Additional Assignment on Miscellaneous Topics

EE512: Error Control Coding

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

1. (Q) Consider $x \in \mathrm{GF}(32)$ and define an operator Tr as
$$\mathrm{Tr}(x) = x + x^2 + x^4 + x^8 + x^{16}.$$
   (a) Show that $\mathrm{Tr}(x)^2 = \mathrm{Tr}(x)$. What is the range of Tr?
   (b) Show that $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$ for $x, y \in \mathrm{GF}(32)$.
   (c) Find all x such that $\mathrm{Tr}(x) = 0$.

2. (Q) Consider $x \in \mathrm{GF}(16) = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{14}\}$ ($\alpha^{15} = 1$, $\alpha^4 = 1 + \alpha$) and define an operator Tr as
$$\mathrm{Tr}(x) = x + x^4.$$
   (a) Show that $\mathrm{Tr}(x)^4 = \mathrm{Tr}(x)$. What is the range of Tr?
   (b) Show that the range of the operator Tr is isomorphic to $\mathrm{GF}(4) = \{0, 1, \beta, \beta^2\}$ ($\beta^3 = 1$, $\beta^2 = 1 + \beta$).
   (c) Show that $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$ for $x, y \in \mathrm{GF}(16)$.
   (d) Find all x such that $\mathrm{Tr}(x) = 1$.

3. (Q) Consider the quadratic equation $f(x) = x^2 + x + k = 0$, where $k \in \mathrm{GF}(32)$ is a constant and $x \in \mathrm{GF}(32)$ is a variable.
   (a) Suppose there exists x such that $x^2 + x + k = 0$. Show that k has to satisfy
$$k + k^2 + k^4 + k^8 + k^{16} = 0.$$
   (b) Using the above condition, find integers i and j such that
$$f(k^i + k^j) = 0.$$
   (c) For the above i and j, $k^i + k^j \in \mathrm{GF}(32)$ is one root of $f(x)$. Find the other root of $f(x)$ in $\mathrm{GF}(32)$.

4. (Q)
   (a) Let $\alpha \in \mathrm{GF}(2^m)$ be a primitive n-th root of unity. Given that the polynomial
$$1 + x + x^2 + \cdots + x^{n-2} + x^{n-1} = \sum_{i=0}^{n-1} x^i$$
   is irreducible over $\mathrm{GF}(2)[x]$, determine the following:

i. The minimal polynomial of α.

ii. The smallest positive integer j for which $2^j = 1 \mod n$.

(b) Using the above problem, determine if the following polynomials from GF(2)[x] are irreducible. Give clear arguments for your conclusion.

i. $1 + x + x^2 + \cdots + x^9 + x^{10} = \sum_{i=0}^{10} x^i$.

ii. $1 + x + x^2 + \cdots + x^{99} + x^{100} = \sum_{i=0}^{100} x^i$.

5. (F) Consider GF(16)=$\{f(\alpha) \in \mathrm{GF}(2)[\alpha] : \deg(f(\alpha)) \leq 3\}$ with addition and multiplication modulo $\pi(\alpha) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$.

   (a) Find all $f_i(\alpha) \in \mathrm{GF}(16)$ with minimal polynomial $x^4 + x^3 + 1$.

   (b) Find all $g_i(\alpha) \in \mathrm{GF}(16)$ with minimal polynomial $x^4 + x + 1$.

6. Let GF(16)= $\{0, 1, \alpha, \alpha^2, \cdots, \alpha^{14}\}$, $\alpha^{15} = 1$, $\alpha^4 = \alpha + 1$.

   (a) Find one solution to the equation $x + y + z = 0$ in GF(16) such that all the variables are nonzero.

   (b) Find one solution to the equation $x^2 + y^2 + z^2 = 0$ in GF(16) such that all the variables are nonzero.

   (c) Solve the following simultaneous system of equations in GF(16):

$$x + y + z = 0.$$
$$x^3 + y^3 + z^3 = 0.$$

7. (Q) Let C_1 be the 2-error-correcting primitive narrow-sense BCH code with block-length $n = 15$. Let $\alpha \in F_{16}$ be primitive. The minimal polynomials of α and α^3 are $1 + x + x^4$ and $1 + x + x^2 + x^3 + x^4$, respectively.

   (a) Determine the dimension of C_1. Find the zeros of C_1.

   (b) Determine the exact minimum distance of C_1.

8. (Q) Let C_1 be the 2-error-correcting primitive narrow-sense BCH code with block-length $n = 15$ as in Question 2. Let C_2 be the 2-error-correcting primitive narrow-sense Reed-Solomon code over F_{16} ($\alpha \in F_{16}$, primitive, $\alpha^4 = 1 + \alpha$).

   (a) Find the block-length and dimension of the binary expansion of C_2.

   (b) Prove or disprove: $C_1 \subset C_2$.

   (c) Using the answer to (b), determine the exact minimum distance of the binary expansion of C_2.

9. (F)

   (a) Consider narrow-sense BCH codes of length $n = 63$ with designed error-correcting capability t. Find the smallest t for which the dimension $k \neq n - 6t$.

