Solutions TD 1

Exo 1 a) Le nombre de codes binaires de longueur 3 est égal au nombre de parties de $\mathbb{F}_2^3$: $2^{|\mathbb{F}_2^3|} = 2^8 = 256$.

b) $2^{|\mathbb{F}_q^n|} = 2^{q^n}$.

Exo 2 Si $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ on a

a) $d(x,y) = \text{card}\{i / x_i \neq y_i\}$
$d(y,x) = \text{card}\{i / y_i \neq x_i\}$ $\Rightarrow d(x,y) = d(y,x)$.

b) $x = y \Rightarrow \forall i \in \{1, \dots, n\}$, $x_i = y_i$, donc $d(x,y) = \text{card}\,\phi = 0$.

Si $d(x,y) = 0$, $x_i = y_i \Rightarrow x = y$.

c) posons $A = \{i / x_i = y_i\}$, $B = \{i / x_i = z_i\}$, $C = \{i / y_i = z_i\}$.

si $i \in B \cap C$, $x_i = z_i$ et $z_i = y_i$ donc $x_i = y_i$ et $i \in A$

d'où $B \cap C \subset A$, Notons $\bar{X}$ le complémentaire de X dans $\{1, \dots, n\}$

alors $\bar{A} \subset \overline{B \cap C} = \bar{B} \cup \bar{C}$ et $|\bar{A}| \leq |\bar{B} \cup \bar{C}| = |\bar{B}| + |\bar{C}| - |\bar{B} \cap \bar{C}|$

$\leq |\bar{B}| + |\bar{C}|$

d'où $|\bar{A}| = \text{card}\{i / x_i \neq y_i\} = d(x,y) \leq d(x,z) + d(z,y)$

Exo 3 a) pour $C = A^n$ et $a, b \in A$ / $a \neq b$ on a $d(a, \dots, a, a) = d(a, \dots, a, b) = 1$

donc $d = 1$

b) pour le code répétition C : $a \neq b \Rightarrow d((a, \dots, a), (b, \dots, b)) = n$

et $d = n$.

EX:4 a) Si $q=2$, les composantes non nulles sont égales à 1 donc le nombre de mots de K^n de poids m c'est C_n^m le nombre de parties à m éléments de l'ensemble à n éléments.

Si $q \neq 2$ le nombre demandé est $C_n^m (q-1)^m$ avec

C_n^m est le nombre de parties à m éléments et $(q-1)^m$ est le nombre de composantes non nulles placées dans m cases.

b) Pour $q=2$, $n=2k$, $m=2$ on a $C_{2k}^2 = k(2k-1)$ formant les nombres hexagonaux 1, 6, 15, 28, ...

EX:5 C_1 et C_3 sont des codes linéaires, ils vérifient les conditions d'un sous-espace vectoriel.

C_2 n'est pas linéaire : $0000 \notin C_2$.

EX:6 a) $x_1 \neq x_2 \Rightarrow d((x_1 \dots x_1 a \dots a), (x_2 \dots x_2 a \dots a)) = d$

et la distance minimale de C est égale à d.

$|C| = |A| = q$.

b) $A = \mathbb{F}_q$, si $a \neq 0$ C n'est pas linéaire : $0 \notin C$

si $a=0$, C vérifie les conditions d'un code linéaire.

EX:7 a) $C = \left\{ (x_1, x_2, x_3) \begin{pmatrix} 1&1&0&0 \\ 0&1&1&0 \\ 0&0&0&1 \end{pmatrix} ; x_i \in \mathbb{F}_2 \right\} = \{(x_1, x_1+x_2, x_2, x_3), x_i \in \mathbb{F}_2\}$

$= \{0000, 1100, 0110, 0001, 1010, 1101, 0111, 1011\}$

$\dim C = k = 3$ (le nombre de lignes libres de G).

$|C| = 2^{\dim C} = 2^3 = 8$, $d=1$ (le poids minimum des mots de C).

