EE512: Error Control Coding

Solution for Assignment on BCH and RS Codes

March 22, 2007

1. To determine the dimension and generator polynomial of all narrow sense binary BCH codes of length $n = 31$, we have to do coset decompostion of the set $\{0, 1, 2, ..., 30\}$ mod 31 under multiplication by 2. It can be verified there would be six cosets each with 5 elements and one coset $\{0\}$. In other words $x^{31} + 1$ can be factorised as follows:

$$x^{31} + 1 = (x + 1)M_{\alpha}(x)M_{\alpha^3}(x)M_{\alpha^5}(x)M_{\alpha^7}(x)M_{\alpha^{11}}(x)M_{\alpha^{15}}(x),$$

where α is a primitive element of $GF(32)$. The degree of each $M(x)$ is equal to 5. The possible degrees for the generator polynomial for narrow sense BCH code are as follows:

$$(n - k) = 5, 10, 15, 20, 25, 30.$$

Therefore, the possible dimensions for the code are as follows:

$$k = 26, 21, 16, 11, 6, 1.$$

The generator polynomial of the $(31, 26)$ BCH code will be $g_1(x) = M_{\alpha}(x)$, while the generator polynomial of the $(31, 21)$ BCH code will be $g_2(x) = M_{\alpha}(x)M_{\alpha^3}(x)$ and so on.

2. Let α be the primitive element of $GF(1024)$, and let $M_{\alpha^i}(x)$ denote the minimal polynomial of α^i. Then required generator polynomials are as follows:

   (a) $t = 1$.
   $$g_1(x) = \text{LCM}\{M_{\alpha}(x), M_{\alpha^2}(x)\} = M_{\alpha}(x).$$

   (b) $t = 2$.
   $$g_2(x) = \text{LCM}\{M_{\alpha}(x), M_{\alpha^2}(x), M_{\alpha^3}(x), M_{\alpha^4}(x)\} = M_{\alpha}(x)M_{\alpha^3}(x).$$

   (c) $t = 3$.
   $$g_3(x) = \text{LCM}\{M_{\alpha}(x), M_{\alpha^2}(x), ..., M_{\alpha^6}(x)\} = M_{\alpha}(x)M_{\alpha^3}(x)M_{\alpha^5}(x).$$

   (d) $t = 4$.
   $$g_4(x) = \text{LCM}\{M_{\alpha}(x), M_{\alpha^2}(x), ..., M_{\alpha^8}(x)\} = M_{\alpha}(x)M_{\alpha^3}(x)M_{\alpha^5}(x)M_{\alpha^7}(x).$$

3. To find the dimensions of length-65 narrow sense binary BCH codes of given designed distance δ, it is sufficient to do the coset decomposition of the set $\{0, 1, 2, 3, ...64\}$ mod 65 under multiplication by 2. The cosets are as follows:

$$C_0 = \{0\},$$
$$C_1 = \{1, 2, 4, 8, 16, 32, 64, 63, 61, 57, 49, 33\},$$
$$C_3 = \{3, 6, 12, 24, 48, 31, 62, 59, 53, 41, 17, 34\},$$
$$C_5 = \{5, 10, 20, 40, 15, 30, 60, 55, 45, 25, 50, 35\},$$
$$C_7 = \{7, 14, 28, 56, 47, 29, 58, 51, 37, 9, 18, 36\},$$
$$C_{11} = \{11, 22, 44, 23, 46, 27, 54, 43, 21, 42, 19, 38\},$$
$$C_{13} = \{13, 26, 52, 39\}.$$

   Since $65|2^{12} - 1$, $GF(2^{12})$ will contain an element of order 65. Since $(2^{12} - 1) = (2^6 - 1)(2^6 + 1) = 63 \times 65$, $\beta = \alpha^{63}$ (α is the primitive element of $GF(2^{12})$) is an element of order 65.

(a) $\delta = 3$, $t = 1$.

$$\begin{aligned}(n-k) &= \deg(\text{LCM}\{M_\beta(x), M_{\beta^2}(x)\}) \\ &= \deg(M_\beta(x)) = |C_1| = 12.\end{aligned}$$

Therefore, $k = 53$.

