either one of the polynomials p^4+p^2+p+1, $p^4+p^3+p^2+1$ can be used as a generator polynomial. With $g(p) = p^4 + p^2 + p + 1$ all the codeword polynomials $c(p)$ can be written as

$$c(p) = X(p)g(p) = X(p)(p^4 + p^2 + p + 1)$$

where $X(p)$ is the message polynomial. The following table shows the input binary sequences used to represent $X(p)$ and the corresponding codewords.

Input	$X(p)$	$c(p) = X(p)g(p)$	Codeword
000	0	0	0000000
001	1	$p^4 + p^2 + p + 1$	0010111
010	p	$p^5 + p^3 + p^2 + p$	0101110
100	p^2	$p^6 + p^4 + p^3 + p^2$	1011100
011	$p + 1$	$p^5 + p^4 + p^3 + 1$	0111001
101	$p^2 + 1$	$p^6 + p^3 + p + 1$	1001011
110	$p^2 + p$	$p^6 + p^5 + p^4 + p$	1110010
111	$p^2 + p + 1$	$p^6 + p^5 + p^2 + 1$	1100101

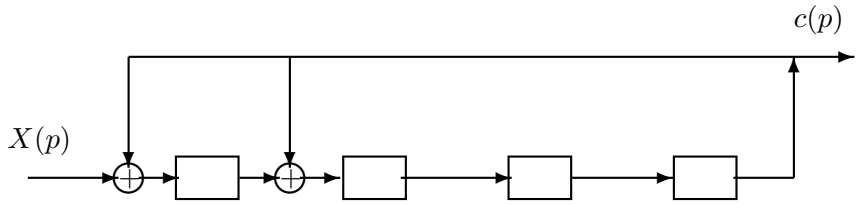
Since the cyclic code is linear and the minimum weight is $w_{\min} = 4$, we conclude that the minimum distance of the (7,3) code is 4.

Problem 9.33

Using Table 9.1 we find that the coefficients of the generator polynomial of the (15,11) code are given in octal form as 23. Since, the binary expansion of 23 is 010011, we conclude that the generator polynomial is

$$g(p) = p^4 + p + 1$$

The encoder for the (15,11) cyclic code is depicted in the next figure.



Problem 9.34

The i^{th} row of the matrix $\mathbf{G}$ has the form

$$\mathbf{g}_i = [\ 0 \quad \cdots \quad 0 \quad 1 \quad 0 \cdots 0 \quad p_{i,1} \quad p_{i,2} \quad \cdots \quad p_{i,n-k}\ ], \quad 1 \le i \le k$$

where $p_{i,1}$, $p_{i,2}$, $\ldots$, $p_{i,n-k}$ are found by solving the equation

$$p^{n-i} + p_{i,1}p^{n-k-1} + p_{i,2}p^{n-k-2} + \cdots + p_{i,n-k} = p^{n-i} \mod g(p)$$

Thus, with $g(p) = p^4 + p + 1$ we obtain

$$\begin{aligned}
p^{14} \bmod p^4+p+1 &= (p^4)^3p^2 \bmod p^4+p+1 = (p+1)^3p^2 \bmod p^4+p+1 \\
&= (p^3+p^2+p+1)p^2 \bmod p^4+p+1 \\
&= p^5+p^4+p^3+p^2 \bmod p^4+p+1 \\
&= (p+1)p+p+1+p^3+p^2 \bmod p^4+p+1 \\
&= p^3+1 \\
p^{13} \bmod p^4+p+1 &= (p^3+p^2+p+1)p \bmod p^4+p+1 \\
&= p^4+p^3+p^2+p \bmod p^4+p+1 \\
&= p^3+p^2+1
\end{aligned}$$

$$
\begin{aligned}
p^{12} \bmod p^4+p+1 &= p^3+p^2+p+1 \\
p^{11} \bmod p^4+p+1 &= (p^4)^2p^3 \bmod p^4+p+1 = (p+1)^2p^3 \bmod p^4+p+1 \\
&= (p^2+1)p^3 \bmod p^4+p+1 = p^5+p^3 \bmod p^4+p+1 \\
&= (p+1)p+p^3 \bmod p^4+p+1 \\
&= p^3+p^2+p \\
p^{10} \bmod p^4+p+1 &= (p^2+1)p^2 \bmod p^4+p+1 = p^4+p^2 \bmod p^4+p+1 \\
&= p^2+p^1 \\
p^9 \bmod p^4+p+1 &= (p^2+1)p \bmod p^4+p+1 = p^3+p \\
p^8 \bmod p^4+p+1 &= p^2+1 \bmod p^4+p+1 = p^2+1 \\
p^7 \bmod p^4+p+1 &= (p+1)p^3 \bmod p^4+p+1 = p^3+p+1 \\
p^6 \bmod p^4+p+1 &= (p+1)p^2 \bmod p^4+p+1 = p^3+p^2 \\
p^5 \bmod p^4+p+1 &= (p+1)p \bmod p^4+p+1 = p^2+p \\
p^4 \bmod p^4+p+1 &= p+1 \bmod p^4+p+1 = p+1
\end{aligned}
$$

The generator and the parity check matrix of the code are given by

$$
\mathbf{G} = \left(\begin{array}{cccccccccc|cccc}
1 & & & & & & & & & & 1 & 0 & 0 & 1 \\
 & 1 & & & & & & & & & 1 & 1 & 0 & 1 \\
 & & 1 & & & & & \mathbf{0} & & & 1 & 1 & 1 & 1 \\
 & & & 1 & & & & & & & 1 & 1 & 1 & 0 \\
 & & & & 1 & & & & & & 0 & 1 & 1 & 1 \\
 & & & & & 1 & & & & & 1 & 0 & 1 & 0 \\
 & & & & & & 1 & & & & 0 & 1 & 0 & 1 \\
 & & & & & & & 1 & & & 1 & 0 & 1 & 1 \\
 & & & \mathbf{0} & & & & & 1 & & 1 & 1 & 0 & 0 \\
 & & & & & & & & & 1 & 0 & 1 & 1 & 0 \\
 & & & & & & & & & & 1 & 0 & 0 & 1 & 1
\end{array}\right)
$$

$$
\mathbf{H} = \left(\begin{array}{cccccccccc|cccc}
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1
\end{array}\right)
$$

Problem 9.35

1) Let $g(p) = p^8 + p^6 + p^4 + p^2 + 1$ be the generator polynomial of an (n, k) cyclic code. Then, $n - k = 8$ and the rate of the code is

$$R = \frac{k}{n} = 1 - \frac{8}{n}$$

The rate R is minimum when $\frac{8}{n}$ is maximum subject to the constraint that R is positive. Thus, the first choice of n is $n = 9$. However, the generator polynomial $g(p)$ does not divide $p^9 + 1$ and therefore, it can not generate a $(9, 1)$ cyclic code. The next candidate value of n is 10. In this case

$$p^{10} + 1 = g(p)(p^2 + 1)$$

and therefore, $n = 10$ is a valid choice. The rate of the code is $R = \frac{k}{n} = \frac{2}{10} = \frac{1}{5}$.

2) In the next table we list the four codewords of the $(10, 2)$ cyclic code generated by $g(p)$.

Input	$X(p)$	Codeword
00	0	0000000000
01	1	0101010101
10	p	1010101010
11	$p+1$	1111111111