Arithmétique et applications, combinatoire et graphes

Contrôle No. 1, 14 fevrier 2018, corps finis, codes correcteurs

Aucun document n'est autorisé, usage de calculatrices interdit

NOM : SOLUTIONS

1. (i) Factoriser le polynôme $x^4 + x^2 + 3$ en polynômes irréductibles sur $\mathbf{Z}/5\mathbf{Z}$.

(ii) Montrer que le polynôme $x^3 + x^2 + 1$ est irréductible sur $\mathbf{Z}/5\mathbf{Z}$.

Soit $\mathbb{K}$ le corps $\mathbb{K} = \dfrac{(\mathbf{Z}/5\mathbf{Z})[x]}{(x^3 + x^2 + 1)}$.

(iii) Combien d'éléments y a-t-il dans $\mathbb{K}$?

(iv) Calculer l'inverse multiplicatif de $2x + 1$ dans $\mathbb{K}$.

(v) Est-ce-que le polynôme $x^3 + x + 1$ est primitif sur $\mathbf{Z}/2\mathbf{Z}$? (justifier)

x^3+x^2+1	x	x^2	x^3	x^4	x^4+x^2+3
1	0	0	0	0	3
3	1	1	1	1	0
3	2	4	3	1	3
2	3	4	2	1	3
1	4	1	4	1	0

(i) x^4+x^2+3 présente $x=1$ et $x=4$ comme racines :

$x^4+x^2+3 = (x-1)(x-4)(\quad)$

$= (x+4)(x^3+x^2+2x+2)$

$= (x+4)(x+1)(x^2+2)$

(ii) On voit du tableau que x^3+x^2+1 n'annulle aucun élément de $\mathbb{F}_5$, d'où il est primitif.

(iii) Il y a $5^3 = 125$ éléments dans $\mathbb{K}$.

(iv) On divise x^3+x^2+1 par $2x+1$

$x^3+x^2+1 = (3x^2+4x+3)(2x+1) + 3$

$3 = x^3+x^2+1 - (3x^2+4x+3)(2x+1)$

$= x^3+x^2+1 + (2x^2+x+2)(2x+1)$

Inverse mult. de 3 dans $\mathbb{F}_5$ est 2 : $3\times 2 = 6 = 1 \mod 5$

$1 = 2(x^3+x^2+1) + (4x^2+2x+4)(2x+1)$

d'où $4x^2+2x+4$ est l'inverse multiplicatif

(vérif : $(4x^2+2x+4)(2x+1) = 3x^3+3x^2+4 = 3(4x^2+4)+3x^2+4$
$= 16 = 1 \mod 5$)

(v) Dans $\frac{\mathbb{Z}}{2\mathbb{Z}}$; $x^3 = x+1$

$a = \bar{x} : \mathbb{F}_2[x]/(x^3+x+1)$

a	a
a^2	a^2
a^3	$a+1$
a^4	a^2+a
a^5	$a^3+a^2 = a^2+a+1$
a^6	$a^3+a^2+a = a^2+1$
a^7	$a^3+a = 1$

Mais $|\mathbb{F}_2[x]/(x^3+x+1)| = 2^3 = 8$

d'où l'ordre du groupe mult. est 7 donc le polynôme est bien primitif

SUITE...

2

2. Soit C le code dans $\mathbb{F}_2{}^{10}$ dont les mots sont donnés par les lignes de la matrice :

$$\begin{matrix} l1 \\ l2 \\ l3 \\ l4 \end{matrix} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Est-ce-que ce code est linéaire ? Calculer la distance minimale $d = d(C)$ pour ce code.

On reçoit les trois vecteurs :

$$r_1 = (0011010011), \quad r_2 = (0001101111), \quad r_3 = (0001011000)\,.$$

On adopte la stratégie de correction au plus proche voisin. Parmi ces vecteurs, lesquels sont corrigibles ? Dans le cas où le vecteur est corrigible, donner le corrigé.

- Puisque $l2 + l3 = l4$ on constate que le code est linéaire
- la distance minimale pour un code linéaire est le poids (minimal) des éléments non-nuls : dans ce cas, il s'agit de 5 ($l4$) (ce code est 2-correcteur)
- $d(r_1, l_1) = 5$, $d(r_1, l_2) = 2$, $d(r_1, l_3) =$ pas nécessaire de calculer puisque le code est 2-correcteur on corrige r_1 en l_2

$d(r_2, l_1) = 6$, $d(r_2, l_2) = 7$, $d(r_2, l_3) = 6$, $d(r_2, l_4) = 3$

l_4 est le voisin unique le plus proche, donc on corrige r_2 en l_1

$d(r_3, l_1) = 3$, $d(r_3, l_2) = 6$, $d(r_3, l_3) = 3$, $d(r_3, l_4) = 6$

Pas de voisin unique le plus proche (l_1 et l_3 sont tous les deux à distance 3)

— on ne peut pas corriger r_3.