Arithmétique et applications, combinatoire et graphes

Contrôle No. 2, 20 mars 2019, codes 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 $r = (010101101010110) \in \mathbb{F}_2{}^{15}$, ce qui correspond au polynôme $r(x) = x + x^3 + x^5 + x^6 + x^8 + x^{10} + x^{12} + x^{13} \in \mathbb{F}_2[x]$. 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) $a^4 = a^3 + 1$

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}	1

puisque $|\mathbb{K}^*| = 15$ ($\mathbb{K} = \mathbb{F}_2[x]/(p(x))$) on voit que a engendre $\mathbb{K}^*$ et $p(x)$ est primitif

(ii) On utilise a, a^2, a^3, a^4 pour construire C

$m_1(x) = p(x)$ est le poly min de a

Par Frobenius

$m_2(x) = m_4(x) = p(x)$.

Soit $m_3(x)$ le poly minimal de a^3.

On essaye $m_3(x) = x^4+x^3+x^2+x+1$

$m_3(a^3) = a^{12}+a^9+a^6+a^3+1$

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

$g(x) = \text{ppcm}\{m_1, m_2, m_3, m_4\} = (x^4+x^3+1)(x^4+x^3+x^2+x+1)$

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

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

(ii) suite $g(x) = x^8 + x^4 + x^2 + x + 1$

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

$\dim \mathcal{C} = 7$

(iii) $r(x) = x + x^3 + x^5 + x^6 + x^8 + x^{10} + x^{12} + x^{13}$

$r_1 = r(a) = a + a^3 + a^5 + a^6 + a^8 + a^{10} + a^{12} + a^{13}$

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

$= a^3 + a^2 + a + 1 = a^6$

Frobenius $r_2 = r_1^2 = a^{12}$, $r_4 = r_2^2 = a^{24} = a^9$ $(a^{15} = 1)$

$r_3 = r(a^3) = a^3 + a^9 + a^{15} + a^{18} + a^{24} + a^{30} + a^{36} + a^{39}$

$= \cancel{a^3} + \cancel{a^9} + \cancel{1} + \cancel{a^3} + \cancel{a^9} + \cancel{1} + a^6 + a^9 = a^6 + a^9 = a^3 + \cancel{a^2} + a + \cancel{1} + \cancel{a^2} + \cancel{1}$

$= a^3 + a = a^{10}$

Poly localisateur d'erreurs: $\begin{pmatrix} r_1 & r_2 \\ r_2 & r_3 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} r_3 \\ r_4 \end{pmatrix}$

$\Leftrightarrow \begin{pmatrix} a^6 & a^{12} \\ a^{12} & a^{10} \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} a^{10} \\ a^9 \end{pmatrix}$ $\quad \det \begin{pmatrix} a^6 & a^{12} \\ a^{12} & a^{10} \end{pmatrix} = a^6 \times a^{10} \begin{vmatrix} 1 & a^6 \\ a^2 & 1 \end{vmatrix}$

Mais $\begin{vmatrix} 1 & a^6 \\ a^2 & 1 \end{vmatrix} = 1 + a^8 = 1 + a^3 + a^2 + a = a^6 \neq 0$

$\begin{cases} a^6 \sigma_2 + a^{12} \sigma_1 = a^{10} \\ a^{12} \sigma_2 + a^{10} \sigma_1 = a^9 \end{cases} \underset{\times a^3}{\overset{\times a^{-6}}{\Rightarrow}} \begin{matrix} \sigma_2 + a^6 \sigma_1 = a^4 \\ \sigma_2 + a^{13} \sigma_1 = a^{12} \end{matrix} \Rightarrow (a^6 + a^{13}) \sigma_1 = a^4 + a^{12}$

$\Rightarrow (a^3 + \cancel{a^2} + \cancel{a} + 1 + \cancel{a^2} + \cancel{a}) \sigma_1 = a^3 + 1 + a + 1$

$\Rightarrow a^4 \sigma_1 = a^{10} \Rightarrow \boxed{\sigma_1 = a^6}$ puis $\sigma_2 = a^{12} + a^4 = a + 1 + a^3 + 1 = a^{10}$

$E(z) = z^2 + \sigma_1 z + \sigma_2 = z^2 + a^6 z + a^{10}$

(iv) Soient a^k, a^l les racines : alors $a^k + a^l = a^6$ et $a^{k+l} = a^{10}$

$k + l = 10 \pmod{15}$

$a^6 = a^3 + a^2 + a + 1$

$k = 0, l = 10$	$1 + a^3 + a$	Non
$k = 1, l = 9$	$a + a^2 + 1$	Non
$k = 2, l = 8$	$a^2 + a^3 + a^2 + a$	Non
$k = 3, l = 7$	$a^3 + a^2 + a + 1$	OUI

$\rightarrow$ racines a^3 et a^7

Poly erreur $e(x) = x^3 + x^7$

On corrige $r(x)$ en

$c(x) = r(x) + e(x)$

$= x + x^5 + x^6 + x^7 + x^8 + x^{10} + x^{12} + x^{13}$

Donc $\boxed{c = 010001111010110} \in \mathcal{C}$