Problems

4.1)

The polynomial is irreducible if it is not divisible by polynomials over *GF(2)* of degree less than 5.

Polynomials of degree 1: $X,\ X+1$ do not divide $p(X)=1+X^2+X^5$ because this polynomial has not ´0´ or `1` as roots

Polynomials of degree 2: $X+X^2,\ 1+X^2,\ 1+X+X^2,\ X^2$ do not divide $p(X)=1+X^2+X^5$

In this case we only need to verify that $1+X+X^2$ does not divide the polynomial, since the other polynomials of degree 2 have ´0´ or `1` as roots

Polynomials of degree 3: $1+X+X^2+X^3,\ 1+X^3,\ X+X^3,\ X^2+X^3,$ $1+X+X^3,\ 1+X^2+X^3,\ X+X^2+X^3,\ X^3$

do not divide $p(X)=1+X^2+X^5$

In this case we only need to verify that $1+X+X^3$ and $1+X^2+X^3$ do not divide the polynomial, since the other polynomials of degree 3 have ´0´ or `1` as roots

Polynomials of degree 4:

$1+X+X^2+X^3+X^4,\ 1+X^4,\ X+X^4,\ X^2+X^4,\ X^3+X^4,$
$1+X+X^4,\ 1+X^2+X^4,1+X^3+X^4,\ X+X^2+X^3+X^4,$
$X^2+X^3+X^4,X+X^3+X^4,\ X+X^2+X^4,\ 1+X^2+X^3+X^4,\ X^4$

do not divide $p(X)=1+X^2+X^5$

In this case we only need to verify that $1+X+X^2+X^3+X^4$, $1+X+X^4$, and $1+X+X^2+X^4$ $1+X^3+X^4$ do not divide the polynomial, since the other polynomials of degree 4 have ´0´ or `1` as roots

If the polynomial is irreducible then it is a factor $X^{2^m-1}+1=X^{2^5-1}+1=X^{31}+1$
By performing the corresponding polynomial division we get:

$$X^{31}+1=(X^{26}+X^{23}+X^{21}+X^{20}+X^{17}+X^{16}+X^{15}+X^{14}+X^{13}+X^9+$$
$$X^8+X^6+X^5+X^4+X^2+1)(X^5+X^2+1)$$

This is another way of verifying that the polynomial $p(X)=1+X^2+X^5$ is an irreducible polynomial. A polynomial $p(X)$ is said to be primitive if the smallest positive integer n for which $p(X)$ divides X^n+1 is $n=2^m-1$. This is the case for the polynomial $p(X)=1+X^2+X^5$.

4.2)

The primitive polynomial $p(X)=1+X^2+X^5$ generates the following Galois Field $GF(2^5)$, with 32 elements. The table shows the exponential, polynomial, and binary representations of the elements.
We know that $p(\alpha)=1+\alpha^2+\alpha^5=0$, that is, $\alpha^5=1+\alpha^2$

0	0	00000	α^{15}	$1+\alpha+\alpha^2+\alpha^3+\alpha^4$	11111
1	1	10000	α^{16}	$1+\alpha+\alpha^3+\alpha^4$	11011
α	α	01000	α^{17}	$1+\alpha+\alpha^4$	11001
α^2	α^2	00100	α^{18}	$1+\alpha$	11000
α^3	α^3	00010	α^{19}	$\alpha+\alpha^2$	01100
α^4	α^4	00001	α^{20}	$\alpha^2+\alpha^3$	00110
α^5	$1+\alpha^2$	10100	α^{21}	$\alpha^3+\alpha^4$	00011
α^6	$\alpha+\alpha^3$	01010	α^{22}	$1+\alpha^2+\alpha^4$	10101
α^7	$\alpha^2+\alpha^4$	00101	α^{23}	$1+\alpha+\alpha^2+\alpha^3$	11110
α^8	$1+\alpha^2+\alpha^3$	10110	α^{24}	$\alpha+\alpha^2+\alpha^3+\alpha^4$	01111
α^9	$\alpha+\alpha^3+\alpha^4$	01011	α^{25}	$1+\alpha^3+\alpha^4$	10011
α^{10}	$1+\alpha^4$	10001	α^{26}	$1+\alpha+\alpha^2+\alpha^4$	11101
α^{11}	$1+\alpha+\alpha^2$	11100	α^{27}	$1+\alpha+\alpha^3$	11010
α^{12}	$\alpha+\alpha^2+\alpha^3$	01110	α^{28}	$\alpha+\alpha^2+\alpha^4$	01101
α^{13}	$\alpha^2+\alpha^3+\alpha^4$	00111	α^{29}	$1+\alpha^3$	10010
α^{14}	$1+\alpha^2+\alpha^3+\alpha^4$	10111	α^{30}	$\alpha+\alpha^4$	01001