(b) $\delta = 5$, $t = 2$.

$$\begin{aligned}(n-k) &= \deg(\text{LCM}\{M_\beta(x), M_{\beta^2}(x), M_{\beta^3}(x), M_{\beta^4}(x)\}) \\ &= \deg(M_\beta(x)M_{\beta^3}(x)) = |C_1 \cup C_3| = 24.\end{aligned}$$

Therefore, $k = 41$.

(c) $\delta = 7$, $t = 3$.

$$\begin{aligned}(n-k) &= \deg(\text{LCM}\{M_\beta(x), M_{\beta^2}(x), ..., M_{\beta^6}(x)\}) \\ &= \deg(M_\beta(x)M_{\beta^3}(x)M_{\beta^5}(x)) = |C_1 \cup C_3 \cup C_5| = 36.\end{aligned}$$

Therefore, $k = 29$.

(d) $\delta = 9$, $t = 4$.

$$\begin{aligned}(n-k) &= \deg(\text{LCM}\{M_\beta(x), M_{\beta^2}(x), ..., M_{\beta^8}(x)\}) \\ &= \deg(M_\beta(x)M_{\beta^3}(x)M_{\beta^5}(x)M_{\beta^7}(x)) = |C_1 \cup C_3 \cup C_5 \cup C_7| = 48.\end{aligned}$$

Therefore, $k = 17$. Notice that β^8, β^9 and β^{10} are also zeros of this code. Therefore, by the BCH bound, we see that $d \geq 11$.

4. Decoder for the 2-error-correcting $(31, 21)$ BCH code.

(a) $r(x) = x^7 + x^3$. Since the received vector $r(x)$ is at a distance 2 from the all-zero codeword, the decoded codeword will be the all-zero vector. Thus, $\hat{c} = \mathbf{0}$.

(b) $r(x) = 1 + x^{17} + x^{28}$. The syndromes, s_1 and s_3, are

$$s_1 = r(\alpha) = 1 + \alpha^{17} + \alpha^{28} = \alpha^2, \text{ and}$$
$$s_3 = r(\alpha^3) = 1 + \alpha^{20} + \alpha^{22} = \alpha^{21},$$

where α is a primitive element of $GF(32)$. If X_1 and X_2 are the error locations, then

$$\begin{aligned}s_1 &= \alpha^2 = X_1 + X_2, \\ s_3 &= \alpha^{21} = X_1^3 + X_2^3.\end{aligned}$$

¿From the above, we get $X_1 + X_2 = \alpha^2$ and $X_1 X_2 = \alpha^{28}$. Hence, X_1 and X_2 are roots of the quadratic equation $q(x) = x^2 + \alpha^2 x + \alpha^{28}$. No element in $GF(32)$ is a root of $q(x)$. Hence, the bounded-distance secoder fails. (More than 2 errors must have occured)

5. C is a t-error correcting narrow-sense BCH code of length $n = 2^m - 1$. If α is a primitive element of $GF(2^m)$, then $\{\alpha, \alpha^2, ...\alpha^{2t}\}$ are zeros of the code C. Since $l = n/(2t+1)$ and $2t + 1 = n/l$, $alpha^{2t+1}$ is of order l (a primitive l-th root of unity). Therefore, the roots of $x^l + 1$ are

$$1, \alpha^{2t+1}, \alpha^{2(2t+1)}, \alpha^{3(2t+1)}, \cdots, \alpha^{(l-1)(2t+1)}, \text{ or}$$
$$x^l + 1 = (x+1)(x+\alpha^{2t+1})(x+\alpha^{2(2t+1)}) \cdots (x+\alpha^{(l-1)(2t+1)}).$$

Now, since α is a primitive n-th root of unity,

$$x^n + 1 = (x+1)(x+\alpha)(x+\alpha^2) \cdots (x+\alpha^{n-1}).$$

Therefore,

$$a(x) = \frac{x^n + 1}{x^l + 1} = (x^{n-l} + x^{n-2l} + ... + x^l + 1)$$

is a polynomial of degree $\leq n - 1$ with $\alpha, \alpha^2, ...\alpha^{2t}$ as zeros. Therefore, $a(x)$ is a codeword of C. Weight of the codeword, $a(x) = 1 + x^l + x^{2l} + ... + x^{2tl}$ is $2t + 1$. Therefore, the minimum distance of the code C is equal to $2t + 1$.

