Les Codes Cycliques et la Correction

M. Belkasmi

ENSIAS 2013-2014

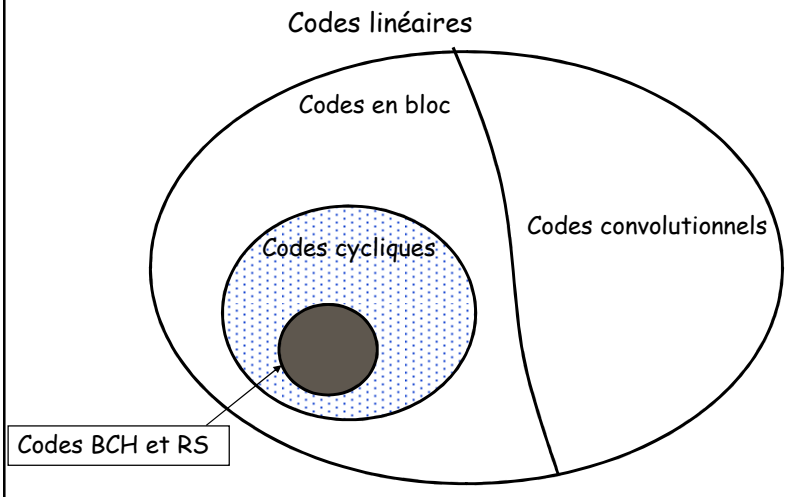
PLAN

Introduction

- Codes BCH et RS
  - Codes BCH conçus par Bose, Chaudhuri (1960) et Hocquenghem (1959)
  - Codes RS conçus par Reed et Solomon
  - Codes Cycliques
  - C'est des codes équivalents aux codes de Hamming quand on veut corriger une erreur simple
  - Capacité de correction d'erreurs multiples
  - Codage et décodage assez simples

p3.

Introduction



p4.

Conception de codes

- Méthode de Construction

  Pour un code BCH ou RS

  → spécifier la capacité de correction (t=(d-1)/2) la longueur n et l'alphabet du code

  → construire le polynôme générateur du code

p5.

Conception de codes

- Un code cyclique (n, k) est un code linéaire (n, k) tel que toute permutation circulaire d'un mot du code est encore un mot du code.
- Le générateur d'un code cyclique divise le polynôme X^n-1.

  si $X^n-1 = g(X)h(X)$ alors $h(X)$ est dit polynôme de parité du code

  → Avant la construction de code

  bien caractériser les diviseurs de X^n-1.

- On désire un code avec un alphabet A = GF(q)

p6.

Conception de codes

- [Def] un élément primitif de GF(q^m) est un élément α t.q. pour tout $\beta \in$ GF(q^m) $\neq 0$, $\beta = \alpha^i$ pour un certain i.

- [Def] un polynôme primitif p(x) sur GF(q) est un irréductible ayant la propriété suivante :

  Dans le corps d'extension GF(q^m) construit modulo p(x), l'élément α (racine de p(x)) est un élément primitif.

p7.

Méthode d'extension :

- Corps d'extension GF(q^m)
  - —Poly. irréductible

$$p(x) = x^m + p_{m-1}x^{m-1} + \ldots + p_1 x^1 + p_0 \ , p_i \in GF(q)$$

  - —Elément (a_{m-1}, …, a_1, a_0)

$$A(x) = a_{m-1}x^{m-1} + \ldots + a_1 x^1 + a_0 \ , a_i \in GF(q)$$

  - —Souscorps : GF(q)
  - —Degré d'extension : m

p8.

Conception de codes

- Théorème :

  Soient $\beta_1, \beta_2, \ldots \beta_{q^m-1}$, représentants les éléments non nuls du corps GF(q^m) :

  Alors $x^{q^m-1} - 1 = (x - \beta_1)(x - \beta_2)\ldots(x - \beta_{q^m-1})$

  ➔ pour un élément quelconque γ de GF(q^m) : $\gamma^{q^m} = \gamma$

p9.

Conception de codes

- Pour construire des codes cycliques il faut trouver des poly. générateurs :
  - Factoriser $x^n - 1 = f_1(x)\, f_2(x) \ldots f_p(x)$
  - $f_i(x)$ irréductible sur GF(q)
  - Toute combinaison de $f_i(x)$ donne naissance à un générateur $g(x)$

p10.

