$$

en posant par définition

$$\begin{aligned} \left(\xi_1(z), \cdots, \xi_n(z)\right) + \left(\eta_1(z), \cdots, \eta_n(z)\right) &= \left(\xi_1(z) + \eta_1(z), \cdots, \xi_n(z) + \eta_n(z)\right) \\ &= \left(\left(\xi_1 + \eta_1\right)(z), \cdots, \left(\xi_n + \eta_n\right)(z)\right) \end{aligned}$$

$$\lambda(z) \cdot \left(\xi_1(z), \xi_2(z), \cdots, \xi_n(z)\right) = \left(\lambda(z)\,\xi_1(z), \lambda(z)\,\xi_2(z), \cdots, \lambda(z)\,\xi_n(z)\right)$$

$\mathbb{F}[z]^n$*est un module à gauche sur* $\mathbb{F}[z]$*.On peut vérifier aussi que* $\mathbb{F}[z]^n$ *comme un* $\mathbb{F}[z]$*-module à droite*

$$\left(\xi_1(z), \xi_2(z), \cdots, \xi_n(z)\right) \cdot \lambda(z) = \left(\xi_1(z)\,\lambda, \xi_2(z)\,\lambda(z), \cdots, \xi_n(z)\,\lambda(z)\right)$$

2.1.2 Sous modules

Définition 32

1. *Soit* V *un* $\mathbb{F}-$*module à gauche (resp. à droite) .On appelle sous- moduleà gauche (resp. à droite) de* V *toute partie* $\widetilde{V}$ *de* V *vérifiant.*
2. $\widetilde{V}$ *est un sous groupe deV.*

3. $\forall \lambda \in \mathbb{F}, \forall x \in \widetilde{V}$ *;* $\lambda x \in \widetilde{V}$ $\left(\textit{resp. } x\lambda \in \widetilde{V}\right)$

Proposition 33

$$\widetilde{V} \textit{ sous-module} \iff \widetilde{V} \neq \phi \textit{ et } \lambda x + \mu y \in \widetilde{V}; \forall \lambda, \mu \in \mathbb{F},\ x, y \in \widetilde{V}$$

Proposition 34 [2]

Soient V *un sous- module de* $\mathbb{F}[z]^n$ *engendré par* $B = \left\{v^{(1)}, v^{(2)}, \cdots, v^{(r)}\right\}$ *et*

$$M = \begin{bmatrix} v^{(1)} \\ v^{(2)} \\ \vdots \\ v^{(r)} \end{bmatrix} \in \mathbb{F}[z]^{r \times n}$$

Alors les propositions suivantes sont équivalantes

1. V *est une somme directe dans* $\mathbb{F}[z]^n$ $\left(ie\ \exists \widetilde{V} \in \mathbb{F}[z]^n \textit{ tel que} V \oplus \widetilde{V} = \mathbb{F}[z]^n\right)$.
2. *Toute base de* V *peut -être complétée en une base de* $\mathbb{F}[z]^n$
3. *La forme de Smith de* M *est donnée par* $\begin{pmatrix} I_k & 0 \\ 0 & 0 \end{pmatrix}$ *où* $k = rang\,(M)$
4. *Si* $\left\{v^{(1)}, v^{(2)}, \cdots, v^{(r)}\right\}$ *est une base de* V *alors* M *est inversible à droite sur* $\mathbb{F}[z]$
5. $\forall v \in \mathbb{F}[z]^n$, $\forall \lambda \in \mathbb{F}[z] \setminus \{0\} : \lambda v \in V \Longrightarrow v \in V$
6. $\exists N \in \mathbb{F}[z]^{n \times l}$ *tel que*

$$V = \ker N = \{v \in \mathbb{F}[z]^n / v \cdot N = 0\}$$

7. *Pour tout sous module* $W \in \mathbb{F}[z]^n$ *de même rang que* V *; si* $V \subseteq W \Longrightarrow V = W$.

Proposition 35 [2]

Soit V *un sous module de* $\mathbb{F}[z]^n$.

1. *V possède une base finie et toutes les bases de V possèdent la même longueur, dite rang de V.*

2. *Si $v^{(1)}, v^{(2)}, \cdots, v^{(r)} \in \mathbb{F}[z]^n$ est une partie génératrice de V, alors*

$$V = \mathrm{Im}(M) = \{uM \ / u \in \mathbb{F}[z]^n\}$$

où

$$M := \begin{bmatrix} v^{(1)} \\ v^{(2)} \\ \vdots \\ v^{(r)} \end{bmatrix} \in \mathbb{F}[z]^{r \times n}$$

M est dite matrice génératrice de V.

3. *Soit $P \in \mathbb{F}[z]^{r \times r}$, alors*

$$V = \mathrm{Im}(PM) \iff P \text{ est inversible .}$$

Définition 36

Soit V un $\mathbb{F}[z]$ sous module du module $\mathbb{F}[z]^n$, alors

•*V est dit non catastrophique si*

$$\forall v \in \mathbb{F}[z]^n, \forall \lambda \in \mathbb{F}[z] \,/ z\, \mathbb{F}[z]\,; \lambda v \in V \Longrightarrow v \in V$$

•*V est dit sans delai(delay-free) si*

$$\forall v \in \mathbb{F}[z]^n \ \text{ et } \lambda = z : z\ v \in V \Longrightarrow v \in V$$

2.1.3 Autre structure de $\mathbb{F}[z]^n$

Soit

$$\mathbb{F}[z]^n = \{v = (v_0, v_1, ..., v_{n-1}) / v_i \in \mathbb{F}[z]\}$$

$$\begin{aligned}
v &= (v_0, v_1, ..., v_{n-1}) \\
v &= \left(\sum_{\nu\geq 0} v_0^{(\nu)} z^\nu, \sum_{\nu\geq 0} v_1^{(\nu)} z^\nu, ..., \sum_{\nu\geq 0} v_{n-1}^{(\nu)} z^\nu\right) \\
&= \left(v_0^{(0)} + v_0^{(1)} z + ..., v_1^{(0)} + v_1^{(1)} z + ..., v_{n-1}^{(0)} v_{n-1}^{(1)} + ...\right) \\
&= \left(v_0^{(0)}, v_1^{(0)}, ..., v_{n-1}^{(0)}\right) + \left(v_0^{(1)} z, v_1^{(1)} z, ..., v_{n-1}^{(1)} z\right) + ... \\
&: = \left(v_0^{(0)}, v_1^{(0)}, ..., v_{n-1}^{(0)}\right) + z\left(v_0^{(1)}, v_1^{(1)}, ..., v_{n-1}^{(1)}\right) + ... \\
&= \sum_{\nu\geq 1} z^\nu v^{(\nu)}
\end{aligned}$$

Alors

$$\mathbb{F}[z]^n = \left\{ v = \sum_{\nu\geq 1} z^\nu v^{(\nu)} / v_\nu = \left(v_0^{(\nu)}, v_1^{(\nu)}, ..., v_{n-1}^{(\nu)}\right) \in \mathbb{F}^n \right\} \tag{2.1}$$

Proposition 37

$\mathbb{F}[z]^n$ possède une structure $\mathbb{F}[z]$-module à gauche.

Preuve

pour $v \in \mathbb{F}[z]^n$, $v = (v_0, v_1, ..., v_{n-1})$ / $v_i \in \mathbb{F}[z]$

$u \in \mathbb{F}[z]^n$, $u = (u_0, u_1, ..., u_{n-1})$ / $u_i \in \mathbb{F}[z]$

$$v_i = \sum_{j=0}^{N} z^j v_i^{(j)}, u_i = \sum_{j=0}^{N'} z^j u_i^{(j)} \tag{2.2}$$

On a :

$$u + v = (u_0 + v_0, ..., u_{n-1} + v_{n-1})$$

avec

$$(u+v)_i = \sum_{\nu \geq 0} z^\nu \, (u+v)_i^{(\nu)} \;\; / \;\; (u+v)_i^{(\nu)} = u_i^{(\nu)} + v_i^{(\nu)}$$

ce qui implique pour tout

$$\alpha(z) = \sum_{\nu \geq 0} z^\nu \alpha^{(\nu)} \in \mathbb{F}[z].$$

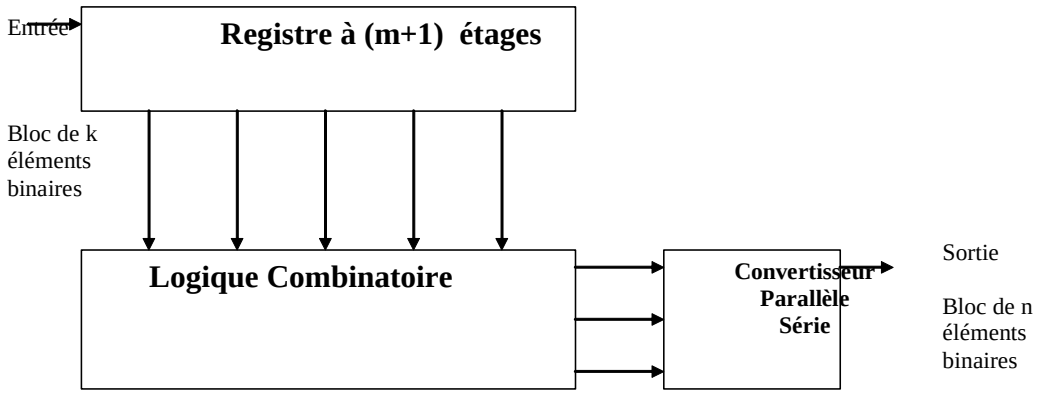
$$\alpha(z)\, u = (\alpha(z)\, u_0, \alpha(z)\, u_1, ..., \alpha(z)\, u_{n-1})$$

où $\alpha(z)\, u_i$ est le produit dans $\mathbb{F}[z]$ donc $\alpha u \in \mathbb{F}[z]^n$. ■

2.2 Les codes convolutionnels et leurs propriétés

Les deux classes les plus importantes des codes utilisés dans la pratique sont les codes en blocs et les codes convolutionnels. Les deux classes jouent un rôle également important dans la pratique en matière de technologie. D'après le premier chapitre on sait que le code en bloc $C(n,k)$ est caractérisé par une $k \times n$ matrice génératrice $G = (g_{ij})$ dans $\mathbb{F}$, un (n,k) code convolutionnel (CC) est également caractérisé par $k \times n$ matrice génératrice G.

Un codeur est constitué d'un registre à $(M+1)k$ étages qui mémorise les $(M+1)$ blocs de k éléments binaires d'information, d'une logique combinatoire qui calcule les blocs de n éléments binaires et d'un convertisseur parallèle série. La quantité $R = k/n$ est appelée rendement du code.Le principe du codage convolutif est illustré par le schéma ci-dessous.



2.3 Les approches d'un code convolutionnel

Les codes convolutionnels peuvent être présentés de différentes façons. Dans cette section on présente les codes convolutionnels par les trois approches : la matrice polynômiale, la matrice scalaire et le décalage de registre.

2.3.1 L'approche de la matrice polynômiale

Etant donné une matrice polynômiale $G = (g_{ij})$ Afin d'employer la à codeur d'information scalaire ; les bits d'information vent appliqués dans les coefficients du $k - tuples$ de polynômiaux

$I = (I_0(z); I_1(z); ...; I_{k-1}(z))$. Alors le mot code $c = (c_0(z), c_1(z), ..., c_{n-1}(z))$; qui est un n-tuple de polynômials ; est définie par : $C = \left\{ I \cdot G : I \in \mathbb{F}[z]^k \right\}$ où le point dénote la multiplication vecteur-matrice.

Définition 38

Soit $\mathbb{F}$ un corps fini, un code convolutionnel $C \subset \mathbb{F}[z]^n$ avec les paramètres (n, k, M) est un sous module de la forme $C = imG$, ou $G \in \mathbb{F}[z]^{k \times n}$ est inversible à droite

(c-à-d : $\exists \hat{G} \in \mathbb{F}_q[z]^{n\times k}$; $G\hat{G} = Id_k$). La matrice G est dite matrice génératrice du code convolutionnel.

Définition 39

Soit CC un code convolutionnel de matrice $G = (g_{ij})$.

1. *$M = \max(\deg(g_{ij}))$ est dit la mémoire de CC.*
2. *$K = M + 1$ est dite la contrainte de CC.*
3. *$R = k/n$ est dit le rendement de CC.*

Exemple 40

Soitent

$$\begin{aligned} I &= \left(I_3 z^3 + I_1 z + I_0\right) \\ G &= \left[z^2 + z \;\; z^2 + z + 1\right] \end{aligned}$$

Alors

$$\begin{aligned} M &= \max(\deg(g_{ij})) \\ &= 2 \\ K &= M + 1 \\ &= 3 \\ R &= k/n \\ &= 1/2 \end{aligned}$$

Donc

$$\begin{aligned} C &= \left\{I \cdot G : I \in \mathbb{F}[z]^k\right\} \\ &= \left(I_3 z^3 + I_1 z + I_0\right) \cdot \left[z^2 + 1 \;\; z^2 + z + 1\right] \\ &= [c_1 \;\; c_2] \end{aligned}$$

où

$$\begin{cases} c_1 = I_3 z^5 + (I_3 + I_1)\, z^3 + I_0 z^2 + I_1 z + I_0 \\ c_{2=} I_3 z^5 + I_3 z^4 + (I_3 + I_1)\, z^3 + (I_1 + I_0)\, z^2 + (I_1 + I_0)\, z + I_0 \end{cases}$$

Exemple 41

Soient

$$\begin{aligned} I &= \left(I_2 z^2 + I_1 z, I_3 z^3 + I_1 z\right) \\ G &= \begin{bmatrix} 1 & 0 & z+1 \\ 0 & 1 & z \end{bmatrix} \end{aligned}$$

Alors

$$\begin{aligned} M &= \max(\deg(g_{ij})) \\ &= 1 \\ K &= M + 1 \\ &= 2 \\ R &= k/n \\ &= 2/3 \end{aligned}$$

$$\begin{aligned} C &= \left\{ I \cdot G : I \in \mathbb{F}[z]^k \right\} \\ &= \left(I_2 z^2 + I_1 z, I_3 z^3 + I_1 z\right) \cdot \begin{bmatrix} 1 & 0 & z+1 \\ 0 & 1 & z \end{bmatrix} \\ &= \left(I_2 z^2 + I_1 z, I_3 z^3 + I_1 z, I_3 z^4 + I_2 z^3 + I_2 z^2 + I_1 z\right) \end{aligned}$$

Remarque 42

1. *Notons que les paramètres algébriques (n, k, M) ne contiennent aucune information sur les propriétés correctrices d'erreurs du code.*

2. Les codes convolutionnels de longueur n est une somme directe dans $\mathbb{F}[z]^n$

(*ie*: $\exists C' \in \mathbb{F}[z]^n$ *tel que* $C \oplus C' = \mathbb{F}[z]^n$).

2.3.2 L'approche de la matrice scalaire

Etant donné un code $CC = \left\{ I \cdot G : I \in \mathbb{F}[z]^k \right\}$ sous forme polynômiale où $G = (g_{ij})$.
Pour tout mot code $c = (c_0(z), c_1(z), ..., c_{n-1}(z))$ avec

$$\begin{aligned} c_0(z) &= c_{00} + c_{01}z + ... + c_{0M}z^{M-1} \\ c_1(z) &= c_{10} + c_{11}z + ... + c_{1M-1}z^{M-1} \\ &\vdots \\ c_{n-1}(z) &= c_{n-10} + c_{n-11}z + ... + c_{n-1M-1}z^{M-1} \end{aligned}$$

on considère les vecteurs $(c_{00}, c_{10}, ..., c_{n-10}, c_{01}, ..., c_{n-11}, ..., c_{0M}, ..., c_{n-1M})$ dans $\mathbb{F}^{M \times n}$.
Soit :

$$g_{ij}(z) = g_{ij}^{(0)}z^0 + g_{ij}^{(1)}z + ... + g_{ij}^{(M)}z^M$$

Implique que

$$G = (c_1 \ c_2 ... c_M)$$

où

$$c_1 = \begin{cases} g_{00}^{(0)} + g_{00}^{(1)} z + ... + g_{00}^{(M)} z^M \\ g_{10}^{(0)} + g_{10}^{(1)} z + ... + g_{10}^{(M)} z^M \\ . \\ . \\ . \\ g_{k-10}^{(0)} + g_{k-10}^{(1)} z + ... + g_{k-10}^{(M)} z^M \end{cases}$$

$$c_2 = \begin{cases} g_{11}^{(0)} + g_{11}^{(1)} z + ... + g_{11}^{(M)} z^M \\ g_{21}^{(0)} + g_{21}^{(1)} z + ... + g_{21}^{(M)} z^M \\ . \\ . \\ . \\ g_{k-11}^{(0)} + g_{k-11}^{(1)} z + ... + g_{k-11}^{(M)} z^M \end{cases}$$

$$\vdots$$

$$c_{_M} = \begin{cases} g_{0n-1}^{(0)} + g_{0n-1}^{(1)} z + ... + g_{0n-1}^{(M)} z^{(M)} \\ g_{1n-1}^{(0)} + g_{1n-1}^{(1)} z + ... + g_{1n-1}^{(M)} z^M \\ . \\ . \\ . \\ g_{k-1M-1}^{(0)} + g_{k-1M-1}^{(1)} z + ... + g_{k-1M-1}^{(M)} z^M \end{cases}$$

Donc

$$G = \begin{pmatrix} g_{00}^{(0)} & g_{01}^{(0)} & \cdots & g_{0M-1}^{(0)} \\ g_{10}^{(0)} & g_{11}^{(0)} & \cdots & g_{1M-1}^{(0)} \\ & & . & \\ & & . & \\ & & . & \\ g_{k-10}^{(0)} & g_{k-11}^{(0)} & \cdots & g_{k-1M-1}^{(0)} \end{pmatrix} + \begin{pmatrix} g_{00}^{(1)} & g_{01}^{(1)} & \cdots & g_{0M-1}^{(1)} \\ g_{10}^{(1)} & g_{11}^{(1)} & \cdots & g_{1M-1}^{(1)} \\ & & . & \\ & & . & \\ & & . & \\ g_{k-10}^{(1)} & g_{k-11}^{(1)} & \cdots & g_{k-1M-1}^{(1)} \end{pmatrix} z + ...$$

$$+ \begin{pmatrix} g_{00}^{(M)} & g_{01}^{(M)} & \cdots & g_{0M-1}^{(M)} \\ g_{10}^{(M)} & g_{11}^{(M)} & \cdots & g_{1M-1}^{(M)} \\ & & . & \\ & & . & \\ & & . & \\ g_{k-10}^{(M)} & g_{k-11}^{(M)} & \cdots & g_{k-1M-1}^{(M)} \end{pmatrix} z^n$$

Alors

$$G = \sum_{\upsilon \geq 0} G_\upsilon z^\upsilon$$

où

$$G_\upsilon = \begin{pmatrix} g_{00}^{(\upsilon)} & g_{01}^{(\upsilon)} & \cdots & g_{0M-1}^{(\upsilon)} \\ g_{10}^{(\upsilon)} & g_{11}^{(\upsilon)} & \cdots & g_{1M-1}^{(\upsilon)} \\ & & . & \\ & & . & \\ & & . & \\ g_{k-10}^{(\upsilon)} & g_{k-11}^{(\upsilon)} & \cdots & g_{k-1M-1}^{(\upsilon)} \end{pmatrix}$$

Donc on peut écrire une version scalaire de G comme suit :

$$G = \sum_{v \geq 0} G_v z^v$$

Remarque 43

La matrice génératrice (scalaire) a un nombre infini des lignes et des colonnes. Du fait que les polynômes des mots code peuvent avoir arbitrairement

$$G = \begin{pmatrix} G_0 & G_1 & G_2 & . & . & . & G_M & & & & \\ & G_0 & G_1 & . & . & . & G_{M-1} & G_M & & & \\ & & G_0 & . & . & . & G_{M-2} & G_{M-1} & G_M & & \\ & & & . & & & & . & . & . & \\ & & & & . & & & & . & . & . \\ & & & & & . & & & & . & . & . \end{pmatrix}$$

la matrice génératrice scalaire de CC

Exemple 44

1. *Etant donné le code convolutionnel CC de matrice polynômiale* $G = (z^3 + 1, z^2 + z + 1)$. *Sachant que* $G = (1,1) + (0,1)\, z + (0,1)\, z^2 + (1,0)\, z^3$. *Alors la matrice génératrice scalaire de CC est :*

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

Pour le message $I = 1 + z + z^3$ *(*$I = 1z^0 + 1z^1 + 0z^2 + 1z^3$*) en format polynômiale lui correspond le message en format scalaire suivant* 1101. *Et le mot code scalaire*

correspondant au mot code polynômiale $I \cdot G = (1 + z + z^2 + z^5, 1 + z^4 + z^5)$ *est* (111010000111) .

2. *Soit la matrice génératrice polynômiale d'un code convolutionnel, noté* $CC2$ *:*

$$G = \begin{pmatrix} z+1 & z^2+z+1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Alors

$$G = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} + z \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + z^2 \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Donc la matrice génératrice scalaire de CC *est :*

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

Pour un mesage sous format polynômiale $I = (z + z^2, z + z^3)$ *lui correspond le message sous format scalaire suivant :* (00111001) *.Et le mot code scalaire correspondant au mot code polynômiale* $I \cdot G = (z^5 + z^2 + z + 1, z^5 + z^4 + 1)$ *est* (111010000111) .

