Université de Jijel. **Janvier 2020**
Département de Mathématiques.
Master II - Mathématiques Fondamentale-

Devoir de T.C.C.E.2

Exercice 1.

Soit C(n, k) un code cyclique sur le corps $\mathbb{K}=F_{2^r}$ des racines nièmes de l'unité, de générateur $g(X)=\sum_{i=0}^{i=t} g_i X^i$.

a- Montrer que C est un code systématique, et que le mot code associé au mot $a(X)=\sum_{i=0}^{i=k} a_i X^i$ est le mot $c(X)=X^t a(X)+S(X^t a(X))$ où S représente le syndrome.

b- Pour n=7, $g(X)=X^3+X^2+1$. Calculer en utilisant un registre à décalage circulaire, le syndrome $S(X^3 a(X))$.

Exercice 2.

Soit C(n=2^r-1, k) un code cyclique sur le corps $\mathbb{K}=F_{2^r}$ des racines nièmes de l'unité, de générateur $g(X)=(X-\alpha)(X-\alpha^2)(X-\alpha^4)\ldots(X-\alpha^{2^{r-1}})$, α une racine primitive de $\mathbb{K}$.

1- Montrer que C est un code BCH primitif au sens strict dont on détermine sa distance construite δ.

2- Pour r=3,

a- Montrer que g(X) est irréductible sur F_2.

b- C est-il un code de Reed-Solomon? Est-il un code de Hamming ? justifier.

Exercice 3.

Soient $\mathbb{K}=F_{2^r}$, le corps des racines 7èmes de l'unité, α une racine primitive de $\mathbb{K}$.

I) Soit C(n=7, k) un code de Reed-Solomon au sens strict sur $\mathbb{K}$, 2-correcteur.

1- Déterminer son générateur g(X) et une matrice de contrôle H.

2- Soit $y(X)=\sum_{i=0}^{i=6} y_i X^i$ le mot reçu. Montrer que son syndrome polynomial est : $S(y(X))=\sum_{j=1}^{j=4}\left(\sum_{i=0}^{i=6} y_i \alpha^{ji}\right)X^{j-1}$.

3- Décoder par la méthode algébrique le mot $y(X)=\alpha X^5+\alpha^6 X^6$, sachant que le poids de l'erreur $w(\varepsilon(X))=2$.

II) Supposons maintenant le code Reed-Solomon de longueur n=7, de générateur $g(X)=X^2+\alpha^4 X+\alpha^3$. Décoder par la méthode de T.F.D (Transformée de Fourier Discrète) le mot reçu $y(X)=\alpha^3+X^2$.

Exercice 4.

I. 1. Soit C(n, k, d) le code cyclique sur le corps $\mathbb{K}=F_{2^r}$ des racines 7eme de l'unité sur F_2, de racine primitive α, engendré par $g(X)=X^3+X+1$. Décrire le corps $\mathbb{K}=F_{2^r}$.

2. Déterminer la longueur n, la dimension k et montrer que la matrice génératrice normalisée $G_N=(I_k, A)$

Tel que $A=\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 1 & 1\\ 1 & 0 & 1\end{pmatrix}$ et déduire une matrice de contrôle H de C.

3. Montrer que C(n, k, d) est un code BCH et déterminer sa capacité e.
   Soit le mot reçu $y(X) = X^6 + X^5 + X^2 + 1$

a. En utilisant un circuit à décalage circulaire, calculer le syndrome de y(X) ?est ce que $y(X) \in C$?.
b. Décoder y(X) par **la méthode Algebrique.**

II- **Application à la cryptographie de McEliece**

1- Pour se communiquer entre eux **ALI** et **BADIS** utilisent la cryptographie de **McEliece**.
BADIS choisit le code C(n, k, e) et choisit comme clés secrètes, la matrice génératrice normalisée
G_N de C, la matrice inversible $S= \tau_{13}(I_k)$ et la matrice de permutation $P=P\ \tau_{23}(I_n)$.
ALI et **BADIS** se mettent d'accord sur le chiffrement des lettres de A à P comme suit :

A	B	C	D	E	F	G	H
0000	0001	0010	0100	1000	0011	0101	1001
I	J	K	L	M	N	O	P
0110	1010	1100	0111	1011	1101	1110	1111

a) Déterminer la clé publique (G', e) ou e est la capacité de correction de C.

b) **ALI** chiffre le mot **m=MF** et l'envoya à **BADIS**. Quel est le message chiffré **c** reçu par **BADIS**.

c) Supposons que **BADIS** a reçu le message **c=0011100110 0100101000** de **ALI.** Déchiffrer **c** pour déterminer le message **m** (en lettres) que **ALI** a envoyé à **BADIS**?

Exercice 5.

Soit le corps de Galois $\mathbb{K}=\mathbb{F}_{2^r}$ / $r \in \mathbb{N}^*$, α une racine primitive de $\mathbb{K}$..

1. Donner la définition d'un code C(n, k, d) de Reed-Solomon au sens strict sur $\mathbb{K}$, de générateur un polynôme g(X) de degré t.
2. Pour r=3. t=4. Déterminer le générateur g(X), n, k et d.

Décoder le mot reçu $y(X)= \alpha^3+\alpha X^5+X^6$ par la méthode T.F.D sachant qu'il contient deux erreurs.

Responsable du Module.
M . CHELGHAM