6. C is a length-n BCH code with $\{\alpha^{-t}, ...\alpha^{-1}, 0, \alpha, ...\alpha^{t}\}$ as zeros.

   (a) The number of consecutive zeros is $2t+1$. By the BCH bound, minimum distance of C is bounded as $d_{min} \geq (2t+2)$.

   (b) If t is odd, $t+1$ will be even, and $\alpha^{(t+1)}$ will be included in the conjugate set of $\alpha^{(t+1)/2}$, where $\alpha^{(t+1)/2} \in \{\alpha^{-t}, ...\alpha^{-1}, 0, \alpha, ...\alpha^{t}\}$. Therefore, $\alpha^{(t+1)}$ will also be a zero of C. Similarly, $\alpha^{-(t+1)}$ will also be a zero of C.

   (c) If t is odd, total number of consecutive zeros is $(2t+3)$. Thus, $d_{min} \geq (2t+4)$.

7. The PGZ decoder could be used here. We will present a different solution. The primitive, narrow sense, 3-error correcting $(15, 5)$ BCH code is used over BSC. The received vector [000001101000100] is represented as $r(x) = x^5 + x^6 + x^8 + x^{12}$. The generator polynomial of the $(15, 5)$ BCH code is $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$. Dividing $r(x)$ by $g(x)$,

$$r(x) = (x^2+1)g(x) + (x^3 + x + 1).$$

   Notice that $(x^2+1)g(x)$ is a codeword that is a distance 3 away from $r(x)$. Since the codeword has minimum distance 7, the closest codeword is $\hat{c}(x) = r(x) + (x^3+x+1)$, or [110101101000100]. How will you generalize this method? Why did this work? To know more, read about error-trapping decoders for cyclic codes.

8. Consider the 2-error correcting RS code over $GF(8)$. Let α be a primitive element of $GF(8)$.

   (a) $n = 7$; $(n-k) = 2t = 4 \Rightarrow k = 3$; Minimum distance, $d = 2t+1 = 5$; Generator polynomial,

$$\begin{aligned} g(x) &= (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4), \\ &= x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3. \end{aligned}$$

   To encode the vector [1 α α^2], $m(x) = 1 + \alpha x + \alpha^2 x^2$ and $x^{(n-k)}m(x) = x^4 m(x) = x^4 + \alpha x^5 + \alpha^2 x^6$. Dividing $x^4 m(x)$ by $g(x)$,

$$x^4 m(x) = g(x)(\alpha^2 x^2 + \alpha^6 x + 1) + (\alpha^6 x^3 + \alpha^5 x^2 + \alpha^4 x + \alpha^3).$$

   Thus, parity to be appended with the message is given by $p(x) = \alpha^6 x^3 + \alpha^5 x^2 + \alpha^4 x + \alpha^3$. Finally, the codeword is $[\alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ 1\ \alpha\ \alpha^2]$.

   (b) The binary-expanded code is a $(21, 9, \geq 5)$ code.

   (c) $r(x) = x + \alpha x^2 + \alpha^2 x^3 + \alpha^3 x^4 + x^5$. Using the PGZ decoder, it can be verified that the number of errors that occured is 2, the error locations are 1 and 3, and error magnitudes are α and α^6, respectively. Thus, the error polynomial is $e(x) = \alpha x + \alpha^6 x^3$, and

$$\hat{c}(x) = r(x) + e(x) = \alpha^3 x + \alpha x^2 + x^3 + \alpha^3 x^4 + x^5.$$

9. Consider the 2-error correcting, narrow-sense, RS code over $GF(16)$. Let α be the primitive element of $GF(16)$.

   (a) Generator polynomial, $g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$; Check polynomial, $h(x) = (x^n+1)/g(x) = (x+\alpha^5)(x+\alpha^6)...(x+\alpha^{14})$.

