ELEC 541: ERROR CORRECTING CODES

HOMEWORK # 4

Q1: Prove the following interesting facts about binary polynomials:

(a) If \( p(x) \) is a binary polynomial, then \( (p(x))^2 = p(x^2) \).
(b) If \( \alpha \) is a root of the binary polynomial \( p(x) \), then so are \( \alpha^2, \alpha^4, \alpha^8 \), etc.
(c) If \( \alpha \) is a root of the binary polynomial \( p(x) \), then \( \alpha^{-1} \) is a root of the reverse polynomial \( p_R(x) \).

Q2: Consider the Galois field \( \mathbb{F}[\alpha] = GF(2^4) \), where \( \alpha \) is primitive (use \( x^4 + x + 1 \) as the primitive polynomial). Express the following elements in \( \gamma \) in terms of the basis elements \( \{1, \alpha, \alpha^2, \alpha^3\} \) (the vector space notation).

(a) \( \gamma = \alpha^{-1} \).
(b) \( \gamma = \frac{1}{1+\alpha^3} \).
(c) \( \gamma = \alpha^{11}(1 + \alpha^5)(1 + \alpha^{-2}) \).
(d) \( \gamma = \sum_{\beta \in GF(2^4)} \beta \).
(e) \( \gamma = \prod_{\beta \in GF(2^4) - \{0\}} \beta \).

Q3: (a) Suppose that the binary polynomial \( f(x) \) has roots \( \gamma, \beta \in \mathbb{F}[\alpha] \) for which the minimal polynomials \( M_\gamma(x), M_\beta(x) \in \mathbb{F}(x) \) are distinct. Show that \( M(x) = M_\gamma(x)M_\beta(x) \) divides \( f(x) \) in \( \mathbb{F}[x] \).

(b) In the general case, suppose that the binary polynomial \( f(x) \) has roots \( \gamma_1, \gamma_2, \ldots, \gamma_t \in \mathbb{F}[\alpha] \) with minimal polynomials \( M_{\gamma_1}(x), M_{\gamma_2}(x), \ldots, M_{\gamma_t}(x) \). Let

\[
M(x) = \text{LCM}\{M_{\gamma_1}(x), M_{\gamma_2}(x), \ldots, M_{\gamma_t}(x)\}
\]

denote the least common multiple of the minimal polynomials. Show that \( M(x) \) divides \( f(x) \) in \( \mathbb{F}[x] \).

Q4: (a) Suppose binary polynomial \( f(x) \) has \( \gamma \in \mathbb{F}[\alpha] \) as a root. Show that

\[
g(x) = \text{LCM}\{(x + \gamma), (x + \gamma^2), (x + \gamma^4), \cdots\}\]

divides \( f(x) \) as polynomials in \( \mathbb{F}[\alpha][x] \). (Hint: Use Q1 above.)

(b) Show that the minimal polynomial of \( \gamma \in \mathbb{F}[\alpha] \) is given by

\[
M_\gamma(x) = \text{LCM}\{(x + \gamma), (x + \gamma^2), (x + \gamma^4), \cdots\}
\]

(Hint: Use the theorem from the class - If \( f(\gamma) = 0 \), then \( M_\gamma(x) \) divides \( f(x) \). )