Chapitre 4 Décodage des codes cycliques.

4.1 Introduction

Les méthodes de décodage des codes cycliques peuvent être classées en deux grandes catégories : les méthodes à base de syndromes et les méthodes à base d'algorithmes de recherche. Les méthodes à base de syndromes exploitent les syndromes, qui sont des indicateurs de l'existence et de la localisation d'erreurs dans le message reçu. Les syndromes sont obtenus en comparant le message reçu avec les motifs cycliques prédéfinis. Les méthodes à base d'algorithmes de décodage tels que l'algorithme de Meggitt, l'algorithme de piégeage d'erreurs, l'algorithme de Transformation de Fourier Discrète et l'algorithme de Peterson-Gorenstein-Zierler sont utilisés pour déterminer les erreurs et les localiser dans le message, permettant ainsi leur correction.

En résumé, les méthodes de décodage des codes cycliques jouent un rôle crucial dans la garantie de la fiabilité des données transmises et stockées. Elles utilisent des techniques mathématiques avancées pour détecter et corriger les erreurs, améliorant ainsi les performances des systèmes de communication et de stockage. Que ce soit en utilisant des méthodes basées sur les syndromes ou des algorithmes de recherche, le décodage des codes cycliques demeure un domaine de recherche essentiel pour assurer l'intégrité des données dans un large éventail d'applications technologiques.

4.2 Décodage par syndrome polynômial.

Soit le code cyclique $C(n,k,d)$ sur le corps $\mathbb{F}_q = \mathbb{F}_{p^r}$, corps des racines *nièmes* de l'unité sur $\mathbb{F}_p$, de polynôme générateur $g(X)$ avec $\deg(g(X)) = t$. Soit e la capacité de C et $y(X) \in \mathbb{F}_q[X]/< X^n - 1 >$. On dit que $y(X)$ est un mot reçu dont l'erreur est $\varepsilon(X)$, si $\omega(\varepsilon(X)) \leq e$ et s'il existe $c(X) \in C$ tel que $y(X) = c(X) + \varepsilon(X)$.

4.2.1 Syndrome polynômial.

Définition 4.1.

On appelle **syndrome polynômial** (ou **syndrome**) d'un mot $y(X) \in \mathbb{F}_q[X]/< X^n - 1 >$, qu'on note $S\big(y(X)\big)$, le reste de la division Euclidienne de $y(X)$ par $g(X)$ dans $\mathbb{F}_q[X]$.

Proposition 4.1.

Soit un mot $y(X) \in \mathbb{F}_q[X]/< X^n - 1 >$ alors $y(X) \in C$ si et seulement si $g(X)$ divise $y(X)$ dans $\mathbb{F}_q[X]$ c.à.d. $y(X) \in \theta(C) \Leftrightarrow S(y(X)) = 0$.

Preuve. Soit $y(X) \in \theta(C) \Leftrightarrow \exists\, y(X) \in \mathbb{F}_q[X] : y(X) = q(X)g(X)$

$\Leftrightarrow$ le reste de la division Euclidienne de $y(X)$ par $g(X)$=0

$\Leftrightarrow S(y(X)) = 0.$

Définition 4.2.

Un **registre à décalage** est une chaines d'éléments de mémoire. Un **décalage linéaire** transfère le contenu de chacune des cellules vers la cellule qui la suit immédiatement. Après un décalage le contenu de la première cellule est zéro.

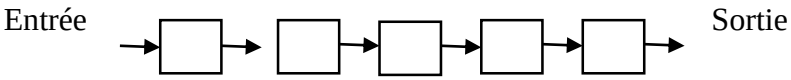

Fig 4.1 registre à décalage linéaire

Par convention les décalages s'effectuent de la gauche à la droite.

Dans la pratique, les calculs dans $\mathbb{F}_q[X]$, en particulier les divisions , s'effectuent au moyen de **registres à décalages circulaire** comme dans le schéma suivant qui représente un circuit à décalage circulaire de la divisions Euclidienne d'un polynôme $y(X) = \sum_{i=0}^{n} y_i X^i$ par un polynôme $g(X) = \sum_{i=0}^{t} g_i X^i$:

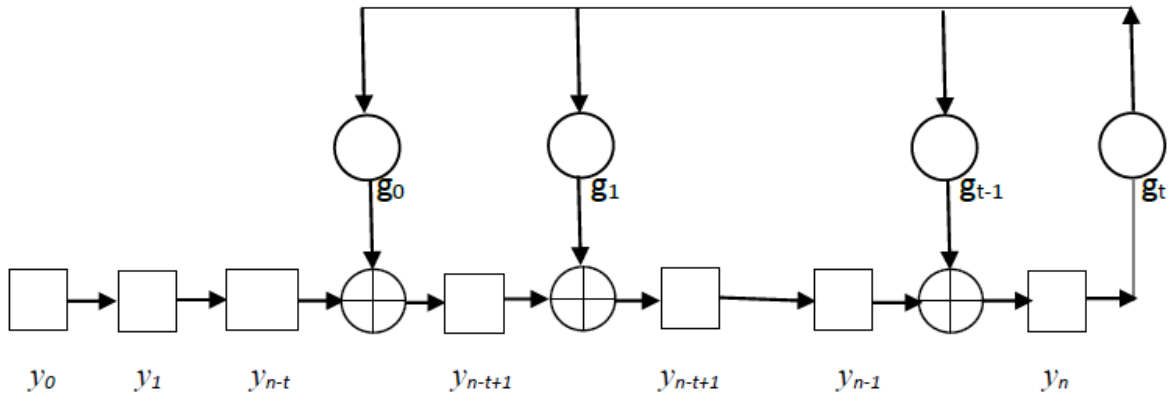

Fig 4.2 Circuit à décalage circulaire de la divisions Euclidienne.

Un bref aperçu sur les registres voir l'annexe (Appendice page 123).

4.2.2 Algorithme de décodage par la méthode de syndrome polynomial.

Soit $C(n,k,d)$un code cyclique sur $\mathbb{F}_q^n$ avec une capacité de correction égale à e. Si $y(X)$ est le mot reçu, alors l'algorithme de décodage est le suivant :

- Calcul du syndrome du mot reçu $S(y(X))$ avec un registre à décalage circulaire.
- Trouver l'erreur $\varepsilon(X)$ qui correspond au syndrome $S(y(X))$ et de poids $w(\varepsilon(X)) \leq e$.
- Soustraction de l'erreur au mot reçu, le mot envoyé est $c(X) = y(X) - \varepsilon(X)$.

Exemple 4.1.

Soit le code cyclique $C(7,4)$ sur $\mathbb{F}_2$ de polynôme générateur $g(X) = X^3 + X^2 + 1$, et soit le mot reçu $y = 0011001$ en représentation polynomiale $y(X) = \sum_{i=0}^{6} y_i X^i = X^6 + X^3 + X^2$.

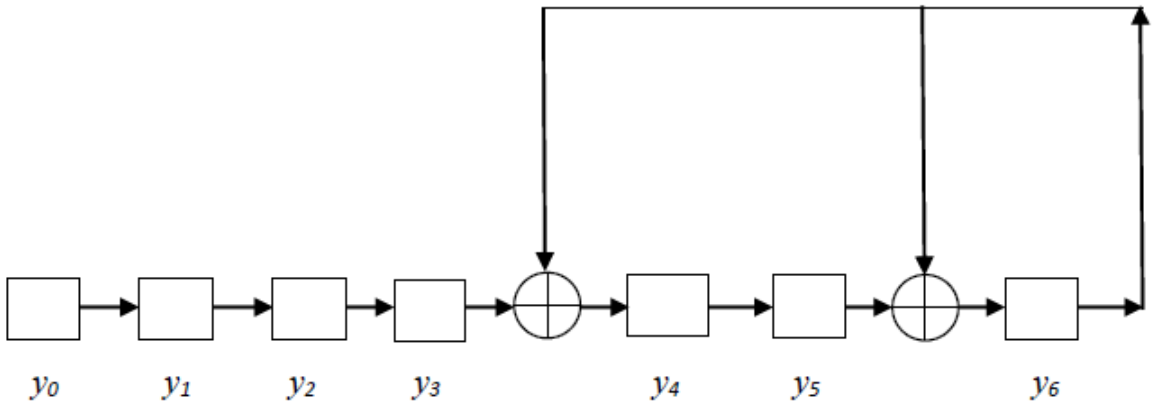

Fig 4.3 Registre à décalages circulaire

Nombre décalage	a_0	a_1	a_2	a_3	a_4	a_5	a_6
0	O	0	1	1	0	0	1
1	0	0	0	1	0	0	1
2	0	0	0	0	0	0	1
3	0	0	0	0	1	0	1
4	0	0	0	0	1	1	1
Reste					r_0	r_1	r_2

Tableau 4.4 Tableau des syndromes.

Alors : $S(y(X)) = r_2X^2 + r_1X + r_0 = X^2 + X + 1$.

Les syndromes des erreurs de poids 1, sont calculés dans le tableau suivant :

$\varepsilon(X)$	$S(\varepsilon(X))$
X^6	$X^2 + X$
X^5	$X + 1$
X^4	$X^2 + X + 1$
X^3	$X^2 + 1$
X^2	X^2
X	X
1	1

Tableau 4.5 Tableau des syndromes-

Cherchons l'erreur $\varepsilon(X)$ de poids $w(\varepsilon(X)) = 1$ et de syndrome $S(\varepsilon(X)) = X^2 + X + 1$ dans le tableau des syndromes, on trouve le mot erreur est $\varepsilon(X) = X^4$ et le mot (polynôme) envoyé est : $C(X) = y(X) + \varepsilon(X) = X^6 + X^4 + X^3 + X^2$, et le mot envoyé $c = 0011101$.

4.3 Méthode de décodage de Meggitt.

Cette méthode tire son nom de l'ingénieur britannique Jack K. Meggitt, qui a développé cette approche dans les années 1960. Elle s'applique aux codes cycliques binaires, mais elle peut se généraliser au cas non binaire. L'idée de base consiste en l'utilisation de la cyclicité du code pour reteindre la table des syndromes et permettre des calculs récursifs. Le décodeur de Meggitt effectue un décodage symbole par symbole. On corrige d'abord une composante erronée du mot reçu au moyen de la méthode décrite ci-dessous, puis on applique de nouveau la méthode au nouveau mot reçu ainsi obtenu.

La méthode de Meggitt se distingue par sa capacité à détecter et à corriger plusieurs erreurs dans les codes cycliques, ce qui en fait une approche assez performante pour les environnements à forte distorsion. Cependant, il convient de noter que la méthode de Meggitt peut être complexe à mettre en œuvre en raison des calculs impliqués et de la nécessité de manipuler les générateurs de syndromes.

