Exercices

Les exercices de 1 à 19 traitent les codes linéaires et ceux de 20 à 40 sont sur les codes cycliques.

Exercice1.

Soit le code binaire C = {0000, 1011, 0101, 1110}.

1. Quelle est la longueur du code ?
2. Quelle est la distance minimale du code ?
3. Ce code C vérifie-t-il la condition de décodage d'ordre e = 1 ? c.à.d. est-il 1-correcteur ?

Exercice 2.

Soit le code ternaire C = {0000, 0121, 1110, 0212, 2220, 1201, 2102, 1022, 2011}.

1. Montrer que C est un code linéaire et donner ces paramètres (n, k, d)?
2. Quelle est la capacité de correction e de ce code ?
3. Déterminer une matrice génératrice G et une matrice de contrôle de C.

Exercice 3.

On considère le code linéaire binaire $C(n, k, d)$ définie par une matrice de contrôle

$$H = \begin{pmatrix} 1\,0\,1\,1\,1\,0\,0\,0 \\ 0\,1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,0\,1\,0\,0\,1\,0 \\ 1\,1\,1\,1\,1\,1\,1\,1 \end{pmatrix}.$$

1. Quelles sont la longueur n, la dimension k et la distance d de ce code?
2. Montrer que C est systématique et donner sa matrice génératrice G_N.
3. Trouver le mot code c provenant du mot x=1010 par G_N.
4. Décoder si possible les mots y_1=11111000, y_2=11000001, y_3=01011101

Exercice 4.

Soit $C(n, k, d)$ un code linéaire de matrice de contrôle H et $r \in \mathbb{N}^*$.

Montrer que : $d \geq (r+1)$ si et seulement si tout sous-ensemble de r colonnes de H est libre.

Exercice 5.

On considère le code linéaire trinaire (sur le corps F_3) $C(n, k, d)$ définie par son code orthogonal

$$C^{\perp} = \{(x_1 + x_3, 2x_1 + 2x_2 + x_3,\ x_1 + 2x_3,\ x_2,\ x_3) / \ x_i \in F_3\ \}$$

1. Déterminer une base de $C^{\perp}$ et déduire la longueur n et la dimension k du code C?
2. Déduire une matrice de contrôle H de C et sa distance minimale d.
3. Montrer que C est systématique et donner sa matrice génératrice normalisée G_N, et construire ce code.

4. Décoder si possible les mots y_1=22021, y_2=21211, y_3=11120, y_4=11110

Exercice 6.

Soit $C(n, k, d)$ un code binaire, et H sa matrice de contrôle.

1. Montrer que la distance minimale d est le plus petit nombre de colonnes de H telles que leur somme soit nulle.
2. Déduire que si tout sous-ensemble de r-1 colonnes de H est libre, alors $d \geq r$.

Exercice 7.

Soit d la distance minimale d'un code linéaire C. Montrer que si $d \geq 3$ alors C vérifie la condition de décodage d'ordre 1.

Exercice 8.

Soit $C(n, k, d)$ le code binaire de matrice génératrice G définie par :

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

1. Déterminer les paramètres n et k. Montrer que C n'est pas systématique.
2. Montrer que C est équivalent à un code systématique C_s (en appliquant la permutation τ_{14}) qu'on détermine sa matrice génératrice normalisée G_N. Construire le code C_s.
3. Déduire une matrice de contrôle H_N du code C_s. Calculer par deux méthodes la distance d.
4. Corriger si possible les mots suivants : y_1=111100, y_2=111101, y_3=100010.

Exercice 9.

Soit $C(n, k, d)$ le code binaire de matrice de contrôle G définie par :

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

1. Montrer que C est systématique et déterminer les paramètres n et k.
2. Détermine sa matrice génératrice normalisée G_N. Construire le code C.
3. Corriger si possible les mots suivants : y_1=0001110, y_2=0010100.

Exercice 10.