Conception de codes

- GF(q^m) est un corps d'extension de GF(q).
  Si on choisi comme longueur $n = q^m-1$

$$x^n - 1 = x^{q^m-1} - 1 = f_1(x)\, f_2(x) \ldots f_p(x) = \prod_j (x - \beta_j)$$

→ Trouver l'expression des $f_k(x)$?

→ polynôme minimal

p11.

Polynôme Minimal

- On se fixe un élément β_j et un corps d'extension GF(q^m) :

- [Def] Le poly. de plus petit degré ayant des coefficients dans le corps de base GF(q) qui a β_j comme zéro dans le corps d'extension GF(q^m) est dit poly. minimal de β_j

p12.

Eléments conjugués

- [Def] Deux éléments de GF(q^m) qui possèdent le même poly. minimal sur GF(q) sont dit éléments conjugués :
- Si f(x) est le poly. minimal de β , alors il est aussi le poly. minimal des éléments de l'ensemble $\{\beta, \beta^q, \beta^{q\hat{}2}, \ldots \beta^{q\hat{}(s-1)}\}$ avec s le plus petit entier i/ $\beta^{q\hat{}i} = \beta$.
- classe cyclotomique de i : $\{i, i.q, i.q^2, \ldots, i.q^{(s-1)}\}$

p13.

Exemple : Poly. Minimaux des éléments de GF(2^4).

$p(z) = z^4 + z + 1$ polynôme primitif avec α une racine

Notation Exponentielle	Notation Polynomiale	Notation Linéaire	Polynôme Minimal
0	0	0000	x
α^0	1	0001	$x + 1$
α^1	α	0010	$x^4 + x + 1$
α^2	α^2	0100	$x^4 + x + 1$
α^3	α^3	1000	$x^4 + x^3 + x^2 + x + 1$
α^4	$\alpha + 1$	0011	$x^4 + x + 1$
α^5	$\alpha^2 + \alpha$	0110	$x^2 + x + 1$
α^6	$\alpha^3 + \alpha^2$	1100	$x^4 + x^3 + x^2 + x + 1$
α^7	$\alpha^3 + \alpha + 1$	1011	$x^4 + x^3 + 1$
α^8	$\alpha^2 + 1$	0101	$x^4 + x + 1$
α^9	$\alpha^3 + \alpha$	1010	$x^4 + x^3 + x^2 + x + 1$
α^{10}	$\alpha^2 + \alpha + 1$	0111	$x^2 + x + 1$
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110	$x^4 + x^3 + 1$
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111	$x^4 + x^3 + x^2 + x + 1$
α^{13}	$\alpha^3 + \alpha^2 + 1$	1101	$x^4 + x^3 + 1$
α^{14}	$\alpha^3 + 1$	1001	$x^4 + x^3 + 1$

p14.

Exemple suite

- Factoriser $X^{15}-1$ sur GF(2) donnera :

$$x^{15}-1 = x^{2^m-1}-1 = f_1(x)\,f_2(x)\ldots f_5(x)$$
$$= (x+1)(x^4+x+1)(x^4+x^3+1)$$
$$(x^4+x^3+x^2+x+1)(x^2+x+1)$$

- 5 classes de conjugaison et donc 5 polynômes minimaux

p15.

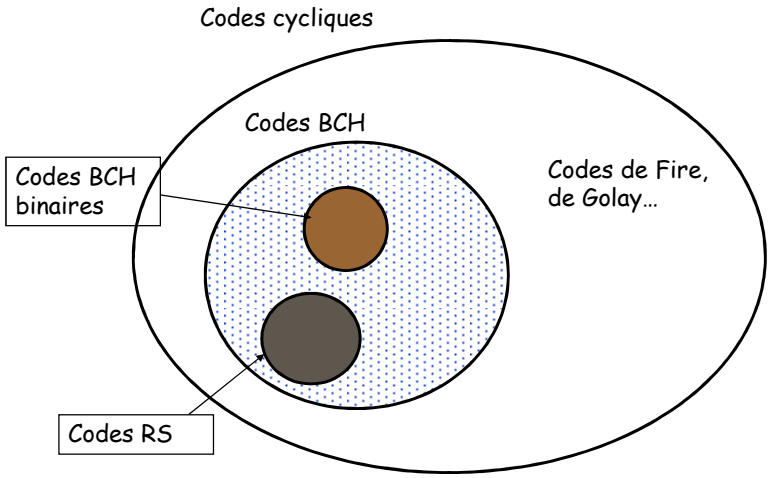
Définition de Codes BCH

- Générateur de BCH en terme de poly. minimaux
  - Trouver le générateur d'un code BCH t-correcteur et ayant une longueur de code $n = q^m-1$ avec un alphabet A = GF(q) :
    - (i) Choisir un polynôme primitif p(x) de degré m et α une racine de p(x)
    - (ii) Construire ainsi la table du corps GF(q^m)
    - (iii) Trouver $f_i(x)$, le poly. minimal de α^i pour $1 =< i =< 2t$
    - (iv) Le poly. générateur du code corrigeant t erreurs est

$$g(x) = \text{PPCM}[f_1(x), f_2(x),\ldots, f_{2t}(x)]$$

p16.

