Question 1

Show that the length 7, single error correcting binary BCH code is perfect.

⇒ Need to show this is a Hamming code

+5 ⇒ $g(x) = x^3 + x + 1$ is valid generator: $\{\alpha, \alpha^2, \alpha^4\}$ is conj. class

+5 ⇒ $h(x) = \frac{x^7+1}{x^3+x+1} = x^4 + x^2 + x + 1$

+5 ⇒ $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$ ⇒ parity check for Hamming code

⇒ Hamming codes are perfect

⇒ $t=1$, BCH code is perfect

Question 2:

A) Consider an n=3, binary cyclic code C. Consider the code C' where a single bit is added to the end of each codeword in C to make the resulting parity even.

Is C' cyclic? Explain

B) Consider a binary cyclic code C of length n. Consider the code C' of length n+1, where a single bit is added to the end of each codeword in C to make the resulting parity even. What is the relationship of the minimum distances of C and C'? Prove your answer

A) There are 2 n=3 cyclic codes: $g_1(x) = x^2+x+1$
$g_2(x) = x+1$

Check each

+10

$g_1(x)$ ⇒ $m(x)$ has degree 0 ⇒ $c(x) = 0$ (000) or 1 (111)
⇒ code is repetition code ⇒
$C' = \{0000, 1111\}$ ⇒ This is cyclic.

$g_2(x)$ ⇒ $m(x)$ has degree 1 ⇒ $g(x) = x+1$ ⇒ $c(x) = \{0, x+1, x^2+x, x^2+1\}$
$C = \{000, 011, 110, 101\}$
$C' = \{0000, 0110, 1100, 1010\}$
Not cyclic

+10

B) $d_{min,C'} \geq d_{min,C}$ ⇒ by example above for
$g_2(x)$: $d_{min,C'} = d_{min,C}$ and certainly
$d_{min,C'} \not< d_{min,C}$

Note: if d_{min} is odd ⇒ $d_{min,C'} = d_{min,C}+1$

Question 3:

Let C be a (narrow-sense) (n,k) RS code with generator polynomial g(x) and parity check polynomial h(x). A codeword c'(x) is in the dual code C' of C if c'(x)c(x) mod $x^n - 1 = 0$, where c(x) is in C.

a) Prove that C' is a Reed-Solomon code and give its generator g'(x) in terms of g(x) and/or h(x) for C.

b) Find (n',k') for C'.

c) If C corrects t errors, how many errors does C' correct?

a) let $c'(x) = g'(x) m'(x) \Leftrightarrow c(x) = m(x) g(x)$

$\Rightarrow m'(x) g'(x) m(x) g(x) = c(x) c'(x)$ = multiple mod $x^n - 1$

$\Rightarrow$ h(x) is a valid generator for C' ? $h(x) = g'(x)$

$m'(x) \underbrace{h(x) g(x)}_{x^n - 1} m(x)$ mod $x^n - 1$

$\Rightarrow h(x) = g'(x)$ is a valid generator for C'

Note: $g(x) = (x - \alpha) \cdots (x - \alpha^{2t})$

$h(x) = (x - \alpha^{2t+1}) \cdots (x - \alpha^{n-1})(x - \alpha^n)(x - \alpha^0) = \frac{x^n + 1}{f(x)}$

b) h(x) has degree $n - 2t = n' - k' \Rightarrow k' = (2t$

$n' = n, \quad t' = 2t = n - k$

c) $t' = \left\lfloor \frac{n' - k'}{2} \right\rfloor = \left\lfloor \frac{n - 2t}{2} \right\rfloor$

$n - (2t)$

Question 4:

Give the generator polynomial g(x) for the narrow-sense, single-error correcting Reed Solomon code of length 7. Let α be a primitive element.

a) How many codewords are in the code?
b) Let $m(x) = \alpha^3 x^4 + 1$, what is c(x)?
c) Suppose $r(x) = \alpha^3 x^6 + \alpha^5 x^5 + \alpha^3 x^4 + x^3 + \alpha^3 x^2 + \alpha^3 x + 1$

i) Find and correct the error (if there exists one) or indicate a decoder failure
ii) Give the original message m(x) if part i) results in a decodable sequence

GF(8): $x^3 + \alpha x + 1$

$0 = 0$
$1 = 1$
$\alpha = \alpha$
$\alpha^2 = \alpha^2$
$\alpha^3 = \alpha + 1$
$\alpha^4 = \alpha^2 + \alpha$
$\alpha^5 = \alpha^2 + \alpha + 1$
$\alpha^6 = \alpha^2 + 1$