Soit $C(n, k, d)$ un code binaire sur l'alphabet A (c.à.d. A={0, 1}, q=|A|=2), $r \in \mathbb{N}^*$

1. Pour tout $x \in A^n$, on note $B(x, r)$=$\{y \in A^n : d(x, y) \leq r\}$ la boule de centre x et de rayon r et $S(x, i) = \{y \in A^n : d(x, y) = i\}$ la sphère de centre x et de rayon i.

Montrer que $|B(x, r)| = \sum_{i=1}^{i=r} |S(x, i)| = \sum_{i=0}^{i=r} C_n^i$.

2. Si le code C est de capacité e et Sachant que : $\bigcup_{x \in C} B(x, e) \subset A^n$.

Montrer que: | C | $\leq \frac{2^n}{\sum_{i=0}^{i=e} C_n^i}$.

Remarques. 1) | **.** | représente le cardinal. 2) $C_n^i = \frac{n!}{i!(n-i)!}$

Exercice 11.

Soit $C(n, k, d)$ un code linéaire binaire, on définit le code étendu $C'(n', k', d')$ comme suit :

$$C' = \{ (x_1, \ldots, x_n, x_{n+1}) \in F_2^{n+1} \text{ tels que } (x_1, \ldots, x_n) \in C \text{ et } \sum_{i=1}^{i=n+1} x_i = 0 \}.$$

1- Déterminer les paramètres n', k' respectivement en fonction des paramètres n, k.

2- Donner selon la polarité de d, la distance d' en fonction de d.

Exercice 12.

Soit $C(n, k, d)$ un code linéaire sur un corps fini $\mathbb{K}$

1. Montrer que C peut détecter d-1 erreurs et peut corriger [(d-1)/2] erreurs.
2. Si $d = 2t+1$ (impaire) et u, v deux mots de $\mathbb{K}^n$ tel que $w(u) \leq t$ et $w(v) \leq t$, montrer qu'ils ont des syndromes différents, et que $\sum_{i=1}^{i=t} C_n^i \leq 2^{n-k}$.

Exercice 13.

Soit $C(n, k, d)$ le code binaire de matrice de contrôle H définie par :

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

1. Déterminer les paramètres n et k. Montrer que C est systématique.
2. Détermine sa matrice génératrice normalisée $\mathrm{G_N}$. Construire le code C.
3. Calculer la distance d.
4. Calculer la capacité de correction e et corriger si possible les mots suivants :

$$y_1 = 1011101,\ y_2 = 1110111,\ y_3 = 0010111.$$

Exercice 14. On considère un code de Hamming $C(7,4)$.

1. Coder le message suivant : x=010110010111
2. Décoder le message suivant : y=010001110010101101001

Exercice 15. On considère le code linéaire en blocs défini par une matrice de contrôle

$$\mathrm{H} = \begin{pmatrix} 1\,0\,1\,1\,1\,0\,0\,0 \\ 0\,1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,0\,1\,0\,0\,1\,0 \\ 1\,1\,1\,1\,1\,1\,1\,1 \end{pmatrix}$$

obtenue en rajoutant à la matrice de contrôle du code C(7,4,3), une colonne de zéros puis une ligne de uns.

1. Quelles sont la longueur *n* et la dimension *k* de ce code ?
2. A quoi correspond pratiquement la modification du code de Hamming ?
3. Mettre la matrice *H* sous forme systématique.
4. Trouver une matrice génératrice *G* de ce code.
5. Montrer que ce code détecte toutes les mots de deux erreurs et corrige toutes les configurations d'une erreur.

Exercice 16. Taille de paquets et taux de transfert (rendement)

L'objet de cet exercice est de comparer les taux de transmission et la fiabilité d'un code par répétition et un code de Hamming. Le but est de démontrer que dans le cas d'un canal bruité, émettre des paquets longs est plus efficace qu'émettre des paquets courts. On désire transmettre un message de 10000 bits à travers un canal bruité. On considère une probabilité d'erreur p= 0,01.

Codage par répétition : Chaque bit est émis trois fois. Le décodage se fait par un vote à la majorité.

1. Quel est le taux de transmission ?
2. Quelle est la probabilité que le décodage soit incorrect ?
3. Combien des 10000 bits du message ne sont pas correctement transmis ?