   (b) Parity check metrix H is given by,

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & .... & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & .... & \alpha^{28} \\ 1 & \alpha^3 & \alpha^6 & .... & \alpha^{42} \\ 1 & \alpha^4 & \alpha^8 & .... & \alpha^{56} \end{pmatrix}$$

(c) The vector $[\alpha^6\alpha^{12}\alpha^9\alpha^{12}000\alpha^8000\alpha^{10}\alpha\alpha^{13}\alpha]$ is decoded using the PGZ decoder. It can be verified that the number of errors that occured is 1, error location is 7, and the error magnitude is α^8. Thus the decoded codeword is

$$\hat{\mathbf{c}} = [\alpha^6\alpha^{12}\alpha^9\alpha^{12}0000000\alpha^{10}\alpha\alpha^{13}\alpha].$$

10. In general, an RS code of length $n = (2^m - 1)$ and error-correcting capability t will have $2t$ consecutive zeros, $\{\alpha^l, \alpha^{(l+1)}..., \alpha^{(l+2t-1)}\}$. The generator polynomial is

$$g(x) = (x + \alpha^l)(x + \alpha^{(l+1)})...(x + \alpha^{(l+2t-1)}),$$

and the check polynomial $h(x)$ will have $(n-2t)$ consecutive roots, namely $\{\alpha^{(l+2t)}, \alpha^{(l+2t+1)}..., \alpha^{(l+n-1)}\}$. Therefore,

$$h(x) = (x + \alpha^{(l+2t)})(x + \alpha^{(l+2t+1)})..(x + \alpha^{(l+n-1)}).$$

Hence, the generator polynomial of the dual code is

$$\tilde{g}(x) = x^{(n-2t)}h(x^{-1}) = (1 + \alpha^{(l+2t)}x)(1 + \alpha^{(l+2t+1)}x)..(1 + \alpha^{(l+n-1)}x).$$

Thus the roots of $\tilde{g}(x)$ are

$$\{\alpha^{-(l+2t)}, \alpha^{-(l+2t+1)}..., \alpha^{-(l+n-1)}\},$$

which is a set of $(n - 2t)$ consecutive roots. Thus, the dual of an RS$(n, k, 2t + 1)$ code is also an RS code. The dual is an RS$(n, 2t, n - 2t + 1)$ code.

11. (a) We show that the binary-expanded version of $(n = (2^m - 1), k, d)$ RS code over $GF(2^m)$ is linear. The binary-expanded version of a RS code consists of the binary expansions of all the codewords of the RS code (expanded using some basis). Since the RS code itself is linear, the binary expanded version will also be linear (Addition in $GF(2^m)$ itself is defined using the vector notation of the elements of $GF(2^m)$ over $GF(2)$ using a particular basis)

    (b) Example given in class

12. We show that the $(2^m - 1, k, d)$ RS code contains the binary BCH code of designed distance d as a subcode. Let α be a primitive element of $GF(2^m)$. The zeros of the $(2^m - 1, k, d)$ RS code are

$$Z_{rs} = \{\alpha, \alpha^2, ...\alpha^{d-1}\}.$$

The generator polynomial of the RS code is

$$g_{rs}(x) = (x + \alpha)(x + \alpha^2)...(x + \alpha^{d-1}).$$

The zeros of the binary BCH code of length $n = 2^m - 1$ and designed distance d are

$$Z_{bch} = C_\alpha \cup C_{\alpha^2} \cup \cdots \cup C_{\alpha^{d-1}}\},$$

where C_{α^i} denotes all the conjugates of α^i. Hence, the generator polynomial of the BCH code is

$$g_{bch}(x) = \text{LCM}\{M_\alpha(x), M_{\alpha^2}(x), ..., M_{\alpha^{d-1}}(x)\},$$

where M_{α^i} is the minimal polynomial of α^i. Since $Z_{rs} \subset Z_{bch}$, $g_{rs}(x)$ divides $g_{bch}(x)$ or $g_{bch}(x) = a(x)g_{rs}(x)$. Any codeword of the BCH code can be written as

$$c_{bch}(x) = m(x)g_{bch}(x) = m(x)a(x)g_{rs}(x),$$

which belongs to the RS code. Thus, the binary BCH code is a subcode of the RS code.

