Modélisation et résolutions numérique et symbolique de problèmes via les logiciels Maple et MATLAB (MODEL)

TD-TME n°5 - Codes correcteurs d'erreurs

1. TD

Exercice 1 (Distance de Hamming)**.** Soit $\mathscr{C}$ un code linéaire. Montrer que

$$\min_{\{u,v\in\mathscr{C}:u\neq v\}}\big(d_{\mathrm{H}}(u,v)\big)=\min_{\{u\in\mathscr{C}:u\neq 0\}}\big(w_{\mathrm{H}}(u)\big).$$

Exercice 2 (Borne de Singleton)**.** Soit $\mathscr{C}$ un code linéaire $[n;k;d]_q$. Montrer que

$$d\leqslant n-k+1.$$

Exercice 3 (Code linéaire)**.** On se place dans l'espace $\mathbb{F}_2^8$ des vecteurs de longueur 8 sur $\mathbb{F}_2$. On considère l'application

$$\begin{array}{rccc} E: & \mathbb{F}_2^4 & \to & \mathbb{F}_2^8 \\ & (m_1,m_2,m_3,m_4) & \mapsto & (m_1,m_2,m_1+m_2,m_3,m_4,m_3+m_4,m_1+m_3,m_2+m_4). \end{array}$$

Soit $\mathscr{C}=E(\mathbb{F}_2^4)$; $\mathscr{C}$ est un sous-espace vectoriel de dimension 4 de $\mathbb{F}_2^8$. Autrement dit, $\mathscr{C}$ est une code linéaire de dimension 4 et de longueur 8.

– Déterminez une base de $\mathscr{C}$. En déduire une matrice génératrice de $\mathscr{C}$. Quelle est la distance minimale de $\mathscr{C}$?

On considère un vecteur $x=(x_1,\ldots,x_8)\in\mathbb{F}_2^8$ qui se trouve à une distance de 1 d'un vecteur $E(m)$ de C. Décrire une méthode permettant, à partir de x de retrouver l'*unique* vecteur m, tel que $d(E(m),x)\leq 1$.

Indication : on pourra écrire le vecteur x sous la forme

x_1	x_2	x_3
x_4	x_5	x_6
x_7	x_8	

Exercice 4 (CRC)**.** Dans une procédure de contrôle d'erreurs on décide d'envoyer des blocs de 12 bits en les codant sur deux octets de façon à ce que les 16 bits envoyés soient multiples de X^4+X+1. Pour envoyer un bloc $\sum_{i=1}^{i=12} b_i$, on l'interprête comme le polynôme $\sum_{i=1}^{i=12} b_i X^{12-i}$. Ainsi le bit b_1 est le terme de plus haut degré du polynôme.

– Interpréter le bloc de 12 bits 100110 011010 où le premier bit b_1 est 1 en un polynôme P_u

– On obtient P_e qui transite sur le réseau en écrivant la division euclidienne

$$X^4P_u=K.(X^4+X+1)-R$$

et P_e vaut X^4P_u+R. Appliquer la procédure de codage sur P_u pour obtenir P_e.

– Interpréter le bloc de 16 bits 10011100 11100110 avec les mêmes conventions que précédement pour obtenir un polynôme P'_e. Appliquer la procédure de vérification sur P'_e, est-il correct ?

Exercice 5 (Matrice génératrice)**.** On considère le code $\mathscr{C}$ binaire dont la matrice génératrice est :

$$M=\begin{bmatrix} 1&0&0&1&0&0&1\\ 0&1&0&0&1&1&0\\ 0&0&1&0&1&0&1 \end{bmatrix}.$$

1. Donner tous les mots de $\mathscr{C}$
2. Donner la distance minimale de $\mathscr{C}$, combien d'erreurs peut on corriger ? Détecter ?

2. TME

On se propose dans ce TME d'implémenter la technique de décodage par tableau standard.

Soit $\mathscr{C}$ un code de longueur n et de dimension k. Soient G une matrice génératrice et H une matrice de controle de ce code. On rappelle que cela veut dire que tous les mots de codes sont une combinaison linéaire des lignes de G, et que

$$c \in \mathscr{C} \Leftrightarrow c \cdot H^T = 0.$$

Pour tout mot x de longueur n, on appelle le résultat du produit $x \cdot H^T$ le syndrome de x, que l'on notera $S(x)$. C'est un mot de longueur k.

Supposons que lors de la transmission d'un mot de code c, le message r reçu comporte une erreur e :

$$r = c + e.$$

Alors, le syndrome de r ne dépend que de l'erreur :

$$S(r) = r \cdot H^T = (c+e) \cdot H^T = c \cdot H^T + e \cdot H^T = e \cdot H^T.$$

Pour décoder, on cherche à retrouver le mot de code le plus proche du mot reçu. Cela revient à décomposer

$$r = c + e$$

avec e de poids minimal.
Pour faire cela rapidement, nous allons construire un tableau contenant pour tout les syndromes possibles le mot d'erreur de poids minimal correspondant. C'est-à-dire un tableau T tel que

$$T[s] = e \text{ tel que } e \cdot H^T = s \text{ et } \forall x,\ x \cdot H^T = s \Rightarrow w_H(x) \geqslant w_H(e).$$

Le décodage se passe alors ainsi :
– on reçoit r
– on calcule $S(r) = r \cdot H^t$
– le mot décodé est $c = r + T[S(r)]$

Implanter cet algorithme en Maple (on supposera ici que le code est systématique).