Problems

5.1)

The generator polynomial of a cyclic code over $GF(4)$ is $g(X)=X+1$, with code length $n=3$. The field elements are generated by the polynomial $\alpha^2+\alpha+1=0$.

Since $\alpha^2=\alpha+1$, the field $GF(4)$ is described below:

$GF(4)$		Binary representation
0	0	*00*
1	1	*10*
α	α	*01*
α^2	$\alpha^2=\alpha+1$	*11*

The code is cyclic and its generator polynomial is $g(X)=X+1$, so that the generator matrix is of he form:

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

with a systematic form:

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

The transpose of the parity check matrix is:

$$\boldsymbol{H}^T=\begin{bmatrix}1\\ 1\\ 1\end{bmatrix}$$

The code table is seen below:

0	*0*		*0*	*0*	*0*
0	*1*		*1*	*0*	*1*
0	α		α	*0*	α
0	α^2		α^2	*0*	α^2
1	*0*		*1*	*1*	*0*
1	*1*		*0*	*1*	*1*
1	α		α^2	*1*	α
1	α^2		α	*1*	α^2
α	*0*		α	α	*0*
α	*1*		α^2	α	*1*
α	α		*0*	α	α
α	α^2		*1*	α	α^2
α^2	*0*		α^2	α^2	*0*
α^2	*1*		α	α^2	*1*
α^2	α		*1*	α^2	α
α^2	α^2		*0*	α^2	α^2

The minimum distance is then $d_{min} = 2$, and the syndrome vector for the received vector $\boldsymbol{r} = (\alpha\ \alpha\ \alpha)$ is equal to:

$$S = r \bullet H^T = \begin{pmatrix} \alpha & \alpha & \alpha \end{pmatrix} \bullet \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \alpha$$

Code table can be obtained by multiplying the message vectors by the systematic generator matrix, or equivalently by doing the polynomial operation $r(X) = Xm(X) \bmod g(X)$. Thus, for instance,

with $m(X) = \alpha + \alpha^2 X$, then $Xm(X) = \alpha X + \alpha^2 X^2$,

$$\begin{array}{ll} \alpha X + \alpha^2 X^2 & / \quad X + 1 \\ \alpha^2 X^2 + \alpha^2 X & \quad \alpha^2 X + 1 \\ \hline X & \\ X + 1 & \\ \hline 1 & \end{array}$$

The code vector for $\boldsymbol{m} = \begin{pmatrix} \alpha & \alpha^2 \end{pmatrix}$ is $\boldsymbol{c} = \begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}$.

5.2)

a) The generator polynomial of a RS code $C_{RS}(n,k)$ that operates over the field $GF(2^4)$ and is able to correct any error pattern of size $t=2$ or less, is obtained by doing:

$$g(X)=(X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)=(X^2+(\alpha+\alpha^2)X+\alpha^3)(X^2+(\alpha^3+\alpha^4)X+\alpha^7)=$$
$$(X^2+\alpha^5X+\alpha^3)(X^2+\alpha^7X+\alpha^7)=X^4+\alpha^{13}X^3+\alpha^6X^2+\alpha^3X+\alpha^{10}$$

where the representation of the field $GF(2^4)$ is that given in the book, Appendix B, Table B4 page 346.

b)

The Euclidean algorithm is applied over the received polynomial $r(X)=\alpha X^3+\alpha^{11}X^7$.

$$S_1=r(\alpha)=\alpha^7,\ S_2=r(\alpha^2)=\alpha^6,\ S_3=r(\alpha^3)=\alpha^4,\ S_4=r(\alpha^4)=\alpha^{10}$$

The syndrome polynomial is then:

$$S(X)=\alpha^7+\alpha^6X+\alpha^4X^2+\alpha^{10}X^3$$

The Euclidean Algorithm is applied using 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	$X^{n-k}=X^4$		0
0	$S(X)=\alpha^{10}X^3+\alpha^4X^2+\alpha^6X+\alpha^7$		1
1	$\alpha^5X^2+\alpha^{14}X+\alpha^6$	$\alpha^5X+\alpha^{14}$	$\alpha^3X+\alpha^3$
2	$\alpha X+\alpha^7$	α^5X	$\alpha^{10}X^2+\alpha^4X+1$

Then:

$$W_1(X)=\alpha X+\alpha^7$$
$$\sigma_1(X)=\alpha^{10}X^2+\alpha^4X+1$$

The polynomial $\sigma_1(X)$ obtained is multiplied by an element of the Galois Field $\lambda\in GF(2^4)$ in order to convert it into a monic polynomial. This value of λ is $\lambda=\alpha^5$. Then:

$$W(X)=\lambda W_1(X)=\alpha^5.(\alpha X+\alpha^7)=\alpha^6X+\alpha^{12}$$

and

$$\sigma(X)=\lambda\sigma_1(X)=\alpha^5(\alpha^{10}X^2+\alpha^4X+1)=X^2+\alpha^9X+\alpha^5$$

The Chien Search is then used to determine the roots of this error location polynomial.

