Algèbre et Arithmétique 3

Feuille n°7 : codes correcteurs d'erreurs

Les premiers exercices de cette feuille sont tirés de la base WIMS.

Exercice 1

1 Votre correspondant vous a transmis un message codé d'après le tableau suivant.

lettre	*a*	*b*	*c*
code	01000	00011	11111

Le message codé que vous avez reçu est 00010 11111 11000 00011.

Chaque mot de code ci-dessus correspond donc à une lettre du message. A cause des interférences pendant la transmission, certains des mots reçus contiennent des erreurs (un mot reçu peut avoir au plus 1 bit erroné). Les mots du tableau ayant une distance de Hamming d'au moins 3 entre eux, des mots reçus n'ayant pas plus que 1 bit erroné sont corrigeables. Votre but est donc de décoder ce message, en corrigeant les mots contenant 1 bit erroné.

2 Votre correspondant vous a transmis un message codé d'après le tableau suivant.

lettre	*a*	*b*	*c*	*d*	*e*	*f*
code	000111	110001	100010	001001	010100	111111

Quelle est la distance de Hamming de ce code ? Combien d'erreurs peut-on détecter ? Combien d'erreurs peut-on corriger ?

Le message codé que vous avez reçu est 010100 100010 110001 111110 010100 000010 101001. Décoder ce message, en corrigeant les mots contenant 1 bit erroné.

3 Votre correspondant vous a transmis un message codé d'après le tableau suivant.

lettre	*a*	*b*	*c*	*d*
code	010000	000111	101010	111101

Le message codé que vous avez reçu est 001111 010000 001111 000111 111000. Décoder ce message.

Exercice 2

Les codes binaires ayant une distance minimum égale à 3 sont très intéressants, car ce sont les premiers codes permettant la correction d'erreur de transmission. Il est donc très important de trouver de tels codes qui soient le plus efficaces possibles, c'est-à-dire, pour une longueur de code fixée, trouver un code comportant le plus de mots possible, tout en respectant la distance minimum entre les mots.

Voici un code 'partiel' avec quelques mots, et c'est à vous d'y ajouter d'autres mots, le plus possible, tout en respectant la distance minimum 3.

1 Considérons le code binaire de longueur 5, composé de 3 mots 10011, 11101, 01110. La distance minimum entre les mots est 3.

Votre but est d'augmenter ce code en y ajoutant le plus de mots possible, tous de longueur 5, tout en vous assurant que la distance minimum entre tous les mots reste 3. (On peut y ajouter au plus 1 mot.)

2 Considérons le code binaire de longueur 6, composé de 4 mots $001100, 110100, 101001, 111010$. La distance minimum entre les mots est 3.

Votre but est d'augmenter ce code en y ajoutant le plus de mots possible, tous de longueur 6, tout en vous assurant que la distance minimum entre tous les mots reste 3. (On peut y ajouter au plus 4 mots.)

Exercice 3

Considérons le code binaire de matrice génératrice

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

1 Faire la liste de ses mots.
2 Quelle est sa distance Hamming ?
3 Déterminer le mot m avec le plus de 0 sur la droite et le polynôme qui lui est associé.
4 Le code est il cyclique ?

Exercice 4

1 Montrer que dans $\mathbb{F}_2[X]$, $X^4 - 1 = (X-1)^4$. Déterminer tous les diviseurs propres unitaires de $X^4 - 1$ dans l'anneau $\mathbb{F}_2[X]$.
2 Pour chacun de ces diviseurs propres, donner une matrice génératrice du code cyclique associé.
3 Pour le code associé au diviseur $1 + X^3$, déterminer une matrice de contrôle. Vérifier ses colonnes sont deux à deux indépendantes et en déduire que la distance de ce code est au moins 3.

Exercice 5

1 Effectuer la division euclidenne de $X^8 - 1$ par $1 + X + X^4 + X^5$ dans $\mathbb{F}_2[X]$.
2 Considérons le code binaire de matrice génératrice

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

Est-il cyclique ?
3 Déterminer une matrice de contrôle de ce code.

Exercice 6

Le code binaire de Hamming est associé au polynôme $1 + X + X^3$ diviseur unitaire propre de $X^7 - 1$ dans $\mathbb{F}_2[X]$.
1 Donner une matrice génératrice de C.
2 Déterminer la liste des éléments du code.
3 Déterminer la distance de ce code.
4 Déterminer une matrice de contrôle H de ce code.
5 Calculer l'image par H de tous les éléments de poids 1.
6 On a reçu le mot $r = 0110011$. Calculer son image par H. Le mot r est-il un mot du code ?
7 Corriger le mot r en supposant qu'il n'y a eu au plus qu'une seule erreur de transmission.
8 Corriger le mot 1011001 en supposant qu'il n'y a eu au plus qu'une seule erreur de transmission.