Ex: 8 $C = ISBN(10) = \left\{ (a_1, \dots, a_{10}) \in \left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^{10} : \sum_{1}^{10} k a_k \equiv 0 \ [11] \right\}$

a) $a = (a_1, \dots, a_{10}) \in C \iff \sum_{k=1}^{10} k a_k = 0 \mod 11$

$$\iff (a_1, \dots, a_{10}) \begin{pmatrix} 1 \\ 2 \\ \vdots \\ 10 \end{pmatrix} = 0 .$$

posons $H = (1, 2, \dots, 10)$, donc $a \in C \iff a \cdot {}^t H = 0$

C est linéaire : 1) $a, b \in C \Rightarrow (a+b)\,{}^t H = a\,{}^t H + b \cdot {}^t H = 0 + 0 = 0$

$\Rightarrow a + b \in C$

2) $\alpha \in \frac{\mathbb{Z}}{11\mathbb{Z}}$, $a \in C \Rightarrow (\alpha a) \cdot {}^t H = \alpha (a \cdot {}^t H) = \alpha \cdot 0 = 0$

$\Rightarrow \alpha a \in C$

Sa matrice de contrôle $H = (1, 2, \dots, 10)$ de type 1×10

b) n : la longueur de C ; $n = 10$.

$n - k = 1 \Rightarrow k = n - 1 = 9$

on a $d \leq n - k + 1 = 2$ donc $d = 1$ ou $d = 2$

Si $d = 1$ il existe un vecteur de poids 1, une composante non nulle $a_k \neq 0$, on $k a_k = 0 \mod 11$ et $k = 0$ (contradiction).

donc $d = 2$.

Ex 9 a) $\sum_{1}^{n} x_i = 0 = (x_1, \dots, x_n)$ posons $H = (1, \dots, 1)$ de type $\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$

$1 \times n$ une matrice de contrôle de C.

b) $n - k = 1 \Rightarrow k = n - 1$, $x \in C \Leftrightarrow x = (x_1, x_2, \dots, x_{n-1}, x_1 + \dots + x_{n-1})$

$x = (x_1, 0, \dots, 0, x_1) \in C \Rightarrow d \leq 2$.

Si $d = 1$, x a une seule composante non nulle par exemple :

$x = (0, \dots, 0, x_n)$, alors $x_n = \sum_{1}^{n-1} x_i = 0$ (contradiction).

donc $d = 2$ et C a pour paramètres : n, $k = n - 1$, $d = 2$.

Ex° 10 1) $d(x,y) = w(x-y)$?

$x-y = (x_1-y_1, \dots, x_n-y_n)$.

$w(x-y) = \text{card}\{i / x_i - y_i \neq 0\} = \text{card}\{i / x_i \neq y_i\}$

$= d(x,y)$.

2) $d_{min} = \min_{\substack{x,y\in C \\ x\neq y}} d(x,y) = \min_{\substack{x,y\in C \\ x\neq y}} w(x-y) = \min_{\substack{X\in C \\ X\neq 0}} w(X)$

$= w_{min}$.

3) nombre de possibilités dans le calcul de d_{min} : C_q^2

" " " " de w_{min} : $|C - \{0\}| = q^k - 1$

posons $N = q^k = |C|$ alors $C_N^2 > N-1$: $\frac{N(N-1)}{2} > N-1$

donc c'est plus rapide de calculer w_{min} que d_{min}

Ex° 11

1) $C = \{(x_1,x_2)\begin{pmatrix} 1 & 1 & 2 & 0 \\ 2 & 1 & 0 & 2 \end{pmatrix} = (x_1+2x_2, x_1+x_2, 2x_1, 2x_2),$

$x_1, x_2 \in \mathbb{F}_3\} = \{0000, 1120, 2102, 0222, 2210, 1201,$

$1012, 2021, 0111\}$

2) $n=4$, $k=2$, $n-k+1 = 3$ et $d = w_{min} = 3$

donc $n-k+1 = d$ et C est MDS.

3) $H = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \end{pmatrix}$ vérifie la relation $\begin{pmatrix} 1 & 1 & 2 & 0 \\ 2 & 1 & 0 & 2 \end{pmatrix} {}^tH = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

ce système a plusieurs solutions on prend par exemple

$H_1 = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 2 \end{pmatrix}$ ou $H_2 = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}$.