Classes de codes BCH



p17.

Classes de codes BCH

- Codes BCH binaire t-correcteur :
  - Alphabet A =GF(2) (cad q=2)
  - Longueur n= 2^m-1
  - Nb de bits de parité r = n-k ≤ mt
  - Distance dmin ≥ 2t+1
- Codes RS t-correcteur :
  - Codes BCH particuliers où l'alphabet A= GF(q) et m=1
  - si q=2^b on manipule des symboles sur b bits
  - Longueur n = q-1 = 2^b-1
  - Nb de symboles de parité r = n-k =2t
  - Distance dmin = 2t+1

p18.

Exemple de codes BCH

- code BCH binaire : m=4 et t=2 ---> n= 15 et t= 2
- le générateur

$g(x) = PPCM[f_1(x), f_2(x), f_3(x), f_4(x)]$

$= (X^4 + X+1)(X^4+X^3+ X^2 +X +1)$

$= X^8+X^7+X^6+X^4+1$

On obtient ainsi un code BCH (15,7,5)
2-correcteur

p19.

TABLE de codes BCH binaires avec des longueurs plus petites à 511

m	n	k	t	m	n	k	t	m	n	k	t	n	k	t	n	k	t
3	7	4	1		63	24	7		127	50	13	255	187	9	255	71	29
4	15	11	1			18	10			43	14		179	10		63	30
		7	2			16	11			36	15		171	11		55	31
		5	3			10	13			29	21		163	12		47	42
5	31	26	1			7	15			22	23		155	13		45	43
		21	2	7	127	120	1			15	27		147	14		37	45
		16	3			113	2			8	31		139	15		29	47
		11	5			106	3	8	255	247	1		131	18		21	55
		6	7			99	4			239	2		123	19		13	59
6	63	57	1			92	5			231	3		115	21		9	63
		51	2			85	6			223	4		107	22	511	502	1
		45	3			78	7			215	5		99	23		493	2
		39	4			71	9			207	6		91	25		484	3
		36	5			64	10			199	7		87	26		475	4
		30	6			57	11			191	8		79	27		…..	

p20.

Codes de Reed-Solomon

- Est une importante sous classe des codes BCH
- Beaucoup d'applications :
  - Support d'enregistrement (BM, CD, DVD…)
  - Communication mobile (réseau CPDP, Wimax)
  - Modems high speed (ADSL, xDSL…)
  - Spatial : RS + convolutionnel
  - DVB

p21.

Codes de Reed-Solomon

- Pour les codes RS
  - Alphabet est le corps $GF(q^m)=GF(q)=GF(2^b)$ tout entier

    ie. $m=1$, $n=q^m-1=q-1$
  - Le poly. min. d'un élément β est $f_\beta(x)= x-\beta$
  - Le générateur d'un code RS t-correcteur est de la forme

    $g(x)= (x-\alpha)\ (x-\alpha^2)\ \ldots(x-\alpha^{2t-1})\ (x-\alpha^{2t})$
  - $\deg(g(x))=2t$, et $n-k=2t$

p22.

Exemple 1

On Considère un code RS 2-correcteur de longueur 15 sur GF(16)

- le corps d' extension GF(16) de GF(2) à partir de $p(z)=z^4+z+1$
- comme t=2

$g(x)= (x-\alpha^1)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$

$= x^4+(\alpha^3+\alpha^2+1)\,x^3+(\alpha^3+\alpha^2)\,x^2+\alpha^3 x+(\alpha^2+\alpha+1)$

$= x^4+\alpha^{13}\,x^3+\alpha^6\,x^2+\alpha^3\,x+\alpha^{10}$

- n-k=4 → k=11

On obtient ainsi un code RS (15,11,5) sur GF(16)

p23.