13. (a)

$$H = \begin{pmatrix} 1 & 0 & 1 & \alpha & \alpha^2 & .... & \alpha^{14} \\ 0 & 1 & 1 & \alpha^2 & \alpha^4 & .... & \alpha^{28} \end{pmatrix}$$

Let $\mathbf{c} = [c_0\ c_1\ c_2 \cdots c_{16}] \in C$, the code over GF(16) with parity-check matrix H, be a nonzero codeword. We will try to find the minimum weight of a nonzero codeword by considering several cases.

i. case 1: $c_0 = c_1 = 0$: Then wt($\mathbf{c}$) =wt($[c_2 \cdots c_{16}]$) and

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & .... & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & .... & \alpha^{28} \end{bmatrix} [c_2 \cdots c_{16}]^T = \mathbf{0}.$$

Using the BCH bound in the above equation, we see that wt($[c_2 \cdots c_{16}] \geq 3$. Hence, wt($\mathbf{c}$) ≥ 3.

ii. case 2: $c_0 = 0$, $c_1 \neq 0$: Then wt($\mathbf{c}$) = 1+wt($[c_2 \cdots c_{16}]$) and

$$[1\ \alpha\ \cdots \alpha^{14}][c_2 \cdots c_{16}]^T = 0.$$

From the above equation, we see that wt($[c_2 \cdots c_{16}] \geq 2$. Hence, wt($\mathbf{c}$) ≥ 3.

iii. case 3: $c_0 \neq 0$, $c_1 = 0$: Then wt($\mathbf{c}$) = 1+wt($[c_2 \cdots c_{16}]$) and

$$[1\ \alpha^2\ \cdots \alpha^{28}][c_2 \cdots c_{16}]^T = 0.$$

From the above equation, we see that wt($[c_2 \cdots c_{16}] \geq 2$. Hence, wt($\mathbf{c}$) ≥ 3.

iv. case 4: $c_0 \neq 0$, $c_1 \neq 0$: Then wt($\mathbf{c}$) = 2+wt($[c_2 \cdots c_{16}]$) and

$$[1\ \alpha\ \cdots \alpha^{14}][c_2 \cdots c_{16}]^T \neq 0.$$

From the above equation, we see that wt($[c_2 \cdots c_{16}] \geq 1$. Hence, wt($\mathbf{c}$) ≥ 3.

Thus, minimum distance $d \geq 3$. Since $\mathbf{c}$ = [1110000000000000] is a valid codeword, $d = 3$.

(b)

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & \alpha & \alpha^2 & .... & \alpha^{14} \\ 0 & 1 & 0 & 1 & \alpha^2 & \alpha^4 & .... & \alpha^{28} \\ 0 & 0 & 1 & 1 & \alpha^3 & \alpha^6 & .... & \alpha^{42} \end{pmatrix}$$

case (1): Let $\mathbf{c}$ = [0 0 0 $\mathbf{c}_1$]. From, the given parity check matrix, it is clear that $\mathbf{c_1}$ has to be a codeword of the $(15, 12, 4)$ RS code if $\mathbf{c}$ is to belong to the given code. Thus minimum weight possible for such codewords is 4.

case (2): Let $\mathbf{c}$ = [0 0 k $\mathbf{c}_2$], where k is some non-zero element of GF(16). From the structure of the given parity check matrix, $c_2(x)$ has α and α^2 as zeros. Thus, $\mathbf{c}_2$ alone has minimum weight at least 3. Thus the whole vector $\mathbf{c}$ has minimum weight $\geq 3 + 1 = 4$.

case (3): Let $\mathbf{c}$ = [k 0 0 $\mathbf{c}_3$]. A similar argument as in case (2) implies that $c_3(x)$ has α^2 and α^3 as roots. The minimum weight of the entire vector is $\geq 3 + 1 = 4$.

case (4): Let $\mathbf{c}$ = [0 k 0 $\mathbf{c}_4$]. Here $c_4(x)$ has α and α^3 as roots.

The minimum weight of $c_4(x)$ can be seen to be 3 using a generalized definition of RS codes over GF(2^m). In general, if a cyclic code over GF(2^m) has $(d-1)$ equispaced roots, i.e. of the form $\{\alpha, \alpha^{(1+r)}, ...\alpha^{(1+r(d-1)}\}$ (r relatively prime to n), rather than $(d-1)$ consecutive roots, the BCH bound still holds. Thus, the whole vector $\mathbf{c}$ has minimum weight $\geq 3+1 = 4$.