These roots are found to be α^8 and α^{12}. Therefore:

$$\alpha^8 = \alpha^{-j_1} = \alpha^{-7}$$
$$j_1 = 7$$

and

$$\alpha^{12} = \alpha^{-j_2} = \alpha^{-3}$$
$$j_2 = 3$$

Errors are thus located at positions $j_1 = 7$ and $j_2 = 3$. The derivative of the error location polynomial is:

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

so the error values are:

$$e_{j_1} = \frac{W(\alpha^{-j_1})}{\sigma'(\alpha^{-j_1})} = \frac{W(\alpha^8)}{\sigma'(\alpha^8)} = \frac{\alpha^5}{\alpha^9} = \alpha^{11}$$

$$e_{j_2} = \frac{W(\alpha^{-j_2})}{\sigma'(\alpha^{-j_2})} = \frac{W(\alpha^{12})}{\sigma'(\alpha^{12})} = \frac{\alpha^{10}}{\alpha^9} = \alpha$$

The error polynomial is then:

$$e(X) = \alpha X^3 + \alpha^{11} X^7$$

and the decoded polynomial is:

$$d(X) = r(X) + e(X) = 0$$

c)

The Euclidean algorithm is applied over the received polynomial $r(X) = \alpha^8 X^5$.

$S_1 = r(\alpha) = \alpha^{13}$, $S_2 = r(\alpha^2) = \alpha^3$, $S_3 = r(\alpha^3) = \alpha^8$, $S_4 = r(\alpha^4) = \alpha^{13}$

The syndrome polynomial is then:

$$S(X) = \alpha^{13} + \alpha^3 X + \alpha^8 X^2 + \alpha^{13} X^3$$

The Euclidean Algorithm is applied using 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	$X^{n-k} = X^4$		0
0	$S(X) = \alpha^{13}X^3 + \alpha^8 X^2 + \alpha^3 X + \alpha^{13}$		1
1	α^{10}	$\alpha^2 X + \alpha^{12}$	$\alpha^2 X + \alpha^{12}$
2			

Then:

$$W_1(X) = \alpha^{10}$$
$$\sigma_1(X) = \alpha^2 X + \alpha^{12}$$

The polynomial $\sigma_1(X)$ obtained is multiplied by an element of the Galois Field $\lambda \in GF(2^4)$ in order to convert it into a monic polynomial. This value of λ is $\lambda = \alpha^{13}$. Then:

$$W(X) = \lambda W_1(X) = \alpha^{13}\alpha^{10} = \alpha^8$$

and

$$\sigma(X) = \lambda\sigma_1(X) = \alpha^{13}\left(\alpha^2 X + \alpha^{12}\right) = X + \alpha^{10}$$

The root is found to be α^{10}. Therefore:

$$\alpha^{10} = \alpha^{-j_1} = \alpha^{-5}$$
$$j_1 = 5$$

An error is located at position $j_1 = 5$. The derivative of the error location polynomial is:

$$\sigma'(X) = 1$$

so the error values are:

$$e_{j_1} = \frac{W(\alpha^{-j_1})}{\sigma'(\alpha^{-j_1})} = \frac{W(\alpha^{10})}{\sigma'(\alpha^{10})} = \frac{\alpha^8}{1} = \alpha^8$$

The error polynomial is then:

$$e(X) = \alpha^8 X^5$$

and the decoded polynomial is:

$$d(X) = r(X) + e(X) = 0$$

5.3)

a) The generator polynomial of an RS code that operates over the field $GF(2^4)$ (see Table B4) and is able to correct any error pattern of size $t=3$ or less, is obtained by doing:

$$g(X)=(X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6)=(X^2+\alpha^5X+\alpha^3)(X^2+\alpha^7X+\alpha^7)(X^2+\alpha^9X+\alpha^{11})=$$
$$(X^4+\alpha^{13}X^3+\alpha^6X^2+\alpha^3X+\alpha^{10})(X^2+\alpha^9X+\alpha^{11})=X^6+(\alpha^9+\alpha^{13})X^5+(\alpha^7+\alpha^6)X^4+(1+\alpha^9+\alpha^3)X^3+$$
$$(\alpha^2+\alpha^{12}+\alpha^{10})X^2+(\alpha^{14}+\alpha^4)X+\alpha^6=X^6+\alpha^{10}X^5+\alpha^{14}X^4+\alpha^4X^3+\alpha^6X^2+\alpha^9X+\alpha^6$$

b)

It is a RS code $C_{RS}(15,9)$.

5.4)

The received vector $\boldsymbol{r}=(000\alpha^7\,00\alpha^3\,00000\alpha^4\,00)$ is decoded by using the Euclidean and the Berlekamp-Massey algorithms.

The Euclidean algorithm is applied over the received polynomial $r(X)=\alpha^7X^3+\alpha^3X^6+\alpha^4X^{12}$.

$$S_1=r(\alpha)=\alpha^{12},\ S_2=r(\alpha^2)=1,\ S_3=r(\alpha^3)=\alpha^{14},$$
$$S_4=r(\alpha^4)=\alpha^{10},\ S_5=r(\alpha^5)=0,\ S_6=r(\alpha^6)=\alpha^{12}$$

The syndrome polynomial is then:

$$S(X)=\alpha^{12}+X+\alpha^{14}X^2+\alpha^{10}X^3+\alpha^{12}X^5$$

The Euclidean Algorithm is applied using 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	$X^{n-k}=X^6$		0
0	$S(X)=\alpha^{12}X^5+\alpha^{10}X^3+\alpha^{14}X^2+X+\alpha^{12}$		1
1	$\alpha^{13}X^4+\alpha^2X^3+\alpha^3X^2+X$	α^3X	α^3X
2	$\alpha^8X^3+\alpha^6X^2+\alpha^{14}X+\alpha^{12}$	$\alpha^{14}X+\alpha^3$	$\alpha^7X^2+\alpha^6X+1$
3	$\alpha^2X+\alpha^{13}$	$\alpha^5X+\alpha$	$\alpha^7X^3+\alpha^5X^2+\alpha^8X+\alpha$
4			

