Arithmétique et applications, combinatoire et graphes

Contrôle No. 1, 8 fevrier 2016, corps finis, codes correcteurs

Aucun document n'est autorisé, usage de calculatrices interdit

NOM : SOLUTIONS

1. (i) Factoriser le polynôme $x^3 + x + 4$ en polynômes irréductibles sur $\mathbf{Z}/7\mathbf{Z}$.

(ii) Montrer que le polynôme $x^3 + x + 1$ est irréductible sur $\mathbf{Z}/7\mathbf{Z}$.

Soit $\mathbb{K}$ le corps $\mathbb{K} = \dfrac{(\mathbf{Z}/7\mathbf{Z})[x]}{(x^3 + x + 1)}$.

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

(iv) Montrer que dans $\mathbb{K}$, l'élément $x + 3$ vérifie l'équation $y^7 + 5y^2 + 5y + 1 = 0$.

(v) Calculer l'inverse multiplicative de $3x^2 + 1$ dans $\mathbb{K}$.

x	x^2	x^3	$x + x^3$
0	0	0	0
1	1	1	2
2	4	1	3
3	2	6	2
4	2	1	5
5	4	6	4
6	1	6	5

(i) x^3+x+4 a une racine $x=2$

$x^3+x+4 = (x+\overset{-2}{5})(x^2+2x+5)$

Seule racine possible de x^2+2x+5 est $x=2$ (car elle sera aussi racine de x^3+x+4), mais $x^2+2x+5 = 6 \neq 0$ lorsque $x=2$,

$$\boxed{x^3+x+4 = (x+5)(x^2+2x+5)}$$

(ii) $x^3+x+1 \neq 0 \quad \forall x \in \{0,\dots,6\} \Rightarrow x^3+x+1$ irréductible

(iii) $\mathbb{K}$ contient 7^3 éléments

(iv) Morphisme de Frobenius $(x+3)^7 = x^7+3^7 = x^7+(3^2)^3.3 = x^7+3 \pmod 7$

$(x+3)^7+5(x+3)^3+5(x+3)+1 = x^7+3+5(x^2+6x+9)+5x+1+1$ (*)

$x^3 = -x-1$: (*) $= (x+1)^2x + 5x^2+2x+3+5x+5$

$= x^3+2x^2+x+5x^2+8 = -x-1+x+1 = 0$

(v) $x^3+x+1 = 5x(3x^2+1)+3x+1$

$3x^2+1 = (x+2)(3x+1)+6$

$1 = 6\times 6 = 6\times[3x^2+1-(x+2)(3x+1)]$

$= 6\times\{3x^2+1-(x+2)[x^2+x+1-5x(3x^2+1)]\}$

$= 6\{1+5x(x+2)\}(3x^2+1) - 6(x+2)(x^2+x+1)$

Inverse : $6(5x^2+3x+1) = \boxed{2x^2+4x+6}$

Vérif : $(3x^2+1)(2x^2+4x+6)$

$= 6x^4+5x^3+6x^2+4x+6$

$= 6x(-x-1)-5x-5+6x^2+4x+6$

$= 1$

SUITE...

2

2. Soit C le code dans $\mathbb{F}_2{}^9$ dont les mots sont donnés par les lignes de la matrice :

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

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

On reçoit les trois vecteurs :

$$r_1 = (001101000), \quad r_2 = (000100111), \quad r_3 = (101010101)\,.$$

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.

En écrivant $\underline{0} = (000)$ et $\underline{1} = (111)$, le code s'écrit

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

On voit que le code est bien linéaire et que $d(C) = 3$.

En adoptant la stratégie de correction au plus proche voisin, quelque soit le vecteur reçu $r = (a_1 a_2 \dots a_9)$, il existe toujours un voisin unique le plus proche. En effet $r = (\underline{a_1 a_2 a_3}\ \underline{a_4 a_5 a_6}\ \underline{a_7 a_8 a_9})$ et on applique la correction à chaque triple $(a_1 a_2 a_3)$, $(a_4 a_5 a_6)$ et $(a_7 a_8 a_9)$ à dire (000) ou dit (111) dépendant sur lequel parmi ces deux vecteurs est plus proche. (on a toujours une solution unique)

r_1 se corrige en (000111000) $\quad d=2$

r_2 ——— (000000111) $\quad d=1$

r_3 ——— (111000111) $\quad d=3$