Arithmétique et applications, combinatoire et graphes

Contrôle No. 2. 10 mars 2016. codes correcteurs linéaires

Aucun document n'est autorisé, usage de calculatrices interdit

NOM : SOLUTIONS

1. Soit C le code linéaire de taille $(n=5, k=2)$ de matrice génératrice

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

(i) Expliciter les éléments de C.

(ii) Calculer une matrice H de contrôle pour ce code (éviter de longs calculs).

(iii) Quelle est la distance minimale pour ce code? Pour quel t est ce code t-correcteur?

(iv) D'abord on applique le décodage par syndrome : En calculant les syndromes des vecteurs $r_1 = (11100)$, $r_2 = (11011)$ et $r_3 = (11111)$, en déduire ceux qui sont corrigibles? Dans le cas où le vecteur est corrigible, donner le corrigé. (Calculer d'abord les syndromes des erreurs de poids $\leq t$).

(v) Construire un tableau standard de décodage pour C. En appliquant le tableau, corriger r_1, r_2 et r_3.

(i) $G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$; $C = \{(0,0)G, (0,1)G, (1,0)G, (1,1)G\} = \{00000, 00111, 11001, 11110\}$

(ii) Soit $\tilde{G} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ $(C_2 \leftrightarrow C_3)$, $\tilde{G} = (I_2 \mid P)$, $\tilde{H} = (P^t \mid I_3) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$

$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ $(C_2 \leftrightarrow C_3)$ (on vérifie que $GH^t = \underline{0}$)

(iii) $d(C)$ = poids minimal des mots $= 3$; $t < \frac{d(C)}{2} \Rightarrow t = 1$: ce code est 1-correcteur.

(iv)

	erreurs de poids $\leq t$	syndrome He^t (= colonnes de H)
e_1	00000	000
e_2	10000	101
e_3	01000	100
e_4	00100	011
e_5	00010	010
e_6	00001	001

$Hr_1^t = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = He_5^t$

le vecteur r_1 est corrigible en $r_1 + e_5 = (11110)$

$Hr_2^t = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = He_5^t$: r_2 est corrigible en $r_2 + e_5 = (11001)$

$Hr_3^t = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = He_6^t$: r_3 est corrigible en $r_3 + e_6 = (11110)$

(v)

00000	00111	11001	11110
10000	10111	01001	01110
01000	01111	10001	10110
00100	00011	11101	11010
00010	00101	11011	11100
00001	00110	11000	11111
10100	10011	01101	01010
10010	10101	01011	01100

Pas encore dedans

le tableau contient $2^5 = 32$ vecteurs — 8 lignes de 4 vecteurs

Corrigé de r_3:

~~Les~~ Puisque tous les mots sont corrigibles, les corrigés sont identiques à ceux de la partie (iv).

SUITE...

2. Utiliser le polynôme primitif $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ afin de construire un code BCH de distance construite 2. Expliciter une base les éléments de ce code. Il s'agit d'un code linéaire de quelle dimension ?

$n = \deg p(x) = 3$, $m = 2^n - 1 = 7$:

On considère $a = \bar{x}$ et $a^2 \in \dfrac{\mathbb{F}_2[x]}{(x^7-1)}$

On calcule le polynôme minimal $M_1(x)$ de a : il s'agit de $p(x)$

On calcule le polynôme minimal $M_2(x)$ de a^2 : puisque $p(a^2) = p(a)^2$, on a $p(a^2) = 0$ et $M_2(x) = p(x)$

On construit $g(x) = \text{ppcm}\{M_1(x), M_2(x)\} = p(x)$

Enfin $C = (g(x)) \lhd \dfrac{\mathbb{F}_2[x]}{(x^7-1)}$ (l'idéal engendré par $g(x) = p(x)$)

Une base par C est alors

$$\{x^3+x+1,\ \underbrace{x^4+x^2+x}_{x\,p(x)},\ \underbrace{x^5+x^3+x^2}_{x^2\,p(x)},\ x^6+x^4+x^3\}$$

est la dimension de C est $4 = 7 - \deg g(x)$.

On peut traduire la base en notation binaire :

$$a_0 + a_1x + \cdots + a_6x^6 \Longleftrightarrow (a_0 a_1 \cdots a_6)$$

Base $\{1101000, 0110100, 0011010, 0001101\}$

(code cyclique)