Paquets de 9 bits : On considère un code Hamming(9,3). Le message est envoyé sous forme de paquets de 9 bits, de la forme (s_1, s_2, s_3, t_1, t_2, t_3, t_4, t_5, t_6). Les trois premiers bits s_1,s_2, s_3 constituent le message original, les six suivants t_1, ... , t_6 sont les bits de contrôle.

4. Quel est le taux de transmission ?
5. Combien y a-t-il de configuration possible de 0 , 1 , ou 2 erreurs dans un tel paquet de 9 bits
6. Supposons qu'il existe un codage tel que les 6 bits de contrôle puissent localiser toutes les configurations jusqu'à deux erreurs. Quel est alors la probabilité qu'un tel paquet de 9 bits ne soit pas décodé correctement ?
7. Combien des 10000 bits du message ne sont pas transmis correctement ?

Exercice 17. On considère l'ensemble *C* définie par :

C={$(2x_1 + x_2 + x_3,\ x_1 + 2x_2 + 2x_3,\ 2x_1 + x_2 + x_3, x_1 + 2x_2 + 2x_3, x_2,\ 2x_1 + x_2 + x_3,\ 2x_2)/\ x_i \in \mathrm{F}_3$ }

1. Montrer que C est un code linéaire dont on détermine une base, sa longueur n et sa dimension k.
2. Donner une matrice génératrice G et déduire que C n'est pas systématique.
3. Soit C_s l'image de C par la transposition τ_{23}. Montrer que C_s est un code systématique dont on détermine sa matrice génératrice normalisée G_N et une matrice de contrôle H_N.
4. Construire le code C_s et déduire sa distance d et sa capacité de correction e.
5. Décoder si possible les mots y_1=0012102, y_2=121211.
6. Bob a envoyé un message $m=m_1m_2$ à Alice qui possède comme clés secrètes les matrices G_N, $S=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}$ et $P=P_\sigma$ tel que la permutation $\sigma = \begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 1 & 2 & 4 & 5 & 3 & 6 & 7\end{bmatrix}$.
   a. Déduire la clé publique (G', e) que Bob a utilisé pour chiffrer m. Quel est le mot c envoyé à Alice ?
   b. Soit c=022211 un message reçu par Alice. Quel est le message clair m que Bob a envoyé à Alice ?

Exercice 18. Construire le code de Reed-Muller $RM(2, 3)$ de matrice génératrice $G(2, 3)$.

Exercice 19. Si q=5, construire le code de Hamming 5-aire pour m=2.

Les exercices suivants sont sur les codes cycliques

Exercice 20

Soit $C(n, k)$ un code cyclique sur le corps $\mathbb{K}=F_{2^r}$ des racines nièmes de l'unité, de générateur

$$g(X) = \sum_{i=0}^{i=t} g_i X^i.$$

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

Exercice 21

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 23

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 :

$S\big(y(X)\big) = \sum_{j=1}^{j=4}\big(\sum_{i=0}^{i=6} y_i \alpha^{ji}\big)X^{j-1}$.

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*(ε(X))=2.

II) Supposons maintenant le code Reed-Solomon de longueur *n*=7, de générateur le polynôme $g(X) = X^2 + \alpha^4 X + \alpha^3$.

Décoder par la méthode de T.F.D (Transformée de Fourier Discrète) le mot (polynôme) reçu $y(X) = \alpha^3 + X^2$.

Exercice 24

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

1. Donner la définition d'un code *C*(*n, k, d*) de Reed-Solomon au sens strict de générateur un polynôme

   $g(X)$ de degré *t*.
2. Donner les paramètres du code *C*(*n, k, d, e*). Est-il M.D.S ?
3. Pour *r*=3. *t*= 3. Calculer le générateur $g(X)$ et le polynôme de control $h(X)$ et déduire une matrice génératrice *G* et une matrice de contrôle *H*.
4. Décoder par la méthode algébrique, le mot $y(X) = \alpha^6 + \alpha X + \alpha^6 X^2$.