Exemple 2

On Considère un code RS 3-correcteur de longueur 15 sur GF(16)

comme t=3

$g(x) = (x-\alpha^1)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)$

$= x^6 + \alpha^{10}x^5+ \alpha^{14}x^4+ \alpha^4x^3 + \alpha^6x^2+ \alpha^9x + \alpha^6$

n-k=6 → k=9

On obtient ainsi un code RS (15,9,7) sur GF(16)

p24.

Décodage de codes BCH

On considère un code BCH de longueur $n = q^m-1$ et corrigeant t erreurs ayant un alphabet A=GF(q).

- On note le poly. erreur :

  $e(x) = e_{n-1}x^{n-1} + e_{n-2}x^{n-2} + \ldots + e_1x^1 + e_0$

  où au plus t coefficients sont non nuls

- On suppose qu'il y a eu ν erreurs ($1 \leq \nu \leq t$) dans les positions $i_1, i_2, \ldots i_\nu$ et ainsi :

$$e(x) = e_{i_1} x^{i_1} + e_{i_2} x^{i_2} + \ldots + e_{i_\nu} x^{i_\nu}$$

p25.

Décodage de codes BCH

- Pour la correction, on doit connaître deux choses
  - Où les erreurs se sont apparues (→ les positions)
  - Quelles sont les amplitudes de ces erreurs

Désignons par v(x) le polynôme reçu
c(x) le polynôme émis

→ $\boxed{v(x) = c(x) + e(x)}$ à résoudre

p26.

Décodage de codes BCH

- On a supposé

$$e(x) = e_{i_1} x^{i_1} + e_{i_2} x^{i_2} + \ldots + e_{i_\nu} x^{i_\nu}$$

Le nombre, les positions et les amplitudes sont inconnues

- Posons :
  - $Y_j = e_{i_j}$ amplitude de l'erreur j ($1 \leq j \leq \nu$)
  - $X_j = \alpha^{i_j}$ position de l'erreur j ($1 \leq j \leq \nu$)

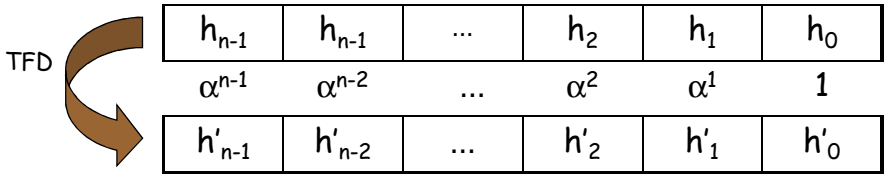
p27.

Décodage de codes BCH

- Pour représenter un polynôme

$$h(x) = h_{n-1}x^{n-1} + h_{n-2}x^{n-2} + \ldots + h_1x^1 + h_0$$

Deux espaces de représentation :



p28.

Décodage de codes BCH

- On commence par un calcul du Syndrome

$S_1 = v(\alpha) = c(\alpha) + e(\alpha) = a(\alpha)g(\alpha) + e(\alpha) = e(\alpha)$

$$e(\alpha) = e_{i_1}\alpha^{i_1} + e_{i_2}\alpha^{i_2} + \ldots + e_{i_v}\alpha^{i_v}$$

alors $S_1 = Y_1X_1 + Y_2X_2 + \ldots + Y_v X_v$

De même on trouve

$S_2 = v(\alpha^2) = Y_1X_1^2 + Y_2X_2^2 + \ldots + Y_v X_v^2$

p29.

Décodage de codes BCH

- Pour $\alpha, \alpha^2, \ldots, \alpha^{2t}$

(1)
$S_1 = v(\alpha) = Y_1X_1 + Y_2X_2 + \ldots + Y_vX_v$ $\quad Y_j \in GF(q)$
$S_2 = v(\alpha^2) = Y_1X_1^2 + Y_2X_2^2 + \ldots + Y_vX_v^2$ $\quad X_j \in GF(q^m)$
…
$S_{2t} = v(\alpha^{2t}) = Y_1X_1^{2t} + Y_2X_2^{2t} + \ldots + Y_vX_v^{2t}$

- Toute méthode permettant de résoudre ce système est un décodage de codes BCH :

  → Algorithme de Peterson-Gorenstein-Zierler
  → Algorithme de Berlekamp Massey
  → Algorithme d'Euclide etendu

p30.