Un mot code d'un code convolutionnel n'a pas de longeur fixe. Cependant pour des raisons pratiques, dans la plupart des applications, il est nécéssaire d'imposer une longueur maximale fixée pour les mots code. Si pour tout $i = 0, 1, ..., k-1$ on pose $\deg[I_i(z)] \leq L - 1$, alors d'après les équations $M = \max[\deg(g_{ig})]$ et $C = I.G$, on aura

que chaque composante de mot code $c = (c_0(z), ..., c_{n-1}(z))$ est de degré $\leq M + L - 1$. Par conséquent on peut représenter le message $I = (I_0(z), ..., I_{k-1}(z))$ par L bits et le mot code c par $n(M + L)$ bits. Donc la notation sous format scalaire se fait comme suit :

$$C = I.G_L$$

où G_L est la matrice suivante :

$$\leftarrow M + L \text{ bloc de } n \rightarrow$$

$$G_L = \begin{pmatrix} G_0 & G_1 & G_2 & . & . & . & G_M & . & . & . & . \\ & G_0 & G_1 & . & . & . & . & G_M. & . & . & . \\ & & G_0 & . & . & . & . & . & .G_M & . & . \\ & & & & & & & & & & . \\ & & & & & & & & & & . \\ & & & & & & & & & . & . \\ & & & & & & .G_0 & . & . & . & G_M \end{pmatrix}$$

Avec cette représentation, une autre quantité caractérisante du code convolutionnel se définit comme :

$$R_L = \frac{kL}{n(M + L)} = R\left(1 - \frac{M}{M + L}\right) \text{ où } R = k/n$$

Exemple 45

a)*D'aprés l'exemple 2.3.1, si on pose* $L = 5$

$$G_{_5} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & & & & & & & & \\ & & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & & & & & & \\ & & & & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & & & & \\ & & & & & & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & & \\ & & & & & & & & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

b)*et si on pose* $L = 6$

$$G_{_6} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & & & & & & & & & & & & \\ & & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & & & & & & & & & & \\ & & & & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & & & & & & & & \\ & & & & & & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & & & & & & \\ & & & & & & & & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & & & & \\ & & & & & & & & & & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & & \\ & & & & & & & & & & & & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Exemple 46

a)*D'aprés l'exemple 2.3.2 et si on pose* $L = 2$

$$G_{_2} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & & & & & & & & & & \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & & & & & & & & & & \\ & & & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & & & & & & & \\ & & & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & & & & & & & \\ & & & & & & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & & & & \\ & & & & & & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & & & & \\ & & & & & & & & & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & \\ & & & & & & & & & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \\ & & & & & & & & & & & & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ & & & & & & & & & & & & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

b)*et si on pose* $L = 3$

$$G_3 = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & & & & & & & & & & & & \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & & & & & & & & & & & & \\
 & & & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & & & & & & & & & \\
 & & & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & & & & & & & & & \\
 & & & & & & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & & & & & & \\
 & & & & & & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & & & & & & \\
 & & & & & & & & & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & & & \\
 & & & & & & & & & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & & & \\
 & & & & & & & & & & & & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
 & & & & & & & & & & & & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0
\end{pmatrix}$$

2.3.3 L'approche du décalage de registre

Etant donné un code $CC = \left\{ I \cdot G : I \in \mathbb{F}[z]^k \right\}$ sous forme polynômiale où $G = (g_{ij})$. Pour tout mot code $c = (c_0(z), c_1(z), ..., c_{n-1}(z))$ avec

$$\begin{aligned}
c_0(z) &= c_{00} + c_{01}z + ... + c_{0M}z^{M-1} \\
c_1(z) &= c_{10} + c_{11}z + ... + c_{1M-1}z^{M-1} \\
&\vdots \\
c_{n-1}(z) &= c_{n-10} + c_{n-11}z + ... + c_{n-1M-1}z^{M-1}
\end{aligned}$$

on a d'une part

$$\begin{aligned} c_j(z) &= \sum_{l=0}^{k-1} I_l(z)\, g_{lj}(z) \\ &= \sum_{l=0}^{k-1} \left[\sum_{p=0}^{\deg I} I_{lp} z^p\right] \left[\sum_{q=0}^{M} a_{lj}^{(q)} z^q\right] \\ &= \sum_{l=0}^{k-1} \left(\sum_{r=0}^{\deg I+M} \left(\sum_{p+q=r}^{M} I_{lp} z^p a_{lj}^{(q)} z^q\right)\right) \\ &= \sum_{l=0}^{k-1} \left(\sum_{r=0}^{\deg I+M} \left(\sum_{p+q=r}^{M} I_{lp} a_{lj}^{(q)}\right)\right) z^r \end{aligned}$$

et d'autre part

$$c_j(z) = c_{j0} + c_{j1} z + ... + c_{jM-1} z^{M-1}$$

Alors

$$\begin{aligned} c_{jr} &= \sum_{l=0}^{k-1} \left(\sum_{p+q=r}^{M} I_{lp}\ a_{lj}^{(q)}\right) \\ &= \sum_{l=0}^{k-1} \left(\sum_{p=0}^{\deg I} I_{lp}\ a_{lj}^{(r-p)}\right) \\ &= \sum_{p=0}^{\deg I} \left(\sum_{l=0}^{k-1} I_{lp} a_{lj}^{(r-p)}\right) \end{aligned}$$

Pour ce code il s'agit de calculer la redondance à partir du bloc d'information courant de taille L et des M blocs précédents.

Les n bits en sortie sont calculés par une combinaison linéaire entre k bits entrés et les M blocs précédents.

Le codeur contient le registre à décalage qui correspond chacun à une entrée.

Le codage se fait avec des registres à décalage exclusivement.

Exemple 47

Pour pour un code convolutionnel $CC1$ on a $G = [z^2 + 1, z^2 + z + 1]$

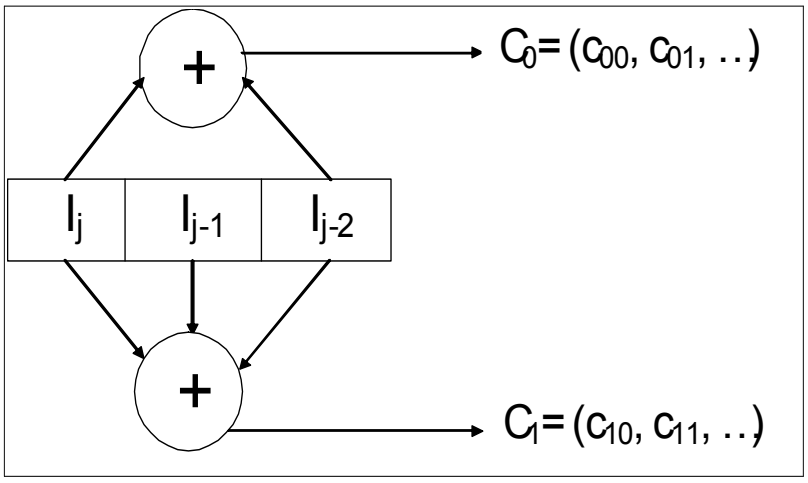
$$\begin{aligned} \bullet c_0(z) &= c_{00} + c_{01}z + c_{02}z^2 + ... \\ &= \left(z^2 + 1\right)\left(I_0 + I_1 z + I_2 z^2 + ...\right) \\ &= \left(z^2 + 1\right) I(z) \end{aligned}$$

$$\begin{aligned} \bullet c_1(z) &= c_{10} + c_{11}z + c_{12}z^2 + ... \\ &= \left(z^2 + z + 1\right)\left(I_0 + I_1 z + I_2 z^2 + ...\right) \\ &= \left(z^2 + z + 1\right) I(z) \end{aligned}$$

Dans cet exemple, on a un élément binaire d'entrée correspondant à deux éléments binaires de sortie qui sont déterminés par les équations suivantes :

$$\begin{cases} c_{0j} = I_j + I_{j-2} \\ c_{1j} = I_j + I_{j-1} + I_{j-2} \end{cases}$$

Alors on a le circuit tel que $j = 0, 1, ...$



2.4 Représentation graphique des codes convolutionnels

En pratique, un codeur convolutionnel, peut être considéré comme une machine d'état, et par conséquent il peut être représenté par un diagramme d'état, une structure en arbre ou une représentation en treillis.

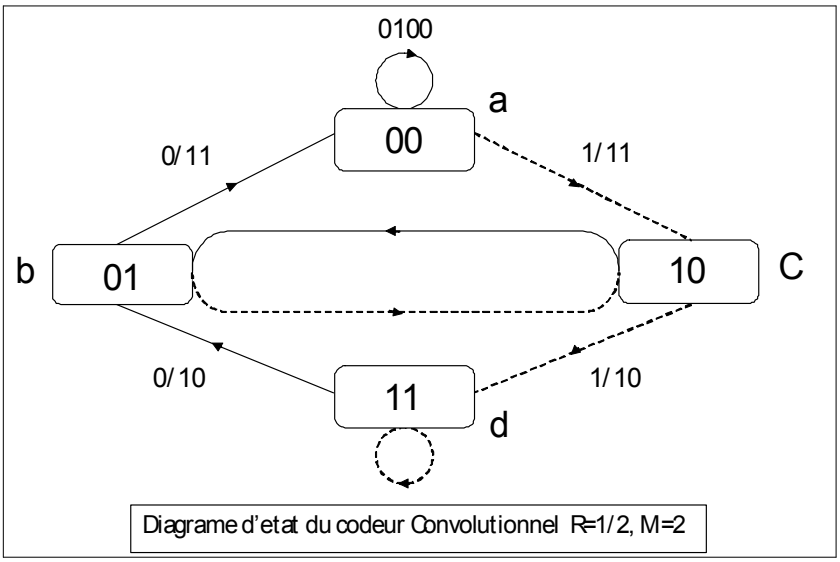
Les représentations polynômiale ou matricielles des codes convolutionnels ne sont pas réellement adaptée au décodage. Aussi pour réaliser les décodeurs, on utilise des représentations graphiques de ces codes. Notons que la représentation en treillis est très efficace pour le décodage car elle est parfaitement adaptée aux algorithmes.

Etant donné un $CC\ (n, k, M)$ de G matrice génératrice.

2.4.1 Diagramme d'état

Le diagramme d'état représente les transitions possibles entre les états. Les valeurs des sorties du codeur sont indiquées sur chacune des transitions.

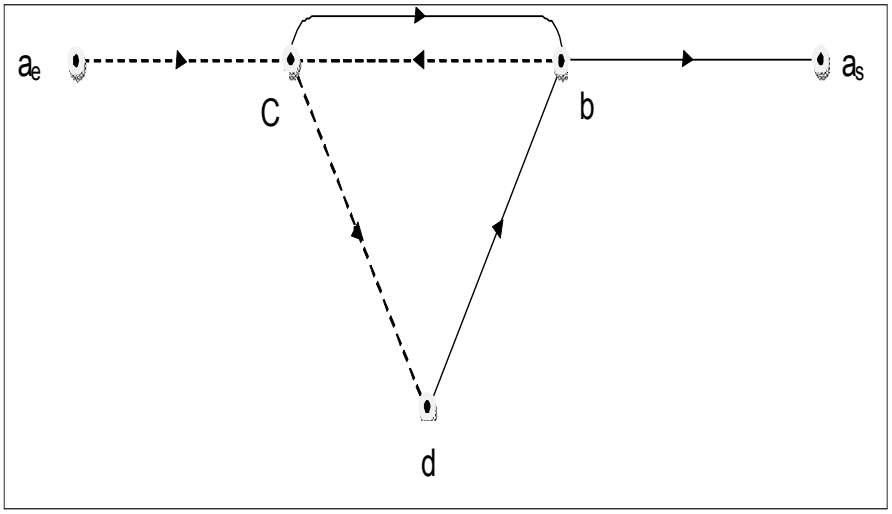
Tous les états internes possibles du codeur sont représentés par des noeuds. Les branches entre les états représentés en pointillés et en traits pleins correspondent respectivement à la présence d'un bit d'information égale à 0 et 1, chacune de ces branches fournit un couple de bits pour la sortie du codeur.Ainsi dans le schéma suivant :



Exemple 48

Etant donnée un codes convolutionnel 101010000111 *pour* $\mathbb{F} = \mathbb{F}_2$, $R = \frac{1}{2}$ *et* $M = 2$ *il existe* $2^M = 4$ *états internes possibles.*

1. *Par exemple on prend* a_e *et* a_s *le noeud d'entrée et de sortie pour* $I = 110110$



bit d'entrée	état du registre	contenu du registre	bits de sortie
1	00	100	10
1	10	110	10
0	11	011	10
1	01	101	00
1	10	010	01
0	01	001	11

Exemple 49 *Etant donnée un CC* $(n,1)$ *un code convolutionnel pour*

$$\begin{aligned} q &= 2 \\ G &= \left[z^3+z+1, z^2+1\right] \\ M &= 3 \\ k &= 4 \\ R &= \frac{1}{2} \end{aligned}$$

Donc

$$\begin{aligned} C &= I \cdot G \\ &= \left(c_0(z), c_1(z)\right) \\ &= \left(I_0 + I_1 z + I_2 z^2 + ...\right)\left(z^3+z+1, z^3+1\right) \end{aligned}$$

Où

$$\Longrightarrow \begin{cases} c_0(z) = I_0 + (I_0+I_1)z + (I_1+I_2)z^2 + (I_0+I_2+I_3)z^3 + \dots \\ c_1(z) = I_0 z^2 + (I_0+I_1)z^3 + (I_1+I_2)z^4 + \dots \end{cases}$$

Alors :

$$\begin{cases} c_j = I_j + I_{j-2} + I_{j-3} \\ c_{1j} = I_j + i_{j-1} \end{cases}$$

$$(I_{j-1}, I_{j-2}, I_{j-3}) \rightarrow (I_j, I_{j-1}, I_{j-3})$$

$$Pour\ I = z^5 + z^3 + z^2 + 1 \Rightarrow I = (101101)$$

$$t = 1 \qquad I_j = 1 \Rightarrow (0,0,0) \rightarrow (0,1,0)$$

$$t = 2 \qquad I_j = 0 \Rightarrow (1,0,0) \rightarrow (0,1,0)$$

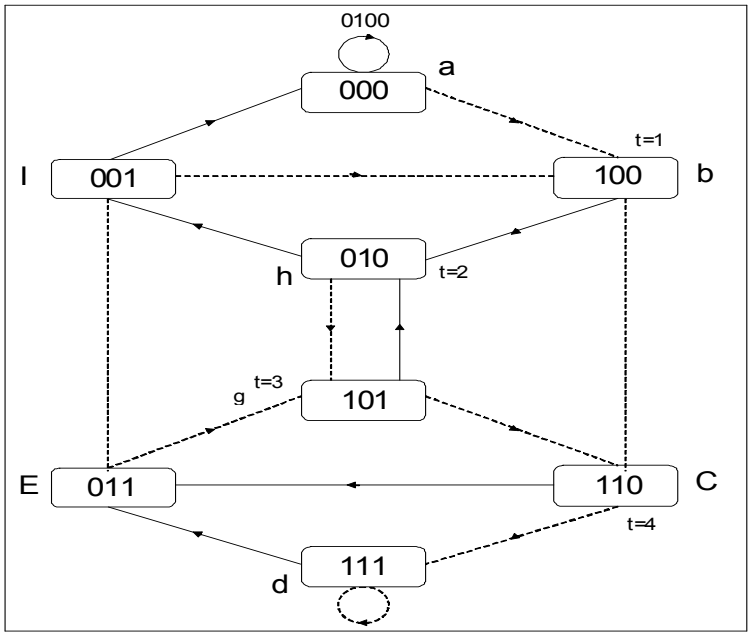
$$t = 3 \qquad I_j = 1 \Rightarrow (0,1,0) \rightarrow (1,0,1)$$

$$t = 4 \qquad I_j = 1 \Rightarrow (1,0,1) \rightarrow (1,1,0)$$

$$t = 5 \qquad I_j = 0 \Rightarrow (1,1,0) \rightarrow (0,1,1)$$

$$t = 6 \qquad I_j = 1 \Rightarrow (0,1,1) \rightarrow (1,0,1)$$

on a le diagramme d'état suivant :



2.4.2 Représentation en treillis

Pour faciliter l'algorithme de décodage, la représentation la plus courante du codage est la représentation en treillis.

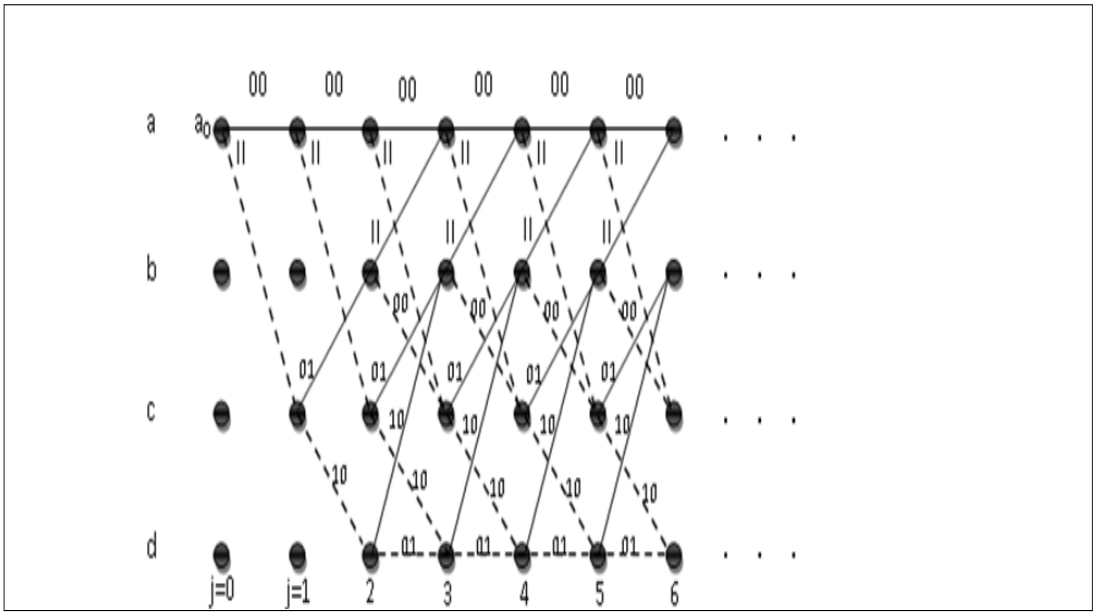
L'état du codeur à l'instant j est représenté par l'état $\{I_{j-1}, I_{j-2}, ..., I_{j-M-1}\}$, chaque branche est indiquée par les bits qui se présentent en entrée et en sortie du codeur e/s.

Chaque mot code est associé à un chemin unique du treillis qu'on appelle séquence d'état.

Un chemin complet commence à l'état a_0 et se termine à l'état a_s.

Il y en a 2^{M-1} s'il ya une entrée $2^{(M-1)k}$ s'il y a k entrée, les branches représentent les différentes transitions possibles d'un noeud à un autre corps de l'arrivée d'un bit d'entrée.

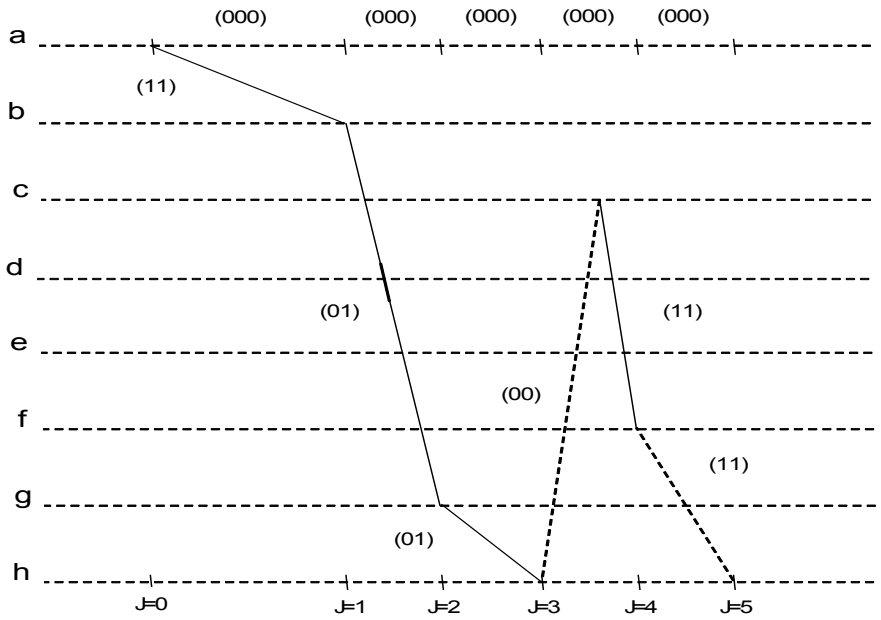
Voici le treillis de code président : les états sont 00, 01, 10, 11.



Exemple 50

Posons $I = z^5 + z^3 + z^2 + 1\,(101101)$ et $G = [z^3 + z + 1, z^3 + 1]$ .On a

$$\begin{cases} c_{0j} = I_j + I_{j-1} + I_{j-2} \\ c_{1j} = I_j + I_{j-1} \end{cases}$$



Alors $c = (110101001111)$

Remarque 51

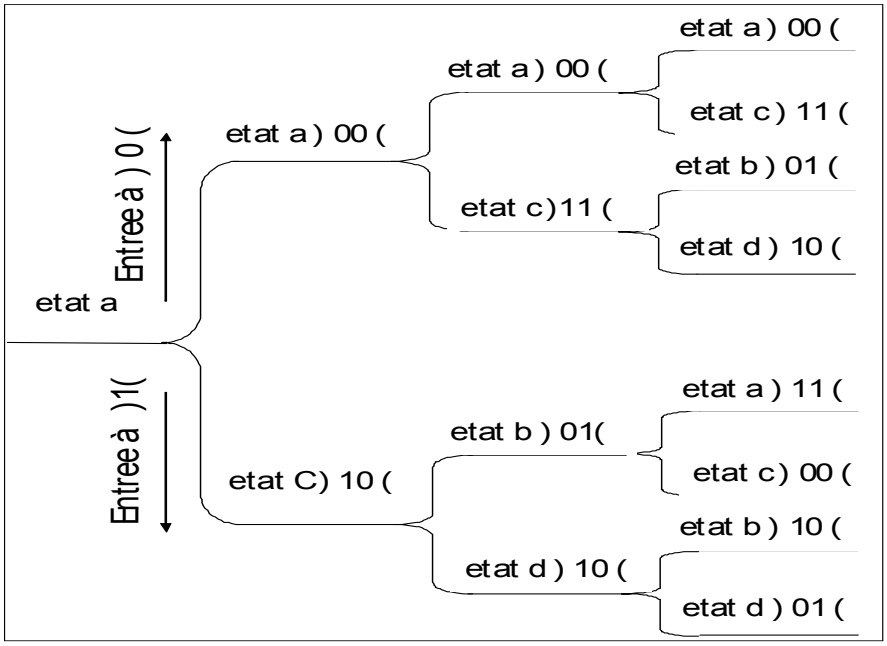
Ces représentations en treillis sont périodiques et après $(M-1)$ *décalages, le mot du treillis se répète.*

2.4.3 Représentation en arbre

Un arbre est une structure partant d'un point appelé racine. Il se compose d'arcs et de noeuds. Les arcs sont des traits verticaux dont le sens est déterminé par le bit d'information. Par convention le 0 est représenté par un arc montant et le 1 par un arc descendant.