Exercice 25

Soit *C*(*n*=10, *k*) un code cyclique binaire sur le corps $\mathbb{K}= \mathbb{F}_{2^r}$ des racines 10eme de l'unité sur $\mathbb{F}_2$, de racine primitive α et de générateur $g(X)$.

1. Décrire le corps $\mathbb{K}=\mathbb{F}_{2^r}$ des racines 10eme de l'unité sur $\mathbb{F}_2$.

2. Déterminer le groupe $G_{10}(\mathbb{K})$ des racines 10^{eme} de l'unité en donnant son générateur β.
3. Décomposer le polynôme X^{10}-1 en produit de polynômes irréductibles sur $\mathbb{F}_2$.
4. Soit le polynôme $g(X) = X^5 - 1$. Montrer que le polynôme de control $h(X) = g(X)$ est un générateur d'un code cyclique C' dont on détermine sa dimension k', une matrice génératrice G' et une matrice de contrôle H'.
5. Soit $g(X) = X^5 + X^3 + X^2 + 1$, le générateur de $C(12, k)$. Montrer que le mot code associé à un mot a(X)= $\sum_{i=0}^{i=k-1} a_i X^i$ est $c(X) = X^5 a(X) + S(X^5 a(X))$. S signifie syndrome.
6. Calculer par un registre à décalage circulaire le syndrome de $X^5(X^3+X+1)$ et le mot code associé au mot X^3+X+1.

Exercice 26

Montrer que le dual d'un code cyclique $C(n, k)$ est un code cyclique $C'(n', k')$ qu'on détermine ces paramètres.

Exercice 27

Soit $C(n, k, d)$ un code cycliques non trivial sur le corps $\mathbb{K}=\mathbb{F}_{2^r}$ des racines $n$ièmes de l'unité sur $\mathbb{F}_2$, de racine primitive α et de générateur $g(X)$.

I- Supposons que la matrice H ci-dessous est une matrice de contrôle de C:

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \end{pmatrix}$$

1- Déterminer n, r et le polynôme primitif $M_\alpha(X)$ de $\mathbb{K}$ et décrire ce corps.

2- Calculer les classes cyclotomiques de α et α^3 et déduire les racines de $M_\alpha(X) et\ M_{\alpha^3}(X)$.

3- Soit c = $(c_0, c_1, \ldots, c_7)$.

Montrer que $c \in C$ si, et seulement si $c(X)$ est un multiple de $M_\alpha(X)M_{\alpha^3}(X)$

4- Déduire que $g(X) = M_\alpha(X)M_{\alpha^3}(X)$. De quel type de code s'agit-il. Déterminer k et d.

II- Supposons que $g(X) = M_{\alpha^3}(X)$.

1- Montrer que $C(n, k, d)$ est un code BCH, déterminer k et montrer que d=3.

2- Pour se communiquer entre eux ALICE et BOB utilisent la cryptographie de McEliece.

BOB choisit le code $C(n, k, d)$ et choisit comme clés secrètes, la matrice génératrice normalisée G_N de C, la matrice inversible $S= \tau_{12}(I_4)$ et la matrice de permutation $P= \tau_{23}(I_7)$.

ALICE et BOB se mettent d'accord sur le chiffrement des lettre de A à P comme suit :

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

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

b) BOB chiffre le mot **m=NON** et l'envoya à ALICE. Quel est le message chiffré **c** reçu par ALICE.

c) Supposons que ALICE a reçu le message **c=**0010110 **0001010** 0010110**.** Utiliser la méthode de piégeage d'erreurs, pour déterminer le message **m** que BOB a envoyé à ALICE?

Exercice 28

Soit *C(n=*2^r*-1, k, d)* un code cyclique sur le corps $\mathbb{K}=\mathbb{F}_{2^r}$ des racines *n*iemes de l'unité sur $\mathbb{F}_2$, de racine primitive α et de générateur $g(X)$.

1- Montrer que si $g(X) = (X-\alpha)(X-\alpha^2)$ ... $(X-\alpha^t)$, tel que *t* >1. Alors C admet la matrice *H* suivante comme matrice de contrôle :

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^t & \alpha^{2t} & \cdots & \alpha^{t(n-1)} \end{pmatrix}$$

2- De quel type de code s'agit-il ? Montrer que *d=t*+1.