Décodeur de Peterson-Gorenstein-Zierler

- On définit le poly. Localisateur d'erreur:

$$\Lambda(x) = (1-X_1x)\,(1-X_2x)\ldots(1-X_vx)$$
$$= \Lambda_v x^v + \Lambda_{v-1}x^{v-1} + \ldots + \Lambda_1 x + 1 \qquad (2)$$

- Si on connaît les coefficients Λ_j de $\Lambda(x)$ on peut trouver les zéros de $\Lambda(x)$ pour en déduire les positions X_i :

$$\{S_i\} \quad \leftrightarrow \quad \{\Lambda j\}$$
$$1 \le i \le 2t \qquad 1 \le j \le v$$

Décodeur de Peterson-Gorenstein-Zierler

- En utilisant les relations (1) et (2) on trouve :

$$\begin{cases} \Lambda_1 S_v + \Lambda_2 S_{v-1} + \ldots + \Lambda_v S_1 + S_{v+1} = 0 \\ \Lambda_1 S_{v+1} + \Lambda_2 S_v + \ldots + \Lambda_v S_2 + S_{v+2} = 0 \\ \quad \ldots \\ \Lambda_1 S_{2v-1} + \Lambda_2 S_{2v-2} + \ldots + \Lambda_v S_v + S_{2v} = 0 \end{cases}$$

- Ou bien :

$$\begin{bmatrix} S_1 & S_2 & \ldots & S_v \\ S_2 & S_3 & \ldots & S_{v+1} \\ \vdots & & & \\ S_v & S_{v+1} & \ldots & S_{2v-1} \end{bmatrix} \begin{bmatrix} \Lambda_v \\ \Lambda_{v-1} \\ \vdots \\ \Lambda_1 \end{bmatrix} = \begin{bmatrix} -S_{v+1} \\ -S_{v+2} \\ \vdots \\ -S_{2v} \end{bmatrix}$$

Décodeur de Peterson-Gorenstein-Zierler

Théorème : La matrice des syndromes M est non singulière si u est égale à ν (le nombre d'erreurs qui se sont produit réellement). La matrice est singulière si u > ν.

$$M = \begin{bmatrix} S_1 & S_2 & . & . & . & S_u \\ S_2 & S_3 & . & . & . & S_{u+1} \\ . & . & & & & . \\ . & . & & & & . \\ . & . & & & & . \\ S_u & S_{u+!} & . & . & . & S_{2u-1} \end{bmatrix}$$

⟶ Idée : Tester la singularité de la matrice M à partir de u=t on s'arrête quand on tombe sur une matrice non singulière.

p33.

Synthèse du décodage

- Etapes du décodage de codes BCH
  - (1) Fixer ν =t, calculer le déterminant de la matrice syndrome M,

    Si det(M)=0, fixer ν =t-1, répéter jusqu'à ce que det(M)≠0
  - (2) Inverser M et en déduire le localisateur $\Lambda(x)$
  - (3) Résoudre $\Lambda(x)$=0 pour déterminer les positions X_1, X_2,…
  - (4) Déterminer les amplitudes Y_j des erreurs

p34.

Synthèse du décodage

(4) Si le code est non binaire, résoudre le système d'équations avec Y_j comme inconnues:

$$\begin{cases} S_1 = v(\alpha) = Y_1X_1 + Y_2X_2 + \dots + Y_vX_v \\ S_2 = v(\alpha^2) = Y_1X_1^2 + Y_2X_2^2 + \dots + Y_vX_v^2 \\ \dots \\ S_{2t} = v(\alpha^{2t}) = Y_1X_1^{2t} + Y_2X_2^{2t} + \dots + Y_vX_v^{2t} \end{cases}$$

Exemple 1

Soit le code BCH(15,5) binaire 3-correcteur.

$g(X) = X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1$

On considère le polynôme reçu suivant

$v(X) = X^7 + X^2$

Dans GF(2^4)

$S_1 = \alpha^7 + \alpha^2 = \alpha^{12}$
$S_2 = \alpha^{14} + \alpha^4 = \alpha^9$
$S_3 = \alpha^{21} + \alpha^6 = 0$
$S_4 = \alpha^{28} + \alpha^8 = \alpha^3$
$S_5 = \alpha^{35} + \alpha^{10} = \alpha^0$
$S_6 = \alpha^{42} + \alpha^{12} = 0$

Posons $v = 3 \quad M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^{12} & \alpha^{9} & 0 \\ \alpha^{9} & 0 & \alpha^{3} \\ 0 & \alpha^{3} & 1 \end{bmatrix} \quad \det(M) = 0$

$v = 2 \quad M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \begin{bmatrix} \alpha^{12} & \alpha^{9} \\ \alpha^{9} & 0 \end{bmatrix} \quad \det(M) \neq 0$