Pour une séquence d'information fournie à l'entrée du codeur la séquence associée en

sortie du codeur correspond à un chemin de l'arbre qui est constitué d'une succession de branches.

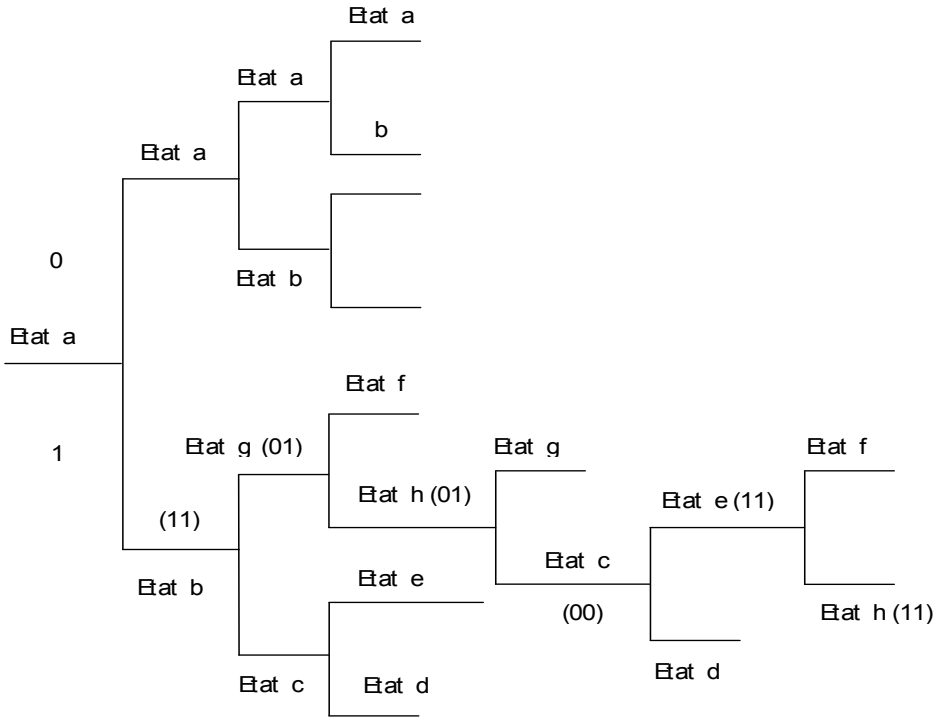


Exemple 52

Posons $I = z^5 + z^3 + z^2 + 1\,(101101)$ *et* $G = [z^3 + z + 1, z^3 + 1]$.

On a

$$\begin{cases} c_{0j} = I_j + I_{j-1} + I_{j-2} \\ c_{1j} = I_j + I_{j-1} \end{cases}$$



Alors $c = (110101001111)$

Chapitre 3

Les codes convolutionnels cycliques

3.1 L'algèbre de Piret et la notion de la cyclicité

Dans l'étude de la cyclicité des codes linéaires en bloc, ces derniers sont représentés sous forme d'idéaux de l'anneau $A := \mathbb{F}[x] \,/\, \langle x^n - 1 \rangle$ à l'aide de l'isomorphisme

$$\begin{aligned} P &: \mathbb{F}^n \longrightarrow A \\ v &= (v_0, v_1, ..., v_{n-1}) \longmapsto P(v) = \sum_{i=0}^{n-1} v_i x^i \end{aligned}$$

Pour le $\mathbb{F}[z]$-module $\mathbb{F}[z]^n$, considérons l'ensemble

$$A[z] = \left\{ \sum_{\nu \geq 0} a^{(\nu)} z^\nu / \; a^{(\nu)} \in A \right\} \tag{3.1}$$

3.1.1 Structure de $A[z]$

L'ensemble possède une structure de $\mathbb{F}[z]$-module à droite triviale définie par :

$$\begin{aligned}
\sum_{\nu\geq 0} a^{(\nu)} z^{\nu} + \sum_{\nu\geq 0} b^{(\nu)} z^{\nu} &= \sum_{\nu\geq 0} \left(a^{(\nu)} + b^{(\nu)}\right) z^{\nu} \\
\alpha(z) \sum_{\nu\geq 0} a^{(\nu)} z^{\nu} &= \left(\sum_{i\geq 0} \alpha_i z^i\right) \left(\sum_{\nu\geq 0} a^{(\nu)} z^{\nu}\right) \\
&= \sum_{\lambda\geq 0} \left[\sum_{i=0}^{\lambda} \alpha_i \cdot a^{(\lambda-i)}\right] z^{\lambda}
\end{aligned}$$

Aussi $A[z]$ possède d'autres structures utiles pour l'étude de certains codes convolutionnels dits cycliques au sens de Piret. Ainsi pour tout élément

$\sum_{\nu=0}^{k} a^{(\nu)} z^{\nu} = a^{(0)} + a^{(1)} z + ... + a^{(k)} z^k$ de $A[z] = \left\{ \sum_{\nu\geq 0} a^{(\nu)} z^{\nu} / \ a^{(\nu)} \in A \right\}$ utilisons la notation suivante :

$$\begin{aligned}
\sum_{\nu=0}^{k} a^{(\nu)} z^{\nu} &= a^{(0)} + a^{(1)} z + ... + a^{(k)} z^k, \ a^{(i)} \in A \\
&= \left(a_0^{(0)} + a_0^{(1)} x + ... + a_0^{(n-1)} x^{n-1}\right) \\
&\quad + ... + \left(a_0^{(0)} + a_0^{(1)} x + ... + a_0^{(k)} x^k\right) z^k \\
&= \left(a_0^{(0)} + a_0^{(1)} x + ... + a_0^{(k)} x^k\right) \\
&\quad + ... + a_k^{(0)} z^k + \left(a_k^{(1)} x\right) z^k + ... + \left(a_k^{(n-1)} x^{n-1}\right) z^k \\
&\vdots \quad = \left(a_0^{(0)} + a_0^{(1)} x + ... + a_0^{(k)} x^k\right) + ... + z^k \left(a_0^{(0)} + a_0^{(1)} x + ... + a_0^{(k)} x^k\right) \\
&= \sum_{\nu\geq 0}^{k} z^{\nu} a^{(\nu)}
\end{aligned}$$

Pour $\sum_{\nu=0}^{k} a^{(\nu)} z^{\nu} = a^{(0)} + a^{(1)} z + ... + a^{(k)} z^k$, $\sum_{\nu=0}^{k} b^{(\nu)} z^{\nu} = b^{(0)} + b^{(1)} z + ... + b^{(k)} z^k$ dans $A[z]$ et $\alpha(z) = \sum_{i\geq 0} \alpha_i z^i$, $\beta(z) = \sum_{i\geq 0} \beta_i z^i$ dans $\mathbb{F}[z]$ on a

$$\begin{aligned}
\sum_{\nu=0}^{k} a^{(\nu)} z^{\nu} + \sum_{\nu=0}^{k} b^{(\nu)} z^{\nu} &= \sum_{\nu\geq 0} \left(a^{(\nu)} + b^{(\nu)}\right) z^{\nu} \\
&= \left[\left(a_0^{(0)} + b_0^{(0)}\right) + ... + \left(a_0^{(n-1)} + b_0^{(n-1)}\right) x^{n-1}\right] \\
&\quad +... + \left[\left(a_1^{(0)} + b_1^{(0)}\right) + ... + \left(a_1^{(n-1)} + b_1^{(n-1)}\right) x^{n-1}\right] z \\
&\quad +... + \left[\left(a_k^{(0)} + b_k^{(0)}\right) + ... + \left(a_k^{(n-1)} + b_k^{(n-1)}\right) x^{n-1}\right] z^k \\
&: = \left[\left(a_0^{(0)} + b_0^{(0)}\right) + ... + \left(a_0^{(n-1)} + b_0^{(n-1)}\right) x^{n-1}\right] \\
&\quad +... + z\left[\left(a_1^{(0)} + b_1^{(0)}\right) + ... + \left(a_1^{(n-1)} + b_1^{(n-1)}\right) x^{n-1}\right] \\
&\quad +... + z^k\left[\left(a_k^{(0)} + b_k^{(0)}\right) + ... + \left(a_k^{(n-1)} + b_k^{(n-1)}\right) x^{n-1}\right]
\end{aligned}$$

et

$$\begin{aligned}
\left(\sum_{\nu\geq 0} a^{(\nu)} z^{\nu}\right) \alpha(z) &= \left(\sum_{\nu\geq 0} a^{(\nu)} z^{\nu}\right)\left(\sum_{i\geq 0} \alpha_i z^i\right) \\
&= \sum_{\lambda\geq 0}\left[\sum_{i=0}^{\lambda} \alpha_i \cdot a^{(\lambda-i)}\right] z^{\lambda} \\
&: = \sum_{\lambda\geq 0} z^{\lambda}\left[\sum_{i=0}^{\lambda} \alpha_i \cdot a^{(\lambda-i)}\right]
\end{aligned}$$

Alors ;

L'ensemble $A[z]$ muni des deux lois précedentes est un $\mathbb{F}[z]$-module à gauche car on a

$$\left(\sum_{\nu\geq 0} a^{(\nu)} z^{\nu}\right)(\alpha(z) + \beta(z)) = \left(\sum_{\nu\geq 0} a^{(\nu)} z^{\nu}\right)\alpha(z) + \left(\sum_{\nu\geq 0} a^{(\nu)} z^{\nu}\right)\beta(z)$$

$$\left(\sum_{\nu\geq 0} a^{(\nu)} z^{\nu} + \sum_{\nu\geq 0} b^{(\nu)} z^{\nu}\right)\alpha(z) = \left(\sum_{\nu\geq 0} a^{(\nu)} z^{\nu}\right)\alpha(z) + \left(\sum_{\nu\geq 0} b^{(\nu)} z^{\nu}\right)\alpha(z)$$

Soit l'application $\tilde{P} : \mathbb{F}[z]^n \longrightarrow A[z]$ définie par $\tilde{P}(v) = \sum_{\nu \geq 0} z^\nu P\left(v^{(\nu)}\right)$ pour tout $v = \sum_{\nu \geq 0} z^\nu v^{(\nu)} \in \mathbb{F}[z]^n$.

Lemme 53

L'application $\tilde{P}$ est un prolongement de P à $\mathbb{F}[z]^n$ (i.e $\tilde{P}_{\mid \mathbb{F}^n} = P$)

En effet pour tout $v = v^{(0)} \in \mathbb{F}^n \subset \mathbb{F}[z]^n$ on a :

$$\begin{aligned} \tilde{P}(v) &= P(v^{(0)}) \\ &= P(v) \end{aligned}$$

L'application $\tilde{P}$ possède les mêmes propriétés que P. Ainsi

Proposition 54 [2] [4]

L'application $\tilde{P}$ est un isomorphisme du $\mathbb{F}[z]$-modules.

Preuve

Montrons que : $\tilde{P}(\alpha v) = \alpha \tilde{P}(v) : \forall \alpha \in \mathbb{F}[z], \forall v \in \mathbb{F}[z]^n$

Pour $v = \sum_{\nu \geq 0} z^\nu v^{(\nu)}$

$$\begin{aligned} \alpha \cdot v &= \sum_{\lambda \geq 0} z^\lambda \left(\sum_{i+\nu=\lambda} \alpha_i v^\nu \right) \\ &= \sum_{\lambda \geq 0} z^\lambda \left(\sum_{i=0}^{\lambda} \alpha_i v^{(\lambda - i)} \right) \end{aligned}$$

Alors

$$\begin{aligned}\tilde{P}(\alpha \cdot v) &= \sum_{\lambda \geq 0} z^{\lambda} P\left(\sum_{i=0}^{\lambda} \alpha_i v^{(\lambda-i)}\right) \\ &= \sum_{\lambda \geq 0} z^{\lambda}\left[\sum_{i=0}^{\lambda} P\left(\alpha_i v^{(\lambda-i)}\right)\right] \\ &= \sum_{\lambda \geq 0} z^{\lambda}\left[\sum_{i=0}^{\lambda} \alpha_i P\left(v^{(\lambda-i)}\right)\right]\end{aligned}$$

car P est un homomorphisme d'anneaux.

Alors

$$\begin{aligned}\tilde{P}(\alpha v) &= \sum_{\lambda \geq 0} z^{\lambda}\left[\sum_{i=0}^{\lambda} \alpha_i \cdot P\left(v^{(\lambda-i)}\right)\right] \\ \tilde{P}(v) &= \sum_{\lambda \geq 0} z^{\lambda} P\left(v^{(\lambda)}\right) \Rightarrow \alpha \tilde{P}(v) = \sum_{\lambda \geq 0} z^{\lambda}\left[\sum_{i=0}^{\lambda} \alpha_i \cdot P\left(v^{(\lambda-i)}\right)\right]\end{aligned}$$

Donc $\tilde{P}$ est un homomorphisme de $\mathbb{F}[z]$ -module. ■

Selon la proposition suivante ; il est impératif de trouver un autre sens de la cyclicité des codes convolutionnels.

Proposition 55 [2]

Soit $C \subseteq \mathbb{F}[z]^n$ un code satisfaisant $CS \subset C$
(i.e pour tout $(v_0, v_1, ..., v_{n-1}) \in C$ on a $(v_{n-1}, v_0, ..., v_{n-2}) \in C$). Alors C est un code en bloc.

Preuve

D'aprés la suposution $CS \subset C$ où

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

Le polynôme minimal de S est donné par $x^n - 1$ (c'est à dire $S^n = 1$).

Soit $x^n - 1 = \pi_1(x) \times \pi_2(x) \times ... \times \pi_r(x)$ la factorisation de $x^n - 1$ en facteurs irréductibles. Alors on obtient la décomposition de $\mathbb{F}[z]^n$ dans $\mathbb{F}[z]$-sous-modules suivante :

$$\mathbb{F}[z]^n = \ker \pi_1(S) \oplus ... \oplus \ker \pi_r(s)$$

où chaque sous-modules $\ker \pi_i(S)$ est invariant par S.

Comme C est la somme directe on obtient :

$$C = \oplus_{i \in t} \ker \pi_i(S) \text{ où } t = \{i / \ker \pi_i(S) \cap C \neq \{0\}\}$$

Puisque $\mathbb{F}^n S = \mathbb{F}^n$, $\mathbb{F}[z]$- sous module $\ker \pi_i(S)$ est engendré par $\ker \pi_i(S) \cap \mathbb{F}^n$ qui donne directement une matrice constante. Alors la mémoire est zéro c'est à dire C est un code en bloc. ■

Ceci a amené Piret à définir une notion générale et complexe de la cyclicité pour les codes convolutionnels.

3.1.2 Cyclicité des codes convolutionnels

Définition 56

Soit C un code convolutionnel de paramètre (n, k, M). On dit que C est cyclique au sens de Piret s'il existe un entier positif m; premier avec n ; tel que pour tout $\sum_{\nu \geq 0} z^{\nu} v^{(\nu)} \in C$:

$$\sum_{\nu \geq 0} z^{\nu} P\left(v^{(\nu)}\right) \in \tilde{P}(C) \Rightarrow \sum_{\nu \geq 0} z^{\nu} \left[P\left(v^{(\nu)}\right) S^{(m^{\nu})}\right] \in \tilde{P}(C) \tag{3.2}$$

On remarque si on remplace la matrice S par la matrice unité I ; on obtient la cyclicité au sens la cyclicité des codes en bloc.

Proposition 57

Soit C un code convolutionnel cyclique (CCC).

Alors :

$$\sum_{\nu \geq 0} z^{\nu} P\left(v^{(\nu)}\right) \in \tilde{P}(C) \Rightarrow \sum_{\nu \geq 0} z^{\nu} \left[x^{(m^{\nu})} P\left(v^{(\nu)}\right)\right] \in \tilde{P}(C) \tag{3.3}$$

pour démontrer cette proposition on a besoin du lemme suivant :

Lemme 58

Pour tout $n \in \mathbb{N}^*$, on a : $P\left(v^{(\nu)} S^{N}\right) = x^{N} P\left(v^{(\nu)}\right)$

Preuve

Pour $N = 1$ on a $P\left(v^{(\nu)} S\right) = xP\left(v^{(\nu)}\right)$. Et par réccurrence sur N

$$\begin{aligned} P\left(v^{(\nu)} S^{N}\right) &= P\left(\left(v^{(\nu)} S^{N-1}\right) S\right) \\ &= xP\left(v^{(\nu)} S^{N-1}\right) \\ &= x\left(x^{N-1} P\left(v^{(\nu)}\right)\right) \\ &= x^{N} P\left(v^{(\nu)}\right) \end{aligned}$$

■

Preuve (Proposition 3.3)

D'aprés la définition (3.1) on a

$$\sum_{\nu\geq 0} z^{\nu} v^{(\nu)} \in C \Rightarrow \sum_{\nu\geq 0} z^{\nu} v^{(\nu)} S^{(m^{\nu})} \in C$$

et comme

$$P\left(v^{(\nu)} S^{N}\right) = x^{N} P\left(v^{(\nu)}\right)$$

Alors

$$\sum_{\nu\geq 0} z^{\nu} P\left(v^{(\nu)}\right) \in \tilde{P}(C) \Rightarrow \sum_{\nu\geq 0} z^{\nu} \left[x^{(m^{\nu})} P\left(v^{(\nu)}\right)\right] \in \tilde{P}(C).$$

■

La notion de Piret de la cyclicité d'un code covolutionnel à été généralisée par Roos de manière la manière suivante.

Pour tout automorphisme σ de l'anneau A on obtient une autre structure de module sur $A[z]$ notée $A[z\,;\sigma]$. Alors la cyclicité au sens de Roos est caractérisée par :

$\sum_{\nu\geq 0}^{d} z^{\nu} g_{\nu} \in \tilde{P}(C) \Rightarrow x *_{\sigma} g = \sum_{\nu\geq 0}^{d} z^{\nu} (\sigma^{\nu}(x)\, g_{\nu}) \in \tilde{P}(C)$ où $*_{\sigma}$ est la loi externe définissant le module.

Avant d'aborder cette question en détail, nous étalons tout d'abord les différentes structures de modules sur l'anneau $A[z]$. Où chaque structure est définie à l'aide d'un autormorphisme d'anneaux. Donc il est prémordial de déterminer ces automorphismes (le groupe $Aut_{\mathbb{F}}(A)$ des automorphismes de A) pour ainsi avoir des informations sur chaque structure. En effet ;

Notation 59

Notons l'ensemble des $\mathbb{F}$-automorphismes de l'anneau A par $Aut_{\mathbb{F}}(A)$.

Rappelons que $\sigma \in Aut_{\mathbb{F}}(A)$ si $\sigma : A \to A$ est une application bijéctive satisfaisant

les propriétés suivantes pour tout $a,\ b \in A$ *et pour tout* $\lambda \in \mathbb{F}$:

$$\begin{aligned} \sigma(a \cdot b) &= \sigma(a) \cdot \sigma(b) \\ \sigma(\lambda) &= \lambda \end{aligned}$$

Pour déterminer σ, il est important de connaître $\sigma(x)$ (l'image du polynôme x). Ainsi si $\sigma(x) = x$, alors σ est l'automorphisme identité.

Soit $x^n - 1 = \pi_1(x) \times ... \times \pi_r(x)$ la décomposition précédente de $x^n - 1$ dans $\mathbb{F}_q[x]$ où la caractéristique de $\mathbb{F}_q$ ne divise pas n. Réorganisant cette décomposition de telle sorte que :

$$\begin{aligned} x^n - 1 &= [\pi_1(x) \cdots \pi_{r_1}(x)] \times \left[\pi_{r_1+1}(x) \cdots \pi_{r_1+r_2}(x)\right] \\ &\quad \times ... \times \left[\pi_{r_1+...+r_{s-1}+1}(x) \cdots \pi_{r_1+r_2+...+r_s}(x)\right] \end{aligned} \tag{3.4}$$

où $\deg \pi_1(x) = ... = \deg \pi_{r_1}(x) \langle ... \langle \deg \pi_{r_1+...+r_{s-1}+1}(x) = ... = \deg \pi_{r_1+r_2+...+r_s}(x)$.

Notons que : $r_1 + ... + r_s = r$.

On peut représenter $A = \mathbb{F}[x] \ / \langle x^n - 1 \rangle$ comme étant $A := \{f(x) \in \mathbb{F}[x] : \deg f(x) < n\}$ où la multiplication est éffectuée modulo $x^n - 1$.

Pour chaque k; $1 \leq k \leq r$; soit

$$K_k := \{f(x) \in \mathbb{F}[x] : \deg f(x) < \deg \pi_k(x)\}$$

L'ensemble K_k muni de la multiplication modulo $\pi_k(x)$ est une extension finie du corps $\mathbb{F}$ de dimension $[K_k : \mathbb{F}] = \deg \pi_k(x)$ qu'on note $K_k = \mathbb{F}[x] / \langle \pi_k(x) \rangle$.

Pour tout $a \in \mathbb{F}[x]$ notons par $\rho_k(a) \in K_k$ le reste de la division de a par $\pi_k(x)$ i.e :

$$a \equiv \rho_k(a) \left[\pi_k(x)\right]$$

Ceci définit une l'application $\rho : A \to K_1 \times ... \times K_r$ donnée par :

$$a \longrightarrow [\rho_1(a), ..., \rho_r(a)]$$

Lemme 60

ρ ainsi défini est un isomorphisme de l'anneau A dans l'anneau produit $K_1 \times ... \times K_r$.

