TDs de Théorie de l'information. Feuille 4

Exercice 1.— Soit $g(x) = 1 + x + x^4$ un polynôme de $\mathbb{F}_2[x]$.
- Montrer que ce polynôme est primitif.
- Donner le taux de transmission d'un codage de Hamming défini par ce polynôme. Dessiner le registre à décalage du codeur et du décodeur. Combien y a t-il de bits d'information et de bits de correction dans un mot du code ?
- Décoder le bloc 000111010000000 en faisant l'hypothèse qu'au plus une erreur est survenue sur le bloc.

Exercice 2.— Soit $g(x) = 1 + x + x^2 + x^3 + x^4$ un polynôme de $\mathbb{F}_2[x]$.
- Montrer que ce polynôme n'est pas primitif.

Exercice 3.— On appelle distance de Hamming, notée d_H, entre deux suites de même longueur, le nombre de bits différents entre les deux suites. Si on prend un ensemble C de mots de même longueur, la distance minimale de C est la plus petite distance entre deux mots distincts de C.
- Montrer que si C est l'ensemble des mots de code d'un code de Hamming, alors $c, c' \in C$ entraine $c+c' \in C$. Ici l'addition des deux mots est l'addition bit à bit dans $\mathbb{F}_2$. Un tel code est dit linéaire.
- Montrer qu'un mot c de longueur n sur l'alphabet $\{0, 1\}$ est un mot de code d'un code de Hamming $[n, n - d, 3]$ de polynôme $g(x)$ si et seulement si $c(x) = 0 \bmod g(x)$.
- Montrer que si C est l'ensemble des mots de code d'un code de Hamming, alors sa distance minimale est 3.
- Soit C l'ensemble des mots de code d'un code de Hamming dont les mots sont de longueur n. Montrer que tout mot de longueur n sur l'alphabet $\{0, 1\}$ est à distance 0 ou 1 d'un mot du code. On dit que les codes de Hamming sont parfaits.
- En déduire une méthode de compression basée sur le code de Hamming $[15, 11, 3]$. Cette méthode a été utilisée en reconnaissance de la parole.

Exercice 4.— On représente quelquefois le codage de Hamming de façon matricielle. Avec un codage de Hamming $[7, 4, 3]$ obtenu par le polynôme $g(x) = 1 + x + x^3$, on note $\mathbf{m}$ la suite de longueur 4 à coder et $\mathbf{c}$ la suite codée de longueur 7. On dit que G est la matrice génératrice du codage si $\mathbf{c} = \mathbf{m}G$. On dit que H est une matrice de parité du code si $\mathbf{c}$ est un mot du code si et seulement si $H\mathbf{c}^t = \mathbf{0}$.
- Préciser les tailles des matrices et vecteurs ci-dessus.
- Calculer G.
- Calculer une matrice de parité pour le code.

Exercice 5.— On dit que C est un code cyclique si c'est un ensemble de mots de longueur n tel que

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C.$$

Montrer qu'un code de Hamming est cyclique.

Exercice 6.— On considère le jeu suivant : on met sur la tête de sept joueurs sept chapeaux blancs ou noirs. La couleur de chaque chapeau est choisie indépendamment de façon uniforme. Chaque joueur ignore la couleur du chapeau qu'il porte mais voit ses six partenaires ainsi que leurs chapeaux. Chaque joueur doit inscrire secrètement sur une feuille la couleur du chapeau qu'il pense porter ou peut ne pas se prononcer. On dépouille les réponses des joueurs ; l'équipe gagne si au moins un joueur s'est prononcé et si tous les joueurs qui se sont prononcés ont bien répondu. Montrer qu'il existe une stratégie qui permet à l'équipe de gagner avec probabilité 7/8.