Les opérations à effectuer sont le shift et le calcul de syndrome on peut les réaliser au moyen de registres à décalage circulaire.

Un autre avantage de cette méthode réside dans le fait qu'on remplace le tableau de déchiffrement qui comporte tous les mots erreurs et tous les syndromes, par un autre tableau où ne figurent que les syndromes des mots erreurs dont le dernier symbole est erroné. On gagne ainsi beaucoup d'espace mémoire et de temps.

4.3.1 Suite des syndromes polynomiaux

La proposition suivante montre que les j^{ieme} shifts du mot reçu et de l'erreur correspondante ont le même syndrome polynomial.

Proposition 4.2.

Soit $\varepsilon(X)$ le mot erreur du mot reçu $y(X)$. Alors, pour tout entier j, $0 \leq j \leq n-1$:

1. le mot $X^j y(X)$) est un mot reçu dont l'erreur est $X^j \varepsilon(X)$.
2. S $(X^j \varepsilon(X))$ = S $(X^j y(X))$.

Preuve.

1. De $y(X)$ =c(X)+$\varepsilon(X)$, avec $c(X) \in \theta(X)$, on déduit $X^j y(X) = X^j c(X) + X^j \varepsilon(X)$. Le code C étant cyclique, on sait que $X^j c(X) \in \theta(X)$. D'autre part $w(X^j \varepsilon(X)) = w(\varepsilon(X))$, car la multiplication par X^j ne modifie pas le poids d'un mot. L'égalité précédente montre que $X^j \varepsilon(X)$ est le mot erreur du mot reçu $X^j y(X)$.
2. Il existe c(X) multiple de g(x) dans $\mathbb{F}_2[X]/\langle X^n - 1\rangle$ tel que $y(X) = c(X) + \varepsilon(X)$, on obtient donc dans $\mathbb{F}_2[X]/\langle X^n - 1\rangle$ une relation de la forme $X^j y(X) = X^j c(X) + X^j \varepsilon(X)$. Ceci implique, dans $\mathbb{F}_2[X]$, une égalité de la forme $X^j y(X) = X^j c(X) + X^j \varepsilon(X) + b(X)(X^n - 1)$. puisque $g(X)$ divise $(X^n - 1)$ dans $\mathbb{F}_2[X]$, on voit que $X^j y(X) = X^j \varepsilon(X)$ modulo $g(X)$, ce qui montre que $X^j y(X)$ et $X^j \varepsilon(X)$ ont le même reste dans la division par $g(X)$, c.à.d. le même syndrome.

Remarque 4.1.

On voit donc d'après (b), que si l'on trouve S $(X^j$y$(X))$ dans une table de syndrome indiquant l'erreur correspondante, on peut retrouver $X^j \mathcal{E}(X)$ et donc aussi l'erreur $\mathcal{E}(X)$.

La proposition suivante montre comment on peut calculer S $(X^j$y$(X))$ à partir de S (y(X)) de manière récursive.

Proposition 4.3.

Avec les notations de la proposition précédente, soit $(S_j(X))_{j\in\mathbb{N}}$ la suite des polynômes de $\mathbb{F}_2[X]/< X^n-1 >$ définie par :

$$\begin{cases} S_0(X) = S(y(X)) \\ S_{j+1}(X) = S(XS_j(X)) \end{cases}$$

Alors pour tout entier j, $0 \le j \le n-1$, on a : $S_j(X) = S(X^j y(X))$.

Preuve.

Pour $j = 0$, la propriété est vraie par définition : $S_0(X) = S(y(X)) = S(X^0 y(X))$.

Démontrons la pour $j = 1$,

Soit $q(X)$ le quotient de la division de $y(X)$ par $g(X)$ dans $\mathbb{F}_2[X]$. D'après la définition du syndrome, on obtient : $y(X) = g(X)q(X) + S(y(X))$, ceci implique

$$Xy(X) = Xg(X)q(X) + XS(y(X)) \ldots(1)$$

Soit l'application φ: $\mathbb{F}_2[X] \to \mathbb{F}_2[X]/< X^n-1 >$ qui associe chaque polynôme de $\mathbb{F}_2[X]$ avec son reste de la division Euclidienne par X^n-1.

Soit $q'(X)$ le quotient de la division Euclidienne de $XS(y(X))$ par X^n-1 dans $\mathbb{F}_2[X]$.

On trouve : $XS(y(X)) = q'(X)(X^n-1) + \varphi(XS(y(X)))$.

Remplaçons dans (1); $Xy(X) = Xg(X)q(X) + q'(X)(X^n-1) + \varphi(XS(y(X)))$.

Puisque g(x) divise X^n-1, on obtient : $Xy(X) = \varphi(XS(y(X)))mod g(X)$.

Soit $q''(X)$ le quotient de la division Euclidienne de $Xy(X)$ par X^n-1,

$Xy(X) = q''(X)(X^n-1) + \varphi(Xy(X))$. Comme $g(X)$ divise X^n-1, on obtient :

$Xy(X) = \varphi(Xy(X))mod g(X)$. D'où $\varphi(XS(y(X))) = \varphi(Xy(X))\, mod g(X)$.

Ceci montre que $\varphi(XS(y(X)))$ et $\varphi(Xy(X))$ ont le même reste de division par $g(X)$ et donc le même syndrome. Cela signifie que $XS(y(X))$ et $Xy(X)$ calculés modulo X^n-1 ont le même syndrome. i.e. $S(XS(y(X))) = S(Xy(X))$. D'où $S_1(X) = S(Xy(X))$. Supposons que le résultat est vrai pour $j = k$, c.à.d. $S_k(X) = S(X^k y(X))$, et montrons le pour $j = k+1$. D'après la définition de la suite, on a :

$S_{k+1}(X) = S(XS_k(X)) = S\left(XS\left(X^k y(X)\right)\right) = S\left(XS\left(y_k(X)\right)\right)$ avec $y_k(X) = X^k y(X)$.

En appliquant le résultat pour $j = 1$ à $y_k(X)$, on trouve

$S(XS(y_k(X))) = S\left(Xy_k(X)\right) = S(X.X^k y(X)) = S(X^{k+1} y(X))$. Cela achève la démonstration par récurrence.

4.3.2 Algorithme de décodage de Meggitt

Soit (T) la table des syndromes des erreurs dont la composante d'indice $n-1$ est erronée. Soit $c(X)$ le mot envoyé, $y(X)$ le mot reçu , et $\varepsilon(X)$ le mot erreur avec $\omega(\varepsilon(X)) \leq e$.

La suite $S_i(X)$ est définie comme dans la Proposition 4.3. L'algorithme de décodage de Meggitt est le suivant :

1. Calcul de $S(y(X))$.
2. Si $S\left(y_k(X)\right) = 0$ alors $y(X) = c(X)$ et l'algorithme se termine.
3. Sinon ;

- On cherche le plus petit entier non nul j tel que $S_j(X)$ se trouve dans la table (T).
- Corriger la composante d'indice $n-1-j$ de $y(X)$, soit $y'(X)$, le nouveau mot obtenu.

4. Repartir au début de l'algorithme avec $y'(X)$.

Exemple 4.2.

Soit $C(7,4,3)$ le code de Hamming 1-correcteur de polynôme générateur $g(X) = X^3 + X + 1$. La table (T) des syndromes des erreurs dont la composante d'indice 6 est égale à 1 se réduit au tableau suivant :

Erreur	X^6
Syndrome	$X^2 + 1$

Tableau 4.6 Tableau des syndrome (T)

Soit $y(X) = X^6 + X^5 + X^4$,le mot reçu, donc le syndrome de $y(X)$ est égale à $S(y(X)) = X^2$ ne figure pas dans la table (T), On cherche le plus petit entier non nul j tel que $S_j(X) \in (T)$, c.à.d. tel que $S_j(X) = S\left(X^j y(X)\right) = X^2 + 1$, on trouve que $j = 4$. Il y a donc une erreur en

position $n-1-j=7-1-4=2$. Avec l'hypothèse que la capacité de correction égale à 1 n'est pas dépassé, l'erreur est $\varepsilon(X)=X^2$ et le mot envoyé est $c(X)=y(X)+\varepsilon(X)=X^6+X^5+X^4+X^2$.

Exemple 4.3.

Soit $C(15,7,5)$ le code cyclique avec polynôme générateur $g(X)=1+X^4+X^6+X^7+X^8$. Alors la liste des polynômes erreurs $\varepsilon(X)$ avec $\omega\big(\varepsilon(X)\big)\leq e=2$ et leurs syndromes est la suivante :

$\varepsilon(X)$	$S(\varepsilon(X))$
X^{14}	$X^3+X^5+X^6+X^7$
$X^{14}+X^{13}$	$X^2+X^3+X^4+X^7$
$X^{14}+X^{12}$	$X+X^4+X^6+X^7$
$X^{14}+X^{11}$	$1+X^2+X^4+X^5+X^6+X^7$
$X^{14}+X^{10}$	$X+X^2+X^3$
$X^{14}+X^9$	$1+X+X^3+X^4+X^7$
$X^{14}+X^8$	$1+X^3+X^4+X^5$
$X^{14}+X^7$	$X^3+X^5+X^6$
$X^{14}+X^6$	$X^3+X^5+X^7$
$X^{14}+X^5$	$X^3+X^6+X^7$
$X^{14}+X^4$	$X^3+X^4+X^5+X^6+X^7$
$X^{14}+X^3$	$X^5+X^6+X^7$
$X^{14}+X^2$	$X^2+X^3+X^5+X^6+X^7$
$X^{14}+X$	$X+X^3+X^5+X^6+X^7$
$X^{14}+1$	$1+X^3+X^5+X^6+X^7$

Tableau 4.7 Tableau des syndromes (T) pour le code $C(15,7,5)$

Soit $y(X)=X^{12}+X^{10}+X^9+X^7+X^4+1$ le mot reçu.

En utilisant un registre à décalage circulaire, on calcule le syndrome du mot reçu on trouve : $S(y(X))=X^5+X^4+X^3+X^2+X$.

On remarque que $S(y(X))$ ne figure pas dans la table, cherchons le plus petit entier j tel que $S_j(X)$ soit dans la table (T). On trouve $j=2$, car après calcul on trouve

$$S(X^2y(X))=X^7+X^6+X^5+X^4+X^3=S(X^{14}+X^4).$$

L'erreur associée au mot $X^2y(X)$ est $X^2\varepsilon(X)=X^{14}+X^4$, d'où le mot erreur associée au mot $y(X)$ est $\varepsilon(X)=X^{12}+X^2$. D'où $c(X)=y(X)+\varepsilon(X)=X^{10}+X^9+X^7+X^4+X^2+1$.