Then:

$$\sigma(X)=\lambda\sigma_1(X)=\alpha^8(\alpha^7X^3+\alpha^5X^2+\alpha^8X+\alpha)=X^3+\alpha^{13}X^2+\alpha X+\alpha^9$$

and

$$W(X) = \lambda W_1(X) = \alpha^8\left(\alpha^2 X + \alpha^{13}\right) = \alpha^{10} X + \alpha^6$$

The Chien Search is then used to determine the roots of this error location polynomial. These roots are found to be:

$$\alpha^3 = \alpha^{-j_1} = \alpha^{-12}$$
$$j_1 = 12$$

$$\alpha^9 = \alpha^{-j_2} = \alpha^{-6}$$
$$j_2 = 6$$

and

$$\alpha^{12} = \alpha^{-j_3} = \alpha^{-3}$$
$$j_3 = 3$$

Errors are thus located at positions $j_1 = 12$, $j_2 = 6$ and $j_3 = 3$. The derivative of the error location polynomial is:

$$\sigma'(X) = X^2 + \alpha$$

so the error values are:

$$e_{j_1} = \frac{W(\alpha^{-j_1})}{\sigma'(\alpha^{-j_1})} = \frac{W(\alpha^3)}{\sigma'(\alpha^3)} = \frac{\alpha^{13} + \alpha^6}{\alpha^6 + \alpha^9} = \alpha^{-11} = \alpha^4$$

$$e_{j_2} = \frac{W(\alpha^{-j_2})}{\sigma'(\alpha^{-j_2})} = \frac{W(\alpha^9)}{\sigma'(\alpha^9)} = \frac{\alpha^4 + \alpha^6}{\alpha^3 + \alpha} = \alpha^3$$

$$e_{j_3} = \frac{W(\alpha^{-j_3})}{\sigma'(\alpha^{-j_3})} = \frac{W(\alpha^{12})}{\sigma'(\alpha^{12})} = \frac{\alpha^7 + \alpha^6}{\alpha^9 + \alpha} = \alpha^7$$

The error polynomial is then:

$$e(X) = \alpha^7 X^3 + \alpha^3 X^6 + \alpha^4 X^{12}$$

and the decoded polynomial is:

$$d(X) = r(X) + e(X) = 0$$

The Berlekamp-Massey algorithm is applied over the received polynomial $r(X) = \alpha^7 X^3 + \alpha^3 X^6 + \alpha^4 X^{12}$.

$S_1 = r(\alpha) = \alpha^{12}$, $S_2 = r(\alpha^2) = 1$, $S_3 = r(\alpha^3) = \alpha^{14}$,
$S_4 = r(\alpha^4) = \alpha^{10}$, $S_5 = r(\alpha^5) = 0$, $S_6 = r(\alpha^6) = \alpha^{12}$

The Berlekamp-Massey Algorithm is applied by means of the following table:

μ	$\sigma_{BM}^{(\mu)}(X)$	d_μ	l_μ	$\mu - l_\mu$	ρ
-1	1	1	0	-1	
0	1	α^{12}	0	0	
1	$1+\alpha^{12}X$	α^7	1	0	-1
2	$1+\alpha^3 X$	1	1	1	0
3	$1+\alpha^{13}X+\alpha^5 X^2$	α^{11}	2	1	1
4	$1+\alpha^4 X+\alpha^{12} X^2$	α^{10}	2	2	2
5	$1+\alpha^9 X+\alpha^4 X^3$	α^{10}	3	2	3
6	$1+\alpha^7 X+\alpha^4 X^2+\alpha^6 X^3$		3		

The error location polynomial is then:
$\sigma_{BM}(X) = 1+\alpha^7 X+\alpha^4 X^2+\alpha^6 X^3$

whose roots are $\beta_1^{-1} = \alpha^3 = \alpha^{-12} = \alpha^{-j_1}$, $\beta_2^{-1} = \alpha^9 = \alpha^{-6} = \alpha^{-j_2}$, and $\beta_3^{-1} = \alpha^{12} = \alpha^{-3} = \alpha^{-j_3}$, so that error positions are $j_1 = 12$, $j_2 = 6$ and $j_3 = 3$.

