Problem 5.1

a) First we find $f(x) = \dfrac{x^n + 1}{g(x)} = \dfrac{x^{15}+1}{x^4+x+1}$

$$
\begin{array}{r|l}
 & x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1 \\
\hline
x^4 + x + 1 & x^{15} + 1 \\
 & x^{15} + x^{12} + x^{11} \\
\cline{2-2}
 & x^{12} + x^{11} + 1 \\
 & x^{12} + x^9 + x^8 \\
\cline{2-2}
 & x^{11} + x^9 + x^8 + 1 \\
 & x^{11} + x^8 + x^7 \\
\cline{2-2}
 & x^9 + x^7 + 1 \\
 & x^9 + x^6 + x^5 \\
\cline{2-2}
 & x^7 + x^6 + x^5 + 1 \\
 & x^7 + x^4 + x^3 \\
\cline{2-2}
 & x^6 + x^5 + x^4 + x^3 + 1 \\
 & x^6 + x^3 + x^2 \\
\cline{2-2}
 & x^5 + x^4 + x^2 + 1 \\
 & x^5 + x^2 + x \\
\cline{2-2}
 & x^4 + x + 1 \\
 & x^4 + x + 1 \\
\cline{2-2}
 & 0
\end{array}
$$

$f(x) = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$

$h(x) = x^k f\left(\frac{1}{x}\right) = x^{11} f\left(\frac{1}{x}\right)$

$= x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1$

b) The generator polynomial for the dual code is

$h(x) = x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1$

c) A generator matrix which is <u>not</u> in systematic form is given by (4.3) of the lecture notes as:

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

By elementary row operations, we can get $G_{sys} = (P\ I)$ in the form

$$G_{sys} = \begin{bmatrix}
1&1&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&1&0&0&0&0&0&0&0&0\\
1&1&0&1&0&0&0&1&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&1&0&0&0&0&0&0\\
0&1&0&1&0&0&0&0&0&1&0&0&0&0&0\\
1&1&1&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&1&1&0&0&0&0&0&0&0&1&0&0&0\\
1&1&1&1&0&0&0&0&0&0&0&0&1&0&0\\
1&0&1&1&0&0&0&0&0&0&0&0&0&1&0\\
1&0&0&1&0&0&0&0&0&0&0&0&0&0&1
\end{bmatrix}$$

Then a parity-check matrix for the code has the form $H_{sys} = (I\ P)$

$$H_{sys} = \begin{bmatrix}
1&0&0&0&1&0&0&1&1&0&1&0&1&1&1\\
0&1&0&0&1&1&0&1&0&1&1&1&1&0&0\\
0&0&1&0&0&1&1&0&1&0&1&1&1&1&0\\
0&0&0&1&0&0&1&1&0&1&0&1&1&1&1
\end{bmatrix}$$

Problem 5.16

From Table ~~2.~~ 9, or by direct factorization:

$$x^{15}+1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

Notice that a polynomial $g(x)$ generates a cyclic code of length 15 if and only if it divides $x^{15}+1$, i.e.,

$$g(x)=(x+1)^{e_1}(x^2+x+1)^{e_2}(x^4+x+1)^{e_3}(x^4+x^3+1)^{e_4}(x^4+x^3+x^2+x+1)^{e_5}$$

where e_1, e_2, e_3, e_4, e_5 are 0 or 1. The dimension of the code is

$k=15-\deg g(x)=15-(e_1+2e_2+4e_3+4e_4+4e_5)$. We consider all possibilities for e_1, e_2, e_3, e_4, e_5.

e_1	e_2	e_3	e_4	e_5	k
0	0	0	0	0	15
1	0	0	0	0	14
0	1	0	0	0	13
1	1	0	0	0	12
0	0	1	0	0	11
1	0	1	0	0	10
0	1	1	0	0	9
1	1	1	0	0	8

e_1	e_2	e_3	e_4	e_5	k
0	0	0	1	0	11
1	0	0	1	0	10
0	1	0	1	0	9
1	1	0	1	0	8
0	0	1	1	0	7
1	0	1	1	0	6
0	1	1	1	0	5
1	1	1	1	0	4

e_1	e_2	e_3	e_4	e_5	k
0	0	0	0	1	11
1	0	0	0	1	10
0	1	0	0	1	9
1	1	0	0	1	8
0	0	1	0	1	7
1	0	1	0	1	6
0	1	1	0	1	5
1	1	1	0	1	4

e_1	e_2	e_3	e_4	e_5	k
0	0	0	1	1	7
1	0	0	1	1	6
0	1	0	1	1	5
1	1	0	1	1	4
0	0	1	1	1	3
1	0	1	1	1	2
0	1	1	1	1	1
1	1	1	1	1	0

From the above, we can form the table below

dimension	number of cyclic codes of length 15
0	1
1	1
2	1
3	1
4	3
5	3
6	3
7	3
8	3
9	3
10	3
11	3
12	1
13	1
14	1
15	1

Problem 5.x The $(15, 7)$ code generated by $g(x) = 1+X+X^2+X^4+X^8$ is double error-correcting. The following is a table of syndromes for the error patterns $0, 1, 1+X, 1+X^2, \ldots, 1+X^{14}$.