4.4 Décodage par piégeage d'erreur

Le décodage par piégeage d'erreur, également connu sous le nom de "Error Trapping Decoding" en anglais, est une approche utilisée pour décoder les codes correcteurs d'erreurs, y compris les codes cycliques. Cette méthode vise à détecter et à corriger les erreurs dans les données en identifiant et en isolant les erreurs potentielles à l'aide de techniques de syndromes et de calculs itératifs. Le décodage par piégeage d'erreur est particulièrement efficace pour les codes cycliques, car il exploite leurs propriétés spécifiques pour améliorer la correction d'erreurs.

4.4.1 Principe de la méthode de piégeage d'erreurs

Soit $C(n,k)$ un code cyclique e-correcteur sur le corps $\mathbb{F}_q$, de polynôme générateur $g(X)$. Supposons que $c(X) \in C$ le mot transmis et $y(X) = c(X) + \varepsilon(X)$ est le mot reçu, où $\varepsilon(X)$ est le mot erreur, avec le poids $\omega(\varepsilon(X)) \leq e$. La méthode de décodage par piégeage d'erreur est une modification de la méthode de Meggitt, il s'agit de déplacer par décalage circulaire, c'est-à-dire « piéger » en quelque sorte, les composantes non nulles de l'erreur sur certaines positions. On considère un code binaire (on peut généraliser au cas non binaire), et on suppose comme cité ci-dessus, que le nombre d'erreurs ne dépasse pas la capacité de correction e.
Le principe du décodage par piégeage d'erreur s'appuie sur les résultats suivants :

Lemme 4.1.

Soit $\varepsilon(X)$ le mot erreur du mot reçu $y(X)$, Si $d^\circ(\varepsilon(X)) \leq n - k - 1$ alors :
$\varepsilon(X) = S(y(I))$.

Preuve.

Dans $\mathbb{F}_q[X]/< X^n - 1 >$ on a $y(X) = c(X) + \varepsilon(X)$, avec $\varepsilon(X) \in C$, soit encore dans $\mathbb{F}_q[X]$ $y(X) = a(X)g(X) + \varepsilon(X) + b(X)(X^n - 1)$. Puisque $g(X)$ divise $X^n - 1$, on trouve $y(X) = d(X)g(X) + \varepsilon(X)$.

Si $d^\circ(\varepsilon(X)) \leq n - k - 1$, alors d'après l'unicité de reste dans la division par $g(X)$, on obtient $S(y(X)) = \varepsilon(X)$.

Lemme 4.2.

Soit $\varepsilon(X)$ le mot erreur du mot reçu $y(X)$, alors $\omega(S(y(X)) \leq e$ si et seulement si $S\big(y(X)\big) = \varepsilon(X)$.

Preuve.

La division dans $\mathbb{F}_q[X]$ de $y(X)$ par $g(X)$ s'exprime par $y(X) = g(X)a(X) + \varepsilon(X)$.
Les conditions sur le degré des polynômes intervenant dans cette égalité, font que celle si également vérifiée dans $\mathbb{F}_q[X]/< X^n - 1 >$. La décomposition d'un mot reçu comme somme d'un mot du code et d'un mot de poids inférieur ou égal à e est unique. Donc si $\omega(S(y(X)) \leq e$, alors $S\big(y(X)\big) = \varepsilon(X)$. Réciproquement si $S\big(y(X)\big) = \varepsilon(X)$, alors $\omega(S(y(X)) \leq e$ puisque le poids de l'erreur est au plus e.

Théorème 4.2. Soit $\varepsilon(X)$ le mot erreur du mot reçu $y(X)$.
Si j est un entier $0 \leq j \leq n-1$ tel que $\omega(S(X^j y(X)) \leq e$, alors $\varepsilon(X) = X^{-j} S\left(X^j y(X)\right)$.

Preuve.

Soit $y_1(X) = X^j y(X)$, c'est le mot erreur du mot reçu dont l'erreur est $\varepsilon_1(X) = X^j \varepsilon(X)$.d'aprée le lemme 2.15.2, si $\omega(S(y_1(X) \leq e$, alors $S\big(y_1(X)\big) = \varepsilon_1(X)$, c.-à-d. $S\left(X^j y(X)\right) = X^j \varepsilon(X)$ donc $\varepsilon(X) = X^{-j} S(X^j y(X))$.

Théorème 4.3.

Soit $\varepsilon(X)$ le mot erreur du mot reçu $y(X)$. Si $\varepsilon(X) = X^j \varepsilon_1(X)$ avec $d^\circ(\varepsilon_1(X)) \leq n - k - 1$, alors $\omega(S(X^{-j} y(X)) \leq e$.

Preuve.

D'après le lemme 2.15.1, comme $d^\circ \varepsilon_1(X) \leq n - k - 1$ alors $\varepsilon_1(X) = X^{-j}\varepsilon(X) = S(X^{-j} y(X))$. On pose $y_1(X) = X^{-j} y(X)$ donc $\varepsilon_1(X) = S(y_1(X)$ d'aprés le lemme 2.15.2 on trouve $\omega(S(y_1(X)) \leq e$ alors $\omega(S(X^{-j} y(X)) \leq I$.

4.4.2 Algorithme de décodage par piégeage d'erreur

Soit $y(X)$ le mot reçu, $\varepsilon(X)$ le mot erreur avec $\omega(\varepsilon(X)) \leq e$.

1. Calcul de $S\big(y(X)\big)$.
2. Si $S\big(y(X)\big) = 0$ alors $\varepsilon(X) = 0$.
3. Sinon,

- Si $\omega(S(y(X)) \leq e$ alors $\varepsilon(X) = S(y(X))$.

4. Sinon on cherche le plus petit entier j tel que $\omega(S\left(X^j y(X)\right)) \leq e$, alors $\varepsilon(X) = X^{-j}S(X^j y(X))$.
5. Le mot envoyé est $c(X) = y(X) - \varepsilon(X)$.

Exemple 4.4.

Soit le code $C(7,4,3)$ sur $\mathbb{F}_2$, Soit $g(X)$ le polynôme générateur, $g(X) = X^3 + X^2 + 1$, Soit $y(X) = X^5 + X^3 + X$, le mot reçu. Le syndrome est le reste de la division $y(X)$ par $g(X)$. On a : $y(X) = (X^3 + X^2 + 1)(X^2 + X) + X^2$, donc $S(y(X)) = X^2$ et $\omega\left(S\left(y(X)\right)\right) = 1$. En supposant que la capacité d'erreurs n'est pas dépassée, l'erreur est $\varepsilon(X) = S(y(X))$ et le mot transmis est donc : $c(X) = y(X) - \varepsilon(X) = X^5 + X^3 + X^2 + X$.

Exemple 4.5.

Soit le code $C(7.4,3)$ sur $\mathbb{F}_2$. Soit le polynôme générateur $g(X) = X^3 + X + 1$. Soit $y(X) = X^5 + X^4 + X^2$, le mot reçu. Le syndrome est le reste de la division de $y(X)$ par $g(X)$. On a : $y(X) = (X^3 + X + 1)(X^2 + X + 1) + (X^2 + 1)$ Donc $S(y(X)) = X^2 + 1$ et $\omega\left(S\left(y(X)\right)\right) = 2$. Puisqu'on suppose que le poids de l'erreur est au plus 1, $S(y(X)) \neq \varepsilon(X)$. Comme $S\left(Xy(X)\right) = 1$, alors le plus petit entier non nul j tel que $\omega\left(X^j S\left(y(X)\right)\right) \leq 1$ est $j = 1$. Donc le mot erreur est $\varepsilon(X) = X^{-1}S\left(Xy(X)\right) = X^{-1} * 1 = X^{7-1} = X^6$.
Donc $\varepsilon(X) = X^6$, et le mot envoyé est $c(X) = y(X) - \varepsilon(X)$ est $c(X) = X^6 + X^5 + X^4 + X^2$.

4.5 Décodage algébriques des codes B.C.H

Le décodage algébrique des codes BCH est une méthode qui repose sur des concepts et des techniques algébriques avancées pour localiser et corriger les erreurs, en exploitant les propriétés caractéristiques des codes BCH.

Voici un aperçu du décodage algébrique des codes BCH :

1. **Propriétés des codes BCH** : Les codes BCH sont construits à partir de polynômes cyclotomiques et ont la propriété remarquable de posséder des distances minimales relativement élevées. Cela signifie qu'ils peuvent détecter et corriger un grand nombre d'erreurs. Ils sont souvent utilisés dans les systèmes où la fiabilité des données est cruciale, tels que les systèmes de stockage et les communications.

2. **Syndromes et générateurs de syndromes** : Les syndromes sont des vecteurs associés à des erreurs spécifiques dans les données reçues. Les générateurs de syndromes sont des polynômes qui permettent de calculer ces syndromes. Le processus de décodage commence par le calcul des syndromes à partir des données reçues.
3. **Localisation d'erreurs avec les polynômes locaux** : Une caractéristique clé des codes BCH est l'utilisation de polynômes locaux pour localiser les erreurs. Ces polynômes permettent de déterminer les positions où les erreurs sont susceptibles de se trouver. Les positions d'erreurs probables sont appelées "positions d'erreur candidates".
4. **Localisation précise d'erreurs avec les équations de localisation** : Les équations de localisation sont des relations algébriques qui associent les syndromes aux positions d'erreur candidates. En résolvant ces équations, il est possible d'obtenir des informations plus précises sur les positions d'erreurs et leurs valeurs.
5. **Correction d'erreurs avec les équations de correction** : Les équations de correction sont utilisées pour calculer les valeurs correctes des bits en fonction des positions d'erreurs identifiées. En appliquant ces équations, les erreurs peuvent être corrigées, ce qui permet de récupérer les données d'origine avec une grande précision.
6. **Itérations et raffinements** : Dans certaines situations, des itérations et des raffinements peuvent être nécessaires pour améliorer davantage la correction d'erreurs. Cela peut impliquer de répéter les étapes précédentes avec des informations mises à jour pour parvenir à une solution plus précise.

Le décodage algébrique des codes BCH nécessite une compréhension approfondie des propriétés algébriques des codes et des techniques de manipulation de polynômes. Cette méthode est généralement plus complexe que les méthodes de décodage basées sur les syndromes, mais elle offre une excellente capacité de correction d'erreurs, ce qui la rend très utile dans des contextes où la fiabilité des données est primordiale.

4.5.1 Syndrome, localisateur et polynôme localisateur

Soit $C(n,k)$ un code BCH, de générateur $g(X)$ admettant $\delta - 1 = 2e$ (où e est la capacité de correction et δ la distance construite) racines successives β^j, $b \leq j \leq b + \delta - 2$, b un entier non nul. Soit v le poids de l'erreur c.à.d. $v = w(\varepsilon(X))$, avec $v \leq e$.

Définition 4.3.