The error location polynomial $\sigma_{BM}(X) = 1+\alpha^7 X+\alpha^4 X^2+\alpha^6 X^3$ is obtained as a function of the error location polynomial $\sigma(X) = \alpha^9 + \alpha X + \alpha^{13} X^2 + X^3$ obtained for the same case by applying the Euclidean Algorithm in the solution using the Euclidean algorithm by multiplying $\sigma_{BM}(X) = 1+\alpha^7 X+\alpha^4 X^2+\alpha^6 X^3$ by α^9. Therefore both polynomials have the same roots.
Calculation of the error values requires to forming the polynomial:

$$Z(X) = 1+(s_1+\sigma_1)X+(s_2+\sigma_1 s_1+\sigma_2)X^2+(s_3+\sigma_1 s_2+\sigma_2 s_1+\sigma_3)X^3$$

$$Z(X) = 1+(s_1+\sigma_1)X+(s_2+\sigma_1 s_1+\sigma_2)X^2+(s_3+\sigma_1 s_2+\sigma_2 s_1+\sigma_3)X^3 =$$
$$1+(\alpha^{12}+\alpha^7)X+\left(1+\alpha^7\alpha^{12}+\alpha^4\right)X^2+\left(\alpha^{14}+\alpha^7+\alpha^4\alpha^{12}+\alpha^6\right)X^3 =$$
$$Z(X) = 1+\alpha^2 X+X^2+\alpha^6 X^3$$

Then:

$$e_{j_1} = \frac{Z(\beta_1^{-1})}{\prod_{\substack{k=1 \\ k\neq 1}}^{3}\left(1+\beta_k\beta_1^{-1}\right)} = \frac{1+\alpha^5+\alpha^6+1}{(1+\alpha^6\alpha^3)(1+\alpha^3\alpha^3)} = \frac{\alpha+\alpha^3}{\alpha^7\alpha^{13}} = \frac{\alpha^9}{\alpha^5} = \alpha^4$$

$$e_{j_2} = \frac{Z(\beta_2^{-1})}{\prod_{\substack{k=1 \\ k\neq 2}}^{3}\left(1+\beta_k\beta_2^{-1}\right)} = \frac{1+\alpha^{11}+\alpha^3+\alpha^3}{(1+\alpha^{12}\alpha^9)(1+\alpha^3\alpha^9)} = \frac{\alpha^{12}}{\alpha^{13}\alpha^{11}} = \frac{\alpha^{12}}{\alpha^9} = \alpha^3$$

$$e_{j_3} = \frac{Z(\beta_3^{-1})}{\prod_{\substack{k=1 \\ k\neq 3}}^{3}\left(1+\beta_k\beta_3^{-1}\right)} = \frac{1+\alpha^{14}+\alpha^9+\alpha^{12}}{(1+\alpha^{12}\alpha^{12})(1+\alpha^6\alpha^{12})} = \frac{\alpha^{13}}{\alpha^7\alpha^{14}} = \frac{\alpha^{13}}{\alpha^6} = \alpha^7$$

The solution is exactly the same as that generated by the Euclidean algorithm.

5.5)

a) How many symbol errors can this code correct?

An RS code with symbols in $GF(2^3)$, with three information symbols, $k=3$, code length $n=7$, has the generator polynomial :

$$g(X) = (X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5) = \left(X^2+\alpha^5X+\alpha^5\right)\left(X^2+X+\alpha^2\right) =$$
$$X^4+\alpha^4X^3+\alpha^2X^2+\alpha^4X+1$$

which is of degree 4, and it has 4 roots. This allow us the construction of a system of 4 equations, thus $t=2$.

b)

We will decode the received vector $\boldsymbol{r}=(0110111)$ to determine the transmitted code vector.

The Euclidean algorithm is applied over the received polynomial $r(X) = X+X^2+X^4+X^5+X^6$.

$S_2 = r(\alpha^2) = \alpha^2$, $S_3 = r(\alpha^3) = \alpha^6$,
$S_4 = r(\alpha^4) = \alpha^4$, $S_5 = r(\alpha^5) = \alpha^3$,

The syndrome polynomial is then:

$S(X) = \alpha^2 + \alpha^6 X + \alpha^4 X^2 + \alpha^3 X^3$

The Euclidean Algorithm is applied using 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	$X^{n-k} = X^4$		0
0	$S(X) = \alpha^3 X^3 + \alpha^4 X^2 + \alpha^6 X + \alpha^2$		1
1	$\alpha^5 X^2 + \alpha^3 X + \alpha^2$	$\alpha^4 X + \alpha^5$	$\alpha^4 X + \alpha^5$
2	$\alpha^3 X + \alpha$	$\alpha^5 X + \alpha^4$	$\alpha^2 X^2 + X + \alpha^6$

Then:

$W(X) = \lambda X W_1(X) = \alpha^5 X(\alpha^3 X + \alpha) = \alpha X^2 + \alpha^6 X$

This modification over $W(X)$ takes into account the displacement of the root's positions.

$\sigma(X) = \lambda \sigma_1(X) = \alpha^5(\alpha^2 X^2 + X + \alpha^6) = X^2 + \alpha^5 X + \alpha^4$

The Chien Search is then used to determine the roots of this error location polynomial. These roots are found to be α^7 and α^4. Therefore:

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

$\alpha^4 = \alpha^{-j_2} = \alpha^{-3}$
$j_2 = 3$

Errors are thus located at positions $j_1 = 1$ and $j_2 = 3$. The derivative of the error location polynomial is:

$\sigma'(X) = \alpha^5$

so the error values are:

$$e_{j_1} = \frac{W(\alpha^{-j_1})}{\sigma'(\alpha^{-j_1})} = \frac{W(\alpha^7)}{\sigma'(\alpha^7)} = \frac{\alpha^5}{\alpha^5} = 1$$

$$e_{j_2} = \frac{W(\alpha^{-j_2})}{\sigma'(\alpha^{-j_2})} = \frac{W(\alpha^4)}{\sigma'(\alpha^4)} = \frac{\alpha^5}{\alpha^5} = 1$$

The error polynomial is then:

$$e(X) = 1 + X^3$$

and the decoded polynomial is:

$$d(X) = r(X) + e(X) = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6$$

So the decoded vector is the all ones code vector. If $m(X) = 1 + X + X^2$, then $X^4 m(X) = X^4 + X^5 + X^6$, and $X^4 m(X) \bmod g(X) = X^3 + X^2 + X + 1$, so that $c(X) = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6$ is a code polynomial.

