Université Mohammed V Agdal
Faculté des Sciences - Rabat
Laboratoire de Mathématiques, Informatique et Applications

Année 2007-08
Master CSI
Théorie des codes
Série 1

Exercice 1. Construire dans chacun des cas suivants, si c'est possible, un code binaire linéaire de longueur n, de distance minimale d et ayant M mots.

1. $n = 3$, $d = 1$, $M = 8$.
2. $n = 4$, $d = 2$, $M = 8$.

Exercice 2. On considère la matrice génératrice suivante d'un code C,

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

1) Déterminer les mots du code, la distance minimale du code, un tableau standard, la matrice de contrôle et la liste des syndrômes de C.
2) Corriger et décoder les messages suivants : 01101, 10000.

Exercice 3. Si C est un code linéaire de type (n, k, d), on définit le code étendu $\overline{C}$ comme le code formé des mots $(x_1, \cdots, x_{n+1}) \in F_2^n$ tels que $(x_1, \cdots, x_n) \in C$ et $\Sigma_{i=1}^{n+1} x_i = 0$. Quel est le type de C '

Exercice 4. On dit que deux codes linéaires de même longueur sont équivalents si l'un s'obtient à partir de l'autre par une permutation des coordonnées. Vérifier que deux codes équivalents ont même type. Montrer que tout code est équivalent à un code donné par un codage systématique.

Exercice 5. Soit C un code linéaire binaire.
1. Montrer que si C est de longueur 17 et de dimension 7, il ne corrige pas plus d'une erreur.
2. Montrer que si C est de longueur 10 et de distance minimum 3, alors $|C| \leq 93$.

Exercice 6. On considère le code C dont une matrice génératrice est

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

1) En utilisant la méthode de Gauss, mettez C sous forme systématique. En déduire une matrice de contrôle H pour C.
2) Calculer le syndrome du mot 1111000. Pouvez-vous le décoder ?

Exercice 7. On considère le code binaire C dont la matrice génératrice est :

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

1. Donner tous les mots de C.
2. Donner la distance minimale de C, combien d'erreurs peut-on corriger ? Détecter ?

Exercice 8. On considère le code binaire où on envoie 16 bits pour 9 bits significatifs de la manière suivante :
- on envoie les trois premiers bits p_1, p_2, p_3 suivis d'un bit de parité (paire) b_1,
- on envoie les trois bits s_1, s_2, s_3 suivants suivis d'un bit de parité (paire) b_2,
- on envoie les trois derniers bits d_1, d_2, d_3 suivis d'un bit de parité (paire) b_3,
- on envoie un paquet de 4 bits de contrôle c_1, c_2, c_3, c_4 où $c_1 = p_1 + s_1 + d_1$, $c_2 = p_2 + s_2 + d_2$, $c_3 = p_3 + s_3 + d_3$ et $c_4 = b_1 + b_2 + b_3$.
1. Montrer que ce code est linéaire, donnez sa matrice génératrice c'est à dire la matrice dont les lignes sont formées des images des vecteurs de base de $\mathbb{F}_2^9$.
2. Coder le mot 100111000.
3. On suppose avoir reçu le mot 0110101101100011. Retrouvez le mot envoyé.

Exercice 9. a) Quels sont les deux seuls polynôomes irréductibles unitaires de degré 3 sur $\mathbb{F}_2$?
b) Factoriser $X^7 + 1$ sous forme d'un produit de polynôomes irreductibles sur $\mathbb{F}_2$.
Dans toute la suite, on s'intéresse aux codes linéaires cyclique sur $\mathbb{F}_2$ de longueur 7.
c) Montrer qu'il n'existe pas de tel code de dimension 2, ni de dimension 5.
d) Que penser du code de dimension 1 ?
e) On considère le code associé au diviseur $X + 1$ de $X^7 + 1$.
Déterminer sa dimension, sa distance minimale, le nombre d'erreurs qu'il détecte et le nombre d'erreurs qu'il corrige. Quelle est sa matrice génératrice ?
f) On considère le code associé au diviseur $X^3 + X + 1$ de $X^7 + 1$. Déterminer sa dimension, sa distance minimale, le nombre d'erreurs qu'il détecte et le nombre d'erreurs qu'il corrige. Quelle est sa matrice génératrice ?

Exercice 10. On transmet des données par paquet de 16 bits, écrits dans un tableau 4 x 4, en ajoutant une ligne et une colonne de contrôole obtenue en associant à chaque ligne et chaque colonne son bit de parité.
a) Que pensez-vous des paquets reçus suivants :

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & \end{pmatrix}$$

b) Quels sont la longueur, la dimension et la distance du code décrit ?
c) Combien repère-t-il d'erreurs ? Combien en corrige-t-il ?
d) Si on ajoute en dernière position le bit de parité de la colonne de contrôle, que deviennent la longueur, la dimension, la distance, le nombre d'erreurs repérées, corrigées du code ?

