Session 4

Exercice 1 (Code par répétition).
Soit le code par p répétitions qui consiste à répéter p fois chaque bit d'information, calculer le rendement de ce code.

Exercice 2 (Rendement et correction).
Soit le code suivant qui pour tout mot binaire $\boldsymbol{m} = (m_1, m_2, m_3, m_4)$, construit le mot de code $\boldsymbol{x} = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9)$ tel que :

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix} = \begin{pmatrix} m_1 & m_2 & m_1 + m_2 \\ m_3 & m_4 & m_3 + m_4 \\ m_1 + m_3 & m_2 + m_4 & m_1 + m_2 + m_3 + m_4 \end{pmatrix}$$

1. Calculer le rendement de ce code.
2. Montrer que ce code est 1-correcteur.

Exercice 3 (Code de Hamming).
Rappelons le code de Hamming : Un *code de Hamming* est défini par la fonction $\phi(\mathbf{s}) = (c_1, \ldots, c_n) \in \{0,1\}^n$ telle que :

- les bits c_i dont l'indice i est une puissance de 2 ($i = 2^\ell$ avec $\ell = 0, 1, \ldots, \lfloor \log_2 n \rfloor$) sont des bits de contrôle ;
- les autres $(n - \lfloor \log_2 n \rfloor - 1)$ bits sont les bits d'information, placés dans l'ordre des indices qui ne sont pas des puissances de 2.

Les bits de contrôle sont construits comme suit :

$$c_{2^\ell} = \bigoplus_{j \text{ tel que } (j/2^\ell) \bmod 2 = 1} c_j.$$

Le bit de contrôle c_{2^ℓ} est la somme modulo 2 de tous les bits d'information c_j dont l'indice j, écrit en base 2, a le $(\ell + 1)$ ième bit (à partir de la gauche) à 1.

1. Donner le code $(7, 4)$ de Hamming.
2. Encoder les messages $(1000, 0100, 0010, 0001, 0101)$.
3. Décoder les messages 0100101 et 0100111.

Exercice 4 (Chiffrement de McEliece).
Rappelons le chiffrement de McEliece :

- $\underline{\mathsf{KeyGen}()}$.
  - **Clé secrète.** $\mathsf{sk} = (\mathbf{S}, \mathbf{G}, \mathbf{P})$ où $\mathbf{G}$ est la matrice génératrice associée d'un code correcteur linéaire (n, k, t) de Goppa qui corrige t erreurs, $\mathbf{S}$ une matrice de taille $k \times k$ inversible dans $\mathbb{F}_2$, $\mathbf{P}$ une matrice $n \times n$ de permutation[1].
  - **Clé publique.** $\mathsf{pk} = \mathcal{G} = \mathbf{S} \cdot \mathbf{G} \cdot \mathbf{P}$.
- $\underline{\mathsf{Enc}(\mathsf{pk}, \mathbf{m})}$. Pour chiffrer un message $\mathbf{m} \in \mathbb{F}_2^k$, représenté par un vecteur de taille k, il faut tirer aléatoirement un vecteur $\mathbf{e}$ de taille n et de poids de Hamming inférieur à t et calculer le chiffré $\mathbf{c} = \mathbf{m} \cdot \mathcal{G} + \mathbf{e}$.
- $\underline{\mathsf{Dec}(\mathsf{sk}, \mathbf{c})}$. Pour déchiffrer le chiffré $\mathbf{c}$ il faut :

[1] Une matrice de permutation ne contient qu'une seule valeur non nulle, 1, dans chaque ligne et colonne.

– Calculer

$$\begin{aligned}\mathbf{a} &= \mathbf{c} \cdot \mathbf{P^{-1}} \\ &= (\mathbf{m} \cdot (\mathbf{S} \cdot \mathbf{G} \cdot \mathbf{P}) + \mathbf{e}) \cdot \mathbf{P^{-1}} \\ &= \mathbf{m} \cdot \mathbf{S} \cdot \mathbf{G} + \mathbf{eP^{-1}} \\ &= (\mathbf{mS}) \cdot \mathbf{G} + \mathbf{e}'\end{aligned}$$

où $\mathbf{e}' = \mathbf{eP^{-1}}$ n'a pas augementé le nombre d'erreurs.

– Corriger les erreurs sur $\mathbf{a}$ pour obtenir $\mathbf{b} = \mathbf{m} \cdot \mathbf{S}$.

– Résoudre le système linéaire $\mathbf{b} = \mathbf{m} \cdot \mathbf{S}$, pour $\mathbf{m}$, c'est-à-dire calculer $\mathbf{m} = \mathbf{b} \cdot \mathbf{S}^{-1}$, car la matrice $\mathbf{S}$ est inversible.

1. À partir des matrices $\mathbf{S}$, $\mathbf{G}$ et $\mathbf{P}$ suivantes, calculer $\mathcal{G}$.

$$\mathbf{S} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \quad \mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

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

2. Déchiffrer le message $\mathbf{c} = (0, 1, 1, 0, 1, 1, 0)$.
3. Vérifier que le message obtenu a été chiffré avec $\mathcal{G}$ et le vecteur d'erreur $\mathbf{e} = (0, 0, 0, 0, 1, 0, 0)$.