5.6)

The redundant symbols of a ½-rate RS code over $GF(5)$ with code length 4 are given by:

$$c_1 = 4k_1 + 2k_2$$

$$c_2 = 3k_1 + 3k_2$$

(a) Find the number of code vectors, the generator matrix and the Hamming distance of the code:

Since messages are of two elements, and these elements belong to $GF(5)$, there are 5^2 codevectors.

The generator matrix is of the form:

$$G = \begin{bmatrix} 1 & 0 & 4 & 3 \\ 0 & 1 & 2 & 3 \end{bmatrix}$$

and code vectors are obtained by doing:

$$c = m \bullet G$$

0	0		0	0	0	0		w
0	1		0	1	2	3		3
0	2		0	2	4	1		3
0	3		0	3	1	4		3
0	4		0	4	3	2		3
1	0		1	0	4	3		3
1	1		1	1	1	1		4
1	2		1	2	3	4		4
1	3		1	3	0	2		3
1	4		1	4	2	0		3
2	0		2	0	3	1		3
2	1		2	1	0	4		3
2	2		2	2	2	2		4
2	3		2	3	4	0		3
2	4		2	4	1	3		4
3	0		3	0	2	4		3
3	1		3	1	4	0		3
3	2		3	2	1	0		3
3	3		3	3	3	3		4
3	4		3	4	0	1		3
4	0		4	0	1	2		3
4	1		4	1	3	0		3
4	2		4	2	0	3		3
4	3		4	3	2	1		4
4	4		4	4	4	4		4

Since the minimum weight in the above table is 3, then the minimum Hamming distance is $d_{min} = 3$.

(b) The redundant symbol equations are:
$c_1 = 4k_1 + 2k_2$
$c_2 = 3k_1 + 3k_2$

Re-arranging, and replacing negative values in $GF(5)$ gives:

$$-4k_1 - 2k_2 + c_1 = 0 = k_1 + 3k_2 + c_1$$
$$-3k_1 - 3k_2 + c_2 = 0 = 2k_1 + 2k_2 + c_2$$

Therefore $(k_1 \quad k_2 \quad c_1 \quad c_2) \bullet \boldsymbol{H}^T = \boldsymbol{0}$, where the transposed parity matrix $\boldsymbol{H}^T$ is:

$$\boldsymbol{H}^T = \begin{bmatrix} 1 & 2 \\ 3 & 2 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \boldsymbol{H} = \begin{bmatrix} 1 & 3 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{bmatrix}$$

We now compute the syndrome of the vector $\boldsymbol{r} = (1 \quad 1 \quad 3 \quad 4)$:

$$S = (1 \quad 1 \quad 3 \quad 4) \bullet \begin{bmatrix} 1 & 2 \\ 3 & 2 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = (2 \quad 3)$$

which is non-zero, indicating that the vector is not a code vector. This is confirmed by substituting the values $k_1 = k_2 = 1$ in the redundant symbol equations, which gives the result $c_1 = c_2 = 1$. So the information symbols $\boldsymbol{m} = (1 \quad 1)$ generate the code vector $\boldsymbol{c} = (1 \quad 1 \quad 1 \quad 1)$, not $(1 \quad 1 \quad 3 \quad 4)$. Computing the syndromes of the 16 possible single-symbol-error patterns enables us to find the one which generates the same syndrome as the vector $(1 \quad 1 \quad 3 \quad 4)$. This turns out to be the error pattern $(0 \quad 4 \quad 0 \quad 0)$, which when subtracted from the vector $(1 \quad 1 \quad 3 \quad 4)$ gives the code vector $(1 \quad 2 \quad 3 \quad 4)$. This code vector has Hamming distance 1 to the vector $(1 \quad 1 \quad 3 \quad 4)$. As shown in part (a) of the problem, the code has minimum Hamming distance 3, so it is single-symbol-correcting. Therefore the code vector $(1 \quad 2 \quad 3 \quad 4)$ must be the one closest to the vector $(1 \quad 1 \quad 3 \quad 4)$. This can be confirmed by generating the whole set of 25 code vectors and thus their Hamming distances to the vector $(1 \quad 1 \quad 3 \quad 4)$.

Please note that the solution to problem 5.6 assumes that the code vector format is $(k_1 \quad k_2 \quad c_1 \quad c_2)$, not $(c_1 \quad c_2 \quad k_1 \quad k_2)$ as in this and the previous chapters. It is still possible to solve the problem using the latter format, but then the vector (1134) should be changed to (3411), and also the answers need to be appropriately re-formatted.