Remarque 61

1. *Le reste de la dévision de a sur les différents facteurs de $x^n - 1$ détermine l'image de a par l'isomorphisme ρ.*
2. *A l'aide de cet isomorphisme on peut identifier A avec $K_1 \times ... \times K_r$ et on écrit*

$$A = K_1 \times ... \times K_r \tag{3.5}$$

Définition 62

Pour tout k ; $k = 1, ..., r$; soit $\varepsilon^{(k)} := \rho^{-1}(0, ..., 0, 1, 0, ..., 0)$.

Posons

$$\begin{aligned} K^{(k)} &= \varepsilon^{(k)} A \\ &= \underbrace{0 \times 0 \times ... \times 0 \times K_k \times 0 \times ... \times 0 \times 0}_{r} \end{aligned} \tag{3.6}$$

$K^{(k)}$ est dit la $k^{ième}$ composante de A suivant ρ.

Proposition 63

1. *Pour tout i, j ; $i, j = 1, ..., r$;on a $\varepsilon^{(i)} \equiv \delta_{ij} [\pi_j]$*
2. *$K^{(k)}$ est un corps fini.*
3. *$K^{(k)} \cong K_k$*
4. *Deux composantes $K^{(k)}$ et $K^{(l)}$ sont isomorphes si et seulement si $\deg \pi_k = \deg \pi_l$.*

Considérons la décomposition $x^n - 1 = [\pi_1(x) \cdots \pi_{r_1}(x)] \times \left[\pi_{r_{1+1}}(x) \cdots \pi_{r_1+r_2}(x)\right] \times ... \times \left[\pi_{r_{1+...+r_{s-1}+1}}(x) \cdots \pi_{r_1+r_2+...+r_s}(x)\right]$. Définissons une relation binaire sur l'ensemble $\left\{K^{(k)} : k = 1, \ldots, r\right\}$ par :

$$K^{(k)} \sim K^{(l)} \Longleftrightarrow \deg \pi_k = \deg \pi_l$$

Lemme 64

La relation $\sim$est une relation d'équivalence.

Pour chaque $k = 1, \ldots, r$ soit $L_k \in \overline{K^{(k)}}$ la classe d'équivalence de $K^{(k)}$.

Proposition 65

L'anneau A possède la décomposition suivante :

$$\begin{aligned} A &= \underbrace{(L_1 \times ... \times L_1)}_{r_1} \times \underbrace{(L_2 \times ... \times L_2)}_{r_2} \times ... \times \underbrace{(L_s \times ... \times L_s)}_{r_s} \\ &= L_1^{r_1} \times L_2^{r_2} \times ... \times L_s^{r_s} \end{aligned} \tag{3.7}$$

cette proposition va nous permettre d'exprimer les éléments de $Aut_{\mathbb{F}}(A)$ à l'aide des éléments $G_j := Aut_{\mathbb{F}}(L_j)$.

Théorème 66

Soit $A = L_1^{r_1} \times L_2^{r_2} \times ... \times L_s^{r_s}$ la décomposition de A. Pour tout j ; $1 \leq j \leq s$ notons par $G_j := Aut_{\mathbb{F}}(L_j)$. Et soit $S_{r_1,...,r_s}$ le sous-groupe S_r de permutations de $\{1, ..., r\}$, qui laissent tous les sous ensembles suivants $\{1, ..., r_1\}, ..., \left\{\sum_{k=1}^{s-1} r_k + 1, ..., \sum_{k=1}^{s} r_k\right\}$ invariants.

Alors :

$$Aut_{\mathbb{F}}(A) = (G_1^{r_1} \times ... \times G_s^{rs}) \circ (S_{r_1 \ldots r_s}) \tag{3.8}$$

où la loi de omposition $\circ$ est définie comme suit :

pour $\alpha_j \in G_j$, $\omega \in S_{r_1,...,r_s}$ et

$$a = \left(\underbrace{a_1, ..., a_{r_1}}, \underbrace{a_{r_1+1}, ..., a_{r_1+r_2}}, ..., \underbrace{a_{r_1+...+r_s-1}, ..., a_{r_1+...+r_s}} \right) \in L_1^{r_1} \times ... \times L_s^{r_s}$$

$$((\alpha_1, ..., \alpha_r) \circ \omega)(a) = \left[\alpha_1 \left(a_{\omega(1)} \right), ..., \alpha_r \left(a_{\omega(r)} \right) \right].$$

Corollaire 67 [2]

Avec les notations de (3.5) et (3.7) posons :

$$\begin{aligned} l_1 &= 1 \\ l_2 &= r_1 + 1 \\ &\vdots \\ l_i &= r_{i-1} + ... + r_1 + 1 \text{ pour } i = 3, ..., s \end{aligned}$$

Alors :

$$|Aut_{\mathbb{F}}(A)| = (\deg \pi_{l_1})^{r_1} ... (\deg \pi_{l_s})^{r_s} \ r_1!...r_s!$$

Dans le paragraphe suivant nous exposons les notions précédentes pour les cas suivants :

Corps	n
$\mathbb{F}_2$	$\preceq 9$
$\mathbb{F}_3$	$\preceq 9$
$\mathbb{F}_4$	$\preceq 9$

Où nous donnons la factorisation de $x^n - 1$ en facteurs premiers pour les valeurs de n premier avec la caratéristique du corps de base $\mathbb{F}$, la décompositions de A, les corps L_i formant A et enfin $|Aut_{\mathbb{F}}(A)|$. Notons que pour $n = 1$; $x^n - 1$ possède un seul facteur et par conséquent la décomposition de A est triviale $A \cong \mathbb{F}_q$ et $Aut_{\mathbb{F}}(A) = Aut(\mathbb{F})$.

3.2 A et ses automorphismes

3.2.1 $\mathbf{A} = \mathbb{F}_2[x] \ / \ \langle x^n - 1 \rangle$ avec $n = 1, 3, 5, 7, 9$

Considérons le corps binaire $\mathbb{F}_2$. Il est évident de prendre pour n les entiers positifs impairs ($char\ \mathbb{F}_2 = 2$).

On a les factorisations en facteurs premiers suivantes :

n	Factorisation de $x^n - 1$
1	$x + 1$
3	$(x+1)(x^2+x+1)$
5	$(x+1)(x^4+x^3+x^2+x+1)$
7	$(x+1)(x^3+x+1)(x^3+x^2+1)$
9	$(x+1)(x^2+x+1)(x^6+x^3+1)$

où les différentes valeurs de s et les r_j sont :

n	s	r_1	r_2	r_3
1	1	1	0	0
3	2	1	1	0
5	2	1	1	0
7	2	1	2	0
9	3	1	1	1

n	$A \cong \prod K_i$
1	$\mathbb{F}_2[x] \,/\, \langle x+1 \rangle$
3	$\mathbb{F}_2[x] \,/\, \langle x+1 \rangle \times \mathbb{F}_2[x] / \langle x^2+x+1 \rangle$
5	$\mathbb{F}_2[x] \,/\, \langle x+1 \rangle \times \mathbb{F}_2[x] \,/\, \langle x^4+x^3+x^2+x+1 \rangle$
7	$\mathbb{F}_2[x] \,/\, \langle x+1 \rangle \times \mathbb{F}_2[x] / \langle x^3+x+1 \rangle \times \mathbb{F}_2[x] / \langle x^3+x^2+x+1 \rangle$
9	$\mathbb{F}_2[x] \,/\, \langle x+1 \rangle \times \mathbb{F}_2[x] \,/\, \langle x^2+x+1 \rangle \times \mathbb{F}_2[x] \,/\, \langle x^6+x^3+1 \rangle$

Notons que pour un facteur premier $p(x)$ dans la décomposition de $x^n - 1$; on a $\mathbb{F}_2[x] \,/\, \langle p(x) \rangle \cong \mathbb{F}_{2^{\deg(p(x))}}$.

Alors :

n	$A \cong L_1^{r_1} \times L_2^{r_2} \times ... \times L_s^{r_s}$
1	$\mathbb{F}_2$
3	$\mathbb{F}_2 \times \mathbb{F}_4$
5	$\mathbb{F}_2 \times \mathbb{F}_{16}$
7	$\mathbb{F}_2 \times (\mathbb{F}_8)^2$
9	$\mathbb{F}_2 \times \mathbb{F}_4 \times \mathbb{F}_{64}$

D'où :

n	$\lvert Aut_{\mathbb{F}}(A) \rvert$
1	1
3	2
5	4
7	18
9	12

Dans le tableau suivant nous donnons le nombre de copies des corps finis dans la

décomposition de A.

n	$\mathbb{F}_2$	$\mathbb{F}_4$	$\mathbb{F}_8$	$\mathbb{F}_{16}$	$\mathbb{F}_{64}$
1	1	0	0	0	0
3	1	1	0	0	0
5	1	0	0	1	0
7	1	0	2	0	0
9	1	1	0	0	1

3.2.2 $\mathbf{A} = \mathbb{F}_3[x] \ / \ \langle x^n - 1 \rangle$ avec $n = 1, 2, 4, 5, 7$

Le corps $\mathbb{F}_3$ est de caractéristique 3, on a les factorisations en facteurs premiers suivantes :

n	Factorisation de $x^n - 1$
1	$x - 1$
2	$(x-1)(x+1)$
4	$(x-1)(x+1)(x^2+1)$
5	$(x-1)(x^4+x^3+x^2+x+1)$
7	$(x-1)(x^6+x^5+x^4+x^3+x+1)$

où les différentes valeurs de s et les r_j sont :

n	s	r_1	r_2
1	1	1	0
2	1	2	0
4	2	2	1
5	2	1	1
7	2	1	1

n	$A \cong \prod K_i$
1	$\mathbb{F}_3[x]/\langle x-1\rangle$
2	$\mathbb{F}_3[x]/\langle x-1\rangle \times \mathbb{F}_3[x]/\langle x+1\rangle$
4	$\mathbb{F}_3[x]/\langle x-1\rangle \times \mathbb{F}_3[x]/\langle x+1\rangle \times \mathbb{F}_3[x]/\langle x^2+1\rangle$
5	$\mathbb{F}_3[x]/\langle x-1\rangle \times \mathbb{F}_3[x]/\langle x^4+x^3+x^2+x+1\rangle$
7	$\mathbb{F}_3[x]/\langle x-1\rangle \times$ $\mathbb{F}_3[x]/\langle x^6+x^5+x^4+x^3+x+1\rangle$
8	$\mathbb{F}_3[x]/\langle x-1\rangle \times \mathbb{F}_3[x]/\langle x+1\rangle \times$ $\mathbb{F}_3[x]/\langle x^2+1\rangle \times \mathbb{F}_3[x]/\langle x^4+1\rangle$

Pour un facteur premier $p(x)$ dans la décomposition de $x^n - 1$;

on a $\mathbb{F}_3[x]/\langle p(x)\rangle \cong \mathbb{F}_{3^{\deg(p(x))}}$.

Alors :

n	$A \cong L_1^{r_1} \times L_2^{r_2} \times ... \times L_s^{r_s}$
1	$\mathbb{F}_3$
2	$(\mathbb{F}_3)^2$
4	$(\mathbb{F}_3)^2 \times \mathbb{F}_9$
5	$\mathbb{F}_3 \times \mathbb{F}_{81}$
7	$\mathbb{F}_3 \times \mathbb{F}_{729}$
8	$(\mathbb{F}_3)^2 \times \mathbb{F}_9 \times \mathbb{F}_{81}$

D'où :

n	$\lvert Aut_{\mathbb{F}}(A)\rvert$
1	1
2	2
4	4
5	4
7	6
8	16

Le nombre de copies des différents corps finis dans la décomposition de A est :

n	$\mathbb{F}_3$	$\mathbb{F}_9$	$\mathbb{F}_{81}$	$\mathbb{F}_{729}$
1	1	0	0	0
2	2	0	0	0
4	2	1	0	0
5	1	0	1	0
7	1	0	0	1
8	2	1	1	0

3.2.3 $\mathbf{A} = \mathbb{F}_4[x] \ / \ \langle x^n - 1 \rangle$ avec $n = 1, 3, 5, 7, 9$

Le corps $\mathbb{F}_4$ est de caractéristique 4, on a les factorisations suivantes :

n	Factorisation de $x^n - 1$
1	$x + 1$
3	$(x + 1)(x + \alpha)(x + \alpha^2)$
5	$(x + 1)(x^2 + \alpha x + 1)(x^2 + \alpha^2 x + 1)$
7	$(x + 1)(x^6 + x^5 + x^4 + x^3 + x + 1)$
9	$(x + 1)(x + \alpha)(x + \alpha^2)(x^3 + \alpha)(x^3 + \alpha^2)$

où les différentes valeurs de s et les r_j sont :

n	s	r_1	r_2
1	1	1	0
3	1	3	0
5	2	1	2
7	2	1	1
9	2	3	2

n	$A \cong \prod K_i$
1	$\mathbb{F}_4[x]/\langle x + 1\rangle$
3	$\mathbb{F}_4[x]/\langle x + 1\rangle \times \mathbb{F}_4[x]/\langle x + \alpha\rangle \times \mathbb{F}_4[x]/\langle x + \alpha^2\rangle$
5	$\mathbb{F}_4[x]/\langle x + 1\rangle \times \mathbb{F}_4[x]/\langle x^2 + \alpha x + 1\rangle \times \mathbb{F}_4[x]/\langle x^2 + \alpha^2 x + 1\rangle$
7	$\mathbb{F}_4[x] \,/\, \langle x + 1\rangle \times \mathbb{F}_4[x]/\langle x^3 + x + 1\rangle \times \mathbb{F}_4[x]/\langle x^3 + x^2 + x + 1\rangle$
9	$\mathbb{F}_4[x]/\langle x + 1\rangle \times \mathbb{F}_4[x]/\langle x + \alpha\rangle \times \mathbb{F}_4[x]/\langle x + \alpha^2\rangle \times \mathbb{F}_4[x]/\langle x^3 + \alpha\rangle \times \mathbb{F}_4[x]/\langle x^3 + \alpha^2\rangle$

Pour un facteur premier $p(x)$ dans la décomposition de $x^n - 1$;
on a $\mathbb{F}_3[x] \,/\, \langle p(x)\rangle \cong \mathbb{F}_{4^{\deg(p(x))}}$.

Alors :

n	$A \cong L_1^{r_1} \times L_2^{r_2} \times ... \times L_s^{r_s}$
1	$\mathbb{F}_4$
3	$(\mathbb{F}_4)^3$
5	$\mathbb{F}_4 \times (\mathbb{F}_{16})^2$
7	$\mathbb{F}_2 \times (\mathbb{F}_8)^2$
9	$(\mathbb{F}_4)^3 \times (\mathbb{F}_{64})^2$

D'où :

n	$\lvert Aut_{\mathbb{F}}(A)\rvert$
1	1
3	6
5	8
7	6
9	108

Et le nombre de copies des différents corps finis composants A est :

n	$\mathbb{F}_4$	$\mathbb{F}_{16}$	$\mathbb{F}_8$	$\mathbb{F}_{64}$
1	1	0	2	0
3	3	0	0	0
5	1	2	0	0
7	1	0	0	0
9	3	0	0	1

Ainsi pour déterminer un élément de $Aut_{\mathbb{F}}(A)$; d'après ce qu'on a dans le théorème (3.1) ;

$Aut_{\mathbb{F}}(A) = (G_1^{r_1} \times ... \times G_s^{rs}) \circ (S_{r_1 ... r_s})$, il suffit de choisir des éléments de $G_1^{r_1}, ..., G_s^{rs}$

et une permutation de $S_{r_1 \ldots r_s}$. Pour $\left(\lambda_{i_1}, \ldots, \lambda_{i_{r_j}}\right) \in \underbrace{G_j \times \cdots \times G_j}_{r_j}$, $j = 1, \ldots, s$ (i.e $\lambda_i \in Aut_{\mathbb{F}}(L_j)$) et $(1\ 2\ \cdots\ n) = \left(\underbrace{1 \cdots\ r_1}\ \cdots\ \underbrace{\cdots r_1 + \ldots + r_s}\right) \in S_{r_1 \ldots r_s}$, notons par $\left(\underbrace{\lambda_1, \ldots, \lambda_{r_1}}, \ldots, \underbrace{\lambda_s, \ldots, \lambda_{r_s}}\right) \circ (1\ 2\ \cdots\ n)$ l'automorphisme de A. $\lambda_j \in Aut_{\mathbb{F}}(L_j)$

Dans ce qui suis nous donnons des exemples avec dans le premier on $s = 2, r_s = 1$ et dans le second $s \neq 2$ et $r_s = 2$

Exemple 68

Prenons pour $\mathbb{F}$ *le corps* $\mathbb{F}_2 = \{0, 1\}$ *et* $n = 5$, *donc* $A = \mathbb{F}_2[x]/\langle x^5 - 1\rangle$. *D'après les tableaux du premier cas on a :*

$$\begin{aligned} x^5 - 1 &= (x+1)\left(x^4 + x^3 + x^2 + x + 1\right) \\ &= \pi_1 \times \pi_2 \end{aligned}$$

où

$$\begin{aligned} \pi_1 &= x + 1 \\ \pi_2 &= x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

donc

$$\begin{aligned} s &= 2 \\ r_1 &= 1 \\ r_2 &= 1 \end{aligned}$$

et

$$\begin{aligned} K_1 &\cong \mathbb{F}_2[x]/\langle x+1\rangle \\ &\cong \mathbb{F}_2 \\ &= L_1 \\ K_2 &\cong \mathbb{F}_2[x]/\langle x^4+x^3+x^2+x+1\rangle \\ &\cong \mathbb{F}_{2^4} \\ &= L_2 \end{aligned}$$

Alors

$$\begin{aligned} |Aut_{\mathbb{F}}(A)| &= (\deg \pi_{l_1})^{r_1} ... (\deg \pi_{l_s})^{r_s} r_1!...r_s! \\ &= 1.4 \\ &= 4 \end{aligned}$$

Pour obtenir tous les automorphismes de A on combine tous les automorphismes de $\mathbb{F}_2$ *avec ceux de* $\mathbb{F}_{2^4}$*. Sachant que* $Aut(\mathbb{F}_2) = \{id\}$ *et* $Aut(\mathbb{F}_{2^4}) = \{id, \lambda_1, \lambda_2, \lambda_3\}$ *où* $\lambda_i(x) = x^{i\ +1}[x^4+x^3+x^2+x+1]$*. Et pour trouver les automorphismes de A ; on a le tableau suivant*

$\mathbb{F}_2 \times \mathbb{F}_{2^4}$	$\mathbb{F}_2[x]/\langle x+1\rangle \times \mathbb{F}_2[x]/\langle x^4+x^3+x^2+x+1\rangle$	$\mathbb{F}_2[x]/\langle x^5-1\rangle$
$(id, \lambda_0 = id)$	$[1, x]$	x
(id, λ_1)	$[1, x^2]$	x^2
(id, λ_2)	$[1, x^3]$	x^3
(id, λ_3)	$[1, x^3+x^2+x+1]$	x^4

Donc les automorphismes de A sont :

$$\begin{array}{ccc} \mathbb{F}_2[x]/\langle x+1\rangle & & \mathbb{F}_2[x]/\langle x+1\rangle \\ \times\mathbb{F}_2[x]/\langle x^4+x^3+x^2+x+1\rangle & \xrightarrow{(id,\lambda_i)} & \times\mathbb{F}_2[x]/\langle x^4+x^3+x^2+x+1\rangle \\ \rho\uparrow & & \rho^{-1}\downarrow \\ \mathbb{F}_2[x]/\langle x^5-1\rangle & \underrightarrow{\sigma_i} & \mathbb{F}_2[x]/\langle x^5-1\rangle \end{array}$$

$$\sigma_i(x) = \rho^{-1} \circ (id, \lambda_i) \circ \rho(x)$$

Ainsi

$\sigma_0(x) = \rho^{-1} \circ (id, \lambda_0) \circ \rho(x)$	$= x$
$\sigma_1(x) = \rho^{-1} \circ (id, \lambda_1) \circ \rho(x)$	$= x^2$
$\sigma_2(x) = \rho^{-1} \circ (id, \lambda_2) \circ \rho(x)$	$= x^3$
$\sigma_3(x) = \rho^{-1} \circ (id, \lambda 3) \circ \rho(x)$	$= x^4$

Exemple 69

Pour $\mathbb{F} = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ *et* $n = 5$. *Rappelons que dans* $\mathbb{F}_4$; α *satisfait* $1+\alpha+\alpha^2 = 0$.

La factorisation de $x^5 - 1$ *est :*

$$x^5 - 1 = (x+1)\left(x^2+\alpha x+1\right)\left(x^2+\alpha^2 x+1\right)$$

d'où

$$\begin{aligned} s &= 2 \\ r_1 &= 1 \\ r_2 &= 2 \end{aligned}$$

Comme $r_2 = 2$ *alors*

$$S_{r_1 r_2} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

Aussi

$$\begin{aligned} K_1 &\cong \mathbb{F}_4[x]/\langle x+1\rangle \\ &\cong \mathbb{F}_4 \\ &= L_1 \\ K_2 &\cong \mathbb{F}_4[x]/\langle x^2+\alpha x+1\rangle \\ &\cong \mathbb{F}_{16} \\ &= L_2 \\ K_3 &\cong \mathbb{F}_4[x]/\langle x^2+\alpha^2 x+1\rangle \\ &\cong \mathbb{F}_{16} \\ &= L_2 \end{aligned}$$

D'après le corrolaire (48) on a $|Aut_{\mathbb{F}_4}(A)| = 1.2^2.1!.2! = 8$.

Sachant que les deux corps K_2 *et* K_3 *sont isomorphes ; considérons l'isomorphisme* Ψ *défini par :*

$$\begin{aligned} \Psi &: \mathbb{F}_4[x]/\langle x^2+\alpha x+1\rangle \to \mathbb{F}_4[x]\langle x^2+\alpha^2 x+1\rangle \\ x &\mapsto \Psi(x) = \alpha^2 x+1 \end{aligned}$$

donc

$$\Psi^{-1}(x) = \alpha x + \alpha$$

Sachant que $Aut(\mathbb{F}_4) = \{id\}$ *et* $Aut(\mathbb{F}_{16}) = \{id, \lambda_1, \lambda_2, \lambda_3\}$
où $\lambda_i(x) = x^{i+1}[x^2+\alpha x+1]$.