   (b) Consider narrow-sense BCH codes of length $n = 255$ with designed error-correcting capability t. Find the smallest t for which the dimension $k \neq n - 8t$.

10. (F) Consider the narrow-sense 1-error-correcting RS code over GF(8).

   (a) Find a nonzero codeword $c = [c_1\ c_2 \cdots c_7]$ with $c_4 = c_5 = c_6 = c_7 = 0$.

(b) Find a nonzero codeword $c = [c_1\, c_2 \cdots c_7]$ with $c_2 = c_4 = c_5 = c_6 = 0$.

11. (F) Consider a narrow-sense, 1-error-correcting RS code with block-length $n = 7$ symbols over GF(8). Let $\alpha \in \text{GF}(8)$ be a primitive element with $\alpha^3 = \alpha + 1$.

    (a) Determine systematic parity-check and generator matrices for the code.

    (b) Decode the received polynomial $r(x) = 1 + x$.

12. (F) Consider narrow-sense binary BCH codes with block-length $n = 15$. Determine the generator polynomial, dimension (k), BCH bound on minimum distance (d_{BCH}) and the exact minimum distance (d) for designed error-correcting capability $t = 1,\ 2,\ 3,\ 4$.

13. Consider the design of 1-error-correcting codes with block-length $n = 15$ bits using the following two methods: (1) Binary BCH code with $n = 15$; (2) Binary-expanded shortened RS code over GF(8). In Method 2, the shortening is such that the binary-expanded block-length is 15.

    (a) Find the dimension of the binary code in each method.

    (b) Find expressions for Prob{Block Error} over a BSC(p) under bounded-distance decoding for both codes. Find the dominant term as $p \to 0$.

    (c) Mention an advantage of Method 1 over Method 2. Mention an advantage of Method 2 over Method 1:

14. Consider the code C obtained by concatenating the $(2, 1)$ code $C_1 = \{00, 11\}$ and a $(6, 4)$ binary code C_2 with systematic encoding i.e.

    2 bits $\to C_1 \to$ 4 bits $\to C_2 \to$ 6 bits

    Determine C_2 such that C becomes a $(6, 2, 3)$ code.

15. Determine if the following entities exist. If yes, provide an example. If not, prove why they cannot exist.

    (a) $(6, 3)$ code C such that $C \cap C^{\perp} = \{000000\}$.

    (b) $(10, 2, 7)$ linear binary codes.

16. A $(7, 3)$ linear code C is such that $[0011101] \in C$ and $[0100111] \in C$. Given that the minimum distance of C is 4, find possible remaining codewords for C.

17. Let C_R be the t-error-correcting narrow-sense RS code over GF(2^m) with $n = 2^m - 1$. Let C_B be a t-error-correcting narrow-sense binary BCH code with blocklength n.

    (a) Provide parity-check matrices for C_R and C_B with elements from GF(2^m).

    (b) Write down precise expressions for probability of block error under bounded-distance decoding for both the codes over a BSC with transition probability p.

18. (F) Consider the concatenated encoder shown in Fig. 1. Every set of 4 bits entering the encoder is first encoded using the (7,4) Hamming code. Each 7-bit codeword of the Hamming code is treated as a symbol over GF(128). Every set of 121 symbols is further encoded using the (127,121) RS code.

    (a) Determine the block-length and dimension of the overall binary code.

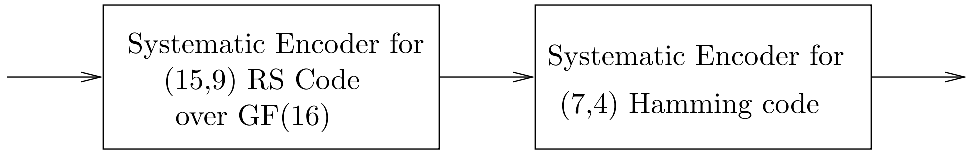

Figure 1: Encoder for Problem 18

Figure 2: Decoder for Problem 18b

(b) Consider the decoder shown in Fig. 2 over a BSC. The RS decoder is a bounded distance decoder. Syndrome decoding is used for the Hamming code. What is the error-correcting capability of the overall code under the above decoder?

19. Let C be a t-error-correcting RS code of length $n = 2^m - 1$ over GF(2^m).

   (a) Determine the exact burst-error-correcting capability of C in bits.

   (b) Let M codewords of C be symbol-interleaved by a row-column interleaver. Determine the burst-error-correcting capability after interleaving.

20. Let a 2-error-correcting $[8, 4]$ RS code over GF(8) be shortened to a $[5, 1]$ code over GF(8).

   (a) Write down the generator and parity-check matrices for the shortened code. Is the shortened code cyclic?

   (b) What is the minimum distance of the shortened code?

   (c) Write down the blocklength and messagelength of the binary expanded version of the shortened code. Are there higher-rate 2-error-correcting binary codes of the same blocklength?

21. Let a 2-error-correcting $[8, 4]$ RS code over GF(8) be punctured to a $[6, 4]$ code over GF(8).

   (a) Write down a systematic generator matrix for the $[8, 4]$ RS code.

   (b) Puncture any two parity symbols and write down a generator and parity-check matrices for the punctured code.

   (c) Can the punctured code be made 1-error-correcting?