ECE 405/511 Assignment 5 2026 Solutions

1. binary BCH code length 21 design distance 8

$n \mid 2^m - 1 \rightarrow 21 \mid 63 \quad m = 6$

let α be a primitive element of GF(64)

then $\alpha^{63} = 1$

and $\beta = \alpha^3$ is an element of order 21

- require 7 consecutive powers of β

$\beta^0, \beta^1, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6$

$\beta_0 = 1 \Rightarrow$ minimal polynomial $x+1$

$\beta^1 = \alpha^3, \beta^2 = \alpha^6, \beta^4 = \alpha^{12} \quad (\beta^8 = \alpha^{24}, \beta^{16} = \alpha^{48}, \beta^{32} = \beta^{11} = \alpha^{33})$

minimal polynomial $x^6 + x^4 + x^2 + x + 1$

$\beta^3 = \alpha^9, \beta^6 = \alpha^{18} \quad (\beta^{12} = \alpha^{36})$

minimal polynomial $x^3 + x^2 + 1$

$\beta^5 = \alpha^{15} \quad (\beta^{10} = \alpha^{30}, \beta^{20} = \alpha^{60}, \beta^{40} = \beta^{19} = \alpha^{57}, \beta^{38} = \beta^{17} = \alpha^{51}, \beta^{34} = \beta^{13} = \alpha^{39})$

$\beta^5 = \alpha^{15} \rightarrow$ minimal polynomial $x^6+x^5+x^4+x^2+1$

$$g(x) = (x+1)(x^6+x^4+x^2+x+1)(x^3+x^2+1)(x^6+x^5+x^4+x^2+1)$$

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

$$= x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{10}+x^8+x^5+x^4+1$$

(21,5) BCH code, design distance 8 (actual $d_{min}=10$)

rate $= \frac{5}{21} = .238$

- the best known linear code (BKLC) is (21,5,10) so the BCH code is optimal (but the BCH decoding algorithm cannot decode beyond the design distance)
- if one considers the design distance, the BKLC is (21,9,8) which has rate .429

2 (a) $r = (0f000f00f000000)$

set $f = 0$ $\quad r_0 = (000000000000000)$ $\quad r_0(x) = 0$

$S_1 = S_2 = S_3 = S_4 = 0 \quad e_0(x) = 0$

$\therefore \; c_0(x) = r_0(x) + e_0(x) = 0$

set $f = 1$ $\quad r_1 = (010001001000000)$

$r_1(x) = x + x^5 + x^8$

$S_1 = r_1(\alpha) = \alpha + \alpha^5 + \alpha^8 = 1$

$S_2 = S_4 = S_1 = 1$

$S_3 = r_1(\alpha^3) = \alpha^3 + \alpha^{15} + \alpha^{24} = \alpha^3 + 1 + \alpha^9 = \alpha^4$

