Problem 7.2

Double Error Correcting ($t = 2$):

$$g(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^3)(X-\alpha^4)$$
$$= X^4 + \alpha^{24}X^3 + \alpha^{19}X^2 + \alpha^{29}X + \alpha^{10}$$

Triple Error Correcting ($t=3$):

$$g(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^3)(X-\alpha^4)(X-\alpha^5)(X-\alpha^6)$$
$$= X^6 + \alpha^{10}X^5 + \alpha^9X^4 + \alpha^{24}X^3 + \alpha^{16}X^2 + \alpha^{24}X + \alpha^{21}.$$

Problem 7.4

$S_1 = r(\alpha) = \alpha^{13}$, $S_2 = r(\alpha^2) = \alpha^{14}$, $S_3 = r(\alpha^3) = \alpha^9$,

$S_4 = r(\alpha^4) = \alpha^7$, $S_5 = r(\alpha^5) = \alpha^8$, $S_6 = r(\alpha^6) = \alpha^3$.

μ	$\sigma^{(\mu)}(X)$	d_μ	l_μ	
-1	1	1	0	
0	1	α^{13}	0	
1	$1+\alpha^{13}X$	α^{10}	1	(took $\rho=-1$)
2	$1+\alpha X$	α^7	1	(took $\rho=0$)
3	$1+\alpha X+\alpha^9X^2$	α^{14}	2	(took $\rho=0$)
4	$1+\alpha^{14}X+\alpha^{12}X^2$	α^8	2	(took $\rho=2$)
5	$1+\alpha^{14}X+\alpha^{13}X^2+\alpha^2X^3$	α^7	3	(took $\rho=2$)
6	$1+\alpha^9X^3$	$-$	$-$	(took $\rho=4$)

$\sigma(X) = 1+\alpha^9X^3$

$$\begin{aligned} Z_0(X) &= S_1 + (S_2+\sigma_1S_1)X + (S_3+\sigma_1S_2+\sigma_2S_1)X^2 \\ &= \alpha^{13} + (\alpha^{14}+0\cdot\alpha^{13})X + (\alpha^9+0\cdot\alpha^{14}+0\cdot\alpha^{13})X^2 \\ &= \alpha^{13}+\alpha^{14}X+\alpha^9X^2 \end{aligned}$$

$\sigma(X)$ has roots α^2, α^7, and α^{12}. Hence, $\beta_1 = \alpha^{-2} = \alpha^{13}$, $\beta_2 = \alpha^{-7} = \alpha^8$, and $\beta_3 = \alpha^{-12} = \alpha^3$.

$$\delta_k = -\frac{Z_0(\beta_k^{-1})}{\sigma'(\beta_k^{-1})} = \frac{\alpha^{13}+\alpha^{14}\beta_k^{-1}+\alpha^9\beta_k^{-2}}{\alpha^9\beta_k^{-2}}$$

Hence, $\delta_1 = \alpha^3$, $\delta_2 = \alpha^9$, and $\delta_3 = \alpha^4$.

$e(X) = \alpha^4X^3+\alpha^9X^8+\alpha^3X^{13}$

$v(X) = r(X) - e(X) = 0$.

Problem 7.5

$S_1 = r(\alpha) = \alpha^{13}$, $S_2 = r(\alpha^2) = \alpha^{14}$, $S_3 = r(\alpha^3) = \alpha^9$,

$S_4 = r(\alpha^4) = \alpha^7$, $S_5 = r(\alpha^5) = \alpha^8$, $S_6 = r(\alpha^6) = \alpha^3$.

$S(X) = S_1 + S_2X + S_3X^2 + S_4X^3 + S_5X^4 + S_6X^5 = \alpha^{13} + \alpha^{14}X + \alpha^9X^2 + \alpha^7X^3 + \alpha^8X^4 + \alpha^3X^5$.

i	$Z_0^{(i)}(X)$	$q_i(X)$	$\sigma_i(X)$
-1	X^6	$-$	0
0	$S(X)$	$-$	1
1	$\alpha^2X^4 + \alpha^5X^3 + \alpha^8X + 1$	$\alpha^{12}X + \alpha^2$	$\alpha^{12}X + \alpha^2$
2	$\alpha^{12}X^3 + \alpha^{13}X + \alpha$	$\alpha X + \alpha^{12}$	$\alpha^{13}X^2 + \alpha X + \alpha^3$
3	$\alpha^3X^2 + \alpha^8X + \alpha^7$	$\alpha^5X + \alpha^8$	$\alpha^3X^3 + \alpha^9$