5.7)

a) The rate of the code is equal to:

$$R_c = \frac{k}{n} = \frac{3}{5} = 0.6$$

The minimum Hamming distance is evaluated as follows:

With $\boldsymbol{G} = \begin{bmatrix} 1 & \alpha & 1 & 0 & 0 \\ 1 & \alpha^2 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

the transpose of the parity check matrix is:

$$\boldsymbol{H}^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & \alpha \\ 1 & \alpha^2 \\ 1 & 1 \end{bmatrix}$$

The parity check matrix is equal to:

$$\boldsymbol{H} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 & 1 \end{bmatrix}$$

Since there are no two columns that added result in the all-zero vector, and the addition of columns 2, 3 and 4 of the above matrix results in the all zero-vector, then the minimum distance of this code is $d_{min} = 3$.

b) The received vector $\boldsymbol{r} = (\alpha^2 \quad \alpha \quad \alpha \quad 0 \quad 1)$ is a code vector of this code.

It corresponds to the message vector $\boldsymbol{m} = (\alpha \quad 0 \quad 1)$, which is obtained by doing:

$$c = \alpha(1 \quad \alpha \quad 1 \quad 0 \quad 0) + (1 \quad 1 \quad 0 \quad 0 \quad 1) = (\alpha^2 \quad \alpha \quad \alpha \quad 0 \quad 1),$$

$\boldsymbol{S} = \boldsymbol{r} \bullet \boldsymbol{H}^T = \left(\alpha^2 + \alpha + 1 \quad \alpha^2 + \alpha + 1\right) = (0 \quad 0)$. The syndrome is the all-zero vector, and therefore this received vector is a code vector.

c)
The received vector $\boldsymbol{r} = \left(0 \quad \alpha \quad 1 \quad \alpha^2 \quad 0\right)$ contains a single error, and the first step for calculating the position and value of this error is to calculate the syndrome vector:

$$\boldsymbol{S} = \boldsymbol{r} \bullet \boldsymbol{H}^T = \left(0 \quad \alpha \quad 1 \quad \alpha^2 \quad 0\right) \bullet \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & \alpha \\ 1 & \alpha^2 \\ 1 & 1 \end{bmatrix} = (\alpha \quad \alpha)$$

Since the minimum Hamming distance of this code is $d_{min} = 3$, then the code is able to correct patterns of one symbol error.
The following is the error pattern-to-syndrome table, for patterns of one error:

e	S		e	S		e	S
10000	10		α 0000	α 0		α^2 0000	α^2 0
01000	01		0 α 000	0 α		0 α^2 000	0 α^2
00100	1 α		00 α 00	α α^2		00 α^2 00	α^2 1
00010	1 α^2		000 α 0	α 1		000 α^2 0	α^2 α
00001	11		0000 α	α α		0000 α^2	α^2 α^2

Our syndrome corresponds to an error pattern of the form (0000 α), and the decoded vector is obtained by adding the error pattern to the received vector, so that;

$$\boldsymbol{d} = \boldsymbol{r} + \boldsymbol{e} = \left(0 \quad \alpha \quad 1 \quad \alpha^2 \quad 0\right) + \left(0 \quad 0 \quad 0 \quad 0 \quad \alpha\right) = \left(0 \quad \alpha \quad 1 \quad \alpha^2 \quad \alpha\right)$$

This decoded vector is a code vector that corresponds to the message vector $\boldsymbol{m} = \left(1 \quad \alpha^2 \quad \alpha\right)$.

5.8)

a) The shortened RS code $C_{RS}(8,4)$ operating over the Galois Field $GF(2^4)$ (see Table B4) with error correction capability $t = 2$ has a generator polynomial of the form:

$$g(X) = (X + \alpha)(X + \alpha^2)(X + \alpha^3)(X + \alpha^4) = \left(X^2 + (\alpha + \alpha^2)X + \alpha^3\right)\left(X^2 + (\alpha^3 + \alpha^4)X + \alpha^7\right) =$$
$$\left(X^2 + \alpha^5 X + \alpha^3\right)\left(X^2 + \alpha^7 X + \alpha^7\right) = X^4 + \alpha^{13} X^3 + \alpha^6 X^2 + \alpha^3 X + \alpha^{10}$$

if $m_{(8,4)}(X) = \alpha^4 + \alpha^7 X + \alpha^5 X^3$
$X^{n-k} m_{(8,4)}(X) = X^4 m_{(8,4)}(X) = \alpha^4 X^4 + \alpha^7 X^5 + \alpha^5 X^7$,

and

$X^4 m_{(8,4)}(X) \bmod g(X) = \alpha^5 X^2 + \alpha X + \alpha^9$, so that,

$$c_{(8,4)}(X) = \alpha^5 X^7 + \alpha^7 X^5 + \alpha^4 X^4 + \alpha^5 X^2 + \alpha X + \alpha^9$$

b) The shortened RS code $C_{RS}(12,8)$ has the same generator polynomial as the shortened RS code $C_{RS}(8,4)$. Serial concatenation of these codes is done by setting:

$$m_{(12,8)}(X) = c_{(8,4)}(X)$$

$$X^4 m_{(12,8)}(X) = \alpha^5 X^{11} + \alpha^7 X^9 + \alpha^4 X^8 + \alpha^5 X^6 + \alpha X^5 + \alpha^9 X^4$$
$$X^4 m_{(12,8)}(X) \bmod g(X) = 0$$