$\Lambda_1 = S_1 = 1$

$$\Lambda_2 = \frac{S_3 + S_1^3}{S_1} = \frac{\alpha^4 + 1}{1} = \alpha$$

$\Lambda_1(x) = 1 + x + \alpha x^2$ $\quad$ roots are α^6, α^8

$\Lambda_1(x) = (1 + \alpha^7 x)(1 + \alpha^9 x)$

$\therefore\ e(x) = x^7 + x^9$

$c_1(x) = r_1(x) + e(x) = x + x^5 + x^7 + x^8 + x^9$

this differs from r in 2 places

$c_0(x)$ differs from r in 0 places

$\therefore\ c(x) = c_0(x) = 0$

2(b) $r = (f0f110110010100)$

set $f=0$ $r_0 = (000110110010100)$

$r_0(x) = x^3 + x^4 + x^6 + x^7 + x^{10} + x^{12}$

$S_1 = r_0(\alpha) = \alpha^2$ $S_2 = \alpha^4$

$S_3 = r_0(\alpha^3) = \alpha^6$ $S_4 = \alpha^8$

$\Lambda_1 = S_1 = \alpha^2$

$\Lambda_2 = \dfrac{S_3 + S_1^3}{S_1} = \dfrac{\alpha^6 + \alpha^6}{\alpha^2}$

$\Lambda(x) = 1 + \alpha^2 x$

$e_0(x) = \alpha^2 x$

$c_0(x) = x^2 + x^3 + x^4 + x^6 + x^7 + x^{10} + x^{12}$

set $f=1$ $r_1 = (101110110010100)$

$r_1(x) = 1 + x^2 + x^3 + x^4 + x^6 + x^7 + x^{10} + x^{12}$

$S_1 = r_1(\alpha) = 1 \qquad S_3 = r_1(\alpha^3) = 1$

$\Lambda_1 = 1 \quad \Lambda_2 = 0$

$\Lambda(x) = 1 + x$

$e_1(x) = 1$

$C_1(x) = x^2 + x^3 + x^4 + x^6 + x^7 + x^{10} + x^{12} = C_0(x)$

thus $C(x) = C_0(x) = C_1(x)$

3. triple error correcting narrow-sense binary BCH code of length 31

(a) $r(x) = 1 + x^2$

$S_1 = r(\alpha) = 1 + \alpha^2 = \alpha^5$

$S_2 = r(\alpha^2) = 1 + \alpha^4 = \alpha^{10}$

$S_3 = r(\alpha^3) = 1 + \alpha^6 = \alpha^{27}$

$S_4 = r(\alpha^4) = 1 + \alpha^8 = \alpha^{20}$

$S_5 = r(\alpha^5) = 1 + \alpha^{10} = \alpha^4$

$S_6 = r(\alpha^6) = 1 + \alpha^{12} = \alpha^{23}$

$$A = \begin{bmatrix} 1 & 0 & 0 \\ \alpha^{10} & \alpha^5 & 1 \\ \alpha^{20} & \alpha^{27} & \alpha^{10} \end{bmatrix} \qquad |A| = \alpha^{15} + \alpha^{27} = \alpha^7 \neq 0$$

$\Lambda_1 = S_1 = \alpha^5$

$$\Lambda_2 = \frac{S_1^2 S_3 + S_5}{S_1^3 + S_3} = \frac{\alpha^{10} \cdot \alpha^{27} + \alpha^4}{\alpha^{15} + \alpha^{27}} = \frac{\alpha^6 + \alpha^4}{\alpha^7} = \frac{\alpha^9}{\alpha^7} = \alpha^2$$

$\Lambda_3 = (S_1^3 + S_3) + S_1 \Lambda_2 = \alpha^7 + \alpha^7 = 0$

$$\Lambda(x) = 1 + \Lambda_1 x + \Lambda_2 x^2 + \Lambda_3 x^3$$

$$= 1 + \alpha^5 x + \alpha^2 x^2$$

let $x = 1$ $\quad \Lambda(1) = 1 + \alpha^5 + \alpha^2 = 0$

$$\begin{array}{r} 1 + \alpha^2 x \\ 1+x \enclose{longdiv}{1 + \alpha^5 x + \alpha^2 x^2} \\ \underline{1 + x \qquad\qquad} \\ \alpha^2 x + \alpha^2 x^2 \\ \underline{\alpha^2 x + \alpha^2 x^2} \\ 0 \end{array}$$

$$\Lambda(x) = (1+x)(1+\alpha^2 x)$$

$$e(x) = 1 + x^2$$

$$c(x) = r(x) + e(x) = 0$$

$c = (0000000000000000000000000000000)$

(b) $S_1 = \alpha^{24}$
$S_2 = \alpha^{17}$
$S_3 = \alpha^{18}$
$S_4 = \alpha^{3}$
$S_5 = \alpha^{26}$
$S_6 = \alpha^{5}$

$$A = \begin{bmatrix} 1 & 0 & 0 \\ \alpha^{17} & \alpha^{24} & 1 \\ \alpha^{3} & \alpha^{18} & \alpha^{17} \end{bmatrix} \qquad |A| = \alpha^{24}\cdot\alpha^{17} + \alpha^{18} = \alpha^{10} + \alpha^{18} = \alpha^{30} \neq 0$$

$$\Lambda_1 = S_1 = \alpha^{24}$$

$$\Lambda_2 = \frac{S_1^2 S_3 + S_5}{S_1^3 + S_3} = \frac{\alpha^{17}\cdot\alpha^{18} + \alpha^{26}}{\alpha^{10} + \alpha^{18}} = \frac{\alpha^{4} + \alpha^{26}}{\alpha^{30}} = \frac{\alpha^{11}}{\alpha^{30}} = \alpha^{12}$$

$$\Lambda_3 = (S_1^3 + S_3) + S_1\Lambda_2 = \alpha^{30} + \alpha^{24}\cdot\alpha^{12} = \alpha^{26}$$