error pattern	syndrome
0	0
1	1
$1+X$	$1+X$
$1+X^2$	$1+X^2$
$1+X^3$	$1+X^3$
$1+X^4$	$1+X^4$
$1+X^5$	$1+X^5$
$1+X^6$	$1+X^6$
$1+X^7$	$1+X^7$
$1+X^8$	$X+X^2+X^4$
$1+X^9$	$1+X+X^2+X^3+X^5$
$1+X^{10}$	$1+X^2+X^3+X^4+X^6$
$1+X^{11}$	$1+X^3+X^4+X^5+X^7$
$1+X^{12}$	$X+X^2+X^5+X^6$
$1+X^{13}$	$1+X+X^2+X^3+X^6+X^7$
$1+X^{14}$	$X+X^3+X^7$

$$\begin{array}{l|l}
r(x) = 1+X+X^3+X^6+X^{10}+X^{11} & s(X) = 1+X+X^2+X^3+X^5+X^7 \\
r^{(1)}(X) = Xr(X) \pmod{X^{15}+1} & s^{(1)}(X) = Xs(X) \pmod{g(X)} = 1+X^3+X^6 \\
r^{(2)}(X) = Xr^{(1)}(X) \pmod{X^{15}+1} & s^{(2)}(X) = Xs^{(1)}(X) \pmod{g(X)} = X+X^4+X^7 \\
r^{(3)}(X) = Xr^{(2)}(X) \pmod{X^{15}+1} & s^{(3)}(X) = Xs^{(2)}(X) \pmod{g(X)} = 1+X+X^4+X^5 \\
r^{(4)}(X) = Xr^{(3)}(X) \pmod{X^{15}+1} & s^{(4)}(X) = Xs^{(3)}(X) \pmod{g(X)} = X+X^2+X^5+X^6
\end{array}$$

Hence, $e^{(4)}(X) = 1+X^{12}$. Since $e^{(4)}(X) = X^4 e(X) \pmod{X^{15}+1}$,

$$e(X) = X^{11}e^{(4)}(X) = X^{11}(1+X^{12}) = X^8+X^{11} \pmod{X^{15}+1}.$$

The transmitted codeword is $v(X) = r(X)+e(X) = 1+X+X^3+X^6+X^8+X^{10}$.

$$\begin{array}{l|l}
r(x) = X+X^2+X^4+X^7+X^8+X^9+X^{11} & s(X) = 1+X+X^2+X^4 \\
r^{(1)}(X) = Xr(X) \pmod{X^{15}+1} & s^{(1)}(X) = Xs(X) \pmod{g(X)} = X+X^2+X^3+X^5 \\
r^{(2)}(X) = Xr^{(1)}(X) \pmod{X^{15}+1} & s^{(2)}(X) = Xs^{(1)}(X) \pmod{g(X)} = X^2+X^3+X^4+X^6 \\
r^{(3)}(X) = Xr^{(2)}(X) \pmod{X^{15}+1} & s^{(3)}(X) = Xs^{(2)}(X) \pmod{g(X)} = X^3+X^4+X^5+X^7 \\
r^{(4)}(X) = Xr^{(3)}(X) \pmod{X^{15}+1} & s^{(4)}(X) = Xs^{(3)}(X) \pmod{g(X)} = 1+X+X^2+X^5+X^6 \\
r^{(5)}(X) = Xr^{(4)}(X) \pmod{X^{15}+1} & s^{(5)}(X) = Xs^{(4)}(X) \pmod{g(X)} = X+X^2+X^3+X^6+X^7 \\
r^{(6)}(X) = Xr^{(5)}(X) \pmod{X^{15}+1} & s^{(6)}(X) = Xs^{(5)}(X) \pmod{g(X)} = 1+X+X^3+X^7 \\
r^{(7)}(X) = Xr^{(6)}(X) \pmod{X^{15}+1} & s^{(7)}(X) = Xs^{(6)}(X) \pmod{g(X)} = 1
\end{array}$$

Hence, $e^{(7)}(X) = 1$. Since $e^{(7)}(X) = X^7 e(X) \pmod{X^{15}+1}$,

$$e(X) = X^8 e^{(7)}(X) = X^8 \pmod{X^{15}+1}.$$

The transmitted codeword is $v(X) = r(X)+e(X) = X+X^2+X^4+X^7+X^9+X^{11}$.

Problem 5.y (1) Since every code polynomial $v(X)$ in the code generated by $(X+1)g(X)$ is divisible by $X+1$, then $v(X) = a(X)(X+1)$ for some polynomial $a(X)$. Setting $X = 1$, it follows that $v(1) = 0$. This is the case if and only if $v(X)$ has an even number of nonzero terms, i.e., its weight is even. Furthermore, since $v(X)$ is divisible by $g(X)$, it follows that if $v(X)$ is nonzero, then its weight is at least d. As d is odd and $v(X)$ has even weight, it follows that $v(X)$ has weight at least $d+1$.

(2) Since $g(X)$ has degree 3, the dimension of the code generated by $g(X)$ is $7-3=4$. If $g(X)$ has a code of weight one, then X^i is divisible by $g(X)$ for some $i = 0, 1, \ldots, 6$. It is possible to check that this is not the case. If $g(X)$ has a code of weight two, then $1 + X^i$ is divisible by $g(X)$ for some $i = 1, 2, \ldots, 6$. It is possible to check that this is not the case. The code has a codeword of weight three, namely, $g(X)$ itself. Hence the minimum distance of the code generated by $g(X)$ is three.

(3) Since $(1+X)g(X)$ has degree 4, the dimension of the code generated by $(1+X)g(X)$ is $7-4=3$. Its minimum distance is at least 4. Actually it is 4 since the code has a codeword of weight four; namely, $(1+X)g(X) = 1 + X^2 + X^3 + X^4$.