Pour $\lambda, \mu \in Aut(\mathbb{F}_{16})$ et pout $\tau \in S_{r_1 r_2}$, on obtient un automorphisme de A de la manière suivante :

$$(id, \lambda, \mu) \circ \tau\,(1, x, x) = \begin{cases} ((id, \lambda, \mu)\,(1, x, x)) & si\ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \\ \left((id, \lambda, \mu)\left(1, \Psi^{-1}(x), \Psi(x)\right)\right) & si\ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \end{cases}$$

Donc les automorphismes de A sont :

$$\begin{aligned}
1.\ ((id, id, id) \circ (1,2,3))\,[1, x, x] &= (id, id, id)\,[1, x, x] \\
&= [1, x, x] \\
2.\ ((id, id, \lambda) \circ (1,2,3))\,[1, x, x] &= (id, id, \lambda)\,[1, x, x] \\
&= \left[1, x, x^4 \bmod \left(x^2 + \alpha^2 x + 1\right)\right] \\
&= \left[1, x, x + \alpha^2\right] \\
3.\ ((id, \lambda, id) \circ (1,2,3))\,[1, x, x] &= (id, id, \lambda)\left[1, x^4, x\right] \\
&= (id, id, \lambda)\left[1, x, x^4\right] \\
&= \left[1, x^4 \bmod \left(x^2 + \alpha x + 1\right), x\right] \\
4.\ ((id, \lambda, \lambda) \circ (1,2,3))\,[1, x, x] &= (id, \lambda, \lambda)\left[1, x^4, x^4\right] \\
&= \left[1, x^4 \bmod \left(x^2 + \alpha x + 1\right), x^4 \bmod \left(x^2 + \alpha^2 x + 1\right)\right] \\
&= \left[1, x + \alpha, x + \alpha^2\right] \\
5.\ ((id, id, id) \circ (1,3,2))\,[1, x, x] &= (id, id, id)\left[1, \Psi^{-1}(x), \Psi(x)\right] \\
&= (id, id, id)\left[1, \alpha x + \alpha, \alpha^2 x + 1\right] \\
&= \left[1, \alpha x + \alpha, \alpha^2 x + 1\right]
\end{aligned}$$

$$
\begin{aligned}
6.\ ((id,id,\lambda)\circ(1,3,2))\,[1,x,x] &= (id,id,\lambda)\,[1,x,x] \\
&= (id,id,\lambda)\left[1,\Psi^{-1}(x),\Psi(x)\right] \\
&= (id,id,\lambda)\left[1,\alpha x+\alpha,\alpha^2x+1\right] \\
&= \left[1,\alpha x+\alpha,\alpha^2x+\alpha^2\right] \\
7.\ ((id,\lambda,id)\circ(1,3,2))\,[1,x,x] &= (id,\lambda,id)\left[1,x^4,x\right] \\
&= (id,\lambda,id)\left[1,\Psi^{-1}(x),\Psi(x)\right] \\
&= \begin{bmatrix} 1,(\alpha x+\alpha)^4 \bmod (x^2+\alpha x+1), \\ \alpha^2x+1 \end{bmatrix} \\
&= \left[1,\alpha x+1,\alpha^2x+1\right] \\
8.\ ((id,\lambda,\lambda)\circ(1,3,2))\,[1,x,x] &= (id,\lambda,\lambda)\left[1,\Psi^{-1}(x),\Psi(x)\right] \\
&= (id,\lambda,id)\left[1,\alpha x+\alpha,\alpha^2x+1\right] \\
&= \begin{bmatrix} 1,(\alpha x+\alpha)^4 \bmod (x^2+\alpha x+1), \\ (\alpha^2x+1)^4\, mod\,(x^2+\alpha^2x+1) \end{bmatrix} \\
&= \left[1,\alpha x+1,\alpha^2x+\alpha^2\right]
\end{aligned}
$$

$\mathbb{F}_4 \times \mathbb{F}_{16}^2$	$\mathbb{F}[x]/\langle x+1\rangle \times \mathbb{F}[x]/\langle x^2+\alpha x+1\rangle \times$ $\mathbb{F}[x]/\langle x^2+\alpha^2 x+1\rangle$	$\mathbb{F}[x]/\langle x^5-1\rangle$
$(id, id, id) \circ (1,2,3)$	$[1, x, x]$	x
$(id, id, \lambda) \circ (1,2,3)$	$[1, x, x+\alpha^2]$	$\alpha x^4 + x^3 +$ $x^2 + \alpha^2 x$
$(id, \lambda, id) \circ (1,2,3)$	$[1, x+\alpha, x]$	$\alpha^2 x + x^3 +$ $x^2 + \alpha^2 x$
$(id, \lambda, \lambda) \circ (1,2,3)$	$[1, x+\alpha, x+\alpha^2]$	x^4
$(id, id, id) \circ (1,3,2)$	$[1, \alpha x+\alpha, \alpha^2 x+1]$	$x^4 + \alpha x^3 +$ $\alpha^2 x^2 + x$
$(id, id, \lambda) \circ (1,3,2)$	$[1, \alpha x+\alpha, \alpha^2 x+1]$	x^3
$(id, \lambda, id) \circ (1,3,2)$	$[1, \alpha x+1, \alpha^2 x+1]$	x^2
$(id, \lambda, \lambda) \circ (1,3,2)$	$[1, \alpha x+1, \alpha^2 x+\alpha^2]$	$x^4 + \alpha^2 x^3 +$ $\alpha x^2 + x$

$$\begin{array}{ccc} \mathbb{F}_4[x]/\langle x+1\rangle \times \mathbb{F}_4[x]/\langle x^2+\alpha x+1\rangle & \xrightarrow{(id,\lambda_i,\mu_i)} & \mathbb{F}_4[x]/\langle x+1\rangle \times \mathbb{F}_4[x]/\langle x^2+\alpha x+1\rangle \\ \times \mathbb{F}_4[x]/\langle x^2+\alpha^2 x+1\rangle & & \times \mathbb{F}_4[x]/\langle x^2+\alpha^2 x+1\rangle \\ \rho \uparrow & & \rho^{-1} \downarrow \\ \mathbb{F}_4[x]/\langle x^5-1\rangle & \xrightarrow{\sigma_i} & \mathbb{F}_4[x]/\langle x^5-1\rangle \end{array}$$

$$\sigma_i(x) = \rho^{-1} \circ (id, \lambda_i, \mu_i) \circ \rho(x)$$

Ainsi

$\sigma_0(x) = \rho^{-1} \circ (id, \lambda_0, \mu_0) \circ \rho(x)$	$= x$
$\sigma_1(x) = \rho^{-1} \circ (id, \lambda_1, \mu_1) \circ \rho(x)$	$= \alpha x^4 + x^3 + x^2 + \alpha^2 x$
$\sigma_2(x) = \rho^{-1} \circ (id, \lambda_2, \mu_2) \circ \rho(x)$	$= \alpha^2 x + x^3 + x^2 + \alpha^2 x$
$\sigma_3(x) = \rho^{-1} \circ (id, \lambda_3, \mu_3) \circ \rho(x)$	$= x^4$
$\sigma_4(x) = \rho^{-1} \circ (id, \lambda_4, \mu_4) \circ \rho(x)$	$= x^4 + \alpha x^3 + \alpha^2 x^2 + x$
$\sigma_5(x) = \rho^{-1} \circ (id, \lambda_5, \mu_5) \circ \rho(x)$	$= x^3$
$\sigma_6(x) = \rho^{-1} \circ (id, \lambda_6, \mu_6) \circ \rho(x)$	$= x^2$
$\sigma_7(x) = \rho^{-1} \circ (id, \lambda_7, \mu_7) \circ \rho(x)$	$= x^4 + \alpha^2 x^3 + \alpha x^2 + x$

3.3 Structure de $A[z\ ;\sigma]$

Après avoir construit les automorphismes de A; on peut aborder la σ- cyclicité des codes convolutionnels en ellaborant la structure de $A[z\ ;\sigma]$.

Soient $\mathbb{F}$ un corps fini et $A = \mathbb{F}[x] / \langle x^n - 1 \rangle$ où n n'est divisible par la caractéristique de $\mathbb{F}$. Pour tout $\sigma \in Aut_{\mathbb{F}}(A)$ on définit $*_\sigma$sur $A[z]$ par :

$$\forall g = \sum_{\nu \geq 0} z^\nu g_\nu \text{ et } h = \sum_{\mu \geq 0} z^\mu h_\mu \in A[z] : \quad h *_\sigma g = \sum_{u \geq 0} h_u z^u *_\sigma \sum_{\nu \geq 0} g_\nu z^\nu$$
$$= \sum_{\lambda \geq 0} z^\lambda \left[\sum_{\mu + \nu = \lambda} \sigma^\mu (h_\nu) g_u \right]$$

Proposition 70

L'ensemble $A[z]$ muni des deux lois $+$ et $*_\sigma$ est une algèbre notée $A[z\ ;\sigma]$. On appelle $A[z\ ;\sigma]$ algèbre de Piret.

Proposition 71 [2]

Pour $a \in A$, $\lambda \in \mathbb{F}$ on a :

1. $a *_\sigma z = z\ \sigma(a)$.
2. $\lambda *_\sigma z = z *_\sigma \lambda$.

Preuve

1.

$$h *_\sigma g = \sum z^\lambda (\sum \sigma^\mu(h_\mu) g_\nu)$$

$$h *_\sigma g = \sigma^0(h_0)\, g_0 + \left[\sigma^0(h_1)\, g_0 + \sigma^1(h_0)\, g_1\right] z + ...$$

pour

$$h = a \text{ et } g = z$$

Alors

$$h *_\sigma g = \sigma(a)\, z$$

Donc

$$a *_\sigma z = \sigma(a)\, z \quad \forall a \in A$$

2.D'après (1) en posant $\lambda = a \in \mathbb{F}$

$$\lambda *_\sigma z = z *_\sigma \sigma(\lambda)$$

sachant que σ est un automorphisme de $\mathbb{F}$-algèbre dans

$$\sigma(1) = 1 \text{ d'où } \sigma(\lambda) = \sigma(\lambda \cdot 1) = \lambda \cdot \sigma(1) = \lambda$$

pour

$$h = a \text{ et } g = z$$

Alors

$$h *_\sigma g = \sigma(a)\, z$$

sachant que σ est un automorphisme de $\mathbb{F}$-algèbre dans

$$\sigma(1) = 1 \text{ d'où } \sigma(\lambda) = \sigma(\lambda \cdot 1) = \lambda \cdot \sigma(1) = \lambda$$

■

Proposition 72

1. *$A[z\,;\sigma]$ est un anneau .*
2. *$A[z\,;\sigma]$ n'est pas commutatif.*

Preuve

1. Trivial
2. Soit

$$a \in A \text{ et } z \in A[z] : a *_\sigma z = z\ \sigma(a)$$

Suposons que

$$z\ \sigma(a) = z\ a$$

Donc

$$z(\sigma(a) - a) = 0 \text{ si } \sigma(a) = a : \forall a \in A$$

Alors $A[z\,;\sigma]$ n'est pas commutatif. ■

Définition 73

L'algèbre $A[z\,;\sigma]$ est dite algèbre de Piret de paramètres $q = |\mathbb{F}|$, n, σ.

Définition 74

Pour $\sigma \in Aut_{\mathbb{F}}(A)$;

un sous-module C de $\mathbb{F}[z]^n$ est dit σ-cyclique (ou cyclique au sens de Piret) si :

$$g = \sum_{\nu \geq 0}^{d} z^\nu g_\nu \in \tilde{P}(C) \Rightarrow x *_\sigma g = \sum_{\nu \geq 0}^{d} z^\nu (\sigma^\nu(x)\, g_\nu) \in \tilde{P}(C) \tag{3.9}$$

le théoèrme suivant caractérise les sous-modules de $\mathbb{F}[z]^n$ qui sont $\sigma-$cycliques :

Théorème 75 [2]

Considérons l'anneau $A[z\,;\sigma]$. Un sous- module C de $\mathbb{F}[z]^n$ est $\sigma-$cyclique si seulement si $\tilde{P}^{-1}(C)$ est un idéal à gauche dans $A[z\,;\sigma]$.

Preuve

Suposons que C est $\sigma-$cyclique et prouvons qu'il est un idéal à gauche de $A[z\,;\sigma]$. On remarque d'abord que C est un sou-module à gauche de $A[z\,;\sigma]$ et d'aprés la définition de la cyclicité on à

$$g=\sum_{\nu\geq 0}^{d} z^{\nu}g_{\nu}\in\tilde{P}(C)\Rightarrow x*_{\sigma}g=\sum_{\nu\geq 0}^{d} z^{\nu}\sigma^{\nu}(x)\,g_{\nu}\in\tilde{P}(C)$$

et par induction sur i on trouve

$$\forall 0\leq i\leq n-1: x^{i}*_{\sigma}g\in\tilde{P}(C)$$

Alors pour tout polynôme $f(x)=\sum a_i x^i$ de A on a :

ce qui montre que C est un idéal à gauche.

Réciproquement, supposons que C est un idéal dans $A[z\,;\sigma]$ donc pour $g\in\tilde{P}\ (C)$ on a particulièrement $x*_{\sigma}g\in\tilde{P}(C)$.

D'où il est cyclique. ■

Dans les exemples suivants nous construisons des codes convolutionnels σ-cycliques en prenant des idéaux à gauche dans $A[z\,;\sigma]$. Les idéaux à gauche sont choisis parmi les idéaux engendrés par un élément de $A[z\,;\sigma]$. En effet

Exemple 76

Pour $n=7$ et $\mathbb{F}=\mathbb{F}_2$, prenons $\sigma(x)=x^5$ et

$$v=\left(1+z^2,z+z^2,1+z,1+z,1+z^2,z,z^2\right)\in\mathbb{F}[z]^7$$

1. i.e

$$\begin{aligned} g &= \tilde{P}(v) \\ &= (1+x^2+x^3+x^4)+z\ \left(x+x^2+x^3+x^5\right)+z^2\left(1+x+x^4+x^6\right) \in A[z;\sigma] \end{aligned}$$

Soit J l'idéal à gauche engendré par g dans $A[z\ ;\sigma]$

$$J = \{f *_\sigma g : f \in A[z\ ;\sigma]\}$$

Alors le code associé est

$$C = \tilde{P}^{-1}(J)$$

où J est engendré par $\{g, x *_\sigma g, ..., x^6 *_\sigma g\}$

On a

$$\begin{aligned} x *_\sigma g &= xg_0 + z\ \sigma(x)\, g_1 + z^2\sigma^2(x)\, g_2 \\ &= x\left(1+x^2+x^3+x^4\right)+z\ x^5\left(x+x^2+x^3+x^5\right) \\ &\quad +z^2\left(1+x+x^4+x^6\right) \\ &= x+x^3+x^4+x^5+z\ \left(1+x+x^3+x^6\right) \\ &\quad +z^2\left(x+x^3+x^4+x^5\right) \end{aligned}$$

Alors

$$\tilde{P}^{-1}(x *_\sigma g) = \left(z, 1+z+z^2, 0, 1+z+z^2, 1+z^2, 1+z^2, z\right)$$

Et

$$\begin{aligned} x^2 *_\sigma g &= x^2 g_0 + z\ \sigma\left(x^2\right) g_1 + z^2 \sigma^2\left(x^2\right) g_2 \\ &= x^2\left(1 + x^2 + x^3 + x^4\right) + z\ x^3\left(x + x^2 + x^3 + x^5\right) \\ &\quad + z^2 x\left(x + x^3 + x^4 + x^5\right) \\ &= \left(x^2 + x^4 + x^5 + x^6\right) + z\ \left(x + x^4 + x^5 + x^6\right) \\ &\quad + z^2\left(1 + x + x^2 + x^5\right) \end{aligned}$$

Alors

$$\tilde{P}^{-1}\left(x^2 *_\sigma g\right) = \left[z^2, z + z^2, 1 + z^2, 0, 1 + z, 1 + z + z^2, 1 + z\right]$$

$$\begin{aligned} x^3 *_\sigma g &= \left(1 + x^3 + x^5 + x^6\right) + z\left(x^2 + x^3 + x^4 + x^6\right) \\ &\quad + z^2\left(1 + x^3 + x^5 + x^6\right) \\ &= g + x^2 *_\sigma g \end{aligned}$$

Par conséquent

$$\begin{aligned} x^4 *_\sigma g &= x *_\sigma g + x^3 *_\sigma g \\ &= g + x^2 *_\sigma g + x^3 *_\sigma g \end{aligned}$$

$$x^5 *_\sigma g = x *_\sigma g + x^3 *_\sigma g + x^4 *_\sigma g$$

$$x^6 *_\sigma g = x^2 *_\sigma g + x^4 *_\sigma g$$

Donc

$$J = span_{\mathbb{F}[x]}\left\{g, x *_\sigma g, x^2 *_\sigma g\right\}$$

D'où

$$\begin{aligned} C &= \tilde{P}^{-1}(J) \\ &= \left\{u \cdot G \ / \ u \in \mathbb{F}[z]^3\right\} \end{aligned}$$

où

$$G = \begin{pmatrix} \tilde{P}^{-1}(g) \\ \tilde{P}^{-1}(x *_\sigma g) \\ \tilde{P}^{-1}(x^2 *_\sigma g) \end{pmatrix}$$

$$G = \begin{pmatrix} 1+z^2 & z+z^2 & 1+z & 1+z & 1+z^2 & z & z^2 \\ z & 1+z+z^2 & 0 & 1+z+z^2 & 1+z^2 & 1+z^2 & z \\ z^2 & z+z^2 & 1+z^2 & 0 & 1+z & 1+z+z^2 & 1+z \end{pmatrix}$$

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} + z \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} + z^2 \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

ceci représente un code convolutionnel cyclique sous forme $(7, 3, 2)$.

Exemple 77

Pour $n = 3$, $\mathbb{F} = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ *avec* $\alpha^2 + \alpha + 1 = 0$.

Prenons pour σ; $\sigma(x) = \alpha^2 x$ *et comme générateur de* J *le polunôme :*

$$g = 1 + \alpha x + \alpha^2 x^2 + z\left(1 + x + x^2\right) + z^2\left(1 + \alpha^2 x + \alpha x^2\right).$$

D'après la structure de $A[z,\sigma]$ *on a :*

$$\begin{aligned} x *_\sigma g &= \sum_{\nu\geq 0}^{2} z^\nu \sigma^\nu(x)\, g_\nu \\ &= xg_0 + z\ \sigma(x)\, g_1 + z^2\sigma^2(x)\, g_2 \\ &= x + \alpha x + \alpha^2 + z\ \left(\alpha^2 x + \alpha^2 x^2 + \alpha^2\right) + z^2\left(\alpha x + x^2 + \alpha^2\right) \\ &= \alpha^2 + x + \alpha x^2 + z\ \left(\alpha^2 + \alpha^2 x + \alpha^2 x^2\right) + z^2\left(\alpha^2 + \alpha x + x^2\right) \\ &= \alpha^2\left[1 + \alpha x + \alpha^2 x^2 + z\ \left(1 + x + x^2\right) + z^2\left(1 + \alpha^2 x + \alpha x^2\right)\right] \\ &= \alpha^2 g \end{aligned}$$

Donc

$$J = span_{\mathbb{F}[x]}\{g, x *_\sigma g\}$$

Et

$$\begin{aligned} C &= \tilde{P}^{-1}(J) \\ &= \{u \cdot G \ /\ u \in \mathbb{F}[z]\} \end{aligned}$$

Alors

$$G = \begin{bmatrix} 1 + z + z^2 & \alpha + z + \alpha^2 z^2 & \alpha^2 + z + \alpha z^2 \end{bmatrix}$$

ceci représente un code convolutionnel cyclique sous forme $(3,1,2)$.

3.4 Générateurs d'idéaux (à gauche) de $A[z\ ;\sigma]$

Dans cette partie ; il est question de déterminer tous les générateurs d'idéaux à gauches de $A[z\ ;\sigma]$(et donc tous les codes convolutionnels σ-cycliques) pour les corps finis ($\mathbb{F}_2$,$\mathbb{F}_3$ et $\mathbb{F}_4$) et pour les valeurs de n allant de 1 à 7.

Etant donné une algèbre de Piret $A[z\ ;\sigma]$. Considérons les composantes $K^{(k)}$ de $A =$

$\mathbb{F}[x]/\langle x^n-1\rangle$ suivant ρ,

$$K^{(k)} = \varepsilon^{(k)} A \text{ pour } k = 1, \ldots, r$$

Pour tout $f \in A[z\,;\sigma]$ on a :

$$\begin{aligned} f &= f_0 + zf_1 + ... + z^d f_d \\ &= \left(\varepsilon^{(1)} f_0 + \varepsilon^{(2)} f_0 + ... + \varepsilon^{(r)} f_0\right) + ... + z^d \left(\varepsilon^{(1)} f_d + \varepsilon^{(2)} f_d + ... + \varepsilon^{(r)} f_d\right) \\ &= \left(\varepsilon^{(1)} f_0 + z\ \varepsilon^{(1)} f_1 + ... + z^d \varepsilon^{(1)} f_d\right) + ... + \left(\varepsilon^{(r)} f_0 + z\ \varepsilon^{(r)} f_1 + ... + z^d \varepsilon^{(r)} f_d\right) \\ &= \varepsilon^{(1)f} + \varepsilon^{(2)} f + ... + \varepsilon^{(r)} f \end{aligned}$$

Notons $\varepsilon^{(k)} f$ par $f^{(k)}$, pour tout $k = 1, \ldots, r$.

Alors f possède la décomposition suivante :

$$f = f^{(1)} + f^{(2)} + ... + f^{(r)}$$

Définition 78

1. *Pour tout $k = 1, \ldots, r$; $f^{(k)}$ est dit la $k^{ième}$ composante de f suivant ρ.*
2. *L'ensemble*

$$T_f := \left\{k\ : f^{(k)} \neq 0\right\}$$

est dit support de f.

