Problem 6.1

a) From Table 2.9:

the minimal polynomial of $\beta = \alpha^7$ is $X^4 + X^3 + 1$,

~ ~ ~ ~ $\beta^2 = \alpha^{14}$ ~ ~

~ ~ ~ ~ $\beta^3 = \alpha^6$ ~ $X^4 + X^3 + X^2 + X + 1$

~ ~ ~ ~ $\beta^4 = \alpha^{13}$ ~ $X^4 + X^3 + 1$

$$g_0(X) = \mathrm{LCM}\{X^4 + X^3 + 1,\ X^4 + X^3 + X^2 + X + 1\}$$

$$= (X^4 + X^3 + 1)(X^4 + X^3 + X^2 + X + 1)$$

$$= X^8 + X^4 + X^2 + X + 1$$

b)
$$f(X) = \frac{X^{15} + 1}{g(X)} = \frac{(X+1)(X^4+X+1)(X^4+X^3+X^2+X+1)(X^2+X+1)(X^4+X^3+1)}{(X^4+X^3+1)(X^4+X^3+X^2+X+1)}$$

$$= (X+1)(X^4+X+1)(X^2+X+1) = X^7 + X^3 + X + 1$$

$$h(X) = X^7 f(X^{-1}) = X^7 + X^6 + X^4 + 1$$

From (4.6) in Lecture notes 4 (which has a typo: G should be H)

$$H = \begin{bmatrix}
1&0&0&0&1&0&1&1&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&1&1&0&0&0&0&0&0\\
0&0&1&0&0&0&1&0&1&1&0&0&0&0&0\\
0&0&0&1&0&0&0&1&0&1&1&0&0&0&0\\
0&0&0&0&1&0&0&0&1&0&1&1&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&1&1&0&0\\
0&0&0&0&0&0&1&0&0&0&1&0&1&1&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&1&1
\end{bmatrix}$$

We can also obtain a parity check matrix as in Example 6.2 in textbook by replacing elements in the matrix

$$\begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 & \beta^9 & \beta^{10} & \beta^{11} & \beta^{12} & \beta^{13} & \beta^{14} \\ 1 & \beta^3 & \beta^6 & \beta^9 & \beta^{12} & \beta^{15} & \beta^{18} & \beta^{21} & \beta^{24} & \beta^{27} & \beta^{30} & \beta^{33} & \beta^{36} & \beta^{39} & \beta^{42} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^7 & \alpha^{14} & \alpha^6 & \alpha^{13} & \alpha^5 & \alpha^{12} & \alpha^4 & \alpha^{11} & \alpha^3 & \alpha^{10} & \alpha^2 & \alpha^9 & \alpha & \alpha^8 \\ 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 & 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 & 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \alpha^9 \end{bmatrix}$$

by its binary vector representation as a column vector of length 4. This gives the parity check matrix

$$H = \left[\begin{array}{ccccccccccccccc} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

(Actually, by elementary row operations, one can obtain the first parity-check matrix from this matrix)

c) $g_0(x) = x^8 g(x^{-1})$.

Problem 6.2

For each $i = 1, \ldots, 30$, we determine the degree of $\phi_i(X)$, the minimal polynomial of α^i. This degree is the number of conjugates of α^i.

conjugates	degree of minimal polynomial
$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}$	5
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}$	5
$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18}$	5
$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}$	5
$\alpha^{11}, \alpha^{22}, \alpha^{13}, \alpha^{26}, \alpha^{21}$	5
$\alpha^{15}, \alpha^{30}, \alpha^{29}, \alpha^{27}, \alpha^{23}$	5

t	$g(X) = \text{LCM}\{\phi_1(X), \phi_3(X), \ldots, \phi_{2t-1}(X)\}$	degree of $g(X)$	
1	$\phi_1(X)$	5	
2	$\text{LCM}\{\phi_1(X), \phi_3(X)\}$	10	
3	$\text{LCM}\{\phi_1(X), \phi_3(X), \phi_5(X)\}$	15	
4	$\text{LCM}\{\phi_1(X), \phi_3(X), \phi_5(X), \phi_7(X)\}$	20	
5	$\text{LCM}\{\phi_1(X), \phi_3(X), \phi_5(X), \phi_7(X), \phi_9(X)\}$	20	since $\phi_9(X) = \phi_5(X)$
6	$\text{LCM}\{\phi_1(X), \phi_3(X), \ldots, \phi_{11}(X)\}$	25	
7	$\text{LCM}\{\phi_1(X), \phi_3(X), \ldots, \phi_{13}(X)\}$	25	Since $\phi_{13}(X) = \phi_{11}(X)$
8	$\text{LCM}\{\phi_1(X), \phi_3(X), \ldots, \phi_{15}(X)\}$	30	
9	$\text{LCM}\{\phi_1(X), \phi_3(X), \ldots, \phi_{17}(X)\}$	30	Since $\phi_{17}(X) = \phi_3(X)$
⋮	⋮	⋮	⋮
15	$\text{LCM}\{\phi_1(X), \phi_3(X), \ldots, \phi_{29}(X)\}$	30	

