Codes correcteurs d'erreurs: travaux dirigés

Mathématiques pour l'informatique - Licence II

18 mars 2015

1 Quelques rappels

On veut transmettre 2^r messages distincts : on les code sur r bits. On rajoute des bits de contrôle pour vérifier que le message a été bien transmis.
Le message tient donc en fait sur n bits.
Si une transformation linéaire permet de passer du code initial de $\mathbb{F}_2^r$ au code émis de $\mathbb{F}_2^n$, on dit que le code est linéaire.

Recherche 1 :
Par exemple, on veut transmettre des mots de 1 bit. On émet le message en le triplant (1 est émis en 111). Le code est-il linéaire ? Quelle est sa matrice G de codage ?

Notons G la matrice du code linéaire.

Recherche 2 :
Il doit y avoir au moins autant de mots codés que de mots au départ : comment cela se traduit-il quant au rang de G ?

Notons C la matrice de contrôle telle que $C \cdot m_r = 0$ si, et seulement si, m_r (le message reçu) est un mot de code (qui a donc été transmis sans erreur).

Recherche 3 :
Que dire du rang de C ?

On notera *syndrome* la fonction associée à s.
On appellera matrice de décodage la matrice D telle que $x = Dy \Leftrightarrow y = Gx$.
Par la méthode de la ℓ-réduite échelonnée de GAUSS-JORDAN on peut déterminer D et C : suivez les explications de votre chargé de TD préféré...

Recherche 4 :
Que donne $R \times (G|m_r)$?

Notons ε l'erreur commise que le message codé émis m_c. Alors $m_c = m_r + \varepsilon$.

Recherche 5 :
Montrez que $s(m_r) = s(\varepsilon)$ et que l'on peut répartir les vecteurs de $\mathbb{F}_2^n$ selon des classes d'équivalences par syndromes.
Montrez que si u est un message reçu quelconque, classe$(u) = u + \mathcal{C}$ avec $\mathcal{C}$ l'ensemble des mots codés.

Un code de HAMMING est un code tel que tous les vecteurs de $\mathbb{F}_2^{n-r}$, sauf le vecteur nul, apparaissent dans C.

2 Exercices

Recherche 6 :
Déterminez une matrice de contrôle du code défini par la matrice génératrice :

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

Après contrôle d'erreur, décodez les messages reçus suivants : 0111101, 0100110, 1010010.
Quel est le défaut de ce code ?

Recherche 7 :
Même style de questions avec :

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

On reçoit 1010110, 1100110, 0100001, 0010001.
Quelle est la nature du code ? Quelle est la matrice de décodage D ?

Recherche 8 :
Même style de questions avec :

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

On reçoit 1100101.
Quelle est la nature du code ? Quelle est la matrice de décodage D ?

Recherche 9 :
Si p est la probabilité d'erreur sur un bit et si les erreurs par bit sont indépendantes, exprimez la probabilité en fnctin de p qu'un message erroné devienne un mot différent du mot émis lorsque le code est de Hamming. Donnez une valeur approchée pour $p = 0,1$. (On rappelle que le code de Hamming ne corrige que les erreurs de poids 1).