$4^{\text{ème}}$ année Ingénieur SISC — Année universitaire 2021 – 2022

U.E : Codes Correcteurs d'Erreurs

Série de TD $n^0 6$

Ex-1- Corps de Galois, Élément primitif, Polynôme primitif.

$GF(2^4)$ est un corps d'extension de $GF(2)$. Le polynôme primitif $p(x) = x^4 + x^3 + 1$ peut être utilisé pour définir les éléments primitifs de $GF(16)$

1. Construire les éléments $GF(2^4) \;/ < p(x) = x^4 + x^3 + 1 >$.
2. Montrer que $\alpha^6\alpha^9$ et $\alpha^{26}\alpha^{19}$ sont également égaux à 1.
3. Dans GF(16) quel est l'inverse multiplicatif de α^i pour $i = 1, 2, 3, ..., 14$?

Ex-2- Code BCH, Polynôme générateur, Codage, Décodage.

On veut concevoir dans $GF(2^3)$ un code BCH (Bose-Chaudhuri-Hocquenghem) noté par la suite $C_{BCH}(n, k)$ avec une longueur de bloc $n = 7$ et une simple puis double capacité de correction d'erreur ($t = 1,\ 2$).

1. Construire les éléments $GF(2^3) \;/ < p(x) = x^3 + x + 1 >$.
2. Trouver les polynômes minimaux relatifs à $GF(2^3)$.
3. Donner le polynôme générateur dans chaque cas de figure ($t = 1, 2$).
4. Trouver le mot de code correspondant à chacun des messages suivants :
   - $t = 1,\ \ d = [1\ 0\ 1\ 1]$.
   - $t = 2,\ \ d = [0]$, puis $d = [1]$.
5. Dans le cas $t = 1$, on reçoit deux messages $r_1 = [1\,0\,1\,1\,1\,0\,0]$ et $r_2 = [1\,0\,1\,0\,0\,0\,0]$ erronés. Corriger ces deux messages, puis donner les deux mots de code correspondants.

Ex-3- Code BCH, Polynôme primitif, Polynôme minimal, Polynôme générateur.

On considère le polynôme $p(x) = x^4 + x + 1$ sur $GF(2)$ utilisé pour construire le corps d'extension $GF(2^4)$.

Racines conjuguées	Polynômes minimaux
0	x
1	$x + 1$
$\alpha,\ \alpha^2,\ \alpha^4,\ \alpha^8$	$x^4 + x + 1$
$\alpha^3,\ \alpha^6,\ \alpha^9,\ \alpha^{12}$	$x^4 + x^3 + x^2 + x + 1$
$\alpha^5,\ \alpha^{10}$	$x^2 + x + 1$
$\alpha^7,\ \alpha^{11},\ \alpha^{13},\ \alpha^{14}$	$x^4 + x^3 + 1$

1. Montrer que le polynôme $p(x)$ est primitif.
2. Déterminer les classes cyclotomiques relatives à $C_{BCH}(n = 15, k)$.
3. Déterminer le polynôme générateur du code $C_{BCH}(n, k)$ de longueur de block $n = 15$ dans le cas des capacités de corrections $t = 1, 2$ et 3 erreur(s).

4. Dans le cas $t = 4$, calculer le polynôme générateur. Quel type de code obtient-on ? Calculer d_c sa distance construite et d_{min} sa distance minimale.
5. Quels polynômes générateurs obtient-on avec $t = 5, 6$ et 7 ? Conclure.

Ex-4- Code BCH, Polynôme minimal.

Construire le corps de Galois $GF(2^m)$ généré par le polynôme $p(x)$, puis donner un tableau avec les représentations polynomiale et binaire de ses éléments dans chacun des cas suivants :

1. $GF(2^3)$ généré par $p(x) = x^3 + x^2 + 1$.
2. $GF(2^4)$ généré par $p(x) = x^4 + x + 1$.
3. Dans le cas de la question précédente, déterminer le polynôme minimal $\Phi(x)$ pour $\beta = \alpha^7$ dans $GF(2^4)$.

Ex-5- Code BCH, Polynôme générateur, Codage, Décodage.

On se propose de construire un code BCH de longueur $n = 15$ afin de corriger toutes les configurations de 2 erreurs.

1. Vérifier la liste donnée dans le tableau ci-dessous de $GF(2^4)\ /< q(x) = x^4 + x + 1 >$ (où α est un élément primitif).
2. Trouver les polynômes minimaux du code qu'on cherche à construire.
3. Donner son polynôme générateur.
4. Quel est le rendement de ce code ?
5. Coder le mot m = [1 0 1 1 0 1 1].
6. Décoder puis corriger le mot reçu d = [0 1 1 1 1 0 0 0 1 1 0 1 0 0 1].

Puissances α^i & Élements du corps	Représentations binaires	Puissances α^i & Élements du corps	Représentations binaires
0	0000	$\alpha^7 = \alpha^3 + \alpha + 1$	1011
$\alpha^0 = 1$	0001	$\alpha^8 = \alpha^2 + 1$	0101
$\alpha^1 = \alpha$	0010	$\alpha^9 = \alpha^3 + \alpha$	1010
$\alpha^2 = \alpha^2$	0100	$\alpha^{10} = \alpha^2 + \alpha + 1$	0111
$\alpha^3 = \alpha^3$	1000	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$	1110
$\alpha^4 = \alpha + 1$	0011	$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$	1111
$\alpha^5 = \alpha^2 + \alpha$	0110	$\alpha^{13} = \alpha^3 + \alpha^2 + 1$	1101
$\alpha^6 = \alpha^3 + \alpha^2$	1100	$\alpha^{14} = \alpha^3 + 1$	1001

Ex-6- Code BCH, Technique du décodage.

Dans une transmission de données numériques le code $C_{BCH}(15, 5)$ à triple correction d'erreur est utilisé avec un polynôme générateur $g(x)$. À la réception, le message intercepté est $r(x) = x^7 + x^2$.

1. Montrer que le polynôme générateur s'écrit $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$.
2. En utilisant la technique du décodage BCH, corriger $r(x)$ puis donner le mot de code transmis.