Another argument for case (4): Since

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & .... & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & .... & \alpha^{42} \end{bmatrix} \mathbf{c}_4 = \mathbf{0},$$

we see that wt($\mathbf{c}_4$) ≥ 2. We will argue by contradiction that wt($\mathbf{c}_4$) $\neq 2$. Supposing wt($\mathbf{c}_4$) = 2, we have from the above equation that

$$\begin{bmatrix} \alpha^i & \alpha^j \\ \alpha^{3i} & \alpha^{3j} \end{bmatrix} \mathbf{x} = \mathbf{0}$$

has a nonzero solution for some $i \neq j$. But determinant of the matrix in the LHS above is seen to be

$$\begin{aligned} \alpha^{i+3j} + \alpha^{j+3i} &= \alpha^{i+j}(\alpha^{2i} + \alpha^{2j}), \\ &= \alpha^{i+j}(\alpha^i + \alpha^j)^2 \neq 0. \end{aligned}$$

This results in a contradiction and $\text{wt}(\mathbf{c}_4) \geq 3$. Thus minimum weight of the entire vector is at least 4.

¿From all the above cases, minimum distance of the given code is at least 4. Since $[11110\cdots0]$ is a codeword, $d = 4$.

14. C is a $(n = 2^m - 1, k, d)$ RS code with zeros $\{\alpha, \alpha^2, ...\alpha^{d-1}\}$, where α is a primitive element of $GF(2^m)$. Length of $\hat{C}$ is clearly 2^m and dimension is k (the same as C, since it contains the same total number of codewords). To prove the minimum distance of the new code is $(d+1)$, it is enough to prove that all minimum weight codewords have a non-zero extended component u_{n+1}.

    Consider a codeword of C $u(x) = m(x)g(x)$. Suppose $u(x)$ has weight d. Then,

    $$u_{n+1} = u_1 + u_2 + .. + u_n = u(1) = m(1)g(1),$$

    and $u_{n+1} = 0 \Rightarrow m(1)g(1) = 0$. Since $g(1) \neq 0$, $m(1) = 0$. But if $m(1) = 0$, then $m(x) = m_1(x)(x+1)$, and $u(x) = m(x)g(x) = m_1(x)(x+1)g(x) \Rightarrow u(x)$ has d consecutive zeros $\{1, \alpha, \cdots, \alpha^{d-1}\}$, which implies that $u(x)$ has a minimum weight of $(d+1)$ resulting in a contradiction. Thus, $m(1) \neq 0$, Thus $u_{n+1} \neq 0$ when $u(x)$ has weight d.

    Thus, the minimum distance of the new extended code is $(d+1)$.

15. Length of the new code is clearly $(n+2)$. Since the matrix H has column rank (equals row rank) $n-k$ (maximum possible), the column rank and row rank of the new parity-check matrix remain $n-k$. Hence, the dimension of the new code is $(n+2)-(n-k) = k+2$. To prove minimum distance is d, we consider several cases.

    case (1): Let $\mathbf{c} = [k\ 0\ \mathbf{c}_1]$, where k is a non-zero element of $GF(2^m)$. $\mathbf{c}_1$ has zeros $\{\alpha, \alpha^2, ...\alpha^{d-2}\}$. Thus weight of $\mathbf{c}_1 \geq (d-2+1) = (d-1)$. Thus the weight of the vector $\mathbf{c}$ is at least d.

    case (2): Let $\mathbf{c} = [0\ k\ \mathbf{c_2}]$, where k is a non-zero element of $GF(2^m)$. $\mathbf{c}_2$ has zeros $\{\alpha^2, \alpha^3, ...\alpha^{d-1}\}$. Since the set of zeros form a set of $(d-2)$ consecutive roots, weight of $\mathbf{c}_2 \geq (d-2+1) = (d-1)$, Thus the weight of the vector $\mathbf{c}$ is at least d.

    case (3): Let $\mathbf{c} = [k_1\ k_2\ \mathbf{c_2}]$, where k_1, k_2 are non-zero elements of GF(2^m). $\mathbf{c}_2$ has zeros $\{\alpha^2, \alpha^3, ...\alpha^{d-2}\}$. Since the set of zeros form a set of $(d-3)$ consecutive roots, weight of $\mathbf{c}_2 \geq (d-3+1) = (d-2)$, Thus the weight of the vector $\mathbf{c}$ is at least d.

    case (4): Let $\mathbf{c} = [0\ 0\ \mathbf{c}_3]$. Then $\mathbf{c}_3$ is a codeword of C and has minimum weight d. Thus the vector $\mathbf{c}$ also has weight at least d.

    ¿From the cases given above, it can be inferred that the minimum weight of the new code is equal to d.

16. Try this on your own using the hints.