4.3)

If β is a root of a polynomial $f(X)$, $\beta\in GF(2^m)$, then β^{2^l}, $l\geq 0$ is also a root of $f(X)$. Thus, for instance, $\alpha,\alpha^2,\alpha^4,\alpha^8,\alpha^{16}$ (Note that $\alpha^{32}=\alpha$) are roots of the same polynomial, and:

$$(X+\alpha)(X+\alpha^2)(X+\alpha^4)(X+\alpha^8)(X+\alpha^{16})=$$
$$(X^2+(\alpha+\alpha^2)X+\alpha^3)(X^2+(\alpha^4+\alpha^8)X+\alpha^{12})(X+\alpha^{16})=$$
$$(X^2+\alpha^{19}X+\alpha^3)(X^2+\alpha^{14}X+\alpha^{12})(X+\alpha^{16})=$$
$$(X^2+\alpha^{19}X+\alpha^3)(X^2+\alpha^{14}X+\alpha^{12})(X+\alpha^{16})=$$
$$(X^4+\alpha^{16}X^3+\alpha X^2+\alpha^{30}X+\alpha^{15})(X+\alpha^{16})=X^5+\alpha^{16}X^4+\alpha X^3+\alpha^{30}X^2+\alpha^{15}X+$$
$$\alpha^{16}X^4+\alpha X^3+\alpha^{17}X^2+\alpha^{15}X+\alpha^0=X^5+X^2+1$$

is the minimal polynomial of roots $\alpha,\alpha^2,\alpha^4,\alpha^8,\alpha^{16}$. The other minimal polynomials can be calculated in the same way.
Thus,

$$(X+\alpha^3)(X+\alpha^6)(X+\alpha^{12})(X+\alpha^{24})(X+\alpha^{17})=$$
$$(X^2+(\alpha^3+\alpha^6)X+\alpha^9)(X^2+(\alpha^{24}+\alpha^{12})X+\alpha^5)(X+\alpha^{17})=$$
$$(X^2+\alpha X+\alpha^9)(X^2+\alpha^4 X+\alpha^5)(X+\alpha^{17})=$$
$$(X^4+\alpha^4 X^3+\alpha^5 X^2+\alpha X^3+\alpha^5 X^2+\alpha^9 X^2+\alpha^6 X+\alpha^{13} X+\alpha^{14})(X+\alpha^{17})=$$
$$(X^4+\alpha^{30} X^3+\alpha^9 X^2+\alpha^{28} X+\alpha^{14})(X+\alpha^{17})=$$
$$X^5+\alpha^{17} X^4+\alpha^{30} X^4+\alpha^{16} X^3+\alpha^9 X^3+\alpha^{26} X^2+\alpha^{28} X^2+\alpha^{14} X+$$
$$\alpha^{14} X+\alpha^{31}=X^5+X^4+X^3+X^2+1$$

is the minimal polynomial of roots $\alpha^3,\alpha^6,\alpha^{12},\alpha^{24},\alpha^{17}$.

The following table determines the conjugated roots and their minimal polynomials:

Conjugated roots	Minimal polynomial
0	X
1	$1+X$
$\alpha,\alpha^2,\alpha^4,\alpha^8,\alpha^{16}$	$1+X^2+X^5$
$\alpha^3,\alpha^6,\alpha^{12},\alpha^{24},\alpha^{17}$	$1+X^2+X^3+X^4+X^5$
$\alpha^5,\alpha^{10},\alpha^{20},\alpha^9,\alpha^{18}$	$1+X+X^2+X^4+X^5$
$\alpha^7,\alpha^{14},\alpha^{28},\alpha^{25},\alpha^{19}$	$1+X+X^2+X^3+X^5$
$\alpha^{11},\alpha^{22},\alpha^{13},\alpha^{26},\alpha^{21}$	$1+X+X^3+X^4+X^5$
$\alpha^{15},\alpha^{30},\alpha^{29},\alpha^{27},\alpha^{23}$	$1+X^3+X^5$

4.4) Generator polynomial of the binary BCH code $C_{BCH}(31,16)$:

Since $t=3$

$$g(X)=LCF\{\Phi_1(X),\Phi_3(X),\Phi_5(X)\}=$$
$$(1+X^2+X^5)(1+X^2+X^3+X^4+X^5)(1+X+X^2+X^4+X^5)=$$
$$(1+X^3+X^5+X^6+X^8+X^9+X^{10})(1+X+X^2+X^4+X^5)=$$
$$1+x+X^2+X^4+X^5+X^3+X^4+X^5+X^7+X^8+X^5+X^6+X^7+X^9+X^{10}$$
$$+X^6+X^7+X^8+X^{10}+X^{11}+X^8+X^9+X^{10}+X^{12}+X^{13}+X^9+X^{10}+X^{11}+X^{13}$$
$$+X^{14}+X^{10}+X^{11}+X^{12}+X^{14}+X^{15}=$$
$$g(X)=1+X+X^2+X^3+X^5+X^7+X^8+X^9+X^{10}+X^{11}+X^{15}$$

