Information and Coding Theory

University of Chinese Academy of Sciences

Fall 2023

Kewei Lv, Liping Wang

Homework 11

Chenkai GUO

2023.12.7

1. *Let α be a root of $1+x+x^4 \in F_2[x]$. Let C be the narrow-sense binary BCH code of length 15 with designed distance 5.*
   (a) Find the generator polynomial of C.
   (b) If possible, determine the error positions of the following received words:
   (i) $w(x) = 1 + x^6 + x^7 + x^8$;
   (ii) $w(x) = 1 + x + x^4 + x^5 + x^6 + x^9$;
   (iii) $w(x) = 1 + x + x^7$.

   SOLUTION
   (a) From the statement, we knew that $1 + \alpha + \alpha^4 = 0, \delta = 5$ and α is a primitive element of F_{16}; Since C is narrow-sense code, thus we need to find $g(x) = lcm[M^{(1)}(x), M^{(2)}(x), M^{(3)}(x), M^{(4)}(x)]$
   Calculate the minimal polynomial:
   $M^{(1)}(x) = M^{(2)}(x) = M^{(4)}(x) = 1 + x + x^4, M^{(3)}(x) = 1 + x + x^2 + x^3 + x^4$
   Thus $g(x) = lcm[M^{(1)}(x), M^{(2)}(x), M^{(3)}(x), M^{(4)}(x)] = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4) = 1 + x^4 + x^6 + x^7 + x^8$

   (b) From the statement, we knew that:

$$H = \begin{pmatrix} 1 & \alpha & (\alpha)^2 & (\alpha)^3 & \cdots & (\alpha)^{14} \\ 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 & \cdots & (\alpha^2)^{14} \\ 1 & \alpha^3 & (\alpha^3)^2 & (\alpha^3)^3 & \cdots & (\alpha^3)^{14} \\ 1 & \alpha^4 & (\alpha^4)^2 & (\alpha^4)^3 & \cdots & (\alpha^4)^{14} \end{pmatrix}$$

   (i) For $w(x) = 1 + x^6 + x^7 + x^8$, we calculate the syndromes $[s_0, s_1, s_2, s_3]$
   $s_0 = w(\alpha) = 1 + \alpha^6 + \alpha^7 + \alpha^8 = \alpha^4$
   $s_1 = w(\alpha^2) = 1 + \alpha^{12} + \alpha^{14} + \alpha^{16 mod 15} = \alpha^8$
   $s_2 = w(\alpha^3) = 1 + \alpha^{18 mod 15} + \alpha^{21 mod 15} + \alpha^{24 mod 15} = \alpha^{12}$

$s_3 = w(\alpha^4) = 1 + \alpha^{24 mod 15} + \alpha^{28 mod 15} + \alpha^{32 mod 15} = \alpha$
Thus $s(z) = \alpha^4 + \alpha^8 z + \alpha^{12} z^2 + \alpha z^3$, *solve the key function* $r(z) \equiv s(z)\sigma(z)\ (mod z^4)$, *s.t.* $deg(r(z)) \leq t - 1 = 1$, $deg(\sigma(z)) \leq t = 2$, *we obtain* $\sigma(z) = \alpha^4 z + 1$ *and* $r(z) = \alpha^4$, *Hence, the error takes place at the 11th position.*

(ii) For $w(x) = 1 + x + x^4 + x^5 + x^6 + x^9$, *we calculate the syndromes* $[s_0, s_1, s_2, s_3]$
$s_0 = w(\alpha) = 1 + \alpha^+ \alpha^4 + \alpha^5 + \alpha^6 + \alpha^9 = 0$
$s_1 = w(\alpha^2) = 1 + \alpha^2 + \alpha^8 + \alpha^{10} + \alpha^{12} + \alpha^{18 mod 15} = 0$
$s_2 = w(\alpha^3) = 1 + \alpha^3 + \alpha^{12} + + \alpha^{15 mod 15} \alpha^{18 mod 15} + \alpha^{27 mod 15} = 0$
$s_3 = w(\alpha^4) = 1 + \alpha^4 + \alpha^{16 mod 15} + \alpha^{20 mod 15} + \alpha^{24 mod 15} + \alpha^{36 mod 15} = 0$
All the syndromes are zero, it indicates that the received word $w(x) = 1 + x + x^4 + x^5 + x^6 + x^9$ *is error-free.*

(iii) For $w(x) = 1 + x + x^7$, *we calculate the syndromes* $[s_0, s_1, s_2, s_3]$
$s_0 = w(\alpha) = 1 + \alpha + \alpha^7 = \alpha^3$
$s_1 = w(\alpha^2) = 1 + \alpha^2 + \alpha^{14} = \alpha^6$
$s_2 = w(\alpha^3) = 1 + \alpha^{13} + \alpha^{21 mod 15} = \alpha^8$
$s_3 = w(\alpha^4) = 1 + \alpha^4 + \alpha^{28 mod 15} = \alpha^{12}$
Thus $s(z) = \alpha^3 + \alpha^6 z + \alpha^8 z^2 + \alpha^{12} z^3$, *solve the key function* $r(z) \equiv s(z)\sigma(z)\ (mod z^4)$, *we obtain* $\sigma(z) = \alpha^6 z^2 + z + \alpha^4$ *and* $r(z) = \alpha^{10} z + \alpha^4$, *Hence, the error takes place at the 2nd and 11th position.*