$$\Lambda(x) = 1 + \alpha^{24}x + \alpha^{12}x^2 + \alpha^{26}x^3$$

try α^{12} $\quad 1 + \alpha^{36} + \alpha^{36} + \alpha^{62} = 0$

$$
\begin{array}{r l}
 & 1+\alpha^{21}x+\alpha^{7}x^{2} \\
\cline{2-2}
1+\alpha^{19}x \; \big) & 1+\alpha^{24}x+\alpha^{12}x^{2}+\alpha^{26}x^{3} \\
 & 1+\alpha^{19}x \\
\cline{2-2}
 & \alpha^{21}x+\alpha^{12}x^{2} \\
 & \alpha^{21}x+\alpha^{9}x^{2} \\
\cline{2-2}
 & \alpha^{7}x^{2}+\alpha^{26}x^{3} \\
 & \alpha^{7}x^{2}+\alpha^{26}x^{3} \\
\cline{2-2}
 & 0
\end{array}
$$

try α^{27} $\quad 1+\alpha^{48}+\alpha^{61} = 1+\alpha^{17}+\alpha^{30} \doteq 0$

$$
\begin{array}{r l}
 & 1+\alpha^{3}x \\
\cline{2-2}
1+\alpha^{4}x \; \big) & 1+\alpha^{21}x+\alpha^{7}x^{2} \\
 & 1+\alpha^{4}x \\
\cline{2-2}
 & \alpha^{3}x+\alpha^{7}x^{2} \\
 & \alpha^{3}x+\alpha^{7}x^{2} \\
\cline{2-2}
 & 0
\end{array}
$$

$$\Lambda(x) = (1+\alpha^{19}x)(1+\alpha^{4}x)(1+\alpha^{3}x)$$

the error locators are $\alpha^{3}, \alpha^{4}, \alpha^{19}$

$e(x) = x^{3}+x^{4}+x^{19}$

$$c(x) = r(x) + e(x)$$

$$= 1 + x + x^7 + x^9 + x^{10} + x^{12} + x^{13} + x^{17} + x^{18} + x^3 + x^4 + x^{19}$$

$$= 1 + x + x^3 + x^4 + x^7 + x^9 + x^{10} + x^{12} + x^{13} + x^{17} + x^{18} + x^{19}$$

$$c = (1101100101101100011100000000000)$$

4. narrow-sense RS code of length 15 and design distance 3

a) let α be a primitive element of $GF(16)$

narrow-sense $b=1$ $\delta=3$

roots of $g(x)$: α, α^2

$$g(x) = (x-\alpha)(x-\alpha^2)$$

$$= x^2 + (\alpha+\alpha^2)x + \alpha^3$$

$$= x^2 + \alpha^5 x + \alpha^3$$

b) $n=15$ and $n-k=2$ so $k=13$

$$\text{rate} = \frac{k}{n} = \frac{13}{15} = .867$$

number of code words is

$$16^{13} = 2^{52} = 4.50 \times 10^{15}$$

c) generator matrix

$$G = \begin{bmatrix} \alpha^3 & \alpha^5 & 1 & & & & \\ & \alpha^3 & \alpha^5 & 1 & & 0 & \\ & & \alpha^3 & \alpha^5 & 1 & & \\ & & & \ddots & & & \\ & 0 & & & \ddots & & \\ & & & & \alpha^3 & \alpha^5 & 1 \end{bmatrix} \quad \text{13 rows}$$

15 columns

parity check matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{13} \end{bmatrix}$$

5. double error correcting RS code of length 31

narrow-sense : $b=1$

$t=2 \Rightarrow 2t=4$ consecutive powers needed

let α be a primitive element of $GF(32)$

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

$$= (x^2+\alpha^{19}x+\alpha^3)(x+\alpha^3)(x+\alpha^4)$$

$$= (x^3+\alpha^{12}x^2+\alpha^{14}x+\alpha^6)(x+\alpha^4)$$

$$= x^4+\alpha^{24}x^3+\alpha^{19}x^2+\alpha^{29}x+\alpha^{10}$$

6. $r(x) = \alpha^5 x + x^2 + x^3 + \alpha^5 x^4 + \alpha^2 x^5$

$S_1 = r(\alpha) = \alpha^6 + \alpha^2 + \alpha^3 + \alpha^2 + 1 = \alpha^5$

$S_2 = r(\alpha^2) = 1 + \alpha^4 + \alpha^6 + \alpha^6 + \alpha^5 = 0$

$S_3 = r(\alpha^3) = \alpha + \alpha^6 + \alpha^2 + \alpha^3 + \alpha^3 = \alpha^3$