$g(x) = (x - \alpha)(x - \alpha^2) = x^2 + (\alpha + \alpha^2)x + \alpha^3$
$= x^2 + \alpha^4 x + \alpha^3$

a) $g(x)$ has degree 2 $\Rightarrow$ $m(x)$ has degree 4.
$c(x)$ " " 6 $\Rightarrow$ 6 coeffs $\Rightarrow$ # codewords $= 8^5 = 2^{15} = 32{,}768$

b) $c(x) = (\alpha^3 x^4 + 1)(x^2 + \alpha^4 x + \alpha^3)$
$= \alpha^3 x^6 + \alpha^7 x^5 + \alpha^6 x^4 + \alpha^2 + \alpha^4 x + \alpha^3$

c) Note: single error $\Rightarrow e_1 = S_1 = r(\alpha) = X_1$
$= \alpha^3 \alpha^6 + \alpha^5 \alpha^5 + \alpha^3 \alpha^4 + \alpha^3 + \alpha^3 \alpha^2 + \alpha^3 \alpha + 1$
$= \alpha^{10} + \alpha^{10} + \alpha^7 + \alpha^3 + \alpha^6 + \alpha^4 + 1$
$= \alpha^3 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^6 + \alpha^4 + 1$
$= 2\alpha^3 + 2\alpha^6 + 2\alpha^4 + 1 = 1$ (coefficients $\bmod 2$)
$\uparrow 0 \quad \uparrow 0 \quad \uparrow 0$

Therefore magnitude $\neq 1 \Rightarrow 1 - e_1 = 1 \Rightarrow e_1 = 1 \Rightarrow e(x) = 1$

$\Rightarrow c(x) = \alpha^3 x^6 + \alpha^5 x^5 + \alpha^3 x^4 + x^3 + \alpha^3 x^2 + \alpha^3 x$

$\Rightarrow m(x) = \frac{c(x)}{g(x)} = \alpha^3 x^2 + x$

Question 5

The H.261 video compression standard uses a narrow-sense (511,493) BCH code to protect compressed video during transmission. (use can assume the appropriate GF() used by the standard is generated as in Appendices of the book)

c) What is the minimum distance of this code? What is the maximum number of errors this code can correct?
d) Give the generator polynomial for this code.
e) Assume that a received polynomial is:
$r(x) = x^{21} + x^{13} + x^{12} + x^{11} + x^{9} + x^{8} + 1$

- Find the location of a single error in this received codeword
- Find the message corresponding to this codeword

For binary code, minimum weight = $n - k = 18$ = degree of $g(x)$

c) Minimum weight code $\Rightarrow \{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}, \alpha^{64}, \alpha^{128}, \alpha^{256}\} \leftrightarrow x^9 + x^4 + 1$

+8 $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{96}, \alpha^{192}, \alpha^{384}, \alpha^{257}\} \leftrightarrow x^9 + x^6 + x^4 + x^3 + 1$

$\Rightarrow g(x)$ is product of these (Least weight)

$\Rightarrow$ Minimum distance: $\{\alpha, \alpha^2, \alpha^3, \alpha^4\} \Rightarrow$ dmin = 5 (Special case)

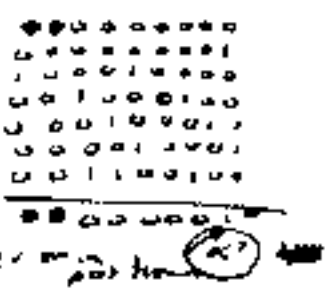
+8 $\Rightarrow t = \frac{d_{min}-1}{2} = 2$

d) $g(x) = (x^4 + x^3 + 1)(x^5 + x^4 + x^3 + x^2 + 1)$

$= x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$

+9 e) Single error correcting formulas: $A_1 = S_1$, $A_2 = \frac{S_3 + S_1^3}{S_1}$

$S_1 = \alpha^{21} + \alpha^{13} + \alpha^{12} + \alpha^{11} + \alpha^9 + \alpha^8 + 1$



$e(x) = x^7$

$\Rightarrow c(x) = x^{21} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^7 + 1$

$= m(x)(x^{18} + x^{15} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^3 + 1)$

$\Rightarrow m(x) = x^3 + 1$