Si $y = (y_0, y_1, \dots, y_{n-1})$ est le mot reçu, $\varepsilon = (\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$ le mot erreur de poids *v* tel que $v = w(\varepsilon(X)) \leq e$, et H la matrice de contrôle du code *C*. Alor le syndrome de y est :

S $= y * H^t$ donné par :

$$\text{S}=\left(\sum_{i=0}^{n-1} y_i \beta^{bi}, \sum_{i=0}^{n-1} y_i \beta^{(b+1)i}, \dots, \sum_{i=0}^{n-1} y_i \beta^{(b+2e-1)i}\right),$$

$$s_j = \sum_{i=0}^{n-1} y_i \beta^{ji} = y(\beta^j), \quad b \leq j \leq b + \delta - 2.$$

Le syndrome se calcule en cherchant les valeurs de $y(X)$ pour les $\delta - 1$ racines successives β^j du polynôme générateur $g(X)$.

Définition 4.4.

On appelle **localisateur de la position** i, l'élément X_i défini par $X_i = \beta^i$, pour 0 ≤ i ≤ n − 1.

On note *I* l'ensemble des positions de l'erreur, $I = \{i, 0 \leq i \leq n-1, \varepsilon_i \neq 0\}$, alors

$v = \text{card}(I)$.

• On appelle **valeur de l'erreur** dans la position i, l'élément Y_i, tel que $Y_i = \varepsilon_i$.

Définition 4.5. On appelle **polynôme localisateur de l'erreur**, le polynôme σ(X) définie par :

$$\sigma(X) = \prod_{i \in I} (1 - X_i X)$$

Par définition du polynôme localisateur, ces racines ne sont que les inverses des localisateurs.

Remarque 4.2.

Soit y(x) un mot reçu avec une erreur ε(X) de poids $w(\varepsilon(X)) \leq$ e, alors :

$y(X) = c(X) + \varepsilon(X)$, avec $c(X) \in C$. On a :

Pour tout $i \in \{b, \dots, b + \delta - 2\}$: $y(\beta^i) = c(\beta^i) + \varepsilon(\beta^i) = \varepsilon(\beta^i)$, avec β une racine nième primitive de l'unité. En d'autres termes, le mot reçu et le mot erreur ont le même syndrome.

$$s_j = y(\beta^j) = \varepsilon(\beta^j)$$

$$s_j = \sum_{i=0}^{n-1} y_i \left(\beta^j\right)^i = \sum_{i=0}^{n-1} \varepsilon_i \left(\beta^j\right)^i$$

$$= \sum_{i \in I} \varepsilon_i \left(\beta^i\right)^j = \sum_{i \in I} Y_i X_i^j$$

Donc $s_j = \sum_{i=1}^{v} Y_i X_i^j,\ b \leq j \leq b + 2e - 1$

Avec $X_i = \beta^i$ et $Y_i = \varepsilon_i$, et les S_j, sont calculés à partir du mot reçu y.

Ces équations sont non linéaires, elles ne peuvent pas être résolues directement, elles nécessitent l'utilisation de variables intermédiaires qui peuvent être calculées à l'aide du syndrome et qui permettent de déterminer les positions de l'erreur.

4.5.2 Principe de décodage des codes B.C.H

La méthode de décodage algébrique ou de **Peterson, Gorenstein et Zierler** se déroule en trois étapes :

1. Calcul du syndrome du mot reçu.
2. Détermination des positions de l'erreur.
3. Calcul de la valeur de l'erreur aux positions trouvées.

- **Détermination des positions de l'erreur**

Pour déterminer les positions de l'erreur, il suffit de déterminer les localisateurs, pour le faire il suffit de déterminer les racines du polynôme localisateur.

le polynôme localisateur $\sigma(X)$ est de la forme :

$$\sigma(X) = \sigma_v X^v + \sigma_{v-1} X^{v-1} + \cdots + \sigma_1 X + 1. \qquad (1)$$

Il s'agit dans un premier temps de déterminer les coefficients du polynôme localisateur de l'erreur.

$$\sigma(X) = (1 - X_1 X) \ldots (1 - X_v X)$$

En multipliant les deux membres de l'équation (1) par $Y_i X_i^{j+v}$ et en remplaçant X par X_i^{-1} l'équation devient

$$\sigma_v X_i^{-v} + \sigma_{v-1} X^{-v+1} + \cdots + \sigma_1 X_i^{-1} + 1 = 0,$$

$$Y_i X_i^{j+v}(\sigma_v X_i^{-v} + \sigma_{v-1} X^{-v+1} + \cdots + \sigma_1 X_i^{-1} + 1) = 0,$$

$$Y_i\left(\sigma_v X_i^{j} + \sigma_{v-1} X_i^{j+1} + \cdots + \sigma_1 X_i^{j+v-1} + X_i^{j+v}\right) = 0.$$

En sommant sur $i, 1 \leq i \leq v$, on obtient

$$\sum_{i=1}^{v} Y_i\left(\sigma_v X_i^{j} + \sigma_{v-1} X_i^{j+1} + \cdots + \sigma_1 X_i^{j+v-1} + X_i^{j+v}\right) = 0,$$

$$\sigma_v \sum_{i=1}^{v} Y_i X_i^{j} + \sigma_{v-1} \sum_{i=1}^{v} Y_i X_i^{j+1} + \cdots + \sigma_1 \sum_{i=1}^{v} Y_i X_i^{j+v-1} + \sum_{i=1}^{v} Y_i X_i^{j+v} = 0.$$

Et donc : $\sigma_v S_j + \sigma_{v-1} S_{j+1} + \cdots + \sigma_1 S_{j+v-1} + S_{j+v} = 0$.

L'équation devient finalement

$$\sigma_v S_j + \sigma_{v-1} S_{j+1} + \cdots + \sigma_1 S_{j+v-1} = -S_{j+v}.$$

Par la définition du syndrome tous les S_j sont connus pour $b \leq j \leq b + 2e - 1$, de plus on a $v \leq e$ d'où le système suivant.

$$\begin{pmatrix} S_b & S_{b+1} & \cdots & S_{b+v-1} \\ S_{b+1} & S_{b+2} & \cdots & S_{b+v} \\ \vdots & \vdots & \vdots & \vdots \\ S_{b+v-1} & S_{b+v} & \cdots & S_{b+2v-2} \end{pmatrix} \begin{pmatrix} \sigma_v \\ \sigma_{v-1} \\ \vdots \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} -S_{b+v} \\ -S_{b+v+1} \\ \vdots \\ -S_{b+2v-1} \end{pmatrix} \qquad \text{(I)}$$

Ce système admet une solution unique. Donc les coefficients du polynôme localisateur sont déterminés par la résolution du système (I). Les coefficients du polynôme localisateur de l'erreur$\sigma_1, \sigma_2, \ldots, \sigma_v$ sont maintenant connus, il s'agit de déterminer les localisateurs de l'erreur.

Soit $\sigma(X) = \sigma_v X^v + \sigma_{v-1} X^{v-1} + \cdots + \sigma_1 X + 1$. Par définition, les racines de $\sigma(X)$ sont les inverses des localisateurs c.à.d. les X_i^{-1} avec $X_i = \beta^i$ et $i \in I$. Parmi tous les éléments de $\mathbb{F}_{p^r}$, on cherche ceux qui sont racine de $\sigma(X)$. On cherche les éléments β^i de $\mathbb{F}_{P^r}$, tel que $\sigma(\beta^i) = 0$. Or $\sigma(\beta^i) = 0$ si et seulementsi $\varepsilon_{n-i} \neq 0$. Donc $\sigma(\beta^i) = 0$ si et seulement si $n - i$ est une position de l'erreur.

- **Calcul de la valeur de l'erreur aux positions trouvées**

Les localisateurs X_i^j sont maintenant connus, il reste à résoudre le système suivant:

$$\sum_{i=1}^{v} Y_i X_i^{j} = S_j, b \leq j \leq b + 2e - 1$$

On prend b=1 sans perte de généralité et $1 \leq j \leq v$:

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_v \\ X_1^2 & X_2^2 & \cdots & X_v^2 \\ \vdots & \vdots & \vdots & \vdots \\ X_1^v & X_2^v & \cdots & X_v^v \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_v \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \\ \vdots \\ S_v \end{pmatrix} \qquad \text{(II)}$$

La matrice du système (II) est une matrice de Vandermonde. Si le poids de l'erreur est *v*, alors les localisateurs $X_1, X_2, \ldots, X_v$, sont non nuls et distincts. D'après le théorème sur les matrices de Vandermonde, la matrice du système est inversible et le système admet donc une solution unique.

4.5.3 Algorithme de décodage algébrique des codes B. C. H

Soient y(X) le mot reçu, ε(X) le mot erreur, avec $w(\varepsilon(X)) = v$ et β^b, $\beta^{b+1}, \ldots, \beta^{b+\delta-2}$, avec $b > 0$, les $\delta - 1 = 2e$ racines du polynôme générateur.

1. Calcul des composantes du syndrome à partir du mot reçu, $S_j = y(\beta^j)$ pour tout j $b \leq j \leq b + 2e - 1$.

2. Résoudre le système (I) afin de déterminer les coefficients du polynôme localisateur de l'erreur, $\sigma_1, \sigma_2, \ldots, \sigma_v$ et ainsi le polynôme localisateur $\sigma(X)$.
3. Déterminer les localisateurs de l'erreur $X_i = \beta^i, 1 \leq i \leq v$, tel que $\sigma(\beta^{-i}) = 0$, avec $\beta^i \in \mathbb{F}_{p^r}$. alors $\varepsilon_i \neq 0$, l'indice i est une position de l'erreur.
4. Substituer les valeurs de $X_1, X_2, \ldots, X_v$, trouvées, et résoudre le système (II) pour déterminer les valeurs de l'erreur, $Y_i = \varepsilon_i, 1 \leq i \leq v$.
5. Correction de l'erreur et trouver le mot transmis $c(X) = y(X) - \varepsilon(X)$.

Exemples 4.6.

Les deux seuls codes BCH avec *n*=7 sont le code de répétition pure *C*(7,1) avec *e*=3 et le code de Hamming *C*(7, 4) avec *e*=1.

1) Exemple 4.6.1. Soit *C*(7,1) un code BCH binaire de polynôme générateur :
$g(X) = (X^3+X+1)(X^3+X^2+1)$ et soit $y(X) = \alpha^2 X^6 + \alpha X^5$ le mot reçu contenant v=2 erreurs, tel que les racines successive de *g(X)* sont $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$

Le polynôme localisateur $\sigma(X) = \sigma_2 X^2 + \sigma_1 X + 1$

1. **Calcul du syndrome S=(s_1, s_2, s_3, s_4, s_5, s_6)**

$\mathbb{K}=\mathbb{F}_2{}^r$ le corps de racine 7^iéme de l'unité sur $\mathbb{F}_2$, avec $r=\min\{t, n=7/2^r-1\}=3$ et donc $\mathbb{K}=\mathbb{F}_2{}^3=\mathbb{F}_8$.