Exemple 79

Soient $\mathbb{F} = \mathbb{F}_2$, $n = 7$ et $\sigma(x) = x^5$

On a

$$x^7 - 1 = \pi_1 \times \pi_2 \times \pi_3$$

telque

$$\begin{aligned}\pi_1 &= x+1\\ \pi_2 &= x^3+x+1\\ \pi_3 &= x^3+x^2+1\end{aligned}$$

$$\begin{aligned}\varepsilon^{(1)} &= 1+x+x^2+x^3+x^4+x^5+x^6\\ \varepsilon^{(2)} &= 1+x+x^2+x^4\\ \varepsilon^{(3)} &= 1+x^2+x^3+x^4\end{aligned}$$

$$\sigma\left(\varepsilon^{(1)}\right)=\varepsilon^{(2)}, \sigma\left(\varepsilon^{(2)}\right)=\varepsilon^{(3)}, \sigma\left(\varepsilon^{(3)}\right)=\varepsilon^{(2)}$$

Pour

$$g=1+x^2+x^3+x^4+z\left(x+x^2+x^3+x^5\right)+z^2\left(1+x+x^4+x^6\right)\in A\left[z\ ;\sigma\right].$$

On a

$$\begin{aligned}\bullet\varepsilon^{(1)}g &= \sum_{\upsilon=0}^{2} z^{\upsilon}\sigma^{\upsilon}\left(\varepsilon^{(1)}\right)g_{\upsilon}\\ &= \varepsilon^{(1)}g_0+z\ \sigma\left(\varepsilon^{(1)}\right)g_1+z^2\sigma^2\left(\varepsilon^{(1)}\right)g_2\\ &= \varepsilon^{(1)}g_0+z\ \varepsilon^{(1)}g_1+z^2\varepsilon^{(1)}g_2\\ &= 0+0+0\\ &= 0\end{aligned}$$

$$
\begin{aligned}
\bullet\varepsilon^{(2)} g &= \sum_{\upsilon=0}^{2} z^{\upsilon}\sigma^{\upsilon}\left(\varepsilon^{(2)}\right) g_{\upsilon} \\
&= \varepsilon^{(2)} g_0 + z\ \sigma\left(\varepsilon^{(2)}\right) g_1 + z^2\sigma^2\left(\varepsilon^{(2)}\right) g_2 \\
&= \varepsilon^{(2)} g_0 + z\ \varepsilon^{(3)} g_1 + z^2\varepsilon^{(2)} g_2 \\
&= 0 + 0 + 0 \\
&= 0
\end{aligned}
$$

$$
\begin{aligned}
\bullet\varepsilon^{(3)} g &= \sum_{\upsilon=0}^{2} z^{\upsilon}\sigma^{\upsilon}\left(\varepsilon^{(3)}\right) g_{\upsilon} \\
&= \varepsilon^{(3)} g_0 + z\ \sigma\left(\varepsilon^{(3)}\right) g_1 + z^2\sigma^2\left(\varepsilon^{(3)}\right) g_2 \\
&= \varepsilon^{(3)} g_0 + z\ \varepsilon^{(2)} g_1 + z^2\varepsilon^{(3)} g_2 \\
&= \left(1 + x + x^2\right) + z\ x + z^2 x
\end{aligned}
$$

Alors

$$
\begin{aligned}
g &= \varepsilon^{(1)} g + \varepsilon^{(2)} g + \varepsilon^{(3)} g \\
&= \left(1 + x + x^2\right) + z\ x + z^2 x
\end{aligned}
$$

Donc

$$T_g = \{3\}$$

Exemple 80

Soient $\mathbb{F} = \mathbb{F}_4$, $n = 3$ *et* $\sigma(x) = \alpha^2 x$.

On a $x^3 - 1 = \pi_1 \times \pi_2 \times \pi_3$ *; telque*

$$
\begin{aligned}
\pi_1 &= x + 1 \\
\pi_2 &= x + \alpha \\
\pi_3 &= x + \alpha^2
\end{aligned}
$$

$$\begin{aligned}\varepsilon^{(1)} &= x^2+x+1\\ \varepsilon^{(2)} &= \alpha x^2+\alpha^2 x+1\\ \varepsilon^{(3)} &= \alpha^2 x^2+\alpha x+1\end{aligned}$$

On a

$$\sigma\left(\varepsilon^{(1)}\right)=\varepsilon^{(2)}, \sigma\left(\varepsilon^{(2)}\right)=\varepsilon^{(3)}, \sigma\left(\varepsilon^{(3)}\right)=\varepsilon^{(1)}.$$

Soit

$$g=\left(\alpha^2x^2+\alpha x+1\right)+z\ \left(1+x+x^2\right)+z^2\left(\alpha x^2+\alpha^2 x+1\right).$$

$$\begin{aligned}\bullet\varepsilon^{(1)}g &= \sum_{\upsilon=0}^{2} z^{\upsilon}\sigma^{\upsilon}\left(\varepsilon^{(1)}\right)g_{\upsilon}\\ &= \varepsilon^{(1)}g_0+z\ \sigma\left(\varepsilon^{(1)}\right)g_1+z^2\sigma^2\left(\varepsilon^{(1)}\right)g_2\\ &= \varepsilon^{(1)}g_0+z\ \varepsilon^{(2)}g_1+z^2\varepsilon^{(3)}g_2\\ &= 0+0+0\\ &= 0\end{aligned}$$

$$\begin{aligned}\bullet\varepsilon^{(2)}g &= \sum_{\upsilon=0}^{2} z^{\upsilon}\sigma^{\upsilon}\left(\varepsilon^{(2)}\right)g_{\upsilon}\\ &= \varepsilon^{(2)}g_0+z\sigma\left(\varepsilon^{(2)}\right)g_1+z^2\sigma^2\left(\varepsilon^{(2)}\right)g_2\\ &= \varepsilon^{(2)}g_0+z\varepsilon^{(3)}g_1+z^2\varepsilon^{(1)}g_2\\ &= 0+0+0\\ &= 0\end{aligned}$$

$$\begin{aligned}
\bullet\varepsilon^{(3)} g &= \sum_{\upsilon=0}^{2} z^{\upsilon}\sigma^{\upsilon}\left(\varepsilon^{(3)}\right) g_{\upsilon} \\
&= \varepsilon^{(3)} g_0 + z\ \sigma\left(\varepsilon^{(3)}\right) g_1 + z^2\sigma^2\left(\varepsilon^{(3)}\right) g_2 \\
&= \varepsilon^{(3)} g_0 + z\ \varepsilon^{(1)} g_1 + z^2\varepsilon^{(2)} g_2 \\
&= 1 + z + z^2
\end{aligned}$$

Alors

$$\begin{aligned}
g &= \varepsilon^{(1)} g + \varepsilon^{(2)} g + \varepsilon^{(3)} g \\
&= 1 + z + z^2
\end{aligned}$$

Donc

$$T_g = \{3\}$$

Théorème 81

Soit $x^n - 1 = \prod_{i=1}^{r} \pi_i$ *la décomposition de* $x^n - 1$*dans* $\mathbb{F}$*. Alors pour* $\tau \in S_{r_1 \ldots r_s}$ *et pour tout* $\sigma = [\lambda_1, \lambda_2, ..., \lambda_r] \circ \tau \in Aut_{\mathbb{F}}(A)$ *on a :*

$$\sigma\left(\varepsilon^{(k)}\right) = \varepsilon^{(\tau(k))}$$

Preuve

Soit

$$\sigma(x) = [\lambda_1, \lambda_2, ..., \lambda_r]\, o\, \tau\left(\rho_1(x), \rho_2(x), ..., \rho_r(x)\right)$$

Alors

$$\begin{aligned}
\sigma_\tau\left(\varepsilon^{(k)}\right) &= [\lambda_1,...,\lambda_r]\left(\rho_1\left(\varepsilon^{(k)}\right),...,\Psi^{-1}\left(\rho_{\tau(k)}\left(\varepsilon^{(k)}\right)\right),...,\Psi\left(\rho_k\left(\varepsilon^{(k)}\right)\right),...,\rho_r\left(\varepsilon^{(k)}\right)\right) \\
&= \left[\begin{array}{c} \lambda_1\left(\rho_1\left(\varepsilon^{(k)}\right)\right),...,\lambda_k\left(\Psi^{-1}\left(\rho_{\tau(k)}\left(\varepsilon^{(k)}\right)\right)\right) \\ ,...,\lambda_{\tau(k)}\left(\Psi\left(\rho_k\left(\varepsilon^{(k)}\right)\right)\right),...,\lambda_r\left(\rho_1\left(\varepsilon^{(k)}\right)\right) \end{array}\right] \\
&= \left[\lambda_1(0),...,\lambda_k\left(\Psi^{-1}(0)\right),...,\lambda_{\tau(k)}(\Psi(0)),...,\lambda_r(0)\right] \\
&= \left[\lambda_1(0),...,\lambda_k\left(\Psi^{-1}(0)\right),...,\lambda_{\tau(k)}(\Psi(1)),...,\lambda_r(0)\right] \\
&= [0,...,0,...,1,...,0] \\
&= \varepsilon^{(\tau(k))}
\end{aligned}$$

■

Le théorème suivant caractérise les générateurs des codes convolutionnels σ-cyclique. Il est utilisé pour construire et d'une manière exhaustive tous les codes convolutionnels σ-cycliques pour les cas cités plus-haut.

Pour tout $g \in A[z\,;\sigma]$, notons par $\dot{\langle g\rangle}$ l'idéal à gauche dans $A[z\,;\sigma]$ engendré par g.

Théorème 82 [2]

Soit C un $\mathbb{F}[z]$ sous-module de $\mathbb{F}[z]^n$ et $J = \tilde{P}(C)$ son image dans $A[z\,;\sigma]$. Alors les propriétés suivantes sont équivalentes :

1. *C est un code convolutionnel σ-cyclique.*
2. *$J = \dot{\langle g\rangle}$ pour un certain $g \in A[z\,;\sigma]$ satisfaisant :*

$$T_g = T_{g_0}$$

Dans le théorème suivant nous donnons tous les générateurs des codes convolutionnels σ-cycliques sur le corps $\mathbb{F}_2$.

Théorème 83

Soit $g \in A[z\ ;\sigma]$, *où* $\mathbb{F} = \mathbb{F}_2$ *et* $n = 3, 5, 7$ *alors*

1. *Si* $n = 3, 5$

$$T_{g_0} = T_g \Longleftrightarrow \begin{cases} 1.\sum_{j=0}^{n-1} a_i^{(j)} = 0\ \forall j \\ 2.a_{n-1}^{(j)} = a_1^{(j)}\ i = 0, ..., n-2 \\ 3.\forall a_i^{(j)} \in \mathbb{F}_2 \end{cases}$$

2. *Si* $n = 7$

$$T_{g_0} = T_g \Longleftrightarrow \begin{cases} 1\ a_6^{(j)} = a_i^{(j)}\ i = 1, ..., 6. \\ 2. \begin{cases} a_0^{(2j)} = a_1^{(2j)} + a_5^{(2j)} = a_2^{(2j)} + a_3^{(2j)} = a_2^{(2j)} + a_3^{(2j)} \\ a_0^{(2j+1)} = a_1^{(2j+1)} + a_3^{(2j+1)} = a_4^{(2j+1)} + a_5^{(2j+1)} = a_2^{(2j+1)} + a_6^{(2j+1)} \end{cases} \\ 3. \begin{cases} a_0^{(2j)} = a_1^{(2j)} + a_3^{(2j)} = a_4^{(2j)} + a_5^{(2j)} = a_2^{(2j)} + a_6^{(2j)} \\ a_0^{(2j+1)} = a_1^{(2j+1)} + a_5^{(2j+1)} = a_2^{(2j+1)} + a_3^{(2j+1)} = a_2^{(2j+1)} + a_3^{(2j+1)} \end{cases} \\ 4. \begin{cases} a_3^{(2j)} \vee a_5^{(2j+1)} + \left(a_2^{(j)} + a_4^{(j)} + a_5^{(j)}\right) \\ a_6^{(2j)} \vee a_3^{(2j+1)} + \left(a_1^{(j)} + a_4^{(j)} + a_5^{(j)}\right) \\ a_4^{(2j)} \vee a_6^{(2j+1)} + \left(a_0^{(j)} + a_3^{(j)} + a_5^{(j)}\right) \end{cases} \\ 5. \begin{cases} a_5^{(2j)} \vee a_3^{(2j+1)} + \left(a_2^{(j)} + a_4^{(j)} + a_5^{(j)}\right) \\ a_3^{(2j)} \vee a_6^{(2j+1)} + \left(a_1^{(j)} + a_4^{(j)} + a_5^{(j)}\right) \\ a_6^{(2j)} \vee a_4^{(2j+1)} + \left(a_0^{(j)} + a_3^{(j)} + a_5^{(j)}\right) \end{cases} \\ 6.\sum_{i=0}^{6} a_i^{(j)} \forall j \\ 7.\forall a_i^{(j)} \in \mathbb{F}_2 \end{cases}$$

Preuve

Soit $g = \sum z^{\mu} g_{\mu} \in A[z\,;\sigma]$ et posons pour tout $j \geq 0$:

$$g_j = a_0^{(j)} + a_1^{(j)} x + \cdots + a_{n-1}^{(j)} x^{n-1}$$

D'après les résultats précédants citant tous les automorphismes de A on a pour :

1.

a)$\mathbb{F} = \mathbb{F}_2$ et $n = 3$

$$\begin{aligned}
&x^3 - 1 = (x+1)(x^2 + x + 1)\\
&\forall \sigma \in Aut_{\mathbb{F}}(A) : \sigma\left(\varepsilon^{(k)}\right) = \varepsilon^{(k)}\\
&g_0 = a_0^{(0)} + a_1^{(0)} x + a_2^{(0)} x^2\\
&\varepsilon^{(1)} g_j = a_0^{(j)} + a_1^{(j)} + a_2^{(j)}\\
&\varepsilon^{(2)} g_j = \left(a_j^{(j)} + a_2^{(j)}\right) x + a_0^{(j)} + a_2^{(j)}
\end{aligned}$$

•$1^{ère}$**cas**

Si $T_{g_0} = \{1\}$ on a

$$T_g = T_{g_0} \Longleftrightarrow \begin{cases} g = g^{(1)}\left(g^{(2)} = 0\right) \\ \Rightarrow a_0^{(j)} = a_1^{(j)} = a_2^{(j)} \end{cases}$$

•$2^{ème}$**cas**

Si$T_{g_0} = \{2\}$

$$T_g = T_{g_0} \iff \begin{cases} g = g^{(2)}\left(g^{(1)} = 0\right) \\ \Rightarrow a_0^{(j)} + a_1^{(j)} + a_2^{(j)} = 0 \end{cases}$$

•$3^{ème}$**cas**

Si $T_{g_0} = \{1, 2\}$

$$T_g = T_{g_0} \Rightarrow g = g^{(2)} + g^{(1)} \forall a_i^{(j)} \in \mathbb{F}_2$$

b)$\mathbb{F} = \mathbb{F}_2$ et $n = 5$

$$\begin{aligned} x^5-1 &= (x+1)\left(x^5+x^4+x^3+x^2+x+1\right) \\ \varepsilon^{(1)} &= x^5+x^4+x^3+x^2+x+1 \\ \varepsilon^{(2)} &= x+1 \end{aligned}$$

$$\begin{aligned} \varepsilon^{(1)} g_j &= a_0^{(j)}+a_1^{(j)}+a_2^{(j)}+a_3^{(j)}+a_4^{(j)} \\ \varepsilon^{(1)} g_j &= \sum_{i=0}^{3}\left(a_4^{(j)}+a_i^{(j)}\right)x^i \end{aligned}$$

•$1^{ère}$**cas**

Si $T_{g_0}=\{1\}$ on a

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g=g^{(1)}\left(g^{(2)}=0\right) \\ &\Longleftrightarrow a_4^{(j)}=a_i^{(j)} \end{aligned}$$

•$2^{ème}$**cas**

Si $T_{g_0}=\{2\}$ on a

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g=g^{(2)}\left(g^{(1)}=0\right) \\ &\Longleftrightarrow a_0^{(j)}+a_1^{(j)}+a_2^{(j)}+a_3^{(j)}+a_4^{(j)}=0 \end{aligned}$$

•$3^{ème}$**cas**

Si$T_{g_0}=\{1,2\}$

$$T_g=T_{g_0} \Longleftrightarrow g=g^{(2)}+g^{(1)}\forall a_i^{(j)}\in\mathbb{F}_2$$

3.$\mathbb{F}=\mathbb{F}_2$ et $n=7$

$$\begin{aligned} x^7-1 &= (x+1)\left(x^3+x+1\right)\left(x^3+x^2+1\right) \\ \varepsilon^{(1)} &= x^6+x^5+x^4+x^3+x^2+x+1 \\ \varepsilon^{(2)} &= x^4+x^2+x+1 \\ \varepsilon^{(3)} &= x^4+x^3+x^2+1 \end{aligned}$$

$$\begin{aligned} g_j &= a_0^{(j)}+a_1^{(j)}x+a_2^{(j)}x^2+a_3^{(j)}x^3+a_4^{(j)}x^4+a_5^{(j)}x^5+a_6^{(j)}x^5 \\ \varepsilon^{(1)}g_j &= \sum_{i=0}^{6} a_i^{(j)} \\ \varepsilon^{(2)}g_j &= \left(a_2^{(j)}+a_4^{(j)}+a_5^{(j)}+a_6^{(j)}\right)x^2+\left(a_1^{(j)}+a_3^{(j)}+a_4^{(j)}+a_5^{(j)}\right)x+ \\ &\quad +a_0^{(j)}+a_3^{(j)}+a_5^{(j)}+a_6^{(j)} \\ \varepsilon^{(3)}g_2 &= \left(a_2^{(j)}+a_3^{(j)}+a_4^{(j)}+a_6^{(j)}\right)x^2+\left(a_1^{(j)}+a_4^{(j)}+a_5^{(j)}+a_6^{(j)}\right)x \\ &\quad +a_0^{(j)}+a_3^{(j)}+a_4^{(j)}+a_5^{(j)} \\ \varepsilon^{(1)}g &= \varepsilon^{(1)}g_0+z\ \varepsilon^{(1)}g_1+z^2\varepsilon^{(1)}g_2+... \\ \varepsilon^{(2)}g &= \varepsilon^{(2)}g_0+z\ \varepsilon^{(3)}g_1+z^2\varepsilon^{(2)}g_2+... \\ \varepsilon^{(3)}g &= \varepsilon^{(3)}g_0+z\ \varepsilon^{(2)}g_1+z^2\varepsilon^{(3)}g_2+... \end{aligned}$$

•1èrecas

Si $T_{g_0}=\{1\}$

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g=g^{(1)}\left(g^{(2)}=g^{(3)}=0\right) \\ &\Longleftrightarrow \begin{cases} \varepsilon^{(2)}g_{2j}=0 \wedge \varepsilon^{(3)}g_{2j+1}=0 \\ \varepsilon^{(3)}g_{2j}=0 \wedge \varepsilon^{(2)}g_{2j+1}=0 \end{cases} \\ &\Longleftrightarrow a_0^{(j)}=a_1^{(j)}=a_2^{(j)}=a_3^{(j)}=a_4^{(j)}=a_5^{(j)}=a_6^{(j)} \end{aligned}$$

•2èmecas

Pour $T_{g_0} = \{2\}$

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(2)} \left(g^{(1)} = g^{(3)} = 0\right) \\ &\Longleftrightarrow \begin{cases} \sum_{i=0}^{6} a_i^{(j)} = 0 \wedge \varepsilon^{(2)} g_{2j+1} = 0 \wedge \varepsilon^{(3)} g_{2j} = 0 \end{cases} \end{aligned}$$

•$3^{ème}$**cas**

Si $T_{g_0} = \{3\}$

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(3)} \left(g^{(1)} = g^{(2)} = 0\right) \\ \Longleftrightarrow \sum_{i=0}^{6} a_i^{(j)} &= 0 \wedge \varepsilon^{(2)} g_{2j} = 0 \wedge \varepsilon^{(3)} g_{2j} + 1 = 0 \end{aligned}$$

•$4^{ème}$**cas**

Si $T_{g_0} = \{1, 2\}$

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(1)} + g^{(2)} \left(g^{(3)} = 0\right) \\ &\Longleftrightarrow \varepsilon^{(2)} g_{2j+1} = 0 \wedge \varepsilon^{(3)} g_{2j} = 0 \end{aligned}$$

•$5^{ème}$**cas**

Si $T_{g_0} = \{1, 3\}$

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(1)} + g^{(3)} \left(g^{(2)} = 0\right) \\ &\Longleftrightarrow \varepsilon^{(2)} g_{2j} = 0 \wedge \varepsilon^{(3)} g_{2j+1} = 0 \end{aligned}$$

•$6^{ème}$**cas**

Si $T_{g_0} = \{2, 3\}$

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(2)} + g^{(3)} \left(g^{(1)} = 0\right) \\ &\Longleftrightarrow \sum_{i=0}^{6} a_i^{(j)} = 0 \end{aligned}$$

•$7^{ème}$**cas**

Si $T_{g_0} = \{1, 2, 3\}$

$$T_g = T_{g_0} \Longleftrightarrow g = g^{(1)} + g^{(2)} + g^{(3)} \ \forall a_i^{(j)} \in \mathbb{F}_2$$

■

Dans le théorème suivant nous donnons tous les générateurs des codes convolutionnels σ-cycliques sur le corps $\mathbb{F}_3$.