$d_{min}=11$

4.5)

Since $t=2$

$$g(X)=LCF\{\Phi_1(X),\Phi_3(X)\}=$$
$$(1+X^2+X^5)(1+X^2+X^3+X^4+X^5)=$$
$$g(X)=1+X^3+X^5+X^6+X^8+X^8+X^9+X^{10}$$

$$d_{min}=7$$

4.6)
a)

The generator polynomial in this case is constructed over $GF(16)$ (See table of this Galois Field in Appendix B) , using the minimal polynomials $X+1$, which corresponds to the root 1, X^4+X+1, which is the minimal polynomial of roots $\alpha,\alpha^2,\alpha^4,\alpha^8$, and $X^4+X^3+X^2+X+1$, which is the minimal polynomial of roots $\alpha^3,\alpha^6,\alpha^{12},\alpha^9$.

$$g(X)=(X+1)(1+X+X^4)(1+X+X^2+X^3+X^4)=$$
$$(1+X^2+X^4+X^5)(1+X+X^2+X^3+X^4)=$$
$$1+X^2+X^4+X^5+X+X^3+X^5+X^6+X^2+X^4+X^6+X^7+X^3+X^5+X^7+X^8$$
$$+X^4+X^6+X^8+X^9=1+X+X^4+X^5+X^6+X^9$$

$$d_{min}=6$$

b)

This code is a cyclic code $C_{cyc}(15,6)$, since the degree of the generator polynomial is $n-k=r=9$, and being $n=15$, then $k=6$. As an example, we get the code polynomial for the input message $\boldsymbol{m}=(100000)$, or $m(X)=1$. Thus, $X^{n-k}m(X)=X^9m(X)=X^9$

$$X^9 \qquad\qquad ! \qquad X^9+X^6+X^5+X^4+X+1$$
$$X^9+X^6+X^5+X^4+X+1 \qquad\quad 1$$

$$\underline{\qquad\qquad\qquad\qquad}$$
$$p(X)=X^6+X^5+X^4+X+1$$

Therefore,

$$c(X)=1+X+X^4+X^5+X^6+X^9$$

Consider now that the received vector is $\boldsymbol{r}=(0100111011\,00000)$, and the received polynomial is $r(X)=X+X^4+X^5+X^6+X^8+X^9$, containing two errors at the first at eighth positions with respect to the code vector.

The decoding of this code can be performed by using the Euclidean algorithm for instance. We need to first calculate the syndrome polynomial:

$r(\alpha) = \alpha^2$
$r(\alpha^2) = \alpha^4$
$r(\alpha^3) = \alpha^7$
$r(\alpha^4) = \alpha^8$

then:

$$S(X) = \alpha^2 + \alpha^4 X + \alpha^7 X^2 + \alpha^8 X^3$$

The Euclidean algorithm is easily implemented in the form of a table:

i	$r_i = r_{i-2} - q_i . r_{i-1}$	q_i	$t_i = t_{i-2} - q_i . t_{i-1}$
-1	$X^{2t} = X^4$		0
0	$S(X) = \alpha^8 X^3 + \alpha^7 X^2 + \alpha^4 X + \alpha^2$		1
1	$\alpha^4 X^2 + \alpha^{13} X + \alpha^8$	$\alpha^7 X + \alpha^6$	$\alpha^7 X + \alpha^6$
2	α^5	$\alpha^4 X + \alpha^8$	$\alpha^{11} X^2 + \alpha^5 X + \alpha^3$

This is the same table as it is the corresponding to example 4.5. This is so because the error event is the same, and the decoding performs in the same way, independently of the code vector (the all zero code vector in the case of the example 4.5)

Thus,

$$t_i(X) = \alpha^{11} X^2 + \alpha^5 X + \alpha^3$$

An element $\lambda \in GF(2^4)$ is used to multiply $t_i(X)$ by, in order to convert it into a monic polynomial. This value of λ is $\lambda = \alpha^4$:

$$W(X) = -\lambda r_i(X) = \lambda r_i(X) = \alpha^4 \alpha^5 = \alpha^9$$

and

$$\sigma(X) = \lambda t_i(X) = \alpha^4 \left(\alpha^{11} X^2 + \alpha^5 X + \alpha^3\right) = X^2 + \alpha^9 X + \alpha^7$$