Si α est une racine primitive de $\mathbb{K}$ alors, $\mathbb{K}=\{0, \alpha^i / 0 \leq i \leq 6\}$. Le polynôme primitif de $\mathbb{K}$ est le polynôme $M_\alpha(X)=X^3+X+1$. On a $M_\alpha(\alpha)=0$ donc $\alpha^3=\alpha+1$, $\alpha^4=\alpha^2+\alpha$, $\alpha^5=\alpha^2+\alpha+1$, $\alpha^6=\alpha^2+1$ et $\alpha^7=1$. Le syndrome est donné par : $s_j=y(\alpha^j)$, $1 \leq j \leq 6$ alors :

$S_1=y(\alpha)=\alpha^8+\alpha^6=\alpha+\alpha^2+1=\alpha^5$

$S_2=y(\alpha^2)=\alpha^{14}+\alpha^{11}=1+\alpha^4=\alpha^2+\alpha+1=\alpha^5$

$S_3=y(\alpha^3)=\alpha^{20}+\alpha^{16}=\alpha^6+\alpha^2=\alpha^2+1+\alpha^2=1$

$S_4=y(\alpha^4)=\alpha^{26}+\alpha^{21}=\alpha^5+1=\alpha^2+\alpha+1+1=\alpha^4$

$S_5=y(\alpha^5)=\alpha^{32}+\alpha^{26}=\alpha^4+\alpha^5=\alpha^2+\alpha+\alpha^2+\alpha+1=1$

$S_6=y(\alpha^6)=\alpha^{38}+\alpha^{31}=\alpha^3+\alpha^3=0$

2. **Calcul du polynôme localisateur et des localisateurs**

Les coefficients σ_2, σ_1 sont les solutions du système :

$$\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix}\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} s_3 \\ s_4 \end{pmatrix} \qquad \text{(I)}$$

$$\text{(I)} \Leftrightarrow \begin{pmatrix} \alpha^5 & \alpha^5 \\ \alpha^5 & 1 \end{pmatrix}\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} 1 \\ \alpha^4 \end{pmatrix} \Leftrightarrow \begin{cases} \alpha^5\sigma_2 + \alpha^5\sigma_1 = 1 & (1) \\ \alpha^5\sigma_2 + \sigma_1 = \alpha^4 & (2) \end{cases}$$

En résolvant ce système on trouve $\sigma_1=\alpha$ et $\sigma_2=\alpha^4$.

Le polynôme localisateur est donc $\sigma(X)=\sigma_2X^2+\sigma_1X+1=\alpha^4X^2+\alpha X+1$

Cherchons les racines de σ(X) dans le corps $\mathbb{F}_8$, on a : $\sigma(0)\neq 0$, $\sigma(1)\neq 0$

$\sigma(\alpha)=\alpha^6+\alpha^2+1=\alpha^2+1+\alpha^2+1=0$

$\sigma(\alpha^2)=\alpha^8+\alpha^3+1=\alpha+\alpha^3+1=\alpha+1+\alpha+1=0$

Donc les racines sont α et α^2 donc les localisateurs sont $X_5=\alpha^{-2}=\alpha^5$ et $X_6=\alpha^{-1}=\alpha^6$.

3. **Calcul des valeurs des erreurs $y_i=\varepsilon_i$**

On résoudre le système :

$$\begin{pmatrix} X_5 X_6 \\ X_5^2 X_6^2 \end{pmatrix}\begin{pmatrix} Y_5 \\ Y_6 \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} \qquad \text{(II)}$$

$$(II) \Leftrightarrow \begin{pmatrix} \alpha^5 & \alpha^6 \\ \alpha^3 & \alpha^5 \end{pmatrix} \begin{pmatrix} Y_5 \\ Y_6 \end{pmatrix} = \begin{pmatrix} \alpha^5 \\ \alpha^5 \end{pmatrix} \Leftrightarrow \begin{cases} \alpha^5 Y + \alpha^6 Y_6 = \alpha^5 & (1) \\ \alpha^3 Y_5 + \alpha^5 Y_6 = \alpha^5 & (2) \end{cases}$$

Après résolution du système dans le corps $\mathbb{F}_8$, on trouve : $y_5=\alpha$ et $y_6= \alpha^2$.

Donc le mot erreur est : $\varepsilon(X)=\alpha X^5+\alpha^2 X^6=y(X)$ et le mot envoyé est $c(X) = y(X)+ \varepsilon(X) = 0$.

2) Exemple 4.6.2. Le code de Hamming C(7,4) ave e=1

Soit C(7, 4) un code BCH binaire sur le corps $\mathbb{K}=\mathbb{F}_8$, de polynôme générateur : $g(X) =X^3 + +X+1 =(X- \alpha)(X- \alpha^2)(X- \alpha^4)$, qui admet 2 racines successives α et α^2. Soit $y(X)=1+ X+X^2$ le mot reçu avec une erreur (c.à.d v=1), le polynôme localisateur est de degré 1 : $\sigma(X)= \sigma_1 X+1$.

1. **Calcul du syndrome $S=(s_1, s_2)$**

$s_1=y(\alpha)= 1+\alpha+\alpha^2= \alpha^3+\alpha^2=\alpha^5$ et $s_2=y(\alpha^2)= 1+ \alpha^2+\alpha^4= \alpha^3$.

2. **Calcul du polynôme localisateur et des localisateurs**

On résout l'équation : $s_1\sigma_1= s_2 \Leftrightarrow \alpha^5\sigma_1= \alpha^3 \Leftrightarrow \sigma_{1=} \alpha^5$. Le polynôme localisateur $\sigma(X)= \alpha^5 X+1$, qui admet une seule racine α^2 et donc le localisateur est $X_5 = \alpha^5$. Il y a une erreur en position i=5.

3. **Calcul de la valeur de l'erreur**

Comme on considérer que les erreurs sont dans le cops $\mathbb{F}_2$ (binaire), alors la valeur de cette erreur est Y_5=1. Le mot erreur est : $\varepsilon(X)=X^5$.

4. **Le mot envoyé**

Le mot envoyé est $c(X)=y(X)+ \varepsilon(X)= 1+ X+ X^2 + X^5$.

Exemple 4.7.

Soit C(15. 7) un code BCH sur le corps $\mathbb{F}_{2^4} = \mathbb{F}_{16}$, de polynôme générateur :

$g(X) =(X^4+X+1)(X^4+X^3+X^2+1)$ qui admet $\alpha,\alpha^2,\alpha^3,\alpha^4$ comme racines successives.

Soit $y(X)= X^2+X^8$ le mot reçu contenant v=2 erreurs.

1. **Calcul du syndrome**

Le syndrome S=(s_1,s_2,s_3,s_4)

$\mathbb{K}$ le corps de racine 15$^{\text{iéme}}$ de l'unité $\mathbb{K}=\mathbb{F}_{16}$. $F_{16}=\{0, \alpha^i / 0 \leq i \leq 14\}$.

Le polynôme primitif de $\mathbb{K}$ est le polynôme $M_\alpha(X)=X^4+X+1$. On a : $M_\alpha(\alpha)=0$ donc $\alpha^4=\alpha+1$

Donc : $\alpha^5=\alpha^2+\alpha$; $\alpha^6=\alpha^3+\alpha^2$; $\alpha^7=\alpha^3+\alpha+1$; $\alpha^8=\alpha^2+1$; $\alpha^9=\alpha^3+\alpha^2$; $\alpha^{10}=\alpha^2+\alpha+1$;

$\alpha^{11}=\alpha^3+\alpha^2+\alpha$; $\alpha^{12}=\alpha^2+1$; $\alpha^{13}=\alpha^3+\alpha^2+\alpha+1$; $\alpha^{14}=\alpha^3+1$.

On a $s_j=y(\alpha^j)$, $0 \leq j \leq 4$.

$s_1=y(\alpha)=\alpha^2+\alpha^8=1$

$s_2=y(\alpha^2)=\alpha^4+\alpha^{16}=\alpha^4+\alpha=1$

$s_3=y(\alpha^3)=\alpha^6+\alpha^{24}=\alpha^6+\alpha^9=\alpha^5$

$s_4=y(\alpha^4)=\alpha^8+\alpha^{32}=\alpha^8+\alpha^2=1$

2. **Calcul du polynôme localisateur et des localisateurs**

Le polynôme localisateur $\sigma(X)=\sigma_2X^2+\sigma_1X+1$. Les coefficients σ_2, $\sigma_1$sont les solutions du système

$$\begin{pmatrix} s_1 & s_2 \\ s_2 & s_3 \end{pmatrix}\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} s_3 \\ s_4 \end{pmatrix} \qquad \text{(I)}$$

$$\text{(I)} \Leftrightarrow \begin{pmatrix} 1 & 1 \\ 1 & \alpha^5 \end{pmatrix}\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} \alpha^5 \\ 1 \end{pmatrix} \Leftrightarrow \begin{cases} \sigma_2+\sigma_1=\alpha^5 & (1) \\ \sigma_2+\alpha^5\sigma_1=1 & (2) \end{cases}$$

Apres résolution du système dans le corps $\mathbb{F}_8$, on trouve : $\sigma_1=1$ et $\sigma_2=\alpha^{10}$, $\sigma(X)=\alpha^{10}X^2+X+1$.

On peut vérifier facilement que les racines de $\sigma(X)$: sont α^7 et α^{10}.

Donc les localisateurs sont $X_5=\alpha^5$ et $X_8=\alpha^8$.

3. **Calcul de la valeur de l'erreur**

Si on considérer que les erreurs sont dans le cops $\mathbb{F}_2$ (binaire), alors $\varepsilon(X)=X^5+X^8$.

4. **Le mot envoyé**

Le mot envoyé est $c(X)=y(X)+\varepsilon(X)=X^2+X^8+X^5+X^8=X^2+X^5$.

4.6 Méthode de décodage des codes Reed-Solomon par transformation de Fourier discrète

4.6.1 Transformation de Fourier discrète sur un corps fini

Soit F un corps fini de caractéristique p et α une racine primitive du corps $\mathbb{K}$ des racines nièmes de l'unité sur F, soit $a(X) = \sum_{i=0}^{n-1} a_i X^i$ un polynôme de $F[X]/\langle X^n - 1\rangle$ et $\hat{a}(X) = \sum_{j=0}^{n-1} \hat{a}_j X^{n-j}$ est un polynôme de $\mathbb{K}[X]/\langle X^n - 1\rangle$ tels que $\hat{a}_j = a(\alpha^j) = \sum_{i=0}^{n-1} a_i \alpha^{ij}$.

Définition 4.6.