Théorème 84

Soit $g \in A[z\ ;\sigma]$ *et* $\mathbb{F} = \mathbb{F}_3$

1. *Si* $n = 5, 7$ *on a*

$$T_{g_0} = T_g \Longleftrightarrow \begin{cases} 1.\sum_{i=0}^{2} a_i^{(j)} = 0 \forall j \\ 2.a_{n-1}^{(j)} = a_i^{(j)} \ \forall j \ et\ 0 \leq i \leq n-2 \\ 3.\forall a_i^{(j)} \in \mathbb{F}_3 \end{cases}$$

2. Si $n = 4$ on a

$$T_{g_0} = T_g \Longleftrightarrow \begin{cases} 1. \begin{cases} a_0^{(2j)} = -(1-x)\, a_1^{(2j)} \\ \wedge \\ a_0^{(2j+1)} = (1+x)\, a_1^{(2j+1)} \end{cases} \\ 2. \begin{cases} a_0^{(2j)} = (1+x)\, a_1^{(2j)} \\ \wedge \\ a_0^{(2j+1)} = -(1-x)\, a_1^{(2j+1)} \end{cases} \\ 3. a_0^{(j)} = a_1^{(j)} = a_2^{(j)} \\ 4. a_2^{(j)} x = a_2^{(j)} - a_0^{(j)} \\ 5. \begin{cases} a_0^{(2j)} = a_1^{(2j)} - a_2^{(2j)} \\ \wedge \\ a_0^{(2j+1)} = a_2^{(2j+1)} - a_1^{(2j+1)} x \end{cases} \\ 6. \begin{cases} a_0^{(2j+1)} = a_1^{(2j+1)} - a_2^{(2j+1)} \\ \wedge \\ a_0^{(2j)} = a_2^{(2j)} - a_1^{(2j)} x \end{cases} \\ 7. \forall a_i^{(j)} \in \mathbb{F}_3 \end{cases}$$

Preuve

1. $\mathbb{F} = \mathbb{F}_3$ et $n = 4$

$$\begin{aligned} x^4 - 1 &= (x-1)(x+1)\left(x^2+1\right) \\ \varepsilon^{(1)} g_j &= a_0^{(j)} + a_1^{(j)} + a_2^{(j)} \\ \varepsilon^{(2)} g_j &= a_0^{(j)} - a_1^{(j)} + a_2^{(j)} \\ \varepsilon^{(2)} g_j &= a_0^{(j)} x + a_1^{(j)} - a_2^{(j)} \\ \varepsilon^{(1)} g &= \varepsilon^{(1)} g_0 + z\, \varepsilon^{(2)} g_1 + z^2 \varepsilon^{(1)} g_2 + ... \\ \varepsilon^{(2)} g &= \varepsilon^{(2)} g_0 + z\, \varepsilon^{(1)} g_1 + z^2 \varepsilon^{(2)} g_2 + ... \\ \varepsilon^{(3)} g &= \varepsilon^{(3)} g_0 + z\, \varepsilon^{(3)} g_1 + z^2 \varepsilon^{(3)} g_2 + ... \end{aligned}$$

•$1^{ère}$**cas**

Si $T_{g_0} = \{1\}$ on a

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(1)} \left(g^{(2)} = 0 \wedge g^{(3)} = 0 \right) \\ &\Longleftrightarrow \begin{cases} \varepsilon^{(2)} g_{2j} = 0 \wedge \varepsilon^{(1)} g_{2j+1} = 0 \\ \wedge \\ \varepsilon^{(3)} g_j = 0 \end{cases} \\ &\Longleftrightarrow \begin{cases} a_0^{(2j)} = -(1-x)\, a_1^{(2j)} \\ \wedge \\ a_0^{(2j+1)} = (1+x)\, a_1^{(2j+1)} \end{cases} \end{aligned}$$

•$2^{ème}$**cas**

Si $T_{g_0} = \{2\}$ on a

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(2)} \left(g^{(1)} = 0 \wedge g^{(3)} = 0 \right) \\ &\Longleftrightarrow a_0^{(j)} + a_1^{(j)} + a_2^{(j)} + a_3^{(j)} + a_4^{(j)} + a_5^{(j)} + a_6^{(j)} = 0 \\ &\Longleftrightarrow \begin{cases} \varepsilon^{(1)} g_{2j} = 0 \wedge \varepsilon^{(2)} g_{2j+1} = 0 \\ \wedge \\ \varepsilon^{(3)} g_j = 0 \end{cases} \\ &\Longleftrightarrow \begin{cases} a_0^{(2j)} = (1+x)\, a_1^{(2j)} \\ \wedge \\ a_0^{(2j+1)} = -(1-x)\, a_1^{(2j+1)} \end{cases} \end{aligned}$$

•$3^{ème}$**cas**

Si $T_{g_0} = \{3\}$

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(3)} \left(g^{(1)} = 0 \wedge g^{(2)} = 0 \right) \\ &\Longleftrightarrow \varepsilon^{(1)} g_j = 0 \wedge \varepsilon^{(2)} g_j = 0 \\ &\Longleftrightarrow a_0^{(j)} = a_1^{(j)} = a_2^{(j)} \end{aligned}$$

•$4^{ème}$**cas**

Si $T_{g_0} = \{1, 2\}$

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(1)} + g^{(2)} \left(g^{(3)} = 0 \right) \\ &\Longleftrightarrow \varepsilon^{(3)} g_j = 0 \\ &\Longleftrightarrow \varepsilon^{(3)} g_j = 0 \\ &\Longleftrightarrow a_2^{(j)} x = a_2^{(j)} - a_0^{(j)} \end{aligned}$$

•$5^{ème}$**cas**

Si $T_{g_0} = \{1, 3\}$:

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(2)} + g^{(3)} \left(g^{(1)} = 0 \right) \\ &\Longleftrightarrow \varepsilon^{(2)} g_{2j} = 0 \wedge \varepsilon^{(1)} g_{2j+1} = 0 \\ &\Longleftrightarrow \begin{cases} a_0^{(2j)} = a_1^{(2j)} - a_2^{(2j)} \\ \wedge \\ a_0^{(2j+1)} = a_2^{(2j+1)} - a_1^{(2j+1)} x \end{cases} \end{aligned}$$

•$6^{ème}$**cas**

Si $T_{g_0} = \{1, 3\}$:

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(1)} + g^{(3)} \left(g^{(2)} = 0\right) \\ &\Longleftrightarrow \varepsilon^{(1)} g_{2j} = 0 \wedge \varepsilon^{(2)} g_{2j+1} = 0 \\ &\Longleftrightarrow \begin{cases} a_0^{(2j+1)} = a_1^{(2j+1)} - a_2^{(2j+1)} \\ \wedge \\ a_0^{(2j)} = a_2^{(2j)} - a_1^{(2j)} x \end{cases} \end{aligned}$$

•$7^{ème}$**cas**

Si $T_{g_0} = \{1, 2, 3\}$

$$T_g = T_{g_0} \Rightarrow g = g^{(1)} + g^{(2)} + g^{(3)} \forall a_i^{(j)} \in \mathbb{F}_3$$

2.$\mathbb{F} = \mathbb{F}_3$ et $n = 5$

$$\begin{aligned} x^5 - 1 &= (x+1)\left(x^5 + x^4 + x^3 + x^2 + x + 1\right) \\ \varepsilon^{(1)} &= x^5 + x^4 + x^3 + x^2 + x + 1 \\ \varepsilon^{(2)} &= x + 1 \end{aligned}$$

$$\begin{aligned} \varepsilon^{(1)} g_j &= a_0^{(j)} + a_1^{(j)} + a_2^{(j)} + a_3^{(j)} + a_4^{(j)} \\ \varepsilon^{(1)} g_j &= \sum_{i=0}^{3} \left(a_4^{(j)} + a_i^{(j)}\right) x^i \end{aligned}$$

•$1^{ère}$**cas**

Si $T_{g_0} = \{1\}$ on a

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(1)} \left(g^{(2)} = 0\right) \\ &\Longleftrightarrow a_4^{(j)} = -a_i^{(j)} \end{aligned}$$

•$2^{ème}$**cas**

Si $T_{g_0} = \{2\}$ on a

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(2)}\left(g^{(1)} = 0\right) \\ &\Longleftrightarrow a_0^{(j)} + a_1^{(j)} + a_2^{(j)} + a_3^{(j)} + a_4^{(j)} = 0 \end{aligned}$$

•$3^{ème}$**cas**

Si $T_{g_0} = \{1, 2\}$

$$T_g = T_{g_0} \Longleftrightarrow g = g^{(2)} + g^{(1)}$$

3.$\mathbb{F} = \mathbb{F}_3$ et $n = 7$

$$x^7 - 1 = (x+1)\left(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\right)$$

$$\begin{aligned} \varepsilon^{(1)} g_j &= a_0^{(j)} + a_1^{(j)} + a_2^{(j)} + a_3^{(j)} + a_4^{(j)} + a_5^{(j)} + a_6^{(j)} \\ \varepsilon^{(1)} g_j &= \sum_{i=0}^{3} \left(a_6^{(j)} + a_i^{(j)}\right) x^i \end{aligned}$$

•$1^{ère}$**cas**

Si $T_{g_0} = \{1\}$ on a

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(1)}\left(g^{(2)} = 0\right) \\ &\Longleftrightarrow a_6^{(j)} = -a_i^{(j)} \end{aligned}$$

•$2^{ème}$**cas**

Si $T_{g_0} = \{2\}$ on a

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(2)}\left(g^{(1)} = 0\right) \\ &\Longleftrightarrow a_0^{(j)} + a_1^{(j)} + a_2^{(j)} + a_3^{(j)} + a_4^{(j)} + a_5^{(j)} + a_6^{(j)} = 0 \end{aligned}$$

•$3^{ème}$**cas**

Si$T_{g_0} = \{1, 2\}$

$$T_g = T_{g_0} \Longleftrightarrow g = g^{(2)} + g^{(1)}$$

■

Dans le théorème suivant nous donnons tous les générateurs des codes convolutionnels σ-cycliques sur le corps $\mathbb{F}_4$.

Théorème 85

Soit $g \in A[z\ ;\sigma]$, *pour* $\mathbb{F} = \mathbb{F}_4$ *et* $n = 3, 5, 7$ *on a*

1. *Si* $n = 3$

$$T_g = T_{g_0} \Longleftrightarrow \begin{cases} 2. \begin{cases} a_0^{(2j)} = a_1^{(2j)} = a_2^{(2j)} \\ \Lambda \\ a_1^{(2j+1)} = \alpha a_0^{(2j+1)} = \alpha^2 a_2^{(2j+1)} \end{cases} \\ 3. \begin{cases} a_1^{(2j)} = \alpha a_0^{(2j)} = \alpha^2 a_2^{(2j)} \\ \Lambda \\ a_0^{(2j+1)} = a_1^{(2j+1)} = a_2^{(2j+1)} \end{cases} \\ 4. \begin{cases} a_0^{(2j+1)} = \alpha a_3^{(2j+1)} + \alpha a_2^{(2j+1)} = \alpha^2 a_1^{(2j+1)} + \alpha^2 a_4^{(2j+1)} \\ a_0^{(2j)} = \alpha^2 a_3^{(2j)} + \alpha^2 a_2^{(2j)} = \alpha a_1^{(2j)} + \alpha a_4^{(2j)} \end{cases} \\ 5. \begin{cases} a_1^{(2j)} + a_0^{(2j)} = \alpha^2 a_2^{(2j)} + \alpha^2 a_4^{(2j)} \\ a_1^{(2j+1)} + a_0^{(2j+1)} = \alpha a_2^{(2j)} + \alpha a_4^{(2j)} \end{cases} \\ 6. \sum_{i=0}^{4} a_i^{(j)} = 0 \\ 7. \forall a_I^{(j)} \in \mathbb{F}_4 \end{cases}$$

2. *Pour* $n = 5$

$$T_g = T_{g_0} \Longleftrightarrow \begin{cases} 1. a_0^{(j)} = a_1^{(j)} = a_2^{(j)} = a_3^{(j)} = a_4^{(j)}. \\ 2. \begin{cases} a_0^{(2j)} = \alpha a_3^{(2j)} + \alpha a_2^{(2j)} = \alpha^2 a_1^{(2j)} + \alpha^2 a_4^{(2j)} \\ a_0^{(2j+1)} = \alpha^2 a_3^{(j)} + \alpha^2 a_2^{(j)} = \alpha a_1^{(j)} + \alpha a_4^{(j)} \end{cases} \\ 3. \begin{cases} a_0^{(2j+1)} = \alpha a_3^{(2j+1)} + \alpha a_2^{(2j+1)} = \alpha^2 a_1^{(2j+1)} + \alpha^2 a_4^{(2j+1)} \\ a_0^{(2j)} = \alpha^2 a_3^{(2j)} + \alpha^2 a_2^{(2j)} = \alpha a_1^{(2j)} + \alpha a_4^{(2j)} \end{cases} \\ 4. \begin{cases} a_0^{(2j+1)} = \alpha a_3^{(2j+1)} + \alpha a_2^{(2j+1)} = \alpha^2 a_1^{(2j+1)} + \alpha^2 a_4^{(2j+1)} \\ a_0^{(2j)} = \alpha^2 a_3^{(2j)} + \alpha^2 a_2^{(2j)} = \alpha a_1^{(2j)} + \alpha a_4^{(2j)} \end{cases} \\ 5. \begin{cases} a_1^{(2j)} + a_0^{(2j)} = \alpha^2 a_2^{(2j)} + \alpha^2 a_4^{(2j)} \\ a_1^{(2j+1)} + a_0^{(2j+1)} = \alpha a_2^{(2j)} + \alpha a_4^{(2j)} \end{cases} \\ 6. \Longrightarrow \sum_{i=0}^{4} a_i^{(j)} = 0. \\ 7. \forall a_i^{(j)} \in \mathbb{F}_4. \end{cases}$$

3. Si $n = 7$

$$T_g = T_{g_0} \Longleftrightarrow \begin{cases} 1. a_6^{(j)} = a_i^{(j)} \ \forall j \ et \ 0 \leq i \leq 5 \\ 2. \sum_{i=0}^{6} a_6^{(j)} = a_i^{(j)} \ \forall j \\ 3. \forall a_i^{(j)} \in \mathbb{F}_3 \end{cases}$$

Preuve

1.$\mathbb{F} = \mathbb{F}_4$ et $n = 3$

$$x^3 - 1 = (x-1)(x+\alpha)\left(x+\alpha^2\right).$$

$$\sigma \in Aut_{\mathbb{F}}(A) : \sigma\left(\varepsilon^{(k)}\right) = \varepsilon^{\tau(k)}.$$

$$g_j = a_0^{(j)} + a_1^{(j)} x + a_2^{(j)} x^2.$$

$$\varepsilon^{(1)} g_j = a_0^{(j)} + a_1^{(j)} + a_2^{(j)}.$$

$$\begin{aligned} \varepsilon^{(2)} g_j &= a_0^{(j)} + \alpha a_1^{(j)} + \alpha^2 a_2^{(j)}. \\ \varepsilon^{(3)} g_j &= a_0^{(j)} + \alpha^2 a_1^{(j)} + \alpha a_2^{(j)} \end{aligned}$$

$$\varepsilon^{(1)} g = \varepsilon^{(1)} g_0 + z\ \varepsilon^{(2,3)} g_1 + z^2 \varepsilon^{(1)} g_2 + z^3 \varepsilon^{(2,3)} g_3 + ...$$

$$\varepsilon^{(2)} g = \varepsilon^{(2)} g_0 + z\ \varepsilon^{(1,3)} g_1 + z^2 \varepsilon^{(2)} g_2 + z^3 \varepsilon^{(1,3)} g_3 + ...$$

$$\varepsilon^{(3)} g = \varepsilon^{(3)} g_0 + z\ \varepsilon^{(1,2)} g_1 + z^2 \varepsilon^{(3)} g_2 + z^3 \varepsilon^{(1,2)} g_3 + ...$$

•$1^{ère}$**cas**

Si $T_{g_0} = \{1\}$ on a

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(1)} \left(g^{(2)} = 0\ \Lambda\ g^{(3)} = 0 \right) \\ &\Longleftrightarrow \begin{cases} \varepsilon^{(2)} g_{2j} = 0\ \Lambda\ \varepsilon^{(3)} g_{2j} = 0 \\ \varepsilon^{(1)} g_{2j+1} = 0\ \Lambda\ \varepsilon^{(3)} g_{2j+1} = 0 \end{cases} \\ &\Longleftrightarrow \begin{cases} a_0^{(2j)} = a_1^{(2j)} = a_2^{(2j)} \\ \Lambda \\ a_1^{(2j+1)} = \alpha a_0^{(2j+1)} = \alpha^2 a_2^{(2j+1)} \end{cases} \end{aligned}$$

•$2^{ème}$**cas**

Si $T_{g_0} = \{2\}$

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(2)} \left(g^{(1)} = 0 \ \Lambda \ g^{(3)} = 0 \right) \\ &\Longleftrightarrow \begin{cases} \varepsilon^{(1)} g_{2j} = 0 \ \Lambda \ \varepsilon^{(3)} g_{2j} = 0 \\ \varepsilon^{(2)} g_{2j+1} = 0 \ \Lambda \ \varepsilon^{(3)} g_{2j+1} = 0 \end{cases} \\ &\Longleftrightarrow \begin{cases} a_1^{(2j)} = \alpha a_0^{(2j)} = \alpha^2 a_2^{(2j)} \\ \Lambda \\ a_0^{(2j+1)} = a_1^{(2j+1)} = a_2^{(2j+1)} \end{cases} \end{aligned}$$

•$3^{ème}$**cas**

Si $T_{g_0} = \{3\}$

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(3)} \left(g^{(1)} = 0 \ \Lambda \ g^{(2)} = 0 \right) \\ &\Longleftrightarrow \begin{cases} \varepsilon^{(1)} g_{2j} = 0 \ \Lambda \ \varepsilon^{(2)} g_{2j} = 0 \\ \varepsilon^{(2)} g_{2j+1} = 0 \ \Lambda \ \varepsilon^{(3)} g_{2j+1} = 0 \end{cases} \\ &\Longleftrightarrow \begin{cases} a_1^{(2j)} = \alpha a_0^{(2j)} = \alpha^2 a_2^{(2j)} \\ \Lambda \\ a_0^{(2j+1)} = a_1^{(2j+1)} = a_2^{(2j+1)} \end{cases} \end{aligned}$$

•$4^{ème}$**cas**

Pour $T_{g_0} = \{1, 2\}$

$$\begin{aligned} T_g &= T_{g_0} \Longleftrightarrow g = g^{(1)} + g^{(1)} \left(g^{(2)} = 0 \right) \\ &\Longleftrightarrow \begin{cases} a_0^{(2j+1)} = \alpha a_3^{(2j+1)} + \alpha a_2^{(2j+1)} = \alpha^2 a_1^{(2j+1)} + \alpha^2 a_4^{(2j+1)} \\ a_0^{(2j)} = \alpha^2 a_3^{(2j)} + \alpha^2 a_2^{(2j)} = \alpha a_1^{(2j)} + \alpha a_4^{(2j)} \end{cases} \end{aligned}$$

2.$\mathbb{F} = \mathbb{F}_4$ et $n = 5$

$$x^5-1=(x-1)\left(x^2+\alpha x=1\right)\left(x^2+\alpha^2x+1\right)$$

$$\sigma\in Aut_{\mathbb{F}}(A):\sigma\left(\varepsilon^{(k)}\right)=\varepsilon^{\tau(k)}$$

$$\varepsilon^{(1)}g_j=a_0^{(j)}+a_1^{(j)}+a_2^{(j)}+a_3^{(j)}+a_4^{(j)}$$

$$\begin{aligned}
g_j &= a_0^{(j)}+a_1^{(j)}x+a_2^{(j)}x^2+a_3^{(j)}x^3+a_4^{(j)}x^4\\
\varepsilon^{(1)}g_j &= \sum_{i=0}^{4}a_i^{(j)}\\
\varepsilon^{(2)}g_j &= \left(a_1^{(j)}+\alpha a_2^{(j)}+\alpha a_3^{(j)}+a_4^{(j)}\right)x+a_0^{(j)}+a_2^{(j)}+\alpha a_3^{(j)}+\alpha a_2^{(j)}\\
\varepsilon^{(3)}g_j &= \left(a_1^{(j)}+\alpha^2 a_2^{(j)}+\alpha^2 a_3^{(j)}+a_4^{(j)}\right)x+a_0^{(j)}+a_2^{(j)}+\alpha^2 a_3^{(j)}+\alpha^2 a_2^{(j)}
\end{aligned}$$

•$1^{ère}$**cas**

Si $T_{g_0}=\{1\}$ on a

$$\begin{aligned}
T_g &= T_{g_0}\Longleftrightarrow g=g^{(1)}\left(g^{(2)}=0\ \Lambda\ g^{(3)}=0\right)\\
&\Longleftrightarrow \begin{cases}\varepsilon^{(2)}g_{2_j}\ \Lambda\ \varepsilon^{(3)}g_{2_j}\\ \varepsilon^{(3)}g_{2_{j+1}}\ \Lambda\ \varepsilon^{(2)}g_{2_{j+1}}\end{cases}\\
&\Longleftrightarrow a_0^{(j)}=a_1^{(j)}=a_2^{(j)}=a_3^{(j)}=a_4^{(j)}
\end{aligned}$$

•$2^{ème}$**cas**

Si $T_{g_0}=\{2\}$ on a

$$
\begin{aligned}
T_g \quad &= \quad T_{g_0} \Longleftrightarrow g = g^{(2)}\left(g^{(1)} = 0 \ \Lambda \ g^{(3)} = 0\right) \\
&\Longleftrightarrow \quad \begin{cases} \varepsilon^{(1)} g_{2_j} \ \Lambda \ \varepsilon^{(3)} g_{2_j} \\ \varepsilon^{(1)} g_{2_{j+1}} \ \Lambda \ \varepsilon^{(2)} g_{2_{j+1}} \end{cases} \\
&\Longleftrightarrow \quad \begin{cases} a_0^{(j)} + a_1^{(j)} + a_2^{(j)} + a_3^{(j)} + a_4^{(j)} = 0 \\ a_1^{(j)} + a_4^{(j)} \left[\left(\alpha^2 a_2^{(2j)} + \alpha^2 a_3^{(2j)}\right) \vee \left(\alpha a_2^{(2j+1)} + \alpha a_3^{(2j+1)}\right)\right] \\ a_1^{(j)} + a_0^{(j)} \left[\left(\alpha^2 a_2^{(2j)} + \alpha^2 a_4^{(2j)}\right) \vee \left(\alpha a_3^{(2j+1)} + \alpha a_4^{(2j+1)}\right)\right] \end{cases} \\
&\Longleftrightarrow \quad \begin{cases} a_0^{(2j)} = \alpha a_3^{(2j)} + \alpha a_2^{(2j)} = \alpha^2 a_1^{(2j)} + \alpha^2 a_4^{(2j)} \\ a_0^{(2j+1)} = \alpha^2 a_3^{(j)} + \alpha^2 a_2^{(j)} = \alpha a_1^{(j)} + \alpha a_4^{(j)} \end{cases}
\end{aligned}
$$