This is so because the 4-position shifted vector $X^4 m_{(12,8)}(X)$ is also a code vector of the general code, and the above operation indicates that the remainder of the division is zero. This is because the two shortened RS codes are shortened versions of the same code, and a shifted version of a given codeword can also belong to the same code.
The redundancy added by the second encoder is the zero polynomial , and the concatenated code vector is:

$$c_{(12,8)}(X) = \alpha^5 X^{11} + \alpha^7 X^9 + \alpha^4 X^8 + \alpha^5 X^6 + \alpha X^5 + \alpha^9 X^4$$

c) The received vector is obtained by doing:

$$r(X) = c_{(12,8)}(X) + e(X) = \alpha^5 X^{11} + \alpha^7 X^9 + \alpha^4 X^8 + \alpha^5 X^6 + \alpha X^5 + \alpha^9 X^4 + X^3 + X^{10} + X^{11} =$$
$$\alpha^{10} X^{11} + X^{10} + \alpha^7 X^9 + \alpha^4 X^8 + \alpha^5 X^6 + \alpha X^5 + \alpha^9 X^4 + X^3$$

The syndrome vector can be directly calculated without needing to know the received polynomial $r(X)$, because we know the error pattern $e(X)$:

$$S_1 = e(\alpha) = 1$$
$$S_2 = e(\alpha^2) = 1$$
$$S_3 = e(\alpha^3) = \alpha^4$$
$$S_4 = e(\alpha^4) = 1$$

Then the syndrome polynomial is :

$$S(X) = X^3 + \alpha^4 X^2 + X + 1$$

The Euclidean Algorithm is applied using 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	$X^{n-k} = X^4$		0
0	$S(X) = X^3 + \alpha^4 X^2 + X + 1$		1
1	$\alpha^2 X^2 + \alpha X + \alpha^4$	$X + \alpha^4$	$X + \alpha^4$
2	α^{12}	$\alpha^{13} X + \alpha^7$	$\alpha^{13} X^2 + \alpha^{12} X + \alpha^{12}$

Then:

$$\sigma(X) = \lambda\sigma_1(X) = \alpha^2\left(\alpha^{13}X^2 + \alpha^{12}X + \alpha^{12}\right) = X^2 + \alpha^{14}X + \alpha^{14}$$

$$W(X) = \lambda W_1(X) = \alpha^2\alpha^{12} = \alpha^{14}$$

The Chien Search is then used to determine the roots of this error location polynomial. These roots are found to be α^6 and α^8. Therefore:

$$\alpha^6 = \alpha^{-j_1} = \alpha^{-9}$$
$$j_1 = 9$$

and

$$\alpha^8 = \alpha^{-j_2} = \alpha^{-7}$$
$$j_2 = 7$$

Errors are thus located at positions $j_1 = 9$ and $j_2 = 7$. The derivative of the error location polynomial is:

$$\sigma'(X) = \alpha^{14}$$

so the error values are:

$$e_{j_1} = \frac{W(\alpha^{-j_1})}{\sigma'(\alpha^{-j_1})} = \frac{W(\alpha^6)}{\sigma'(\alpha^6)} = \frac{\alpha^{14}}{\alpha^{14}} = 1$$

$$e_{j_2} = \frac{W(\alpha^{-j_2})}{\sigma'(\alpha^{-j_2})} = \frac{W(\alpha^8)}{\sigma'(\alpha^8)} = \frac{\alpha^{14}}{\alpha^{14}} = 1$$

The error polynomial is then:

$$e(X) = X^7 + X^9$$

and the decoded polynomial is:

$$d(X) = r(X) + e(X) = \alpha^{10}X^{11} + X^{10} + \alpha^{7}X^{9} + \alpha^{4}X^{8} + \alpha^{5}X^{6} + \alpha X^{5} + \alpha^{9}X^{4} + X^{3} + X^{7} + X^{9} =$$
$$\alpha^{10}X^{11} + X^{10} + \alpha^{9}X^{9} + \alpha^{4}X^{8} + X^{7} + \alpha^{5}X^{6} + \alpha X^{5} + \alpha^{9}X^{4} + X^{3}$$

If we now calculate the syndrome vector over the decoded vector we get:

$$S_1 = r(\alpha) = 0$$
$$S_2 = r(\alpha^2) = 0$$
$$S_1 = r(\alpha) = 0$$
$$S_4 = r(\alpha^4) = 0$$

The received vector contained three errors, and the decoder added two more errors to the received vector, which now has five errors. This is an amount of errors that is equal to the distance of this code. Thus, the decoder accepts the decoded vector as a valid vector, performing an erroneous decoding.

The error pattern $e(X) = X + X^6 + X^9$ is related to the received polynomial:

$$r(X) = c_{(12,8)}(X) + e(X) = \alpha^{5}X^{11} + \alpha^{7}X^{9} + \alpha^{4}X^{8} + \alpha^{5}X^{6} + \alpha X^{5} + \alpha^{9}X^{4} + X + X^{6} + X^{9} =$$
$$\alpha^{5}X^{11} + \alpha^{9}X^{9} + \alpha^{4}X^{8} + \alpha^{10}X^{6} + \alpha X^{5} + \alpha^{9}X^{4} + X$$

$$S_1 = e(\alpha) = \alpha^2$$
$$S_2 = e(\alpha^2) = \alpha^4$$
$$S_1 = e(\alpha) = \alpha^{12}$$
$$S_4 = e(\alpha^4) = \alpha^8$$