$S_4 = r(\alpha^4) = \alpha^2 + \alpha + \alpha^5 + 1 + \alpha = \alpha$

k	S_k	$\Lambda^{(k)}(x)$	$\Delta^{(k)}$	L	$T(x)$
0	—	1	—	0	x
1	α^5	$1+\alpha^5 x$	α^5	1	$\alpha^2 x$
2	0	1	α^3	1	$\alpha^2 x^2$
3	α^3	$1+\alpha^5 x^2$	α^3	2	$\alpha^4 x$
4	α	$1+\alpha^5 x+\alpha^5 x^2$	α		

$$\Lambda(x) = 1 + \alpha^5 x + \alpha^5 x^2$$

$$= (1+\alpha^3 x)(1+\alpha^2 x)$$

$$X_1 = \alpha^2 \quad X_2 = \alpha^3$$

$$\Omega(x) = \Lambda(x)[1+S(x)] \bmod x^5$$

$$= (1+\alpha^5 x+\alpha^5 x^2)(1+\alpha^5 x+\alpha^3 x^3+\alpha x^4) \bmod x^5$$

$$= 1+\alpha^2 x^2$$

$$\Lambda'(x) = \alpha^5$$

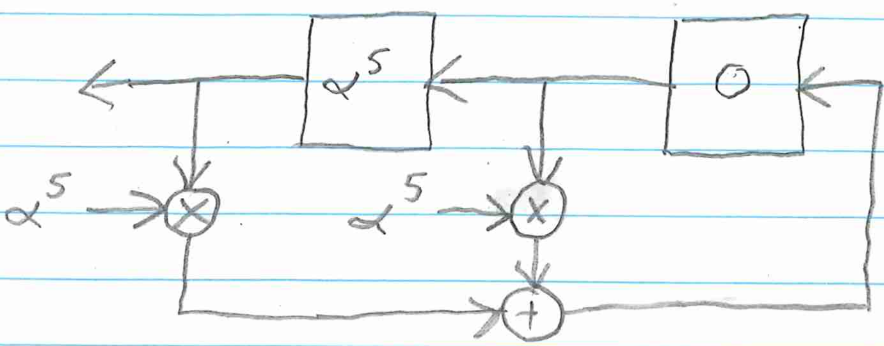
$$e_2 = \frac{-\alpha^2\,\Omega(\alpha^5)}{\alpha^5} = \alpha^4(1+\alpha^5) = \alpha$$

$$e_3 = \frac{-\alpha^3\,\Omega(\alpha^4)}{\alpha^5} = \alpha^5(1+\alpha^3) = \alpha^6$$

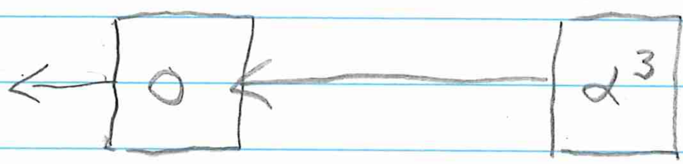
$$e(x) = \alpha x^2+\alpha^6 x^3$$

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

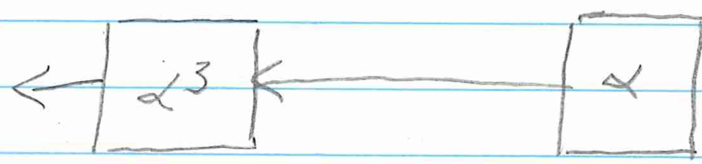
$$= \alpha^2 x\, g(x)$$



$$\alpha^5 \cdot \alpha^5 = \alpha^3$$



$$\alpha^3 \cdot \alpha^5 = \alpha$$



Thus the output is

$$\alpha^5, 0, \alpha^3, \alpha = S_1, S_2, S_3, S_4$$

7. Construct an encoder for the convolutional code represented by the following transfer function matrix

$$G(D) = \begin{bmatrix} 1+D+D^2 & 1+D+D^3 & 1+D^2+D^3 \\ 1+D^3 & 1+D^2 & 1+D+D^3 \end{bmatrix}$$

rate 2/3 code $K = 4$ (3,2,4) code