$M^{-1} = \begin{bmatrix} 0 & \alpha^{6} \\ \alpha^{6} & \alpha^{9} \end{bmatrix}$

$\therefore \begin{bmatrix} \Lambda_2 \\ \Lambda_1 \end{bmatrix} = M^{-1} \bullet \begin{bmatrix} 0 \\ \alpha^{3} \end{bmatrix} = \begin{bmatrix} \alpha^{9} \\ \alpha^{12} \end{bmatrix}$

$\therefore \Lambda(X) = 1 + \alpha^{12} x + \alpha^{9} x^2$

$= (1 + \alpha^{2} x)(1 + \alpha^{7} x)$

$= \alpha^{9} (x - \alpha^{8})(x - \alpha^{13})$

$\frac{1}{\alpha^{8}} = \alpha^{7}$

$\frac{1}{\alpha^{13}} = \alpha^{2}$

$\therefore e(X) = X^{7} + X^{2}$

p37.

Exemple 2

Soit le code RS(15,9,7) 3-correcteur.

$$g(X) = x^6 + \alpha^{10}x^5 + \alpha^{14}x^4 + \alpha^4x^3 + \alpha^6x^2 + \alpha^9x + \alpha^6$$

C'est un code avec un alphabet A= GF(16)

On transmet c(x) = 0

On reçoit le polynôme suivant

$$r(x) = \alpha x^{14} + \alpha^2 x^{12} + \alpha^{13} x^4$$

p38.

Exemple 2

$$r(x) = \alpha x^{14} + \alpha^2 x^{12} + \alpha^{13} x^4$$

$$\begin{aligned} S_1 = r(x=\alpha) &= \alpha(\alpha^{14}) + \alpha^2(\alpha^{12}) + \alpha^{13}(\alpha^4) \\ &= \alpha^{1+14} + \alpha^{2+12} + \alpha^{13+4} \\ &= 1 + \alpha^3 + 1 + \alpha^2 \\ &= \alpha^3 + \alpha^2 = \alpha^6 \end{aligned}$$

$$S_2 = r(x=\alpha^2) = \alpha\left((\alpha^2)^{14}\right) + \alpha^2\left((\alpha^2)^{12}\right) + \alpha^7\left((\alpha^2)^4\right) = \alpha^7$$

$$S_3 = r(x=\alpha^3) = \alpha\left((\alpha^3)^{14}\right) + \alpha^2\left((\alpha^3)^{12}\right) + \alpha^7\left((\alpha^3)^4\right) = \alpha^{12}$$

$$S_4 = r(x=\alpha^4) = \alpha\left((\alpha^4)^{14}\right) + \alpha^2\left((\alpha^4)^{12}\right) + \alpha^7\left((\alpha^4)^4\right) = 0$$

$$S_5 = r(x=\alpha^5) = \alpha\left((\alpha^5)^{14}\right) + \alpha^2\left((\alpha^5)^{12}\right) + \alpha^7\left((\alpha^5)^4\right) = \alpha$$

$$S_6 = r(x=\alpha^6) = \alpha\left((\alpha^6)^{14}\right) + \alpha^2\left((\alpha^6)^{12}\right) + \alpha^7\left((\alpha^6)^4\right) = \alpha^8$$

p39.

Exemple 2

Fixons v=3 on a alors :

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^6 & \alpha^7 & \alpha^{12} \\ \alpha^7 & \alpha^{12} & 0 \\ \alpha^{12} & 0 & \alpha \end{bmatrix}$$

On obtient alors le polynôme local. suivant

$\Lambda(X) = X^3 + \alpha^2 X^2 + \alpha^8 X + 1$

Vérifier que les inverses des positions sont les racines de ce polynôme et trouver les amplitudes des erreurs

p40.

Exemple 3

- Le code BCH binaire 3-Correcteur
- Mot reçu :

$$v(X) = X^7 + X^5 + X^2$$

Les Syndromes ?

p41.

Exemple 3

- Syndromes :
  - $S_1 = \alpha^{14}$
  - $S2 = \alpha^{13}$
  - $S3 = 1$
  - $S4 = \alpha^{11}$
  - $S5 = \alpha^{5}$
  - $S6 = 1$
- *Le polynome localisateur :*
- $\Lambda(x) = 1 + \alpha^{14}x + \alpha^{11}x^2 + \alpha^{14}x^3$
- $= (1 + \alpha^{7}x)(1 + a^{5}x)(1 + \alpha^{2}x)$

- *Verifier que les racines donnent bien les positions des erreurs*

p42.