3- Pour *r*=3 et *t*=4. Donner les paramètres du code *C* et développer le polynôme $g(X)$.

4- Soit $y(X) = X^3 + \alpha X^2 + \alpha^3 X$, le mot reçu ayant *v*=2 erreurs.
Décoder le mot $y(X)$ en utilisant la méthode algébrique.

Exercice 29

1. Soit $\mathbb{K}$ le corps des racines 7eme de l'unité sur $\mathbb{F}_2$, de racine primitive α et de polynôme primitif $M_\alpha(X)$ et soit *C*(*n*=7, *k, d*) le code linéaire sur $\mathbb{K}$ dont son code orthogonal (dual) $C^\perp$ est engendré par la matrice *H* donnée par:

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

a. Décrire le corps $\mathbb{K}$ et décomposer $X^7 - 1$ en produit de polynômes irréductibles sur $\mathbb{F}_2$.

b. Montrer que *C* est un code cyclique et déterminer son polynôme de control $h(X)$ et son polynôme générateur $g(X)$.

2. Déterminer les racines du polynôme $g(X)$ dans $\mathbb{K}$ et déduire que C est un code BCH dont on détermine sa distance d et sa capacité de correction e.
3. Soit le mot reçu $y(X) = X^6 + X^5 + X^4 + X + 1$.

a. En utilisant un circuit à décalage circulaire, calculer le syndrome de $y(X)$?

b. Décoder le mot $y(X)$ par la méthode de Meggitt.

Exercice 30

Soit *C*(*n, k*) un code cycliques binaire sur le corps $\mathbb{K}=\mathbb{F}_{2^r}$ des racines nièmes de l'unité sur $\mathbb{F}_2$, de racine primitive α et de générateur $g(X)$.

I- supposons que la matrice de contrôle *H* est définie par :

$$H = (1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6)$$

1. Déterminer *n* et *r* et le polynôme primitif $M_\alpha(X)$ et déduire le corps $\mathbb{K}$.
2. Déterminer les classes cyclotomiques de $\mathbb{K}^*= \mathbb{K}-\{0\}$ et déduire la décomposition du polynôme $X^n - 1$ sur $\mathbb{F}_2$ en polynômes minimaux (irréductibles).
3. Soit c = $(c_0, c_1, \ldots, c_6)$.

Montrer que $c \in C$ si et seulement si $c(X)$ est un multiple de $M_\alpha(X)$

4. Déduire que g(X) = $M_\alpha(X)$ et que *C* est un code BCH primitif au sens strict dont on détermine sa dimension *k* et sa distance construite δ.
5. Supposons $y(X) = X^5 + X^4 + X^3 + X^2 + X + 1$ le mot reçu.

a- Calculer par un registre à décalage circulaire S($y(X)$) le syndrome de $y(X)$.

b- Donner l'algorithme de Meggitt et décoder le mot $y(X)$ par cette méthode.

II- supposons que $g(X) = M_\alpha(X)\, M_{\alpha^3}(X)$.

1. Déterminer tous les racines de $g(X)$, et déduire que *C* est un code BCH et déterminer sa dimension k et montrer dans ce cas que d=7.
2. Soit $y(X) = \alpha^2 X^6 + \alpha X^5$ le mot reçu contenant *v*=2 erreurs. Calculer le polynôme localisateur et ces racines.
3. Donner l'algorithme de décodage algébrique du code et décoder le mot y(X) par cette méthode.

Exercice 31

Soit *C*(7, *k*) un code cycliques binaire sur le corps $\mathbb{K}=\mathbb{F}_{2^r}$ des racines 7^{iemes} de l'unité sur $\mathbb{F}_2$, de distance minimale *d*, de racine primitive α et de générateur $g(X)$.

