1 Codes correcteurs d'erreurs

Exercice 1.1 Soit C le code binaire : $C = \{00001100, 00001111, 01010101, 11011101\}$.

1. Quelle est la longueur de C ?
2. La distance minimale de C est la plus petite des distances entre 2 éléments de C. Quelle est sa valeur ?

Exercice 1.2 Soit E l'application d'encodage qui à un message $m = (m_1, m_2, m_3, m_4) \in \mathbb{F}_2^4$ associe le mot de code $c = E(m) = (m_1, m_2, m_3, m_4, c_5, c_6, c_7) \in \mathbb{F}_2^7$ où $c_5 = m_1+m_3+m_4$, $c_6 = m_1+m_2+m_3$, et $c_7 = m_2 + m_3 + m_4$, et soit C le code linéaire binaire image de E.

1. Donner la matrice génératrice G de C associée à l'application d'encodage E.
2. Soit $m = (1010)$. Quel est le mot de code associé ?
3. Soit $\gamma = (1111001)$. Est-ce un mot du code ?
4. Déterminer tous les éléments $c \in C$ tels que $d(c, \gamma) \leq 1$.

Exercice 1.3 Soit C le code binaire : $C = \{0000, 1100, 1010, 0110, 1001, 0101, 0011, 1111\}$.

1. Quelle est la longueur n de C ?
2. Combien C a-t-il d'éléments ? Si C était un code linéaire sur $\mathbb{F}_2$, quelle serait sa dimension k ? Choisir k éléments $m_1, \ldots, m_k$ de C, linéairement indépendant, et considérer le code linéaire C' engendré par $(m_1, \ldots, m_k)$. Montrer que $C' = C$. Conclusion ?
3. Quelle est la distance minimale de C ? (Il est inutile de déterminer toutes les distances entre deux éléments de C : si $c_1 \in C$ et $c_2 \in C$ alors $d(c_1, c_2)$ est le nombre de coordonnées non nulles de $c_1 - c_2$ qui est lui-même un élément de C.)
4. Montrer que $G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ est une matrice génératrice de C.
5. Montrer que $c = (c_1, c_2, c_3, c_4)$ appartient à C si et seulement si $c_1 + c_2 + c_3 + c_4 = 0$.

Exercice 1.4 Soit G_1 la matrice à coefficients dans $\mathbb{F}_2$:

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

1. Quel est le rang de G_1 ?
2. En déduire que G_1 est la matrice génératrice d'un code linéaire binaire C de longueur $n = 6$ et de dimension $k = 4$.
3. Le code C est-il systématique ? Si oui, donner une matrice génératrice G_2 de C sous forme standard.
4. Donner une matrice de contrôle H de C.
5. Y a-t-il dans C des mots de poids 1 ? Des mots de poids 2 ? Quelle est la distance minimale de C ?

Exercice 1.5 Soit C le code linéaire binaire ayant pour matrice de contrôle :

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

1. Donner la longueur n et la dimension k de C.
2. Les mots $\gamma_1 = (111011)$ et $\gamma_2 = (100110)$ sont-ils des mots du code C ?
3. Donner une matrice génératrice G de C ainsi que l'application d'encodage $E : \mathbb{F}_2^k \to \mathbb{F}_2^n$ associée.
4. Pour chacun des mots γ_i de la question 2, donner, quand cela est possible, le message m_i tel que $\gamma_i = E(m_i)$.

Exercice 1.6 Soit C le code linéaire binaire de matrice de contrôle :

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

1. Quelle est la longueur n de C ? Quelle est la dimension k de C ?
2. Soit $\gamma = 1111111$. Est-ce un mot du code ?
3. Y a-t-il dans C des mots de poids 1 ? Des mots de poids 2 ? Des mots de poids 3 ? Quelle est la distance minimale d de C ? Quelle est la capacité de correction t de C ?
4. Le code C est-il parfait ?
5. Soit $c \in C$ et $\gamma \in \mathbb{F}_2^7$ tel que $d(c, \gamma) > t$. Montrer qu'il existe $c' \in C$ tel que $d(c', \gamma) \leq t$.
6. Si p est la probabilité d'erreur sur un bit (une coordonnée) lors d'une transmission, et si les erreurs par bit sont indépendantes, exprimer en fonction de p la probabilité P qu'un mot $\gamma \in \mathbb{F}_2^7$ reçu lors d'une transmission devienne, après correction, un mot de code c' différent du mot de code c émis. Donner une valeur approchée de P pour $p \in \left\{\frac{1}{10}, \frac{1}{100}, \frac{1}{1000}\right\}$.

Exercice 1.7 Comme dans l'exercice 1.6, soit C le code linéaire binaire de matrice de contrôle :

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

1. Réordonner les colonnes de H pour obtenir une matrice H' de la forme $H' = (B|I_3)$ où B une matrice 3×4 et I_3 la matrice identité 3×3. Soit C' le code équivalent à C de matrice de contrôle H'. Donner une matrice G' génératrice de C' et en déduire une matrice G génératrice de C. On notera E l'application d'encodage associée à G.
2. Les mots suivants sont reçus : $\gamma_1 = 0101000$, $\gamma_2 = 1110010$, $\gamma_3 = 1100011$, $\gamma_4 = 1011011$, $\gamma_5 = 1101011$, $\gamma_6 = 1000011$. Montrer qu'il existe pour chacun des γ_i un mot c_i du code C tel que $d(c_i, \gamma_i) \leq t$. Déterminer les mots de code c_i ainsi que les messages m_i tels que $c_i = E(m_i)$.