Arithmétique et applications, combinatoire et graphes

Contrôle No. 2, 11 mars 2020, codes BCH

Aucun document n'est autorisé, usage de calculatrices interdit

NOM : Solutions

1. (i) Montrer que le polynôme $p(x) = x^4 + x + 1$ est primitif et calculer toutes les puissances a^i dans le corps $\mathbb{F}_2[x]/(p(x))$ où $a = \overline{x} = x + (p(x))$.

On a la factorisation:

$$x^{15} - 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

dans $\mathbb{F}_2[x]$.

(ii) Utiliser le polynôme $p(x)$ afin de construire un code BCH C de distance construite 4. Calculer le polynôme générateur $g(x)$ pour ce code. Il s'agit d'un code linéaire de quelle dimension?

(iii) Un mot c est transmis avec ce code et on reçoit le vecteur $r = (010011001000100) \in \mathbb{F}_2{}^{15}$, ce qui correspond au polynôme $r(x) = x + x^4 + x^5 + x^8 + x^{12} \in \mathbb{F}_2[x]$. Calculer les syndromes r_1, r_2, r_3, r_4 comme puissances de a (utiliser votre tableau), puis calculer le polynôme localisateur d'erreurs $E(z)$.

(iv) Enfin trouver les racines de ce polynôme afin de localiser les erreurs. Corriger le vecteur r afin de trouver le mot c de C.

(i) $p(x)$ est irréductible: pas de facteur linéaire car $p(0) = p(1) = 1 \neq 0$

Si $p(x) = (x^2 + ax + 1)(x^2 + bx + 1)$ on aurait $a + b = 0$ (coeff x^3)

$1 + 1 + ab = 0$

et $a + b = 1$ (coeff x)

Impossible. Donc $p(x)$ irréductible

Tableau de puissances : $a^4 = a + 1$ dans $\mathbb{F}_2[x]/(p(x))$

a	a
a^2	a^2
a^3	a^3
a^4	$a+1$
a^5	a^2+a
a^6	a^3+a^2
a^7	$a^4+a^3 = a^3+a+1$
a^8	$a^4+a^2+a = a^2+1$
a^9	a^3+a
a^{10}	$a^4+a^2 = a^2+a+1$
a^{11}	a^3+a^2+a
a^{12}	$a^4+a^3+a^2 = a^3+a^2+a+1$
a^{13}	$a^4+a^3+a^2+a = a^3+a^2+1$
a^{14}	$a^4+a^3+a = a^3+1$
a^{15}	$a^4+a = 1$

(ii) On utilise les puissances a, a^2, a^3, a^4

Soit M_i le poly minimal de a^i

$M_1 = M_2 = M_4 = p(x)$ (Frobenius)

On essaye $M_3(x) = x^4 + x^3 + x^2 + x + 1$

$M_3(a^3) = a^{12} + a^9 + a^6 + a^3 + 1$

$= a^3 + a^2 + a + 1 + a^3 + a + a^3 + a^2 + a^3 + 1 = 0$

donc $M_3(x) = x^4 + x^3 + x^2 + x + 1$

et $g(x) = \text{ppcm}\,\{M_i(x)\}$

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

$= x^8 + x^7 + x^6 + \cancel{x^5} + \cancel{x^4} + \cancel{x^5} + \cancel{x^4} + \cancel{x^3} + \cancel{x^2} + \cancel{x}$

$+ x^4 + \cancel{x^3} + \cancel{x^2} + \cancel{x} + 1$

$= x^8 + x^7 + x^6 + x^4 + 1$

base : $\{g(x), x.g(x), x^2 g(x), x^3 g(x), x^4 g(x), x^5 g(x), x^6 g(x)\}$

dimension = 7

(iii) On reçoit $r = (010011001000100)$

$\iff r(x) = x + x^4 + x^5 + x^8 + x^{12}$

$r_1 = r(a) = a + a^4 + a^5 + a^8 + a^{12}$

$= \cancel{a} + \cancel{a} + \cancel{1} + \cancel{a^2} + \cancel{a} + \cancel{a^2} + \cancel{1} + a^3 + a^2 + \cancel{a} + 1$

$= a^3 + a^2 + 1 = a^{13}$

$r_2 = r_1^2 = a^{26} = a^{11}$ (car $a^{15} = 1$)

$r_4 = r_2^2 = a^{22} = a^7$

$r_3 = r(a^3) = a^3 + a^{12} + a^{15} + a^{24} + a^{36} = \cancel{a^3} + \cancel{a^3} + \cancel{a^2} + \cancel{a} + \cancel{1} + \cancel{1} + \cancel{a^3} + \cancel{a} + \cancel{a^3} + \cancel{a^2}$

$= 0$

On calcule $E(z) = z^2 + \sigma_1 z + \sigma_2$ où

$$\begin{pmatrix} r_1 & r_2 \\ r_2 & r_3 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} r_3 \\ r_4 \end{pmatrix}$$

$$\iff \begin{pmatrix} a^{13} & a^{11} \\ a^{11} & 0 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} 0 \\ a^7 \end{pmatrix} \Rightarrow a^{11}\sigma_2 = a^7$$

(rang de la matrice est 2 car son déterminant $= a^{22} = a^7 \neq 0$) $\overset{+a^4}{\Rightarrow} \sigma_2 = a^{11}$

Puis $a^{13}\sigma_2 + a^{11}\sigma_1 = 0 \Rightarrow a^{13} \times a^{11} = \sigma_1 a^{11}$

$\Rightarrow \sigma_1 = a^{13}$

$E(z) = z^2 + a^{13} z + a^{11}$

Soit $E(z) = (z + a^k)(z + a^l)$ (racines a^k, a^l)

alors $k + l = 11 \pmod{15}$ et $a^k + a^l = a^{13} = a^3 + a^2 + 1$

On teste les possibilités:

k	l	$a^k + a^l$	
0	11	$1 + a^3 + a^2 + a$	Non
1	10	$a + a^2 + a + 1 = a^2 + 1$	Non
2	9	$a^2 + a^3 + a$	Non
3	8	$a^3 + a^2 + 1$	Oui

racines a^3 et a^8, d'où le polynôme erreur est $e(x) = x^3 + x^8$

et $c(x) = r(x) + e(x) = x + x^3 + x^4 + x^5 + x^{12}$

Vérification $c(a^i) = 0 \quad i = 1, 2, 3, 4$

$c(a) = a + a^3 + a^4 + a^5 + a^{12} = \cancel{a} + \cancel{a^3} + \cancel{a} + \cancel{1} + \cancel{a^2} + \cancel{a} + \cancel{a^3} + \cancel{a^2} + \cancel{a} + \cancel{1} = 0$

$c(a^2) = c(a)^2 = 0$ et $c(a^4) = c(a)^4 = 0$

$c(a^3) = a^3 + a^9 + a^{12} + a^{15} + a^{36} = a^3 + a^9 + a^{12} + 1 + a^6$

$= \cancel{a^3} + \cancel{a^3} + \cancel{a} + \cancel{a^3} + \cancel{a^2} + \cancel{a} + \cancel{1} + \cancel{1} + \cancel{a^3} + \cancel{a^2} = 0$