Mathématiques discrètes. L1 Informatique I23

TD7. Codes correcteurs d'erreurs.

Claude Elwood SHANNON (1916 - 2001). Père fondateur de la théorie de l'information. Pendant la seconde guerre mondiale, il travaille pour les services secrets de l'armée en cryptographie. Il est chargé de localiser de manière automatique dans le code ennemi les parties signifiantes cachées au milieu du brouillage. Son travail est centré autour de la problématique de la transmission du signal.

"Un peu d'Eire, ça fait Dublin !" (Le Canard Enchaîné)

Exercice 1. Le Quizz.

On définit C, un code sur le corps à deux éléments $\mathbf{F}_2$ par :

$$C := \{0000, 1010, 1001, 1110, 1011\}.$$

1. Quelle est la longueur de ce code ?
2. Le code C est-il linéaire ?
3. Quelle est sa capacité de correction ?
4. Quel est son rayon de recouvrement ?
5. Quel est le plus petit code linéaire C' de longueur 4 (en terme d'ensemble) contenant C ? Quelle est sa dimension ? Déterminez une matrice génératrice de C' et une matrice de controle.

Exercice 2. Condition de décodage d'ordre e

On rappelle qu'un code C de longueur n sur un alphabet A satisfait la condition de décodage d'ordre e si et seulement si pour tout mot $x \in A^n$, il existe au plus un mot c de C tel que $d(x, c) \leq e$. Les codes binaires suivants satisfont-ils la condition de décodage d'ordre 1 ?

$$C = \{(0,1,1,1,0), (1,0,1,0,1), (1,1,0,1,1)\}$$
$$C' = \{(0,0,0), (1,0,1)\}$$

Exercice 3. Borne d'empilement des sphères

Soit C un code en bloc de longueur n sur l'alphabet A à q éléments. Soit $x \in A^n$ et soit $r \in \mathbf{N}$, $r \geq 1$. On désigne par $B(x, r)$ la boule fermée de centre x et de rayon r pour la distance de Hamming.

1. Montrez que

$$\#B(x, r) = \sum_{i=0}^{r} \#S(x, i) \tag{1}$$

où $S(x, i)$ désigne la sphère de centre x et de rayon i.

2. Vérifiez que
$$\#S(x, i) = (q-1)^i \binom{n}{i}.$$
3. On note e la capacité de correction du code C. Montrez que
$$\#C \sum_{r=0}^{e} (q-1)^r \leq \binom{n}{r} \leq q^n.$$
4. Quel est le nombre minimum de mots que doit contenir un code C pour avoir un rayon de recouvrement ρ fixé ?
5. Existe-t-il un code de longueur 5 sur $\mathbf{F}_2$ de capacité de correction $e = 1$ possédant 6 mots de code ?

Exercice 4.

Soit C un $[n, k, d]$-code binaire dans lequel certains mots ont un poids impair. On forme un nouveau code $\hat{C}$ en ajoutant le symbole 0, respectivement 1, à la fin de chaque mot de C de poids pair, respectivement de poids impair. Tous les mots de $\hat{C}$ sont donc de poids pair et $\hat{C}$ vérifie la nouvelle équation de contrôle de parité :

$$x_1 + \cdots + x_n = 0.$$

1. Si d est impair, quels sont les paramètres de $\hat{C}$?
2. Calculez la matrice de contrôle de $\hat{C}$ en fonction de celle de C ?
3. On considère le code de Hamming H_3 de paramètres $[7, 4, 3]$ et son code étendu $\hat{H}_3$. Que vaut le syndrome dans le cas où il n'y a : aucune erreur, une erreur, deux erreurs ?
4. Montrez que le code de Hamming H_3 de paramètres $[7, 4, 3]$ est un code parfait.