$\sigma(X) = \alpha^3X^3 + \alpha^9$. $Z_0(X) = \alpha^3X^2 + \alpha^8X + \alpha^7$

(Notice that $\sigma(X)$ and $Z_0(X)$ here are the same as $\sigma(X)$ and $Z_0(X)$ in the Berlekamp-Massey algorithm except that they are multiplied by α^9.)

$\sigma(X)$ has roots α^2, α^7, and α^{12}. Hence, $\beta_1 = \alpha^{-2} = \alpha^{13}$, $\beta_2 = \alpha^{-7} = \alpha^8$, and $\beta_3 = \alpha^{-12} = \alpha^3$.

$$\delta_k = -\frac{Z_0(\beta_k^{-1})}{\sigma'(\beta_k^{-1})} = \frac{\alpha^3\beta_k^{-2} + \alpha^8\beta_k^{-1} + \alpha^7}{\alpha^3\beta_k^{-2}}$$

Hence, $\delta_1 = \alpha^3$, $\delta_2 = \alpha^9$, and $\delta_3 = \alpha^4$.

$e(X) = \alpha^4X^3 + \alpha^9X^8 + \alpha^3X^{13}$

$v(X) = r(X) - e(X) = 0$.

Problem 7.6

$S_1 = r(\alpha) = \alpha^{27}$, $\quad S_2 = r(\alpha^2) = \alpha$, $\quad S_3 = r(\alpha^3) = \alpha^{28}$,

$S_4 = r(\alpha^4) = \alpha^{29}$, $\quad S_5 = r(\alpha^5) = \alpha^{15}$, $\quad S_6 = r(\alpha^6) = \alpha^8$

$$S(X) = \alpha^8 X^5 + \alpha^{15} X^4 + \alpha^{29} X^3 + \alpha^{28} X^2 + \alpha X + \alpha^{27}$$

i	$Z_0^{(i)}(X)$	$q_i(X)$	$\sigma_i(X)$
-1	X^6	$-$	0
0	$S(X)$	$-$	1
1	$\alpha^5 X^4 + \alpha^9 X^3 + \alpha^{22} X^2 + \alpha^{11} X + \alpha^{26}$	$\alpha^{23} X + \alpha^{30}$	$\alpha^{23} X + \alpha^{30}$
2	$\alpha^8 X^3 + \alpha^4 X + \alpha^6$	$\alpha^3 X + \alpha^5$	$\alpha^{26} X^2 + \alpha^{30} X + \alpha^{10}$
3	$\alpha^{26} X^2 + \alpha^6 X + \alpha^{18}$	$\alpha^{28} X + \alpha$	$\alpha^{23} X^3 + \alpha^9 X + \alpha^{22}$

$\sigma(X) = \alpha^{23} X^3 + \alpha^9 X + \alpha^{22}$, $\quad Z_0(X) = \alpha^{26} X^2 + \alpha^6 X + \alpha^{18}$

$\sigma(X)$ has roots α^0, α^{11}, and α^{19}.

Hence, $\beta_1 = \alpha^{-0} = \alpha^0$, $\beta_2 = \alpha^{-11} = \alpha^{20}$, and $\beta_3 = \alpha^{-19} = \alpha^{12}$.

$$\delta_k = -\frac{Z_0(\beta_k^{-1})}{\sigma'(\beta_k^{-1})} = \frac{\alpha^{26}\beta_k^{-2} + \alpha^6 \beta_k^{-1} + \alpha^{18}}{\alpha^{23}\beta_k^{-2} + \alpha^9}$$

$\delta_1 = \alpha^2$, $\quad \delta_2 = \alpha^7$, and $\delta_3 = \alpha^{21}$

$$e(X) = \alpha^2 + \alpha^{21} X^{12} + \alpha^7 X^{20}$$

$$v(X) = r(X) - e(X) = 0.$$