Exercice 11. i) Quel lien existe entre la dimension et la longueur d'un code 1-correcteur MDS ?
i) Que peut-on dire des codes 1-correcteurs MDS parfaits sur le corps fini $\mathbb{F}_q$?

Exercice 12. 1) Montrez que le polynôme $P(X) = X^4 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.
2) vérifier que $P(X)$ est un diviseur de $X^{15} + 1$.
3) On considère le code cyclique C engendré par P quelle est sa longueur ' Quelle est sa dimension ?

On rappelle que le codage cyclique d'un polynôme $P_u(X)$ s'obtient en faisant une multiplication par X^k (où k est le degré du polynôme générateur du code) suivie d'une division euclidienne.

Coder le polynôme $P_u(X) = X^{10} + X^7 + X^5 + X^4 + X + 1$. Comment obtenir la matrice génératrice de C ?

Exercice 13. Soit C le code linéaire sur $\mathbb{F}_3$ de matrice génératrice

$$G = \begin{pmatrix} 2 & 1 & 0 & 1 & 2 \\ 0 & 2 & 1 & 1 & 1 \end{pmatrix}$$

1. Montrer que C est systématique et en donner une matrice génératrice normalisée G'.
2. Encoder le message (12) avec G, puis avec G' .
3. Construire une matrice de contrôle de C et calculer sa distance minimale. Le code est-il MDS (Maximum Distance Separable) ?
4. On reçoit le message 11102 codé par G. Quel est le message d'origine ? Le mot 12121 est-il un mot de code ? Le décoder sachant qu'il a été encodé par G.

Exercice 14. Soit C le code linéaire sur $\mathbb{F}_5$ de matrice génératrice

$$G = \begin{pmatrix} 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{pmatrix}$$

1. Donner le nombre de mots de C.
2. Le code C est-il systématique ?
3. Déterminer une matrice de contrôle de C.
4. Calculer la capacité de correction t de C. Le code est-il MDS ?
5. Donner la table de contrôle contenant tous les vecteurs erreurs possibles de poids $\leq t$.
6. Décoder quand c'est possible les mots 3001, 1101 et 2311.

Exercice 15. Soit C le code de Hamming binaire de longueur 7.
1. Déterminer une matrice génératrice normalisée de C à l'aide de la méthode du pivot de Gauss.
2. En déduire une matrice de contrôle de C.
3. Décoder quand c'est possible les mots 1111111, 1101011, 0110110 et 1111010.

Exercice 16. Soit C le code binaire linéaire de matrice génératrice

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

1. Le code est-il systématique ?
2. Déterminer une matrice de contrôle et la capacité de correction de C.
3. Le code est-il MDS ?
4. Décoder si possible les mots 111110 et 111111.

Exercice 17. Soit un code de Hamming défini par la matrice de parité 4 x 6

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & h_{1,6} \\ 1 & 1 & 0 & 0 & 0 & h_{2,6} \\ 1 & 0 & 1 & 0 & 0 & h_{3,6} \\ 0 & 1 & 1 & 1 & 0 & h_{4,6} \end{pmatrix}$$

(a) Si l'on choisit $h_{1,6} = h_{2,6} = h_{3,6} = h_{4,6} = 1$, déterminer la liste des mots code. Quel est le nombre de bits d'information et de parité ? Combien d'erreurs ce code corrige-t-il ?

(b) Montrer que les variables $h_{1,6}, h_{2,6}, h_{3,6}, h_{4,6}$ peuvent être choisies de manière à ce que le code corrige les erreurs simples, mais aussi détecte (sans corriger) les erreurs doubles. Déterminer la liste des mots code, et montrer que la distance minimale du code est égale à 4. (Indication : Si la distance minimale de Hamming vaut x alors tout ensemble de $x-1$ colonnes de H doit être linérairement indépendant).

Exercice 18. Démontrer que la distance minimale d'un code de Hamming est égale à d si et seulement si tous les mots code non nuls ont au moins d bits égaux à 1, et au moins l'un d'entre eux a exactement d bits égaux à 1.

Exercice 19. Générateur d'un code de Hamming. On appelle générateur d'un code binaire $(n; k)$ une matrice $k \times n$ dont les lignes sont k mots code linéairement indépendants. Chacun des $2k$ mots code peut alors s'exprimer comme une combinaison linéaire des lignes de G.
(a) Déterminer la matrice de parité du code dont le générateur est

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Quelles sont les propriétés de correction et/ou détection d'erreur de ce code ?
(b) Même question pour le code de générateur

$$G_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Exercice 20. Montrer qu'un code de Hamming corrige jusqu'à t et détecte (mais ne corrige pas nécessairement) jusqu'à t erreurs si et seulement si tout ensemble de $2t-1$ colonnes de la matrice de parité est constitué de colonnes linéairement indépendantes.