•$3^{ème}$**cas**

Si $T_{g_0} = \{3\}$ on a

$$
\begin{aligned}
T_g \quad &= \quad T_{g_0} \Longleftrightarrow g = g^{(3)}\left(g^{(1)} = 0 \ \Lambda \ g^{(2)} = 0\right) \\
&\Longleftrightarrow \quad \begin{cases} \varepsilon^{(1)} g_{2_j} = 0 \ \Lambda \ \varepsilon^{(2)} g_{2_j} = 0 \\ \varepsilon^{(1)} g_{2_{j+1}} = 0 \ \Lambda \ \varepsilon^{(3)} g_{2_{j+1}} = 0 \end{cases} \\
&\Longleftrightarrow \quad \begin{cases} a_0^{(j)} + a_1^{(j)} + a_2^{(j)} + a_3^{(j)} + a_4^{(j)} = 0 \\ a_1^{(j)} + a_4^{(j)} \left[\left(\alpha^2 a_2^{(2j+1)} + \alpha^2 a_3^{(2j+1)}\right) \vee \left(\alpha a_2^{(2j)} + \alpha a_3^{(2j)}\right)\right] \\ a_1^{(j)} + a_0^{(j)} \left[\left(\alpha^2 a_2^{(2j+1)} + \alpha^2 a_4^{(2j+1)}\right) \vee \left(\alpha a_3^{(2j)} + \alpha a_4^{(2j)}\right)\right] \end{cases} \\
&\Longleftrightarrow \quad \begin{cases} a_0^{(2j+1)} = \alpha a_3^{(2j+1)} + \alpha a_2^{(2j+1)} = \alpha^2 a_1^{(2j+1)} + \alpha^2 a_4^{(2j+1)} \\ a_0^{(2j)} = \alpha^2 a_3^{(2j)} + \alpha^2 a_2^{(2j)} = \alpha a_1^{(2j)} + \alpha a_4^{(2j)} \end{cases}
\end{aligned}
$$

•$4^{ème}$**cas**

Si $T_{g_0} = \{1, 2\}$ on a

$$T_g = T_{g_0} \Longleftrightarrow g = g^{(1)} + g^{(2)} \left(g^{(3)} = 0\right)$$
$$\Longleftrightarrow \varepsilon^{(3)} g_{2j} = 0 \ \Lambda \ \varepsilon^{(2)} g_{2j+1} = 0$$
$$\Longleftrightarrow \begin{cases} a_0^{(2j+1)} = \alpha a_3^{(2j+1)} + \alpha a_2^{(2j+1)} = \alpha^2 a_1^{(2j+1)} + \alpha^2 a_4^{(2j+1)} \\ a_0^{(2j)} = \alpha^2 a_3^{(2j)} + \alpha^2 a_2^{(2j)} = \alpha a_1^{(2j)} + \alpha a_4^{(2j)} \end{cases}$$

•$5^{ème}$cas

Pour $T_{g_0} = \{1, 3\}$ on a

$$\begin{aligned} T_g \quad &= \quad T_{g_0} \Longleftrightarrow g = g^{(1)} + g^{(3)} \left(g^{(2)} = 0\right) \\ &\Longleftrightarrow \quad \begin{cases} a_1^{(2j)} + a_0^{(2j)} = \alpha^2 a_2^{(2j)} + \alpha^2 a_4^{(2j)} \\ a_1^{(2j+1)} + a_0^{(2j+1)} = \alpha a_2^{(2j)} + \alpha a_4^{(2j)} \end{cases} \end{aligned}$$

•$6^{ème}$**cas**

Si $T_{g_0} = \{2, 3\}$ on a

$$\begin{aligned} T_g \quad &= \quad T_{g_0} \Longleftrightarrow g = g^{(2)} + g^{(3)} \left(g^{(1)} = 0\right) \\ &\Longleftrightarrow \quad \sum_{i=0}^{4} a_i^{(j)} = 0 \end{aligned}$$

•$7^{ème}$**cas**

Si $T_{g_0} = \{1, 2, 3\}$ on a

$$T_g = T_{g_0} \Longleftrightarrow g = g^{(1)} + g^{(2)} + g^{(3)} \ \forall a_i^{(j)} \in \mathbb{F}_4$$

3.$\mathbb{F} = \mathbb{F}_4$ et $n = 7$

$$x^7 - 1 = (x - 1)\left(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\right)$$

$$
\begin{aligned}
g_j &= a_0^{(j)} + a_1^{(j)} x + a_2^{(j)} x^2 + a_3^{(j)} x^3 + a_4^{(j)} x^4 + a_5^{(j)} x^5 + a_6^{(j)} x^5 \\
\varepsilon^{(1)} g_j &= \sum_{i=0}^{6} a_i^{(j)} \\
\varepsilon^{(2)} g_j &= \sum_{i=0}^{5} \left(a_6^{(j)} + a_i^{(j)} \right) x^i \\
\varepsilon^{(1)} g &= \varepsilon^{(1)} g_0 + z\, \varepsilon^{(1)} g_1 + z^2 \varepsilon^{(1)} g_2 + ... \\
\varepsilon^{(2)} g &= \varepsilon^{(2)} g_0 + z\, \varepsilon^{(2)} g_1 + z^2 \varepsilon^{(2)} g_2 + ...
\end{aligned}
$$

•$1^{ère}$**cas**

Si $T_{g_0} = \{1\}$ on a

$$
\begin{aligned}
T_g &= T_{g_0} \Longleftrightarrow g = g^{(1)} \left(g^{(2)} = 0 \right) \\
&\Longleftrightarrow a_6^{(j)} = a_i^{(j)} \forall i = 1, ..., 5
\end{aligned}
$$

•$2^{ème}$**cas**

Si $T_{g_0} = \{2\}$ on a

$$
\begin{aligned}
T_g &= T_{g_0} \Longleftrightarrow g = g^{(2)} \left(g^{(1)} = 0 \right) \\
&\Longleftrightarrow \sum_{i=0}^{6} a_0^{(j)} = 0
\end{aligned}
$$

•$3^{ème}$**cas**

Pour $T_{g_0} = \{1, 2\}$

$$
T_g = T_{g_0} \Longleftrightarrow g = g^{(2)} + g^{(1)} \forall a_i^{(j)} \in \mathbb{F}_4
$$

■

3.5 Les codes convolutionnels doublement cycliques

Etant donné un code convolutionnel cyclique C où $\tilde{P}(C) \subset A[z\,;\sigma]$.

Posons $E = \left\{\varepsilon^{(1)}, \varepsilon^{(2)}, ..., \varepsilon^{(r)}\right\}$.

Il est clair que $\sigma(E) = E$.

Si $\sigma = (\lambda_1, \lambda_2, \ldots, \lambda_r) \circ \tau$ pour une certaine permutation non triviale $\tau \in S_{r_1 \ldots r_s}$; alors il existe un sous-ensemble $S \subset E$ tel que $S \cap \sigma(S) = \phi$.

Soit S un tel sous-ensemble.Soit $b \in \mathbb{N}$ le plus grand nombre naturel satisfaisant :

$$S \cap \sigma^b(S) = \phi$$

Alors on a :

$$S \cap \sigma^j(S) = \phi \text{ pour tout } 1 \leq j \leq b$$

Lemme 86

D'après les hypothèses précédentes on a :

$$\sigma^i(S) \cap \sigma^j(S) = \phi \text{ pour tout } 0 \leq i < j \tag{3.10}$$

Preuve

Supposons qu'ils existent i et j $(i < j)$dans $[1, b]$ tels que $\sigma^i(S) \cap \sigma^j(S) \neq \phi$. Soit $\varepsilon^{(l)} \in \sigma^i(S) \cap \sigma^j(S)$; alors $\varepsilon^{(l)} = \sigma^i\left(\varepsilon^{(k)}\right) = \sigma^j\left(\varepsilon^{(k')}\right)$ où $\varepsilon^{(k)}$ et $\varepsilon^{(k')} \in S$. $\varepsilon^{(k)} = \sigma^{-i}\left(\varepsilon^{(l)}\right) = \sigma^{j-i}\left(\varepsilon^{(k')}\right) \in S \cap \sigma^{j-i}(S)$ ce qui contredit le choix de S. ■

Proposition 87

Soit $S \subset E$ défini comme précédemment et notons par :$l := |S|$.

Alors

1. $(b+1)\, l \leq r$.
2. $(b+1)\, l = r \Leftrightarrow E = \overset{b}{\underset{i=0}{\cup}} \sigma^i(S)$.

Preuve

1.Pour tout j dans $[1,b]$ on a :

$$\left|\sigma^{j}(S)\right| = l$$

et comme $\sigma^{i}(S) \cap \sigma^{j}(S) = \phi$ $0 \leq i < j$ alors :

$$\left|S \cup \sigma(S) \cup ... \cup \sigma^{b}(S)\right| = (b+1)\, l$$

Or $S \cup \sigma(S) \cup ... \cup \sigma^{b}(S) \subset E$ alors $(b+1)\, l \leq r$.

2.Si $(b+1)\, l = r$.alors $\left|S \cup \sigma(S) \cup ... \cup \sigma^{b}(S)\right| = r$.

Et comme $\sigma^{i}(S) \cap \sigma^{j}(S) = \phi$ pour tout $0 \leq i < j$ alors

$$|E| = \left|S \cup \sigma(S) \cup ... \cup \sigma^{b}(S)\right|$$

Donc

$$E = \overset{b}{\underset{i=0}{\cup}} \sigma^{i}(S)$$

Inversement si $E = \overset{b}{\underset{i=0}{\cup}} \sigma^{i}(S)$ alors $|E| = \left|\overset{b}{\underset{i=0}{\cup}} \sigma^{i}(S)\right|$

donc

$$r = (b+1)\, l$$

■

Remarque 88

$\{\sigma^{i}(S) : 1 \leq j \leq b\}$ *est une partition de* E.

Etant donné un code convolutionnel cyclique C où $\tilde{P}(C) \subset A[z\,;\sigma]$. Et $S \subset E$ tel que $S \cap \sigma(S) = \phi$.

Considérons le code linéaire (en bloc) cyclique engendré par le polynôme :

$$c := \sum_{\varepsilon^{(i)} \in S} \varepsilon^{(i)}$$

La matrice génératrice de ce code est :

$$\begin{pmatrix} c \\ xc \\ \vdots \\ x^{k-1}c \end{pmatrix}$$

où $k = \dim_{\mathbb{F}} \langle c \rangle$, $\left(k = \sum \deg \pi_i\right)$.

Soit la matrice $G := \sum_{\nu \geq 0}^{\varepsilon^{(i)} \in S} z^\nu G_\nu \in \mathbb{F}[z]^{k \times n}$ où

$$G_\nu := \begin{pmatrix} \tilde{P}^{-1}(\sigma^\nu(c)) \\ \tilde{P}^{-1}(\sigma^\nu(xc)) \\ \vdots \\ \tilde{P}^{-1}\left(\sigma^\nu\left(x^{k-1}c\right)\right) \end{pmatrix} \in \mathbb{F}[z]^{k \times n}$$

Posons

$$g := c\sum_{\nu \geq 0} z^\nu = \sum_{\nu \geq 0} z^\nu \sigma^\nu(c) \in A[z\,;\sigma] \tag{3.11}$$

Alors pour tout $i \in \mathbb{N}$ on a : $x^i *_\sigma g = \sum_{\nu \geq 0} z^\nu \sigma^\nu(x^i c)$.

Et

$$G = \begin{pmatrix} \tilde{P}^{-1}(g) \\ \tilde{P}^{-1}(x *_\sigma g) \\ \vdots \\ \tilde{P}^{-1}\left(x^{k-1} *_\sigma g\right) \end{pmatrix}$$

Théorème 89 [3]

Soit les hypothèses précedentes.le sous-module $C := imG$ est un code convolutionnel cyclique de paramètres $(n, k; km)$.

Lemme 90

On a : $C = \tilde{P}^{-1}\left(\dot{\langle g \rangle}\right)$

Définition 91

Avec les hypothèses précédentes ; le code $C := imG$ est dit code convolutionnel doublement cyclique.

Dans l'exemple suivant nous traitons un cas particulier où $\mathbb{F}_q = \mathbb{F}_2$ et $n = 7$.

Exemple 92

D'après l'exemple (57) ; on a

$$\begin{aligned} \varepsilon^{(1)} &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \\ \varepsilon^{(2)} &= 1 + x + x^2 + x^4 \\ \varepsilon^{(3)} &= 1 + x^2 + x^3 + x^4 \end{aligned}$$

donc $E = \left\{\varepsilon^{(1)}, \varepsilon^{(2)}, \varepsilon^{(3)}\right\}$. Prenons $S = \left\{\varepsilon^{(2)}\right\}$ et $\sigma(x) = x^5$. Sachant que

$$\begin{aligned} \sigma\left(\varepsilon^{(1)}\right) &= \varepsilon^{(1)} \\ \sigma\left(\varepsilon^{(2)}\right) &= \varepsilon^{(3)} \\ \sigma\left(\varepsilon^{(3)}\right) &= \varepsilon^{(2)} \end{aligned}$$

Alors $b = 1$. Le polynôme générateur du code binaire cyclique est

$$\begin{aligned} c &= \varepsilon^{(2)} \\ &= 1 + x^3 + x^5 + x^6 \end{aligned}$$

et sa matrice génératrice est

$$\begin{pmatrix} 1+x+x^2+x^4 \\ x+x^2+x^3+x^5 \end{pmatrix}$$

vu que $dim_{\mathbb{F}_2}\langle c\rangle = 2$. *Donc*

$$\begin{aligned} g &= c + z\ \sigma(c) \\ &= 1+x+x^2+x^4+z\ \left(1+x^2+x^3+x^4\right) \end{aligned}$$

Et comme

$$x^i *_\sigma g = \sum_{\nu\geq 0} z^\nu \sigma^\nu\left(x^i c\right)$$

on a :

$$\begin{aligned} x *_\sigma g &= xc + z\ \sigma(xc) \\ &= x+x^2+x^3+x^5+z\ \left(x+x^3+x^4+x^5\right) \end{aligned}$$

$$\begin{aligned} x^2 *_\sigma g &= x^2c + z\ \sigma\left(x^2c\right) \\ &= x^2+x^3+x^4+x^6+z\ \left(x+x^2+x^3+x^6\right) \end{aligned}$$

Donc la matrice génératrice du code convolutionnel doublement cyclique est :

$$G = \begin{pmatrix} 1+z & 1 & 1+z & z & 1+z & 0 & 0 \\ 0 & 1+z & 1 & 1+z & z & 1+z & 0 \\ 0 & 0 & 1+7 & 1 & 1+z & z & 1+z \end{pmatrix}$$

Dans ce qui suit ; nous présentons tous les codes convolutionnels doublement cycliques pour les cas $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$ avec $n \leq 9$ et avec un choix d'un automorphisme non trivial.

Pour $\mathbb{F}_2$ prenons $\sigma(x) = x^5$ donc d'après l'exemple précédent on a :

n	S	$\lvert S\rvert = l$
3	ϕ	0
5	ϕ	0
7	$\left\{\varepsilon^{(2)}\right\}$	1
9	ϕ	0

Alors la matrice du code convolutionnel doublement cyclique est (exemple précédent)

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

Pour $\mathbb{F}_3$ on a :

n	S	$\lvert S\rvert = l$
2	$\left\{\varepsilon^{(1)}\right\}$	1
4	$\left\{\varepsilon^{(1)}\right\}$	1
5	ϕ	0
7	ϕ	0

Pour $n = 2$ et avec $\sigma\left(\varepsilon^{(1)}\right) = \varepsilon^{(2)}$ ($\sigma(x) = x + 1$ par exemple) on obtient le code de matrice génératrice

$$G = \begin{pmatrix} 1+2z & 2+z \end{pmatrix}$$

Pour $n = 4$ et $\sigma\left(\varepsilon^{(1)}\right) = \varepsilon^{(2)}$ ($\sigma(x) = x^2 + 2x + 1$)
on obtient le code de matrice

$$G = \begin{pmatrix} 1+z & 1+2z & 1+z & 1+2z \end{pmatrix}$$

Pour $\mathbb{F}_4$

n	S	$\lvert S\rvert = l$
3	$\left\{\varepsilon^{(1)}\right\}$	1
5	$\left\{\varepsilon^{(2)}\right\}$	1
7	ϕ	0
9	$\left\{\varepsilon^{(2)}, \varepsilon^{(4)}\right\}$	2

Pour $n = 3$ et σ tel que : $\sigma\left(\varepsilon^{(1)}\right) = \varepsilon^{(2)}$, $\sigma\left(\varepsilon^{(2)}\right) = \varepsilon^{(3)}$ et $\sigma\left(\varepsilon^{(3)}\right) = \varepsilon^{(1)}$ ($\sigma(x) = \alpha^2 x$ par exemple) on obtient le code de matrice génératrice :

$$G = \begin{pmatrix} 1 + z + z^2 & 1 + \alpha^2 z + \alpha z^2 & 1 + \alpha z + \alpha^2 z^2 \end{pmatrix}$$

Pour $n = 5$ et $\sigma\left(\varepsilon^{(2)}\right) = \varepsilon^{(3)}$ ($\sigma(x) = x^3$) on obtient le code de matrice

$$G = \begin{pmatrix} 1+z & \alpha + \alpha^2 z & \alpha + \alpha^2 z & 1+z \\ 1+z & 1+z & \alpha + \alpha^2 z & \alpha + \alpha^2 z \end{pmatrix}$$

Pour $n = 9$ et $\sigma\left(\varepsilon^{(1)}\right) = \varepsilon^{(2)}$, $\sigma\left(\varepsilon^{(2)}\right) = \varepsilon^{(3)}$ et $\sigma\left(\varepsilon^{(4)}\right) = \varepsilon^{(5)}$ on obtient le code de matrice

$$G = \begin{pmatrix} 0 & \alpha + \alpha^2 z & \alpha^2 + \alpha z & 0 & \alpha + \alpha^2 z & \alpha^2 + \alpha z & \alpha z & \alpha + \alpha^2 z & \alpha^2 + \alpha z \\ \alpha^2 + \alpha z & 0 & \alpha + \alpha^2 z & \alpha^2 + \alpha z & 0 & \alpha + \alpha^2 z & \alpha^2 + \alpha z & \alpha z & \alpha + \alpha^2 z \\ \alpha + \alpha^2 z & \alpha^2 + \alpha z & 0 & \alpha + \alpha^2 z & \alpha^2 + \alpha z & 0 & \alpha + \alpha^2 z & \alpha^2 + \alpha z & \alpha z \\ \alpha z & \alpha + \alpha^2 z & \alpha^2 + \alpha z & 0 & \alpha + \alpha^2 z & \alpha^2 + \alpha z & 0 & \alpha + \alpha^2 z & \alpha^2 + \alpha z \end{pmatrix}$$

conclusion

L'objectif principal de ce travail est de construire exhaustivement les codes convolutionnels cyclique au sens de Piret.

Notre travail consiste à construire l'algèbre de Piret $A[z\ ;\sigma]$ tout en exibant les automorphismes de A ; soit le groupe $Aut_{\mathbb{F}}(A)$ et ceci après une présentation sur les codes convolutionnels et leurs différentes approches.

Selon les travaux de [2] ; ces codes sont caractérisés par l'égalité du support de générateur $g = \sum_{\nu=0}^{d} z^{\nu} g_{\nu}$ et de sa limite libre g_0. Ainsi pour les corps $\mathbb{F}_2$, $\mathbb{F}_3$ et $\mathbb{F}_4$ nous avons donné tous les générateurs des codes convolutionnels de longueur allant de 1 à 7.

Ces générateurs peuvent donner donner des informations sur une autre classe de codes convolutionnels dits doublement cyclique.

Une question naturelles se concernant la cyclicité de type t ($t = 3, 4...$). Si le support du générateur caractérise la cyclicité du code ; qui prend le relai pour la cyclicité de type t ?

Bibliographie

[1] GHECHAMI NAANAA . *Etude comparative des codes classiques* . Thèse de magister l'université de batna ,**2001** .

[2] H.GLUSING-LUERSSEN et W.SCHMALE .*On cyclic convolutionnal codes.*Acta applicatae Mathemacae ,**2004**.

[3] H.GLUSING-LUERSSEN et W.SCHMALE .*On Doubly- cyclic convolutionnal codes.*Preprint **2004**.Submitted.

[4] H.GLUSING-LUERSSEN et B.LANGFELD. *On the algebric parametres of the convolutionnal codes with structure.*Preprint **2003**.Accepted for publication in journal of algebra and its application.

[5] H.GLUSING-LUERSSEN et W.SCHMALE.*Distance bounds for convolutionnal codes and some optimal codes* .Preprint **2003**.

[6] H.GLUSING-LUERSSEN et W.SCHMALE, M.STRIHA.*Some small cyclic convolutional codes.*Department of Mathematics University of Oldenburg

[7] H.GLUSING-LUERSSEN ,LANGFELD.*A class of one-dimensional MDS convolutionnal codes.* Journal of algebra and its application **2006**.

[8] H.GLUSING-LUERSSEN.*On the Weight Distibution of convolutional codes* .arXiv :cs.IT/0501016v1.10 Jan 2005.

[9] H.GLUSING-LUERSSEN et G.SCHNEDER.*State space Realzations and Monomial Equivalence for Convolutional Codes.*arXiv :IT/0603049v1.13 Mar 2006.

[10] H.GLUSING-LUERSSEN et G.SCHNEDER.*On the Mac Williams Identity for convolutional codes*.arXiv :IT/0603013v1.2 Mar 2006..

[11] R.LIDL et G.PILZ.Applied Abstract Algebra.Springer (1991).

[12] R.J.MCELIEC. *the theory of information and coding* .Cambridge University Pres, Amsterdam, 1998.

[13] N.C.AMANI.*Quantum convolutional stabizer codes* Thèse de Master de science.Texas University. May 2004.

[14] G.NEBE,E.M.RIAINS,NJA.SLOANE.*Self-dual codes and invariants*.Springer-Verelag, Berlin.Heidelberg 2006.

[15] G. M. RAINS et NJASLOANE,*Self-dual in HANDBOOK OF CODING THEOR*, V.Pless and W.C. Huffmaned, Elserdam, Amsterdam.1998.