Soit F un corps fini, n un entier tel que $n \geq 1$, $\mathbb{K}$ le corps des racines nièmes de l'unité sur F, et α une racine primitive nième de l'unité sur F. La **transformation de Fourier discrète** (**TFD**) sur F est l'application F_α aussi appelée **transformation de Mattson-Solomon**, telle que :

$$F_\alpha : F[X]/\langle X^n - 1\rangle \rightarrow \mathbb{K}[X]/\langle X^n - 1\rangle$$

$$a(X) \mapsto \hat{a}(X)$$

Le polynôme $\hat{a}(X) = \sum_{j=0}^{n-1} \hat{a}_j X^{n-j}$ est appelé le polynôme de Mattson-Solomon .

Remarque 4.3.

Le polynôme $\hat{a}(X)$ s'écrit $\hat{a}(X) = \sum_{k=0}^{n-1} \hat{a}_{-k} X^k$, avec $\hat{a}_{-k} = a(\alpha^{-k})$.

En effet, on fait un changement d'indice k=n-j sur $\hat{a}(X) = \sum_{j=0}^{n-1} \hat{a}_j X^{n-j}$, on obtient :

$$\hat{a}(X) = \sum_{k=1}^{k=n} \hat{a}_{n-k} X^k,$$

et comme les indices sont calculés modulo *n,* alors

$$\hat{a}(X) = \sum_{k=0}^{n-1} \hat{a}_{-k} X^k.$$

Lemme 4.3.

Soit $\lambda \in \mathbb{K}$ une racine nième de l'unité, alors :

$$\sum_{i=0}^{n-1} \lambda^i = \begin{cases} 0 & si \quad \lambda \neq 1 \\ n & si \quad \lambda = 1 \end{cases} .$$

Preuve.

Si $\lambda \neq 1$, comme $\lambda^n = 1$, alors

$$\sum_{i=0}^{n-1}\lambda^i = \frac{\lambda^n - 1}{\lambda - 1} = 0 \ .$$

Théorème 4.4. (Formule d'inversion)

Si $p \wedge n = 1$, alors la transformation de Mattson-Solomon $\hat{a}(X)$ admet une transformation inverse, i.e. si $\hat{a}(X) = F_\alpha\big(a(x)\big)$, alors

$$a(X) = \frac{1}{n}\sum_{i=0}^{n-1}\hat{a}(\alpha^i)X^i.$$

Preuve On a

$$\begin{aligned}\hat{a}(\alpha^i) &= \sum_{j=0}^{n-1}\hat{a}_j\,\alpha^{-ij}\\ &= \sum_{j=0}^{n-1}a(\alpha^j)\,\alpha^{-ij}\\ &= \sum_{j=0}^{n-1}\sum_{k=0}^{n-1}a_k\alpha^{kj}\,\alpha^{-ij}\\ &= \sum_{k=0}^{n-1}a_k\sum_{j=0}^{n-1}\alpha^{j(k-i)}\\ &= na_i.\end{aligned}$$

Donc, pour tout $i \in \{0,1,...,n-1\}$.

$$a_i = \frac{1}{n}\hat{a}(\alpha^i).$$

D'où

$$a(X) = \frac{1}{n}\sum_{i=0}^{n-1}\hat{a}(\alpha^i)X^i.$$

Remarque 4.4.

Si $F = \mathbb{F}_2$ alors $a(X) = \sum_{i=0}^{n-1}\hat{a}(\alpha^i)X^i$.

Définition 4.7.

Soient $A(X), B(X)$ deux polynômes de $\mathbb{K}[X]/< X^n - 1 >$ tels que : $A(X) = \sum_{i=0}^{n-1}A_i\,X^i$ et $B(X) = \sum_{i=0}^{n-1}B_i\,X^i$, alors, le **produit d'Hadamard** de A(X) et B(X) est défini par :

$$A(X) \otimes B(X) = \sum_{j=0}^{j=n-1}A_j\,B_jX^j.$$

Théorème 4.5.

La transformation de Mattson-Solomon est un morphisme d'anneaux
de $(F[X]/\langle X^n - 1\rangle, +, \times)$ dans $(\mathbb{K}[X]/< X^n - 1 >, +, \otimes)$.

En particulier,

$$F_\alpha\big(p(X)\ \times q(X)\big)\ =\ F_\alpha\big(P(X)\big)\ \otimes\ F_\alpha\big(q(X)\big).$$

Preuve.

Il suffit montrer la condition de la somme, les deux autres sont claires.

Soient $a(X)=\sum_{i=0}^{n-1} a_i\,X^i$, $b(X)=\sum_{j=0}^{n-1} b_j\,X^j$ de $F[X]/<X^n-1>$.

$$c(X)=a(X)b(x)=\left(\sum_{i=0}^{n-1} a_i\,X^i\right)\left(\sum_{j=0}^{n-1} b_j\,X^j\right)=\sum_{i=0}^{n-1} c_i\,X^i$$

On a c_i est le coefficient de X^i, et comme le produit est dans $F[X]/<X^n-1>$, et en considérant que $b_{n+i}=b_i$ alors

$$\begin{aligned}
c_0 &= a_0b_0+a_1b_{n-1}+a_2b_{n-2}+\ldots+a_{n-1}b_1=\sum_{j=0}^{n-1} a_jb_{n-j+0}\,.\\
c_1 &= a_0b_1+a_1b_0+a_2b_{n-1}+\ldots+a_{n-1}b_2=\sum_{j=0}^{n-1} a_jb_{n-j+1}\,.\\
&\vdots\\
c_i &= a_0b_i+a_1b_{i-1}+a_2b_{i-2}+\ldots+a_{n-1}b_{i+1}=\sum_{j=0}^{n-1} a_jb_{n-j+i}\,.
\end{aligned}$$

On obtient,

$$a(X)b(X)=\sum_{i=0}^{n-1} c_iX^i=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_jb_{n-j+i}\,X^i.$$

$$\begin{aligned}
F_\alpha(a(X)b(X)) &= \sum_{k=0}^{n-1}\hat{c}_{-k}X^k\\
&= \sum_{k=0}^{n-1} c(\alpha^{-k})X^k,
\end{aligned}$$

D'où

$$F_\alpha(a(X)b(X))=\sum_{k=0}^{n-1}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_jb_{n-j+1}\,\alpha^{-ki}\,X^k\ \ldots\ (*)$$

D'autre part,

$$\begin{aligned}
\left(F_\alpha(a(X))\right) \otimes \left(F_\alpha(b(X))\right) &= \left(\sum_{i=0}^{n-1} \hat{a}_{-i} X^i\right) \otimes \left(\sum_{j=0}^{n-1} \hat{b}_{-j} X^j\right) \\
&= \sum_{k=0}^{n-1} \hat{a}_{-k} \hat{b}_{-k} X^k \\
&= \sum_{k=0}^{n-1} a(\alpha^{-k}) b(\alpha^{-k}) X^k \\
&= \sum_{k=0}^{n-1} \left(\sum_{i=0}^{n-1} a_i \alpha^{-ki}\right)\left(\sum_{j=0}^{n-1} b_j \alpha^{-kj}\right) X^k \\
&= \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_j \alpha^{-kj} b_{n-j+i}\, \alpha^{-k(n-j+i)}\, X^k \\
&= \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_j b_{n-j+1}\, \alpha^{-ki}\, X^k \\
&\overset{(*)}{=} F_\alpha(a(X)b(X)).
\end{aligned}$$

Corollaire 4.1.

Si $p \wedge n = 1$, ou p est la caracteristique du corps fini F et $\mathbb{K}$ le corps des racines *nièmes* de l'unité sur *F*, alors la transformation de Mattson-Solomon est un isomorphisme d'anneaux de $(F[X]/\langle X^n - 1\rangle, +, \times)$ dans $(\mathbb{K}[X]/< X^n - 1 >, +, \otimes)$.

Preuve.

On a la transformation de Mattson-Solomon est injective, de plus elle est surjective (théorème d'inversion), donc d'après le théorème précédent la transformation de Mattson-Solomon est un isomorphisme d'anneaux.

4.6.2 Algorithme de décodage par transformation de Fourier discrète

Soit $C(\mathrm{n}, \mathrm{k}, \mathrm{d})$ un code Reed-Solomon sur un corps fini $\mathbb{K}=\mathbb{F}_{2^m}$ *e*-correcteur, et de polynôme générateur $g(X) = (X - \alpha^b)(X - \alpha^{b+1}) \ldots (X - \alpha^{b+d-2})$ où α une racine primitive de l'unité du corps $\mathbb{K}=\mathbb{F}_{2^m}$ (corps des racines *n*iémes de l'unité sur $\mathbb{F}_2$).

Donc g(x) admet $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+d-2}$ $(b > 0)$ comme racines.

On prend F= $\mathbb{K} = \mathbb{F}_{2^m}$.

- **Calcul du syndrome de l'erreur**

Soit y(X) le mot reçu, ε(X) le mot erreur avec $(\varepsilon(X)) \leq e$, le syndrome de l'erreur est donc :

$$y\left(\alpha^{b+j}\right) = \varepsilon\left(\alpha^{b+j}\right), 0 \leq j \leq d - 2, (b > 0) \ \ldots \ (**),$$

le mot erreur s'écrit :

$$\varepsilon(X) = \varepsilon_0 + \varepsilon_1 X + \varepsilon_2 X^2 + \cdots + \varepsilon_{n-1} X^{n-1}.$$

La transformée de Fourrier de ε(X) est égale à :

$\hat{\varepsilon}(X) = \sum_{i=0}^{n-1} \hat{\varepsilon}_{n-i} X^i = \hat{\varepsilon}_0 + \hat{\varepsilon}_{n-1} X + \hat{\varepsilon}_{n-1} X^2 + \cdots + \hat{\varepsilon}_2 X^{n-2} + \hat{\varepsilon}_1 X^{n-1}.$

D'après la relation $(**)$, les d $-$ 1 coefficients de $\hat{\varepsilon}(X)$ sont trouvés.

il reste donc de déterminer les autres coefficients de ε̂(X).

- **Détermination du polynôme localisateur de l'erreur**

Soit v le poids de l'erreur c.à.d. $v = w(\varepsilon(X))$ avec $v \leq e$. Les localisateurs des positions des erreurs, sont les $X_i = \alpha^i$, pour $1 \leq i \leq v$.

On note I l'ensemble des positions de l'erreur : $I = \{i, 0 \leq i \leq n-1 / \varepsilon_i \neq 0\}$

Le polynôme localisateur de l'erreur est $\sigma(X) = \prod_{i \in I} (1 - X_i X)$.

