Homework Assignment 7, Solutions

Problem 1.

(a) $S = HR^T = \begin{pmatrix} A \\ 9 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix}$, $S_1^3 = A^3 = F \neq S_3 \Rightarrow$ There is more than one error.

$\sigma_1 = S_1 = A$, $\sigma_2 = (S_1^3 + S_3)/S_1 = E \Rightarrow \sigma(x) = x^2 + Ax + E = 0$.

$\sigma(x) = 0$ has two roots: 6 and C⇒There are 2 errors.

∴The corrected codeword is (1 0 1 0 1 0 0 0 0 0 1 1 0 0 0).

(b) $S = HR^T = \begin{pmatrix} 0 \\ 6 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix} \Rightarrow$ More than 2 errors.

(c) $S = HR^T = \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix}$, $S_1^3 = 1 \neq S_3 \Rightarrow$ More than 1 error.

$\sigma_1 = S_1 = 1$, $\sigma_2 = (S_1^3 + S_3)/S_1 = 3 \Rightarrow \sigma(x) = x^2 + x + 3 = 0$.

$\sigma(x) = 0$ has two roots: C and D⇒There are 2 errors.

∴The corrected codeword is (1 1 1 1 1 1 0 0 0 0 0 0 0 0 0).

(d) $S = HR^T = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow$ No error.

(e) $S = HR^T = \begin{pmatrix} 7 \\ 1 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix}$, $S_1^3 = 7^3 = 1 = S_3 \Rightarrow$ There is 1 error.

The corrected codeword is (0 0 1 0 1 0 1 0 0 0 0 0 0 1 1).

Problem 2.

(a) Proof: ∀ codeword $C=(C_0\ C_1\ C_2 \ldots\ldots C_{14})$, $C^R=(C_{14}\ C_0\ C_1\ C_2 \ldots\ldots C_{13})$.

$$H'C^T = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow \begin{cases} \sum_{i=0}^{14} C_i 2^i = 0 \\ \sum_{i=0}^{14} C_i (2^i)^3 = 0 \end{cases} \Rightarrow \begin{cases} 2\sum_{i=0}^{14} C_i 2^i = 0 \\ 2^3 \sum_{i=0}^{14} C_i (2^i)^3 = 0 \end{cases} \Rightarrow \begin{cases} \sum_{i=0}^{14} C_i 2^{i+1} = 0 \\ \sum_{i=0}^{14} C_i (2^{i+1})^3 = 0 \end{cases}$$

$$\overset{2^{15}=1}{\Longrightarrow} \begin{cases} C_{14} + \sum_{i=1}^{14} C_{i-1} 2^i = 0 \\ C_{14} + \sum_{i=1}^{14} C_{i-1} (2^i)^3 = 0 \end{cases} \Rightarrow H'C^R = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow C^R \text{ is also a codeword.}$$

⇒The (15, 7) linear code is cyclic.

(b) $\deg(g(x)) = n-k = 15-7 = 8$, $g(x) \mid x^{15}-1$,

$x^{15}-1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$,

So: $g(x) = (x^4+x+1)(x^4+x^3+1) = 1+x+x^3+x^4+x^5+x^7+x^8$, whose corresponding codeword is $(1\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0) \stackrel{\Delta}{=} C_A$

or $g(x) = (x^4+x+1)(x^4+x^3+x^2+x+1) = 1+x^4+x^6+x^7+x^8$, whose corresponding codeword is $(1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0) \stackrel{\Delta}{=} C_B$

or $g(x) = (x^4+x^3+1)(x^4+x^3+x^2+x+1) = 1+x+x^2+x^4+x^8$, whose corresponding codeword is $(1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0) \stackrel{\Delta}{=} C_C$.

$$\because H'C_A^T \neq \begin{pmatrix}0\\0\end{pmatrix},\ H'C_B^T = \begin{pmatrix}0\\0\end{pmatrix},\ H'C_C^T \neq \begin{pmatrix}0\\0\end{pmatrix},$$

$\therefore$ C_B is the codeword for g(x). So $g(x) = 1+x^4+x^6+x^7+x^8$.

Problem 3.

(a)
$$\begin{cases} c_0 = a_0b_0 + a_1b_3 + a_2b_2 + a_3b_1 \\ c_1 = a_0b_1 + a_1b_0 + a_1b_3 + a_2b_2 + a_3b_1 + a_2b_3 + a_3b_2 \\ c_2 = a_0b_2 + a_1b_1 + a_2b_0 + a_2b_3 + a_3b_2 + a_3b_3 \\ c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 + a_3b_3 \end{cases}$$

(b)
$$\begin{cases} D = (1101)_2 \\ 4 = (0100)_2 \end{cases} \Rightarrow \begin{cases} (a_0a_1a_2a_3) = (1011) \\ (b_0b_1b_2b_3) = (0010) \end{cases} \Rightarrow (c_0c_1c_2c_3) = (1000) \Rightarrow D \bullet 4 = (0001)_2 = 1$$

Problem 4.

$F = (1111)_2 \leftrightarrow x^3+x^2+x+1$

Apply the extended Euclidean algorithm, we get:

i	s_i	t_i	r_i	q_i
-1	1	0	x^4+x+1	__
0	0	1	x^3+x^2+x+1	__
1	1	$x+1$	x	$x+1$
2	x^2+x+1	x^3	1	x^2+x+1

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

$\therefore x^3(x^3+x^2+x+1) = 1 \bmod (x^4+x+1)$, $x^3 \leftrightarrow (1000)_2 = 8$.

$\therefore F^{-1} = 8$.