Arithmétique et applications, combinatoire et graphes

Contrôle No. 2, 15 mars 2018, codes correcteurs BCH

Aucun document n'est autorisé, usage de calculatrices interdit

NOM : SOLUTIONS

1. (i) Montrer que le polynôme $p(x) = x^4 + x^3 + 1$ 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 $r = (100110000100100) \in \mathbb{F}_2{}^{15}$, ce qui correspond au polynôme $r(x) = 1 + x^3 + x^4 + x^9 + x^{12} \in \mathbb{F}_2[x]$. 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.

FIN

(i) $a^4 = a^3 + 1$

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

(ii) On considère les puissances de a: a, a^2, a^3, a^4

Soit $M_i(x)$ le poly minimal de a^i

$M_1(x) = p(x)$

$M_1(a^2) = M_1(a)^2 = 0$ (Frobenius) $\Rightarrow M_2 = M_1$

$M_1(a^4) = (M_1(a^2))^2 = 0$ (Frob) $\Rightarrow M_4 = M_1$

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

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

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

$g(x) = \text{ppcm}\{M_1, \dots, M_4\} = M_1(x) M_3(x)$

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

$= x^8+x^7+x^6+x^5+x^4+x^7+x^6+x^5+x^4+x^3+x^4+x^3+x^2+x+1$

$= x^8 + x^4 + x^2 + x + 1$

$C = \{ u(x) g(x) \mid \deg u g \leq 14 \}$

base $\{g, xg, x^2g, x^3g, x^4g, x^5g, x^6g\}$; $\dim C = 7$

On reçoit $r = (1001100001001100)$

$\Leftrightarrow r(x) = 1 + x^3 + x^4 + x^9 + x^{12}$

$r_1 = r(a) = 1 + a^3 + a^4 + a^9 + a^{12} = 1 + a^3 + a^3 + 1 + a^2 + 1 + a + 1 = a^2 + a = a^{13}$

$r_2 = r(a^2) = r(a)^2$ (Frobenius) $= a^{26} = a^{11}$ $(a^{15} = 1)$

$r_4 = r(a^4) = r(a^2)^2 = a^{22} = a^7$

$r_3 = r(a^3) = 1 + a^9 + a^{12} + a^{27} + a^{36} = 1 + a^9 + a^{12} + a^{12} + a^6 = 1 + a^2 + 1 + a^3 + a^2 + a + 1$

$= a^3 + a + 1 = a^5$

$E(z) = z^2 + \sigma_1 z + \sigma_2$ où σ_1, σ_2 sont solutions du système

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

$\Leftrightarrow$ $\begin{cases} a^{13}\sigma_2 + a^{11}\sigma_1 = a^5 \\ a^{11}\sigma_2 + a^5\sigma_1 = a^7 \end{cases} \xrightarrow{\times a^2} \begin{cases} \sigma_2 + a^{13}\sigma_1 = a^7 \\ \sigma_2 + a^9\sigma_1 = a^{11} \end{cases}$

Somme $\Rightarrow$ $(a^{13} + a^9)\sigma_1 = a^7 + a^{11} \Rightarrow (a^2 + a + a^2 + 1)\sigma_1 = a^2 + a + 1 + a^3 + a^2 + 1$

$\Rightarrow$ $(a+1)\sigma_1 = (a^3 + a) \Rightarrow a^{12}\sigma_1 = a^{10} \xrightarrow{\times a^3} \sigma_1 = a^{13}$

Puis $\sigma_2 = a^{13}\sigma_1 + a^7 = a^{26} + a^7 = a^{11} + a^7 = a^3 + a^2 + 1 + a^2 + a + 1 = a^3 + a = a^{10}$

$E(z) = z^2 + a^{13}z + a^{10}$

Soient a^k, a^ℓ les racines de $E(z)$: $E(z) = (z + a^k)(z + a^\ell)$

$= z^2 + (a^k + a^\ell)z + a^{k+\ell}$

Donc $k + \ell = 10 \pmod{15}$ et $a^k + a^\ell = a^{13} = a^2 + a$

On teste les différents cas :

k	ℓ	$a^k + a^\ell$	
0	10	$1 + a^3 + a$	Non
1	9	$a + a^2 + 1$	Non
2	8	$a^2 + a^3 + a^2 + a = a^3 + a$	Non
3	7	$a^3 + a^2 + a + 1$	Non
4	6	$a^3 + 1 + a^3 + a^2 + a + 1 = a^2 + a$	OUI

$k = 4$ et $\ell = 6$ d'où le polynôme erreur

$e(x) = x^4 + x^6$

Mot $c(x) = r(x) + e(x) = 1 + x^3 + x^6 + x^9 + x^{12}$

$\leftrightarrow (1001001001001000)$

On vérifie que $c(x)$ est multiple de $g(x)$

$x^{12} + x^9 + x^6 + x^3 + 1 = (x^4 + x + 1)(x^8 + x^4 + x^2 + x + 1)$

$c(x)$ $\qquad$ $g(x)$

Etc.