Problem 6.3

$r_1(X) = X^7 + X^{30}$

Syndrome Computations:

$$S_1 = r_1(\alpha) = \alpha^7 + \alpha^{30} = \alpha^{19}$$

$$S_2 = S_1^2 = \alpha^7$$

$$S_3 = r_1(\alpha^3) = \alpha^{21} + \alpha^{90} = \alpha^{12}$$

$$S_4 = S_2^2 = \alpha^{14}$$

Berlekamp-Massey Algorithm:

μ	$\sigma^{(\mu)}(X)$	d_μ	l_μ	
-1	1	1	0	
0	1	α^{19}	0	
1	$1+\alpha^{19}X$	0	1	$(\rho = -1)$
2	$1+\alpha^{19}X$	α^{25}	1	
3	$1+\alpha^{19}X+\alpha^6X^2$	0	2	$(\rho = 0)$
4	$1+\alpha^{19}X+\alpha^6X^2$	$-$	$-$	

Error locator polynomial: $\sigma(X) = X^6X^2 + \alpha^{19}X + 1$.

By substituting $X = \alpha^i$, $i = 0, 1, \ldots, 30$, the roots of $\sigma(X)$ are found to be α and α^{24}.

Error location numbers: $\alpha^{-1} = \alpha^{30}$ and $\alpha^{-24} = \alpha^7$

$e_1(X) = X^7 + X^{30}$

$v_1(X) = r_1(X) + e_1(X) = 0$

$r_2(X) = 1 + X^{17} + X^{28}$

Syndrome Computations:

$$S_1 = r_2(\alpha) = 1 + \alpha^{17} + \alpha^{28} = \alpha^2$$
$$S_2 = S_1^2 = \alpha^4$$
$$S_3 = r_2(\alpha^3) = 1 + \alpha^{51} + \alpha^{84} = \alpha^{21}$$
$$S_4 = S_2^2 = \alpha^8$$

Berlekamp-Massey Algorithm:

μ	$\sigma^{(\mu)}(X)$	d_μ	l_μ	
-1	1	1	0	
0	1	α^2	0	
1	$1 + \alpha^2 X$	0	1	$(\rho = -1)$
2	$1 + \alpha^2 X$	α^{30}	1	
3	$1 + \alpha^2 X + \alpha^{28} X^2$	0	2	$(\rho = 0)$
4	$1 + \alpha^2 X + \alpha^{28} X^2$	—	—	

Error locator polynomial: $\sigma(X) = \alpha^{28} X^2 + \alpha^2 X + 1$.

By substituting $X = \alpha^i$, $i = 0, 1, \ldots, 30$, no roots for $\sigma(X)$ are found. Hence, the decoder fails. The reason is that there are more than 2 errors while the decoder can correct only 2 errors.

Problem 6.4

Let $n = l(2t+1)$. We will show that

$$v(X) = \frac{X^n + 1}{X^l + 1} = 1 + X^l + X^{2l} + \cdots + X^{2tl}$$

is a code polynomial. Since α is a primitive element in $GF(2^m)$, where $n = 2^m - 1$, it follows that

$\alpha^{in} + 1 = 0$ and $\alpha^{il} + 1 \neq 0$ for $i = 1, 2, \ldots, 2t$.

Hence $v(\alpha^i) = 0$ for $i = 1, 2, \ldots, 2t$. This proves that $v(X)$ is a code polynomial. It represents a codeword of weight $2t+1$. Hence, $d_{min} \leq 2t+1$.

Since $d_{min} \geq 2t+1$ for any t-error correcting BCH code, we have $d_{min} = 2t+1$.