1. Montrer que si $g(\alpha) = g(\alpha^2) = g(\alpha^3) = 0$, alors la matrice *H* suivante est une matrice de contrôle

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} \end{pmatrix}$$

2. En déduire qu'il existe un entier δ tel que $d \geq \delta$.
3. Si $\delta = n$ déduire dans ce cas que *C* est de distance $d = n$.

Exercice 32

I. **Code cyclique**

1. Soit $C(n, k, d)$ le code cyclique sur le corps $\mathbb{K}$ des racines 7eme de l'unité sur $\mathbb{F}_2$, de racine primitive α, engendré par $g(X) = X^4 + X^3 + X^2 + 1$. Décrire le corps $\mathbb{K}$ et donner la longueur *n*, la dimension *k*.
2. Déterminer une matrice génératrice de C, de la forme $G_S = (I_k/A)$ et déduire une matrice de contrôle *H*.
3. Déterminer la distance *d* et la capacité de correction e de *C*.
4. Soit le mot reçu $y(X) = X^6 + X^5 + X^3 + X^2 + 1$.

a. En utilisant un circuit à décalage circulaire, calculer le syndrome de $y(X)$.

b. Donner l'algorithme de la méthode de piégeage d'erreurs et décoder le mot $y(X)$ par cette méthode**.**

II- Application à la cryptographie de McEliece

Pour se communiquer entre eux, **ALICE** et **BOB** utilisent la cryptographie de **McEliece**.

BOB choisit le code $C(n, k, d)$ dans la partie **(I)** et choisit comme clés secrètes, la matrice génératrice G_S de *C*, la matrice inversible $S = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ et la matrice de permutation $P = P\tau_{23}(I_n)$.

ALICE et **BOB** se mettent d'accord sur le chiffrement des lettres suivantes :

A	B	C	D	E	F	M	N
000	100	010	001	110	101	011	111

1. Déterminer la clé publique (G', e) ou e est la capacité de correction de *C*.
2. **ALICE** chiffre le mot **m="MFD"** et l'envoya à **BOB**. Quel est le message chiffré **c** reçu par **BOB**.
3. Supposons que **BOB** a reçu le message **c=0010101**0101100**0010101**.

Déchiffrer **c** pour déterminer le message **m** (en lettres) qu'**ALICE** a envoyé à **BOB**?

Exercice 33 Soit le corps de Galois $\mathbb{K}=\mathbb{F}_8$, α une racine primitive de $\mathbb{K}$.

1. Soit $C(n, k, d)$ un code BCH primitif sur $\mathbb{K}$ de générateur le polynôme $g(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^3)(X-\alpha^4)$. De quel code s'agit-il ? Déterminer les paramètres n, k et d.
2. Soit le mot reçu $y(X)=\alpha^3X+\alpha X^2+X^5$ contenant deux erreurs.

a- Calculer le syndrome $S=(s_j)$ / $1\leq j\leq d-1$ du mot $y(X)$.

b- Déterminer le polynôme localisateur $\sigma(X)$ et ses racines dans $\mathbb{K}$.

c- Déduire les localisateurs X_i.

d- Corriger en utilisant **la méthode Algébrique** le mot $y(X)$.

Exercice 34

Montrer que le dual d'un code cyclique $C(n, k)$ est un code cyclique $C'(n', k')$ qu'on détermine ses paramètres.

Exercice 35

I- Code cyclique

1. Soit $C(n, k, d)$ le code cyclique sur le corps $\mathbb{K}=\mathbb{F}_{2^r}$ des racines 7^{eme} de l'unité sur $\mathbb{F}_2$, de racine primitive α, engendré par $g(X) = (X-1)(X^3 + X + 1)$. Décrire le corps $\mathbb{K}$.
2. Déterminer la longueur n, la dimension k et montrer que la matrice $G_S=(I_k/A)$ tel que:

$A=\begin{bmatrix}1 & 0 & 1 & 1\\ 1 & 1 & 1 & 0\\ 0 & 1 & 1 & 1\end{bmatrix}$ est une matrice génératrice de C et déduire une matrice de contrôle H.

a. Déterminer la distance d et la capacité de correction e de C.

