M1MI2016 Codes et Cryptologie

Feuille d'exercices n° 9.

Espace de Hamming, codes linéaires

Poids et distance de Hamming :

1 Calculez :

1. $\mathrm{wt}(x)$ pour $x = 1110,\ 10101010101010,\ 1^n$.
2. $\mathrm{wt}(\overline{x})$ en fonction de $\mathrm{wt}(x)$.
3. $d_H(x, y)$ pour $x = 1110000,\ y = 1101110$; pour $x = 1010101010,\ y = 0101010101$; pour $x \in H_n,\ y = 1^n$; pour $x \in H_n, y = 0^n$.

2

1. Montrez que $d_H(x + z, y + z) = d_H(x, y)$ pour tout $x, y, z \in H_n$.
2. Montrez que $d_H(\sigma(x), \sigma(y)) = d_H(x, y)$ pour toute permutation σ des coordonnées.

3 Quel est le nombre de mots de poids 1 dans $\{0, 1\}^n$? de poids 2 ? de poids k ?

4 On appelle boule de centre x et de rayon $k \in \mathbb{N}$ l'ensemble

$$B_n(x, k) = \{y \in H_n : d_H(x, y) \leq k\}$$

1. Quel est le nombre de mots de H_n de poids inférieur ou égal à k ?
2. En déduire le cardinal de $B_n(0^n, k)$.
3. Montrez que pour tout $x \in H_n$,

$$B_n(x, k) = \{x + y : y \in B_n(0^n, k)\} = \{x + y : \mathrm{wt}(y) \leq k\}.$$

4. En déduire le cardinal de $B_n(x, k)$.

5

1. Montrez que, si $d_H(x, y) \geq 2k + 1$, alors les boules $B_n(x, k)$ et $B_n(y, k)$ sont disjointes.
2. Quelle est l'intersection de $B_6(0^6, 2)$ et $B_6(111000, 2)$?

Codes linéaires :

6 Quels sont les codes qui sont linéaires dans cette liste ?

$C = \{101, 111, 010\}$	$C = \{000000, 101010, 010101, 111111\}$
$C = \{0000, 0001, 1110\}$	$C = \{000, 001, 010, 011\}$
$C = \{00000, 11111\}$	$C = \{00000, 11100, 00111, 11011\}$
$C = \{00000, 11110, 01111, 10001\}$	$C = \{00, 10, 01, 11\}$

7 Soit C le code linéaire dont une matrice génératrice est

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

Faites la liste de ses éléments. Quels sont ses paramètres (longueur, dimension, distance minimale) ?

8 *Le code de Hamming :* déterminez les paramètres du code dont une matrice génératrice est

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

9 Montrez que $C = \{(x_1, \ldots, x_n) \in H_n : x_1 + x_2 + \cdots + x_n = 0\}$ est un code linéaire. Donnez-en une matrice génératrice. Quelle est sa dimension ? sa distance minimale ? On l'appelle *le code de parité.*

10 Soit C un code linéaire de longueur n et de dimension k. On appelle *code étendu par parité de* C le code C^* défini ainsi :

$$C^* = \{(x \mid (x_1 + \cdots + x_n)) \in \{0,1\}^{n+1} : x \in C\}.$$

1. Montrez que C^* est un code linéaire, de dimension k et de longueur $n+1$.
2. Montrez que, si G est une matrice génératrice de C, alors on obtient une matrice génératrice de C^* en ajoutant à chaque ligne de G un bit de parité.
3. Donnez une matrice génératrice du code de Hamming étendu par parité et calculez ses paramètres.

11 Montrez que, si C^* est le code étendu par parité de C, alors $d(C^*)$ est pair. Montrez que, si $d(C)$ est pair, alors $d(C^*) = d(C)$, et si $d(C)$ est impair, alors $d(C^*) = d(C) + 1$.

12 Soit C le code engendré par les lignes de la matrice :

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

1. Calculez G', la forme (ligne) échelonnée réduite de G.
2. Expliquez pourquoi les lignes non nulles de G' forment une base de C.
3. Soit $x = 101100$. Utilisez G' pour déterminer si $x \in C$.