By performing the Chien search, the roots of the error location polynomials are found to be $\alpha^{-j1} = 1$ and $\alpha^{-j2} = \alpha^7$. Then, and since:

$$\alpha^0 = \alpha^{-j1} = \alpha^{-0}$$

$j_1 = 0$
and
$\alpha^7 = \alpha^{-j2} = \alpha^{-8}$

$j_2 = 8$

Errors are located in positions $j_1 = 0$ and $j_2 = 8$. Values of the errors are determined by evaluating the derivative of the error location polynomial:

$\sigma'(X) = \alpha^9$

Then,

$$e_{j1} = \frac{W(\alpha^{-j1})}{\sigma'(\alpha^{-j1})} = \frac{W(\alpha^0)}{\sigma'(\alpha^0)} = \frac{\alpha^9}{\alpha^9} = 1$$

$$e_{j2} = \frac{W(\alpha^{-j2})}{\sigma'(\alpha^{-j2})} = \frac{W(\alpha^7)}{\sigma'(\alpha^7)} = \frac{\alpha^9}{\alpha^9} = 1$$

The result is obvious as this BCH code is a binary code, and so errors are always of value 1. The error polynomial is therefore:

$e(X) = X^0 + X^8 = 1 + X^8$

and

$$c(X) = r(X) + e(X) = X + X^4 + X^5 + X^6 + X^8 + X^9 + 1 + X^8 = 1 + X + X^4 + X^5 + X^6 + X^9$$

4.7) $g(X) = (1 + X + X^4)(1 + X + X^2 + X^3 + X^4)$
a)

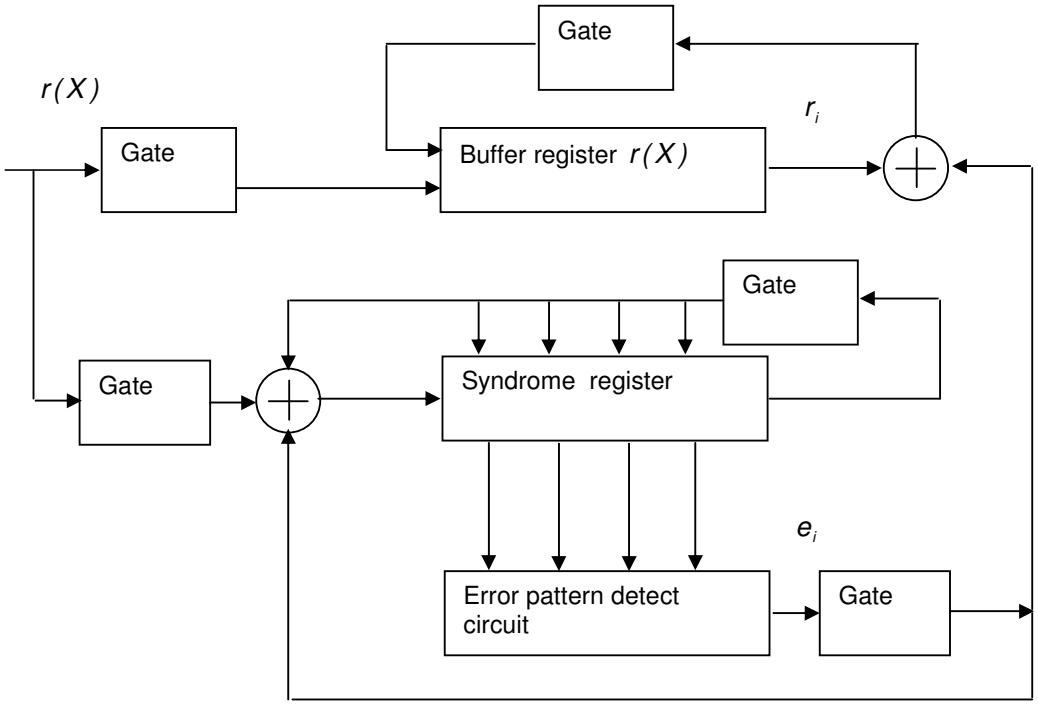
$$g(X) = (1 + X + X^4)(1 + X + X^2 + X^3 + X^4) =$$
$$1 + X + X^4 + X + X^2 + X^5 + X^2 + X^3 + X^6 + X^3 + X^4 + X^7 + X^4 + X^5 + X^8 =$$
$$1 + X^4 + X^6 + X^7 + X^8$$

Then, $r = n - k = 8$ and $d_{min} = 5$

Since the generator polynomial is constructed as the LCF between the minimal polynomials $\Phi_1(X)$ and $\Phi_3(X)$ defined over $GF(2^m) = GF(2^4)$, then $m = 4$, and the minimum code length is $n = 2^m - 1 = 2^4 - 1 = 15$. The generator polynomial has $\alpha, \alpha^2, \alpha^3, \alpha^4$ as its roots and this code can correct any error pattern of size $t = 2$.