b. Soit le mot reçu $y(X) =X^6+X^5+ X^3 + X^2+1$

c. En utilisant un circuit à décalage circulaire, calculer le syndrome de $y(X)$?

d. En utilisant la méthode de Meggitt, décoder le mot $y(X)$**.**

II- Application à la cryptographie de McEliece

1. Pour se communiquer entre eux, **ALICE** et **BOB** utilisent la cryptographie de **McEliece**.

BOB choisit le code $C(n, k, d)$ dans la partie **(I)** et choisit comme clés secrètes, la matrice génératrice G_S de C, la matrice inversible $S=\begin{bmatrix}0 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 0\end{bmatrix}$ et la matrice de permutation $P=P\tau_{23}(I_n)$.

ALICE et **BOB** se mettent d'accord sur le chiffrement des lettres suivantes:

A	B	C	D	E	F	M	N
000	100	010	001	110	101	011	111

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

2. **ALICE** chiffre le mot **m="MNM"** et l'envoya à **BOB**. Quel est le message chiffré **c** reçu par **BOB**.
3. Supposons que **BOB** a reçu le message **c=0010101**0101100**0010101**.
   Déchiffrer **c** pour déterminer le message **m** (en lettres) qu'**ALICE** a envoyé à **BOB**?

Exercice 36

1. Soit $\mathbb{K}= \mathbb{F}_4$ le corps des racines 4^{eme} de l'unité sur $\mathbb{F}_2$ de racine primitive α. Décrire le corps $\mathbb{K}$.
2. 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 $y(X) = X + 1$, le mot reçu avec v=1 erreur. Corriger en utilisant **la méthode TFD,** le mot $y(X)$.

Exercice 37

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

Exercice 38

Soit $C(n, k)$ un code cyclique dont le polynôme générateur $g(X)$ est divisible par $X - 1$.

Montrer alors que tout mot reçu $y(X)$ de longueur n, comportant un nombre **impair** d'erreurs (c.à.d. $w(\varepsilon(X))$ impair) est détecté comme message erroné.

Exercice 39

1. Soit le polynôme $M(X)= X^3+ X^2+1$ de $\mathbb{F}_2[X]$, montrer que $M(X)$ est irréductible sur $\mathbb{F}_2$.
2. Soit $\mathbb{K}=\mathbb{F}_2[X]/< M(X) >$ posons $\alpha = \bar{X}$ la classe de X.

   Montrer que tout élément $x=\bar{P}$ de $\mathbb{K}$ s'écrit sous la forme $x=a_0+ a_1\alpha+ a_2\alpha^2 / a_i \in \mathbb{F}_2$.
3. Déterminer β l'inverse de α dans $\mathbb{K}$.
4. Montrer que $M(X)$ a trois racines dans $\mathbb{K}$ et exprimer les en fonction de 1, α, α^2.

Exercice 40

I. Soit $C(n=12, k)$ un code cycliques trinaire sur le corps $\mathbb{K}= \mathbb{F}_{3^r}$ des racines 12^{eme} de l'unité sur $\mathbb{F}_3$, de racine primitive α et de générateur $g(X)$.

1. Décomposer par deux méthodes, le polynôme $X^{12}-1$ en produit de polynômes irréductibles sur $\mathbb{F}_3$.
2. Soit $g(X) = X^2 + 2X^2 + 2X + 1$. Montrer que $g(X)$ est un générateur de $C(12, k)$, déterminer k et montrer que ce code est systématique.
3. Soit le mot $a(X) = X^3 + X + 1$ associé au mot $a=(1,1,0,1,0,0,0,0,0)$ de $\mathbb{K}^9$

Calculer par un registre à décalage circulaire le syndrome de $X^3a(X)$ et déduire le mot code $c(X)$ associé à $a(X)$.

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

a. Soit $C(n=2^r-1, k, d)$ un code cyclique sur $\mathbb{K}$, de générateur le polynôme

$g(X) = (X-\alpha)(X-\alpha^2) \dots (X-\alpha^{2^{r-1}})$. De quel code s'agit-il ?

Donner les paramètres du code $C(n, k, d, e)$. Est-il M.D.S ?