Qu'on peut écrire : $\sigma(X) = \sigma_v X^v + \sigma_{v-1} X^{v-1} : + \ldots + \sigma_1 X + 1$

Les racines de $\sigma(X)$ sont les inverses des localisateurs des positions erronées, on a donc :

$$\text{si } i \in I : \ \sigma(X_i^{-1}) = \sigma(\alpha^{-i}) = 0 \text{ et } \varepsilon_i \neq 0$$

$$\text{si } i \notin I : \sigma(X_i^{-1}) = \sigma(\alpha^{-i}) \neq 0 \text{ et } \varepsilon_i = 0$$

Les $\sigma(\alpha^{-i})$ pour $i \in \{1, \ldots, n\}$ sont les coefficients de la transformée de Fourrier de $\sigma(X)$, ce qui permet d'écrire $\varepsilon(X) \otimes \hat{\sigma}(X) = 0$, où $\hat{\sigma}(X)$ est la transformée de Fourrier de $\sigma(X)$. Alors,

$$\hat{\varepsilon}(X) \times \sigma(X) \equiv 0 \ (mod\ (X^n - 1))$$

En effet :

Calculons d'abord $\hat{\varepsilon}(X) \times \sigma(X)$

On a : $\hat{\varepsilon}(X) = \sum_{i=0}^{n-1} \hat{\varepsilon}_{n-i} X^i$

Et $\sigma(X) = \sum_{i=0}^{v} \sigma_i X^i = \sum_{i=0}^{n-1} \sigma_i X^i$, tels que : $\sigma_i = 0$ pour $v + 1 \leq i \leq n$.

Donc, $\hat{\varepsilon}(X) \times \sigma(X) = (\hat{\varepsilon}_0 + \hat{\varepsilon}_{n-1} X + \ldots + \hat{\varepsilon}_1 X^{n-1})(\sigma_0 + \sigma_1 X + \ldots + \sigma_{n-1} X^{n-1})$

$= \sum_{k=0}^{n-1} c_k X^k$

tels que : $c_0 = \hat{\varepsilon}_0\sigma_0 + \hat{\varepsilon}_{n-1}\sigma_{n-1}+\ldots+\hat{\varepsilon}_1\sigma_1 = \sum_{i=0}^{n-1}\hat{\varepsilon}_i\sigma_i$

$c_1 = \hat{\varepsilon}_0\sigma_1 + \hat{\varepsilon}_{n-1}\sigma_{0=n} + \hat{\varepsilon}_{n-2}\sigma_{n-1}+\ldots+\hat{\varepsilon}_1\sigma_2 = \sum_{i=0}^{n-1}\hat{\varepsilon}_i\sigma_{i+1}$

$c_2 = \hat{\varepsilon}_0\sigma_2 + \hat{\varepsilon}_{n-1}\sigma_{1=n+1} + \hat{\varepsilon}_{n-2}\sigma_{0=n} + \hat{\varepsilon}_{n-3}\sigma_{n-1}+\ldots+\hat{\varepsilon}_1\sigma_3 = \sum_{i=0}^{n-1}\hat{\varepsilon}_i\sigma_{i+2}$

$\vdots$

Et ainsi de suite, à la fin on trouve :

$$\hat{\varepsilon}(X) \times \sigma(X) = \sum_{k=0}^{n-1}\sum_{i=0}^{n-1}\hat{\varepsilon}_i\sigma_{i+k}\,X^k = \sum_{k=0}^{n-1}\sum_{j=0}^{n-1}\hat{\varepsilon}_{j-k}\sigma_j\,X^k$$

$$= \sum_{k=0}^{n-1}\sum_{j=0}^{n-1}\varepsilon\left(\alpha^{j-k}\right)\sigma_j X^k$$

$$= \sum_{k=0}^{n-1}\sum_{i=0}^{n-1}\varepsilon_i\alpha^{-ik}X^k\sum_{j=0}^{n-1}\sigma_j\alpha^{ij}$$

$$= \sum_{k=0}^{n-1}\sum_{i=0}^{n-1}\varepsilon_i\sigma(\alpha^i)\alpha^{-ik}X^k$$

$$= \sum_{k=0}^{n-1}\sum_{i=0}^{n-1}\varepsilon_i\hat{\sigma}_i\alpha^{-ik}X^k = \sum_{k=0}^{n-1}\varepsilon \otimes \hat{\sigma}(\alpha^{-k})\,X^k$$

$$\equiv 0\ \left(mod(X^n - 1)\right)$$

Ceci donne un système d'équations à résoudre.

Supposons qu'il y a au plus *e* erreurs, le polynôme σ a donc au plus v racines, il est donc au plus de degré v, et donc $\sigma_i = 0$, pour $v+1 \le i \le n$. Il reste à déterminer $\sigma_1, \sigma_2, \ldots, \sigma_v$ et $\hat{\varepsilon}_d, \ldots, \hat{\varepsilon}_n$.

Le système s'écrit, où les calculs sur les indices sont effectués modulo *n* comme suit:

$$\begin{cases} \hat{\varepsilon}_0 + \hat{\varepsilon}_1\sigma_1 + \hat{\varepsilon}_2\sigma_2+\ldots+\hat{\varepsilon}_v\sigma_v = 0 \\ \hat{\varepsilon}_{n-1} + \hat{\varepsilon}_0\sigma_1 + \hat{\varepsilon}_1\sigma_2+\ldots+\hat{\varepsilon}_{v-1}\sigma_v = 0 \\ \hat{\varepsilon}_{n-2} + \hat{\varepsilon}_{n-1}\sigma_1 + \hat{\varepsilon}_0\sigma_2+\ldots+\hat{\varepsilon}_{v-2}\sigma_v = 0 \\ \vdots \\ \hat{\varepsilon}_{n-1} + \hat{\varepsilon}_{n-i+1}\sigma_1 + \hat{\varepsilon}_{n-i+2}\sigma_2+\ldots+\hat{\varepsilon}_{v-i}\sigma_v = 0 \\ \vdots \\ \hat{\varepsilon}_1 + \hat{\varepsilon}_2\sigma_1 + \hat{\varepsilon}_3\sigma_2+\ldots+\hat{\varepsilon}_{v+1}\sigma_v = 0 \end{cases}$$

Les $d-1$ coefficients de la transformée de Fourier de l'erreur. $\hat{\varepsilon}_0, \hat{\varepsilon}_1, \ldots, \hat{\varepsilon}_{d-1}$sont connus. En considérant les dernières équations du système il est possible de déterminer les coefficients du polynôme localisateur de l'erreur $\sigma_1, \sigma_2, \ldots, \sigma_v$.

- **Détermination des autres coefficients de la transformée de Fourier de l'erreur**

Les $n-v$ premières équations du système permettent de déterminer $\hat{\varepsilon}_d, \hat{\varepsilon}_{d+1}, \ldots, \hat{\varepsilon}_n$. En remplaçant $\sigma_1, \sigma_2, \ldots, \sigma_v$ par les valeurs trouvées précédemment. La transformée de Fourier de l'erreur $\hat{\varepsilon}(X)$ est désormais connue.

- **Détermination de $\boldsymbol{\varepsilon(X)}$ par transformation de Fourier inverse**

On applique la transformation de Fourier inverse pour trouver le mot erreur $\varepsilon(X)$ tel que :

$$\varepsilon(X) = \frac{1}{n} \sum_{i=0}^{n-1} \hat{\varepsilon}(\alpha^i) X^i.$$

L'Algorithme de Décodage par transformation de Fourier discrète se résume en cinq étapes :
Soient $y(X)$ le mot reçu, $\varepsilon(X)$ le mot erreur avec $w(\varepsilon(X)) \leq e$ et $g(X)$ le polynôme générateur. Soit les $\delta - 1$ racines de $g(X)$ d'exposants consécutifs. $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{\delta+b-2}$ avec $b > 0$:

1) Calcul des $\delta - 1$ coefficients de la transformée de Fourier de l'erreur $\varepsilon(X)$ par le calcul des composantes du Syndromes.

2) Détermination des coefficients $\sigma_1, \sigma_2, \ldots, \sigma_v$ du polynôme localisateur de l'erreur, par la résolution des v dernières équations du système.

$$\hat{\varepsilon}(X) \times \sigma(X) \equiv 0 \left(mod\ (X^n - 1) \right)$$

3) Détermination de tous les coefficients de la transformée de Fourier de l'erreur $\hat{\varepsilon}(X)$ par la résolution des $n-v$ premières équations du même système.

4) Détermination de $\varepsilon(X)$ par la transformation de Fourier inverse de $\hat{\varepsilon}(X)$.

5) Correction de l'erreur i.e. trouver le mot envoyé c(X).

$$c(X) = y(X) - \varepsilon(X).$$

Exemple 4.8.

Soit le code de Reed-Solomon C(3,1,3) sur $\mathbb{F}_4$ de polynôme générateur $g(X) = X^2 + X + 1$, ce polynôme a 2 racines : α et α^2. Soit $y(X) = X^2 + 1$, le mot reçu avec *v*=1 erreur.

1. Calcul du syndrome :

$$s_1 = y(\alpha) = \alpha$$
$$s_2 = y(\alpha^2) = \alpha^2$$

Le syndrome donne les 2 premiers coefficients de la transformée de Fourier de $\varepsilon(X)$:

$\hat{\varepsilon}_1 = \alpha$et $\hat{\varepsilon}_2 = \alpha^2$. On a donc:

$$\hat{\varepsilon}(X) = \sum_{i=0}^{2} \hat{\varepsilon}_{3-i} X^i = \hat{\varepsilon}_0 + \hat{\varepsilon}_2 X + \hat{\varepsilon}_1 X^2.$$

Le polynôme localisateur de l'erreur est de degré v=1. Il est de la forme :

$$\sigma(X) = \sigma_1 X + 1.$$

L'équation suivante :

$$\hat{\varepsilon}(X) \times \sigma(X) = \sum_{k=0}^{2} \sum_{j=0}^{1} \hat{\varepsilon}_{j-k} \sigma_j X^i \equiv 0(\mathrm{mod}(X^3 - 1))$$

Donne le système suivant :

$$\begin{cases} \hat{\varepsilon}_0 + \hat{\varepsilon}_1 \sigma_1 = 0 \\ \hat{\varepsilon}_2 + \hat{\varepsilon}_0 \sigma_1 = 0 \\ \hat{\varepsilon}_1 + \hat{\varepsilon}_2 \sigma_1 = 0 \end{cases}$$

2. Détermination du polynôme localisateur de l'erreur :
   Les coefficients $\hat{\varepsilon}_1$ et $\hat{\varepsilon}_2$ sont connus ($\hat{\varepsilon}_1 = \alpha$ et $\hat{\varepsilon}_2 = \alpha^2$) .
   La résolution de système précédent donne $\sigma_1 = \alpha^2$.
3. Détermination des autres coefficients de la transformée de Fourier de l'erreur :
   σ_1 est remplacés par leur valeur dans les autres équations du système nécessaire à la détermination de $\hat{\varepsilon}_0$. La résolution de ce nouveau système donne : $\hat{\varepsilon}_0 = \alpha^3 = 1$.