b)

The Meggitt decoder is seen in the following figure:



The operation of this decoder is based on the fact that if $S(X)$ is the syndrome for $r(X)$, then $S^i(X)$ is the syndrome for $r^i(X)$. The decoder takes $r(X)$ and calculates $S(X)$. If this syndrome does not correspond to the error pattern in the most significant position, $e(X)=X^{n-1}$, then received vector and the syndrome vector, stored in the corresponding registers, are both cyclically shifted. This generates $r^{(1)}(X)=r_{n-1}+r_0X+...+r_{n-2}X^{n-1}$, and the contents of the syndrome register form the syndrome $S^1(X)$ that corresponds to $r^1(X)$.

If this syndrome corresponds to the error pattern in the most significant position, $e(X)=X^{n-1}$, then the corresponding bit is corrected by doing $r_{n-1}\oplus 1$. After this the received vector is modified and it is $r_1(X)=r_{01}+r_1X+...+(r_{n-1}\oplus 1)X^{n-1}$, and the error effect over the syndrome has to be removed. This is done by adding the syndrome of $e(X)=X^{n-1}$ to $S(X)$. The new received and syndrome vectors are again cyclically shifted to obtain $r_1^{(1)}(X)$ and $S_1^{(1)}(X)$. This syndrome $S_1^{(1)}(X)$ of $r_1^{(1)}(X)$ is obtained by taking the remainder of the division between $X[S(X)+X^{n-1}]$ and $g(X)$, which is the same to do:

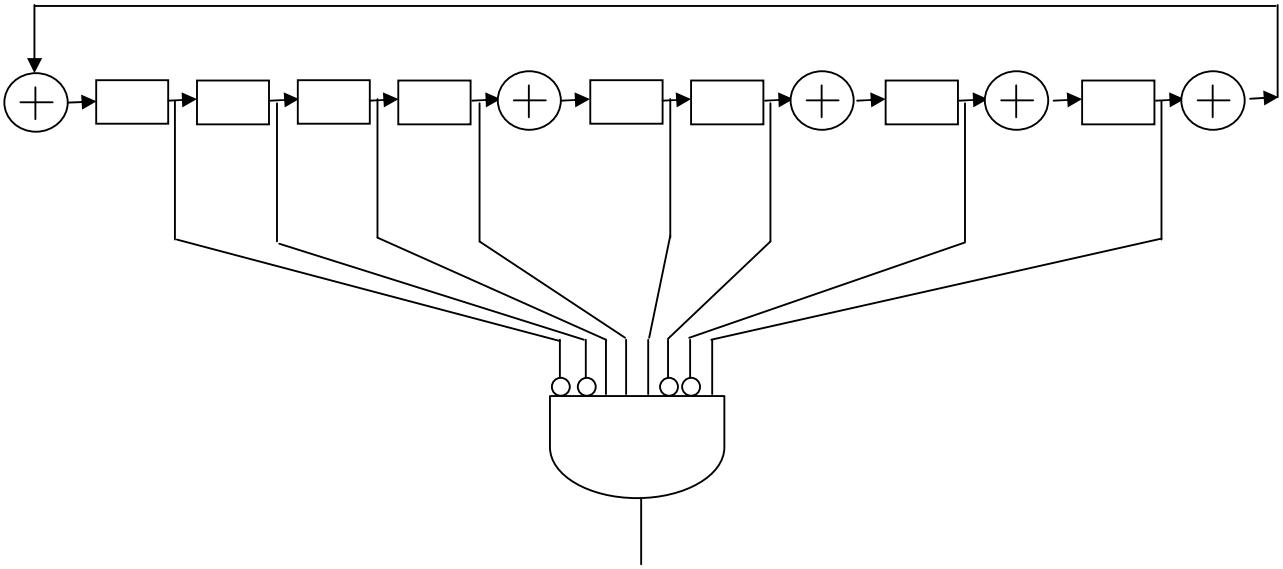
$$S_1^{(1)}(X)=S^{(1)}(X)+1$$

This procedure takes n steps.

c)

In the case of the code of this problem, and with the propose of decoding an error pattern of two consecutive bits, we can calculate the syndrome polynomial corresponding to an error pattern of two consecutive bits at the most significant position, which is of the form $e(X) = X^{14} + X^{13}$, that has as a syndrome polynomial $s(X) = X^2 + X^3 + X^4 + X^7$

The syndrome register and the error detection circuit are as shown in the following figure,



When the states of the register are (00111001), then the gate generates an indication of that the error pattern $e(X) = X^{14} + X^{13}$ is detected.

