Assignment on BCH and RS Codes

EE512: Error Control Coding

Questions marked (Q) or (F) are questions from previous quizzes or final exams, respectively.

1. Determine the dimension and generator polynomial of all the narrow-sense binary BCH codes of length 31.
2. Find the generator polynomial of the length-1023, narrow-sense binary BCH code with designed error-correcting capability (a) $t = 1$. (b) $t = 2$. (c) $t = 3$. (d) $t = 4$.
3. Find the dimension of the length-65, narrow-sense binary BCH code with designed distance (a) $\delta = 3$. (b) $\delta = 5$. (c) $\delta = 7$. (d) $\delta = 9$.
4. Suppose that the double-error-correcting narrow-sense binary BCH code of length 31 is used over a BSC. Decode the received polynomials $x^7 + x^{30}$ and $1 + x^{17} + x^{28}$.
5. Let C be the t-error correcting narrow-sense binary BCH code of length $n = 2^m - 1$. If $(2t+1)|n$, show that $\dfrac{x^n+1}{x^l+1}$ (with $l = n/(2t+1)$) is a codeword of C. What is the exact minimum distance of C?
6. Let C be a length n binary BCH code with the following consecutive zeros (α - primitive n-th root of unity)
$$\alpha^{-t}, \cdots, \alpha^{-1}, \alpha^0, \alpha^1, \cdots, \alpha^t$$
   (a) Obtain a lower bound for the minimum distance of C using the BCH bound.
   (b) If t is odd, show that α^{-t-1} and α^{t+1} are also zeros of C.
   (c) Obtain a better lower bound for the minimum distance when t is odd.
7. (Q) The primitive, narrow-sense, triple-error-correcting $(15, 5)$ BCH code is being used over a BSC. Decode the received vector [000001101000100].
8. Consider the 2-error correcting RS code over GF(8). Let α be a primitive element of GF(8).
   (a) List the parameters of the code. Find the generator polynomial of the code. Encode the message $[1\ \alpha\ \alpha^2]$ systematically.
   (b) List the parameters of the binary expanded code. Provide binary equivalents of the encoding above.
   (c) Decode the received word $[0\ 1\ \alpha\ \alpha^2\ \alpha^3\ 1\ 0]$.
9. (F) Consider the 2-error correcting, narrow-sense RS code over GF(16) (α: primitive element).
   (a) Write down the generator polynomial and the check polynomial.
   (b) Provide a parity check matrix for the code.
   (c) Decode the received vector $[\alpha^6\alpha^{12}\alpha^9\alpha^{12}000\alpha^8000\alpha^{10}\alpha\ \alpha^{13}\alpha]$.
10. Show that the dual of an RS code is also an RS code (and hence MDS). Find the parameters of the dual code.
11. (a) Show that the binary expanded version of a $(n = 2^m - 1, k, d)$ RS code over GF(2^m) is linear. Find the parameters of the expanded code.
    (b) Show that the binary expanded version of a RS code over GF(2^m) is not necessarily cyclic by a counterexample using a code over GF(4).
12. Show that a $(2^m - 1, k, d)$ RS code contains a binary BCH code of designed distance d as a subcode.

13. (F) Find the minimum distance of a code over GF(16) (α: primitive element) defined by the parity-check matrix

(a)

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

(b)

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{14} \\ 0 & 1 & 0 & 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{28} \\ 0 & 0 & 1 & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \cdots & \alpha^{42} \end{bmatrix}.$$

14. Let C be the $(n = 2^m - 1, k, d)$ RS code with zeros $\alpha, \alpha^2, \cdots, \alpha^{d-1}$ ($\alpha \in$GF(2^m) is primitive). Show that

$$\hat{C} = \{[\mathbf{u}\; u_{n+1}] : \mathbf{u} = [u_1 \cdots u_n] \in C,\; u_{n+1} = u_1 + u_2 + \cdots + u_n\}$$

formed by extending C by adding a overall parity-check symbol is a $(2^m, k, d + 1)$ code.

15. Let H be a parity check matrix of an $(n = 2^m - 1, k, d)$ RS code over GF(2^m). Show that the code with parity check matrix

$$\begin{bmatrix} 0 & 1 & \\ 0 & 0 & \\ \vdots & \vdots & H \\ 0 & 0 & \\ 1 & 0 & \end{bmatrix}$$

is an $(n + 2, k + 2, d)$ code.

16. Here is the original construction of RS codes due to Reed and Solomon. Consider polynomials of degree less than or equal to $k - 1$ with coefficients from GF(q) (α : primitive element). There are $K = q^k$ such polynomials. Let them be $f_1(x), f_2(x), \cdots, f_K(x)$. Consider the code C with codewords

$$c_i = [f_i(1)\; f_i(\alpha)\; f_i(\alpha^2)\; \cdots\; f_i(\alpha^{q-2})], \tag{1}$$

for $1 \leq i \leq K$.

(a) Show that C is an $(n = q - 1, k)$ linear code over GF(q).

(b) Show that the minimum distance of C is $n-k+1$. (Hint: How many zeros can a degree $k-1$ polynomial have?)

(c) Show that C is a cyclic code over GF(q). (Hint: Show that the cyclic left shift of the codeword c_i in (1) is actually c_j for a suitable j.)

(d) Show that C is the narrow-sense $(n, k, n - k + 1)$ RS code over GF(q). (Hint: Show that $c(\alpha^i) = 0,\ 1 \leq i \leq n - k$ for all $c(x) \in C$.)