   Donc la transformée de Fourier de $\varepsilon(X)$ est : $\hat{\varepsilon}(X) = 1 + \alpha^2 X + \alpha X^2$.

   En utilisant la transformation de Fourier inverse : $\varepsilon(X)$.

   On trouve : $\hat{\varepsilon}(1) = 0, \hat{\varepsilon}(\alpha) = 1$ et $\hat{\varepsilon}(\alpha^2) = 0$. Donc $\varepsilon(X) = X$.

   Et le mot envoyé est $c(X) = y(X) - \varepsilon(X)$.

   Donc $c(X) = X^2 + X + 1$.

Exemple 4.9.

Soit le code de Reed-Solomon C(15,9,7) sur le corps $\mathbb{F}_{16}$, de polynôme générateur

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

Ce polynôme a 6 racines : $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$ et α^6. Soit le mot reçu $y(X) = \alpha X^{14} + \alpha^2 X^{12} + \alpha^{13} X^4$, avec $w(\varepsilon(X)) = 3$.

1) Construction du corps $\mathbb{F}_{16}$

$\mathbb{F}_{16}$=*{0,*$\alpha^i / 0 \leq i \leq 14$*}*, son polynôme primitif est : $M_\alpha(X)=X^4+X+1$.

On a : $M_\alpha(\alpha)=0$ *donc* $\alpha^4=\alpha+1$, *donc :* $\alpha^6=\alpha^3+\alpha^2$; $\alpha^5=\alpha^2+\alpha$; $\alpha^7=\alpha^3+\alpha+1$; $\alpha^8=\alpha^2+1$;

$\alpha^9=\alpha^3+\alpha^2$; $\alpha^{10}=\alpha^2+\alpha+1$; $\alpha^{11}=\alpha^3+\alpha^2+\alpha$; $\alpha^{12}=\alpha^2+1$; $\alpha^{13}=\alpha^3+\alpha^2+\alpha+1$; $\alpha^{14}=\alpha^3+1$.

2) Calcul du syndrome :

On a $s_j = y(\alpha^j)$, $1 \leq j \leq 6$.

$$s_1 = y(\alpha) = \alpha^6$$
$$s_2 = y(\alpha^2) = \alpha^7$$
$$s_3 = y(\alpha^3) = \alpha^{12}$$
$$s_4 = y(\alpha^4) = 0$$
$$s_5 = y(\alpha^5) = \alpha$$
$$s_6 = y(\alpha^6) = \alpha^8$$

Le syndrome donne les 6 premiers coefficients de la transformée de Fourier de $\varepsilon(X)$;

$$\hat{\varepsilon}_1 = \alpha^6, \hat{\varepsilon}_2 = \alpha^7, \hat{\varepsilon}_3 = \alpha^{12}, \hat{\varepsilon}_4 = 0, \hat{\varepsilon}_5 = \alpha, \hat{\varepsilon}_6 = \alpha^8,$$

la transformée de Fourier de $\varepsilon(X)$:

$$\hat{\varepsilon}(X) = \sum_{i=0}^{14} \hat{\varepsilon}_{15-i} X^i = \hat{\varepsilon}_0 + \hat{\varepsilon}_{14} X + \hat{\varepsilon}_{13} X^2 + \ldots + \hat{\varepsilon}_2 X^{13} + \hat{\varepsilon}_1 X^{14}$$

Le polynôme localisateur de l'erreur est de degré v=3. Il est de la forme :

$\sigma(X) = \sigma_3 X^3 + \sigma_2 X^2 + \sigma_1 X + 1.$

L'équation suivante : $\hat{\varepsilon}(X) \times \sigma(X) = \sum_{k=0}^{14} \sum_{j=0}^{3} \hat{\varepsilon}_{j-k}\, \sigma_j X^k \equiv 0 (\mathrm{mod}(X^{15} - 1))$

Donne le système suivant :

$$\begin{cases} \hat{\varepsilon}_0 + \hat{\varepsilon}_1\sigma_1 + \hat{\varepsilon}_2\sigma_2 + \hat{\varepsilon}_3\sigma_3 = 0 \\ \hat{\varepsilon}_{14} + \hat{\varepsilon}_0\sigma_1 + \hat{\varepsilon}_1\sigma_2 + \hat{\varepsilon}_2\sigma_3 = 0 \\ \hat{\varepsilon}_{13} + \hat{\varepsilon}_{14}\sigma_1 + \hat{\varepsilon}_0\sigma_2 + \hat{\varepsilon}_1\sigma_3 = 0 \\ \hat{\varepsilon}_{12} + \hat{\varepsilon}_{13}\sigma_1 + \hat{\varepsilon}_{14}\sigma_2 + \hat{\varepsilon}_0\sigma_3 = 0 \\ \hat{\varepsilon}_{11} + \hat{\varepsilon}_{12}\sigma_1 + \hat{\varepsilon}_{13}\sigma_2 + \hat{\varepsilon}_{14}\sigma_3 = 0 \\ \hat{\varepsilon}_{10} + \hat{\varepsilon}_{11}\sigma_1 + \hat{\varepsilon}_{12}\sigma_2 + \hat{\varepsilon}_{13}\sigma_3 = 0 \\ \hat{\varepsilon}_9 + \hat{\varepsilon}_{10}\sigma_1 + \hat{\varepsilon}_{11}\sigma_2 + \hat{\varepsilon}_{12}\sigma_3 = 0 \\ \hat{\varepsilon}_8 + \hat{\varepsilon}_9\sigma_1 + \hat{\varepsilon}_{10}\sigma_2 + \hat{\varepsilon}_{11}\sigma_3 = 0 \\ \hat{\varepsilon}_7 + \hat{\varepsilon}_8\sigma_1 + \hat{\varepsilon}_9\sigma_2 + \hat{\varepsilon}_{10}\sigma_3 = 0 \\ \hat{\varepsilon}_6 + \hat{\varepsilon}_7\sigma_1 + \hat{\varepsilon}_8\sigma_2 + \hat{\varepsilon}_9\sigma_3 = 0 \\ \hat{\varepsilon}_5 + \hat{\varepsilon}_6\sigma_1 + \hat{\varepsilon}_7\sigma_2 + \hat{\varepsilon}_8\sigma_3 = 0 \\ \hat{\varepsilon}_4 + \hat{\varepsilon}_5\sigma_1 + \hat{\varepsilon}_6\sigma_2 + \hat{\varepsilon}_7\sigma_3 = 0 \\ \hat{\varepsilon}_3 + \hat{\varepsilon}_4\sigma_1 + \hat{\varepsilon}_5\sigma_2 + \hat{\varepsilon}_6\sigma_3 = 0 \\ \hat{\varepsilon}_2 + \hat{\varepsilon}_3\sigma_1 + \hat{\varepsilon}_4\sigma_2 + \hat{\varepsilon}_5\sigma_3 = 0 \\ \hat{\varepsilon}_1 + \hat{\varepsilon}_2\sigma_1 + \hat{\varepsilon}_3\sigma_2 + \hat{\varepsilon}_4\sigma_3 = 0 \end{cases}$$

3) Détermination du polynôme localisateur de l'erreur :

   Les coefficients $\hat{\varepsilon}_1, \hat{\varepsilon}_2, \hat{\varepsilon}_3, \hat{\varepsilon}_4, \hat{\varepsilon}_5, \hat{\varepsilon}_6$ sont connus tels que $\hat{\varepsilon}_1 = \alpha^6, \hat{\varepsilon}_2 = \alpha^7, \hat{\varepsilon}_3 = \alpha^{12}, \hat{\varepsilon}_4 = 0, \hat{\varepsilon}_5 = \alpha$ et $\hat{\varepsilon}_6 = \alpha^8$

   La résolution du système constitué par les trois dernière equations donne :

$$\begin{cases} \sigma_1 = \alpha^2 \\ \sigma_2 = \alpha^8 \\ \sigma_3 = 1 \end{cases}$$

   Le polynôme localisateur est : $\sigma(X) = X^3 + \alpha^8 X^2 + \alpha^2 X + 1$.

4) Détermination des autres coefficients de la transformée de Fourier de l'erreur :

   $\sigma_1, \sigma_2, \sigma_3$ sont remplacés par leurs valeurs dans les autres équations du système.

   Après les calculs en trouve :

   $\hat{\varepsilon}_0 = \alpha^7, \hat{\varepsilon}_{14} = \alpha^3, \hat{\varepsilon}_{13} = \alpha^7, \hat{\varepsilon}_{12} = \alpha^{12}, \hat{\varepsilon}_{11} = 0, \hat{\varepsilon}_{10} = \alpha^{13}, \hat{\varepsilon}_9 = \alpha^{11}, \hat{\varepsilon}_8 = 1, \hat{\varepsilon}_7 = \alpha^9$

   Donc la transformée de Fourier de $\boldsymbol{\varepsilon(X)}$ est :

$$\hat{\varepsilon}(X) = \alpha^7 + \alpha^3 X + \alpha^7 X^2 + \alpha^{12} X^3 + \alpha^{13} X^5 + \alpha^{11} X^6 + X^7 + \alpha^9 X^8 + \alpha^8 X^9 + \alpha X^{10} + \alpha^{12} X^{12} + \alpha^7 X^{13} + \alpha^6 X^{14}.$$

   En utilisant la transformation de Fourier inverse, on trouve:

$$\varepsilon(X) = \frac{1}{15} \sum_{i=0}^{14} \hat{\varepsilon}(\alpha^i)\, X^i = \sum_{i=0}^{14} \hat{\varepsilon}(\alpha^i)\, X^i.$$

   On trouve :

$$\hat{\varepsilon}(1) = \hat{\varepsilon}(\alpha) = \hat{\varepsilon}(\alpha^2) = \hat{\varepsilon}(\alpha^3) = \hat{\varepsilon}(\alpha^5) = \hat{\varepsilon}(\alpha^6) = \hat{\varepsilon}(\alpha^7) = \hat{\varepsilon}(\alpha^8) = \hat{\varepsilon}(\alpha^9) = \hat{\varepsilon}(\alpha^{10}) = \hat{\varepsilon}(\alpha^{11}) = \hat{\varepsilon}(\alpha^{13}) = 0.$$

Et $\hat{\varepsilon}(\alpha^4) = \alpha^{13}, \hat{\varepsilon}(\alpha^{12}) = \alpha^2, \hat{\varepsilon}(\alpha^{14}) = \alpha$.

Donc $\varepsilon(X) = \alpha X^{14} + \alpha^2 X^{12} + \alpha^{13} X^4 = y(X)$.

Et le mot envoyé est : $c(X) = y(X) - \varepsilon(X)$=0 (le mot nul).