4.8)

a)

The generator polynomial is

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

The weight of this polynomial is four, and the minimum Hamming distance is $d_{min} = 4$.

To see this:

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}, \qquad \boldsymbol{G}' = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

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

The addition of columns 1, 2, 3 and 6 results into the all zero vector. Since there is now way of adding three columns to result into the all zero vector (this is because the submatrix $\boldsymbol{P}^T$ contains linearly independent column vectors of weight 3), then $d_{min} = 4$.

b)
What is the minimum Hamming distance if $n = 14$ and why?

The division of $X^{14} + 1$ and $g(X) = 1 + X^2 + X^3 + X^4$ is equal to $X^{10} + X^9 + X^7 + X^3 + X^2 + 1$ and the remainder is zero, so that the polynomial is a generator polynomial of a cyclic code $C_{Cycil}(14,10)$.

The generator polynomial is $g(X) = 1 + X^2 + X^3 + X^4$. So $n - k = 4$, and if $n = 14$ then $k = 10$. Therefore the cyclic form of the generator matrix of the code has dimensions 10 x 14, and its rows consist of shifted versions of the binary representation of the generator polynomial, as follows:

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

Now take the sum of rows 1, 3 and 4 (counting from the top), which gives the vector $(1000000100\ 0000)$. This is a consequence of the fact that $g(X)$ belongs to the exponent $p = 7$; that is, the smallest value of p for which $g(X)$ exactly divides $X^p + 1$ is 7. Similarly, the sum of rows 2, 4 and 5 gives the vector $(0100000010\ 0000)$, and so on. All these vectors have weight 2 and are codewords in the cyclic code, so the minimum Hamming distance of the this cyclic code is $d_{min} = 2$. This is a general result: for a given $g(X)$ belonging to exponent p, the block length n of a cyclic code can be $n = ip$, where $i = 1,2,3,...$ i = 1, 2, 3, ..., but $d_{min} = 2$ for all $i > 1$.

Another ay of evaluating the minimum distance is the analysis of the BCH bound.
The above generator matrix in non systematic form can be modified to have the systematic form:

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

Then the parity check matrix is:

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

Now the minimum Hamming distance is $d_{min} = 2$ because the addition of columns 1 and 8 results into the all zero vector.

4.9)

The syndrome vector components are:

$$s_1 = r(\alpha) = \alpha^2$$
$$s_2 = r(\alpha^2) = \alpha^4$$
$$s_3 = r(\alpha^3) = \alpha^7$$
$$s_4 = r(\alpha^4) = \alpha^8$$

Therefore the syndrome polynomial is:

$$S(X) = \alpha^8 X^3 + \alpha^7 X^2 + \alpha^4 X + \alpha^2$$

The Euclidean algorithm is applied by constructing the following table:

i	$r_i = r_{i-2} - q_i . r_{i-1}$	q_i	$t_i = t_{i-2} - q_i . t_{i-1}$
-1	$X^{2t} = X^4$		0
0	$S(X) = \alpha^8 X^3 + \alpha^7 X^2 + \alpha^4 X + \alpha^2$		1
1	$\alpha^4 X^2 + \alpha^{13} X + \alpha^8$	$\alpha^7 X + \alpha^6$	$\alpha^7 X + \alpha^6$
2	α^5	$\alpha^4 X + \alpha^8$	$\alpha^{11} X^2 + \alpha^5 X + \alpha^3$

When the degree of the polynomial in column $r_i(X)$ is lower than the degree of the polynomial in column $t_i(X)$, the recursion is halted. In this case:

$$r_i(X) = \alpha^5$$

$$t_i(X) = \alpha^{11} X^2 + \alpha^5 X + \alpha^3$$

An element $\lambda \in GF(2^4)$ is conveniently selected to multiply $t_i(X)$ by, in order to convert it into a monic polynomial. This value of λ is $\lambda = \alpha^4$. Therefore:

$$W(X) = -\lambda r_i(X) = \lambda r_i(X) = \alpha^4 \alpha^5 = \alpha^9$$

and

$$\sigma(X) = \lambda t_i(X) = \alpha^4 \left(\alpha^{11} X^2 + \alpha^5 X + \alpha^3\right) = X^2 + \alpha^9 X + \alpha^7$$

