Coding and cryptography

Weeks 5 and 6 (2022-2023)

Problems.

1. Let $F = GF(2^3)$ be constructed using the primitive irreducible polynomial $1 + x + x^3$ and let β be the class of x. Find a parity check matrix for the cyclic Hamming code of length 7 with generator polynomial $m_\beta(x)$. Decode the following under CMLD.

   (a) $w = 0110111$

   (b) $w = 1001011$

   (c) $w = 0010101$

2. Let $F = GF(2^4)$ be the field constructed using the primitive irreducible polynomial $1 + x + x^4$ (a table for this field is on the next page), and let $C \subseteq K^{15}$ be the cyclic Hamming code with generator polynomial $m_\alpha(x) = 1 + x + x^4$. Decode the following under CMLD.

   (a) $w(x) = x^7 + x^{11} + x^{14}$;

   (b) $w(x) = x^2 + x^5 + x^8 + x^9$;

   (c) $w(x) = 1 + x^3 + x^7 + x^9 + x^{10} + x^{12}$.

3. Let $F = GF(2^4)$ constructed using the primitive irreducible polynomial $1 + x + x^4$ (a table for this field is on the next page). Use $\beta = \alpha$, and let C_{15} be the BCH code with generator polynomial $m_\beta(x)m_{\beta^3}(x)$. Decode the following under IMLD, where we correct at most two errors.

   (a) $w = 111101111111101$

   (b) $w = 111110110011100$

   (c) $w = 110111101011000$

4. Let $F = GF(2^3)$ and β be as in the first exercise. Let $g(x) = (1 + x)(\beta^3 + x)$ in $F[x]$ generate a code of length 7 over F.

   (a) How many codewords does C have?

   (b) Construct a generating matrix G for C.

   (c) Encode the following using G:

      i. $m(x) = 1 + \beta^6$

      ii. $m(x) = \beta^4 x^4$

      iii. $m(x) = 1 + x + x^2$

   (d) Find the generator polynomial $g_K(x)$ of the cyclic binary subfield subcode.

5. Let $F = GF(2^3)$ and β be as in the first problem. Let C be the $RS(7, 5)$ of length 7 with generator polynomial $g(x) = (1 + x)(\beta + x)(\beta^2 + x)(\beta^3 + x)$ in $F[x]$.

   (a) Find n, k, d and $|C|$.

   (b) Construct a generating matrix G for C.

   (c) Encode the following using G to a codeword in C and then to a codeword in $\widehat{C}$:

      i. $10\beta^2$

      ii. 111

      iii. $\beta^2\beta^4\beta^6$

In the remaining exercises we use $F = GF(2^4)$ constructed using the primitive irreducible polynomial $1 + x + x^4$. With α the class of x in F we have $\alpha^{15} = 1$, as well as the following table.

0000	0	0001	α^3	1101	α^7	0111	α^{11}
1000	1	1100	α^4	1010	α^8	1111	α^{12}
0100	α^1	0110	α^5	0101	α^9	1011	α^{13}
0010	α^2	0011	α^6	1110	α^{10}	1001	α^{14}

6. Let $\beta = \alpha$, and let C be the $RS(15, 7)$ of length 15 with generator polynomial

$$g(x) = (1 + x)(\beta + x)(\beta^2 + x)(\beta^3 + x)(\beta^4 + x)(\beta^5 + x)$$

in $F[x]$. Decode the following using the method of Section 6.3:

   (a) $0\alpha^3\alpha\alpha^5\alpha^3\alpha^2\alpha^6\alpha^{10}0000000$
   (b) $1\alpha^4\alpha^2\alpha0010\alpha\alpha^5\alpha^3\alpha^20\alpha^{10}\alpha$
   (c) $\alpha0\alpha^70\alpha^{12}\alpha^3\alpha^310000000$
   (d) $\alpha^5\alpha^9\alpha\alpha^{13}\alpha^{13}\alpha^6000000000$

7. Let $\beta = \alpha^4$. Verify that $1, \beta, \beta^2, \beta^3, \ldots, \beta^{14}$ are distinct. Let C be the $RS(15, 5)$ of length 15 with generator polynomial $g(x) = (\beta + x)(\beta^2 + x)(\beta^3 + x)(\beta^4 + x)$ in $F[x]$. Decode the following using the transform method:

   (a) $\alpha^{10}\alpha^{12}\alpha^9\alpha^7\alpha^8\alpha^9000000000$
   (b) $\alpha^{10}1\alpha^{13}\alpha^2\alpha^5\alpha^710\alpha^5000000$
   (c) $\alpha^21\alpha^{13}\alpha\alpha^5\alpha^3\alpha^{12}\alpha^50000000$

8. Let $\beta = \alpha^3$ so that $1, \beta, \beta^2, \beta^3, \beta^4$ are distinct and $\beta^5 = 1$. Let C be the $RS(5, 5) \subseteq F^5$ of length 5 (which divides $2^4 - 1$) with generator polynomial $g(x) = (1 + x)(\beta + x)(\beta^2 + x)(\beta^3 + x)$.

   (a) Decode the words $w(x)$ by means of the algorithm in Section 6.3, using the syndromes $s_i = w(\beta^i)$ for $i = 0, 1, 2, 3$:
      i. $w_1(x)$ with syndromes $s_0 = \alpha^{11}$, $s_1 = \alpha^7$, $s_2 = \alpha^9$ and $s_3 = \alpha^3$;
      ii. $w_2(x)$ with syndromes $s_0 = 1$, $s_1 = \alpha^2$, $s_2 = \alpha^{14}$ and $s_3 = \alpha^8$;
      iii. $w_3(x)$ with syndromes $s_0 = 1$, $s_1 = \alpha^9$, $s_2 = \alpha^3$ and $s_3 = \alpha$;
      iv. $w_4(x)$ with syndromes $s_0 = \alpha^{10}$, $s_1 = \alpha^4$, $s_2 = \alpha^{13}$ and $s_3 = \alpha^7$.
   (b) Now also decode $w_1(x)$, $w_2(x)$, $w_3(x)$ and $w_4(x)$ using the transform method.
   (c) How many words are there in C? What is the information rate of the associated binary code $\widehat{C}$ of length 20?