Arithmétique et applications, combinatoire et graphes

Contrôle No. 2, 13 mars 2017, codes correcteurs BCH

Aucun document n'est autorisé, usage de calculatrices interdit

NOM : SOLUTIONS

(i) Montrer que le polynôme $p(x) = x^4 + x + 1$ est primitif et construire un tableau de 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 $r = (010000000101110) \in \mathbb{F}_2{}^{15}$, ce qui correspond au polynôme $r(x) = x + x^9 + x^{11} + x^{12} + x^{13} \in \mathbb{F}_2[x]$. 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 transmis c de C.

FIN

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

a^n	
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^3+a+1
a^8	a^2+1
a^9	a^3+a
a^{10}	a^2+a+1
a^{11}	a^3+a^2+a
a^{12}	a^3+a^2+a+1
a^{13}	a^3+a^2+1
a^{14}	a^3+1
a^{15}	1

racines de $x^{15}-1$: $a_1 = a$, $a_2 = a^2$, $a_3 = a^3$, $a_4 = a^4$

Polynôme minimal $m_j(x)$ de a_j :

$m_1 = m_2 = m_4 = x^4 + x + 1$ (par le morphisme de Frobenius)

$m_3(x) = x^4 + x^3 + x^2 + x + 1$; en effet

$a^{12} + a^9 + a^6 + a^3 + 1 = a^3 + a^2 + a + 1 + a^3 + a + a^3 + a^2 + a^3 + 1 = 0$

d'où $g(x) = (x^4+x+1)(x^4+x^3+x^2+x+1)$

$= x^8 + x^7 + x^6 + x^4 + 1$ degré $= 14$

Base par C : $\{g, xg, x^2g, x^3g, x^4g, x^5g, x^6g\}$

$\dim C = 7$

SUITE →

$P(x) = x + x^9 + x^{11} + x^{12} + x^{13}$

Syndromes :

$S_1 = a + a^9 + a^{11} + a^{12} + a^{13} = a + a^3 + a + a^3 + a^2 + a + a^3 + a^2 + a + 1 + a^3 + a^2 + 1 = a^2$

Par le morphisme de Frobenius.

$S_2 = a^4$, $S_4 = a^8$

$S_3 = a^3 + a^{27} + a^{33} + a^{36} + a^{39} = a^3 + a^{12} + a^3 + a^6 + a^9$ $(a^{15} = 1)$

$= a^3 + a^2 + a + 1 + a^3 + a^2 + a^3 + a = a^3 + 1 = a^{14}$

On résout $\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix}\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_3 \\ S_4 \end{pmatrix}$ c'est à dire $\begin{pmatrix} a^2 & a^4 \\ a^4 & a^{14} \end{pmatrix}\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} a^{14} \\ a^8 \end{pmatrix}$

On vérifie d'abord que $\det \begin{pmatrix} a^2 & a^4 \\ a^4 & a^4 \end{pmatrix} = a^{16} + a^8 = a + a^8 = a + a^2 + 1 \neq 0$

Puis $\begin{cases} a^2\sigma_2 + a^4\sigma_1 = a^{14} \\ a^4\sigma_2 + a^{14}\sigma_1 = a^8 \end{cases} \Rightarrow \begin{cases} \sigma_2 + a^2\sigma_1 = a^{12} & (\times \sigma^{-2}) \\ \sigma_2 + a^{10}a_1 = a^4 & (\times \sigma^{-4}) \end{cases}$

$\Rightarrow a^2(1 + a^8)\sigma_1 = a^4(1 + a^8) \Rightarrow a^2\sigma_1 = a^4 \Rightarrow \sigma_1 = a^2$

$\sigma_2 = a^4 + a^{12} = a + x + a^3 + a^2 + a + x = a^3 + a^2 = a^6$

Polynôme localisateur d'erreurs $E(z) = z^2 + \sigma_1 z + \sigma_2 = z^2 + a^2 z + a^6$

On trouve les deux racines :

$E(1) = 1 + a^2 + a^6 = 1 + a^2 + a^3 + a^2 \neq 0$

$E(a) = a^2 + a^3 + a^6 = a^2 + a^3 + a^3 + a^2 = 0$ ($z = a$ racine)

$E(a^2) = a^4 + a^4 + a^6 = a^6 \neq 0$

$E(a^3) = a^6 + a^5 + a^6 = a^5 \neq 0$

$E(a^4) = a^8 + a^6 + a^6 = a^8 \neq 0$

$E(a^5) = a^{10} + a^7 + a^6 = a^2 + a + 1 + a^3 + a + 1 + a^3 + a^2 = 0$

Ce qui nous permet d'identifier les erreurs en positions : x^1 et x^5

On corrige $P(x)$ alors en $C(x) = x^5 + x^9 + x^{11} + x^{12} + x^{13} = P(x) + x + x^5$

c'est à dire en (0000010001011110)