The following step consists of applying the Chien search. Thus, the roots of the error location polynomials are found to be $\alpha^{-j1} = 1$ and $\alpha^{-j2} = \alpha^7$. Then, and since:

$$\alpha^0 = \alpha^{-j1} = \alpha^{-0}$$

$$j_1 = 0$$

and

$$\alpha^7 = \alpha^{-j2} = \alpha^{-8}$$

$$j_2 = 8$$

Errors are located in positions $j_1 = 0$ and $j_2 = 8$. Values of the errors are determined by evaluating the derivative of the error location polynomial:

$$\sigma'(X) = \alpha^9$$

Then:

$$e_{j1} = \frac{W(\alpha^{-j1})}{\sigma'(\alpha^{-j1})} = \frac{W(\alpha^0)}{\sigma'(\alpha^0)} = \frac{\alpha^9}{\alpha^9} = 1$$

$$e_{j2} = \frac{W(\alpha^{-j2})}{\sigma'(\alpha^{-j2})} = \frac{W(\alpha^{7})}{\sigma'(\alpha^{7})} = \frac{\alpha^{9}}{\alpha^{9}} = 1$$

The error polynomial is therefore:

$$e(X) = X^{0} + X^{8} = 1 + X^{8}$$

After the correction of the received polynomial, the decoded polynomial is the zero polynomial, that is, the all-zero vector.

For the Barlekamp-Massey algorithm:

The following table is used to apply the Barlekamp-Massey Algorithm in order to determine the error location polynomial:

μ	$\sigma_{BM}^{(\mu)}(X)$	d_μ	l_μ	$\mu - l_\mu$	ρ
-1	1	1	0	-1	
0	1	α^2	0	0	
1	$1+\alpha^2 X$	0	1	0	-1
2	$1+\alpha^2 X$	α^{10}	1	1	
3	$1+\alpha^2 X+\alpha^8 X^2$	0	2	1	0
4	$1+\alpha^2 X+\alpha^8 X^2$				

The procedure ends at row $\mu = 4$, where the error location polynomial is finally:

$$\sigma_{BM}(X) = \sigma_{BM}^{(4)}(X) = 1 + \alpha^2 X + \alpha^8 X^2$$

whose roots are $\beta_1^{-1} = 1 = \alpha^0 = \alpha^{-j_1}$ and $\beta_2^{-1} = \alpha^7 = \alpha^{-8} = \alpha^{-j_2}$, so that error positions are at $j_1 = 0$ and $j_2 = 8$.

4.10)

$s_3 = s_1^2 + s_1^2\beta_l + s_1\beta_l^2$ where $\beta_l = \alpha^{j_l}$

In order to verify the validity of this equation we can form its terms as follows:

In a BCH code with an error correction capability of $t = 2$, the syndrome equation for s_1 is:

$$s_1 = e(\alpha) = e_{j_1}\alpha^{j_1} + e_{j_2}\alpha^{j_2} = \alpha^{j_1} + \alpha^{j_2}$$

This is so because BCH codes are binary codes, and $e_{j_1} = e_{j_2} = 1$. We can form the expression:

$$s_1^3 = \left(\alpha^{j_1} + \alpha^{j_2}\right)^3 = \left(\alpha^{j_1} + \alpha^{j_2}\right)\left(\alpha^{j_1} + \alpha^{j_2}\right)^2 = \left(\alpha^{j_1} + \alpha^{j_2}\right)\left(\alpha^{2j_1} + \alpha^{2j_2}\right) = \alpha^{3j_1} + \alpha^{j_1+2j_2} + \alpha^{j_2+2j_1} + \alpha^{3j_2}$$

we can form also the expression:

$$\alpha^{j_1} s_1^2 = \alpha^{j_1}\left(\alpha^{j_1} + \alpha^{j_2}\right)^2 = \alpha^{j_1}\left(\alpha^{2j_1} + \alpha^{2j_2}\right) = \alpha^{3j_1} + \alpha^{j_1+2j_2}$$

and the expression:

$$\alpha^{2j_1} s_1 = \alpha^{2j_1}\left(\alpha^{j_1} + \alpha^{j_2}\right) = \alpha^{3j_1} + \alpha^{j_2+2j_1}$$

By adding these three expressions:

$$s_1^3 + \alpha^{j_1} s_1^2 + \alpha^{2j_1} s_1 = \alpha^{3j_1} + \alpha^{j_1+2j_2} + \alpha^{j_2+2j_1} + \alpha^{3j_2} + \alpha^{3j_1} + \alpha^{j_1+2j_2} + \alpha^{3j_1} + \alpha^{j_2+2j_1} = \alpha^{3j_1} + \alpha^{3j_2} = s_3$$

For the received vector $\boldsymbol{r} = (000100111111011)$ in the case of the cyclic BCH code $C_{BCH}(15,7)$ generated by $g(X) = (1 + X + X^4)(1 + X + X^2 + X^3 + X^4)$ we have:

$$r(X) = X^3 + X^6 + X^7 + X^8 + X^9 + X^{10} + X^{11} + X^{13} + X^{14}$$

Then

$$s_1 = r(\alpha) = \alpha^3 + \alpha^6 + \alpha^7 + \alpha^8 + \alpha^9 + \alpha^{10} + \alpha^{11} + \alpha^{13} + \alpha^{14} = \alpha^{13}$$

$$s_3 = r(\alpha^3) = \alpha^9 + \alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12} + 1 + \alpha^3 + \alpha^9 + \alpha^{12} = \alpha^{10}$$

Therefore:

$$s_3 = \alpha^9 + \alpha^{11}\beta_1 + \alpha^{13}\beta_1^2 = \alpha^{10}$$

A Chien search drives to the solutions:

$$\beta_1 = \alpha^4 \qquad \beta_2 = \alpha^{11}$$

So that positions of errors are at:

$$\beta_1 = \alpha^4 = \alpha^{j_1} \qquad \beta_2 = \alpha^{11} = \alpha^{j_2}$$

$$j_1 = 4 \qquad j_2 = 11$$

and the corrected vector is

$$\boldsymbol{r} = (000110111110011)$$

which corresponds to the vector polynomial:

$c(X) = X^3 + X^4 + X^6 + X^7 + X^8 + X^9 + X^{10} + X^{13} + X^{14}$, which is in turn the code polynomial of the message polynomial:

$m(X) = 1 + X + X^2 + X^5 + X^6$

4.11)
a)
The received polynomial is $r_1(X) = X^7 + X^{30}$ for the BCH code $C_{BCH}(31,21)$ obtained in Problem 4.5

We apply the Euclidean algorithm.

The syndrome values are:

$s_1 = r(\alpha) = \alpha^7 + \alpha^{30} = \alpha^{19}$
$s_2 = r(\alpha^2) = \alpha^{14} + \alpha^{60} = \alpha^7$
$s_3 = r(\alpha^3) = \alpha^{21} + \alpha^{90} = \alpha^{12}$
$s_4 = r(\alpha^4) = \alpha^{28} + \alpha^{120} = \alpha^{14}$

The syndrome polynomial is:

$S(X) = \alpha^{19} + \alpha^7 X + \alpha^{12} X^2 + \alpha^{14} X^3$

i	$r_i = r_{i-2} - q_i . r_{i-1}$	q_i	$t_i = t_{i-2} - q_i . t_{i-1}$
-1	$X^{2t} = X^4$		0
0	$S(X) = \alpha^{19} + \alpha^7 X + \alpha^{12} X^2 + \alpha^{14} X^3$		1
1	$\alpha^{22} X^2 + \alpha^4 X + \alpha^3$	$\alpha^{17} X + \alpha^{15}$	$\alpha^{17} X + \alpha^{15}$
2	α^{22}	$\alpha^{23} X + \alpha^{14}$	$\alpha^9 X^2 + \alpha^{22} X + \alpha^3$

$r_i(X) = \alpha^{22}$

$t_i(X) = \alpha^9 X^2 + \alpha^{22} X + \alpha^3$

$\sigma(X) = \lambda t_i(X) = \alpha^{22}\left(\alpha^9 X^2 + \alpha^{22} X + \alpha^3\right) = X^2 + \alpha^{13} X + \alpha^{25}$
$W(X) = -\lambda r_i(X) = \alpha^{22} r_i(X) = \alpha^{22}\alpha^{22} = \alpha^{13}$

Roots of $\sigma(X)$ are determined using the Chien search:

$\sigma(\alpha^1) = \alpha^2 + \alpha^{14} + \alpha^{25} = 0$
$\sigma(\alpha^{24}) = \alpha^{17} + \alpha^6 + \alpha^{25} = 0$

$\alpha^{-j_1} = \alpha^1 = \alpha^{-30}$, $j_1 = 30$

$\alpha^{-j_2} = \alpha^{24} = \alpha^{-7}$, $\quad j_1 = 7$

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

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

$s_1 = r(\alpha) = 1 + \alpha^{17} + \alpha^{28} = \alpha^2$
$s_2 = r(\alpha^2) = 1 + \alpha^3 + \alpha^{25} = \alpha^4$
$s_3 = r(\alpha^3) = 1 + \alpha^{20} + \alpha^{22} = \alpha^{21}$
$s_4 = r(\alpha^4) = 1 + \alpha^6 + \alpha^{19} = \alpha^8$

These values of the syndromes can be used in either the Euclidean or the B-M algorithm to determine the error location polynomial. After applying one of these algorithms we can determine that the error location polynomial is of the form:

$\sigma(X) = X^2 + \alpha^5 X + \alpha^3$

The Chien search over this polynomial is not successful, that is, there are no roots in $GF(2^5)$ for this polynomial. Then, the decoding fails and it is not able to determine the positions of the errors. The error pattern is not correctable.