Then the syndrome polynomial is:

$$S(X) = \alpha^{8}X^{3} + \alpha^{12}X^{2} + \alpha^{4}X + \alpha^{2}$$

The Euclidean Algorithm is applied using 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	$X^{n-k} = X^4$		0
0	$S(X) = \alpha^{8}X^{3} + \alpha^{12}X^{2} + \alpha^{4}X + \alpha^{2}$		1
1	$\alpha^{7}X^{2} + \alpha^{7}X + \alpha^{13}$	$\alpha^{7}X + \alpha^{11}$	$\alpha^{7}X + \alpha^{11}$
2	α^{8}	$\alpha X + \alpha^{2}$	$\alpha^{8}X^{2} + \alpha^{8}X + \alpha^{6}$

Then:

$$\sigma(X) = \lambda\sigma_1(X) = \alpha^{7}\left(\alpha^{8}X^{2} + \alpha^{8}X + \alpha^{6}\right) = X^{2} + X + \alpha^{13}$$

$$W(X) = \lambda W_1(X) = \alpha^7 \alpha^8 = 1$$

The Chien Search is then used to determine the roots of this error location polynomial. This search however does not find any root. The decoder truncates the vector and it passes to the second decoder, that corresponding to the RS code $C_{RS}(8,4)$. In this process the error pattern that is of weight three is converted into an error pattern of weight two, for the second decoder.

For this second decoder, the received vector is:

$$r(X) = \alpha^5 X^7 + \alpha^9 X^5 + \alpha^4 X^4 + \alpha^{10} X^2 + \alpha X + \alpha^9$$

$$S_1 = r(\alpha) = \alpha$$
$$S_2 = r(\alpha^2) = \alpha^2$$
$$S_1 = r(\alpha) = \alpha^{13}$$
$$S_4 = r(\alpha^4) = \alpha^4$$

$$S(X) = \alpha^4 X^3 + \alpha^{13} X^2 + \alpha^2 X + \alpha$$

The Euclidean Algorithm is applied using 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	$X^{n-k} = X^4$		0
0	$S(X) = \alpha^4 X^3 + \alpha^{13} X^2 + \alpha^2 X + \alpha$		1
1	$\alpha^8 X^2 + \alpha^2 X + \alpha^6$	$\alpha^{11} X + \alpha^5$	$\alpha^{11} X + \alpha^5$
2	α	$\alpha^{11} X$	$\alpha^7 X^2 + \alpha X + 1$

Then:

$$\sigma(X) = \lambda \sigma_1(X) = \alpha^8 \left(\alpha^7 X^2 + \alpha X + 1\right) = X^2 + \alpha^9 X + \alpha^8$$

$$W(X) = \lambda W_1(X) = \alpha^8 \alpha = \alpha^9$$

The Chien Search is then used to determine the roots of this error location polynomial. These roots are found to be α^{10} and α^{13}. Therefore:

$$\alpha^{10} = \alpha^{-j_1} = \alpha^{-5}$$
$$j_1 = 5$$

and

$$\alpha^{13} = \alpha^{-j_2} = \alpha^{-2}$$
$$j_2 = 2$$

Errors are thus located at positions $j_1 = 5$ and $j_2 = 2$. The derivative of the error location polynomial is:

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

so the error values are:

$$e_{j_1} = \frac{W(\alpha^{-j_1})}{\sigma'(\alpha^{-j_1})} = \frac{W(\alpha^{10})}{\sigma'(\alpha^{10})} = \frac{\alpha^9}{\alpha^9} = 1$$

$$e_{j_2} = \frac{W(\alpha^{-j_2})}{\sigma'(\alpha^{-j_2})} = \frac{W(\alpha^{13})}{\sigma'(\alpha^{13})} = \frac{\alpha^9}{\alpha^9} = 1$$

The error polynomial is then:

$$e(X) = X^5 + X^2$$

The decoded vector is then:

$$d(X) = r(X) + e(X) = \alpha^5 X^7 + \alpha^9 X^5 + \alpha^4 X^4 + \alpha^{10} X^2 + \alpha X + \alpha^9 + X^5 + X^2 =$$
$$\alpha^5 X^7 + \alpha^7 X^5 + \alpha^4 X^4 + \alpha^5 X^2 + \alpha X + \alpha^9 ,$$

Since $S(X) = 0$ for the decoded polynomial, the decoded polynomial is a code polynomial, and the decoded message is $m(X) = \alpha^5 X^3 + \alpha^7 X + \alpha^4$.
The error pattern of weight 3 was converted by the truncation process into an error pattern of weight 2, thus, it was successfully decoded by the second decoder.

5.9)

The use of an interleaver in the middle of the serial concatenation of two shortened RS codes is similar to the way it is used in the coding scheme of a CD. The idea is to distribute burst errors typically present in this sort of channels, into different codewords. A given block code collapses when the number of errors per received word is larger than the number of errors the code can correct. A burst of errors easily makes the corresponding code collapse.
In a common way of using this concatenated code, the first decoder tries to decode the received vector, and when it is not able to correct the error pattern (a burst error pattern), it passes the truncated received vector to the second decoder. This second decoder is able to correct up to 2 symbol errors in the received vector per word. Thus, the error event that makes the scheme collapse is an error event of 3 elements per word. For this to happen, and due to the action of the interleaver seen in the figure below, a burst of 17 elements in

error makes the second decoder be not able to correct that pattern. Therefore the scheme is able to correct a burst of up to 16 elements, in this case, a burst of 64 bits.
However and in the case of burst error channels, we can think of using the proposed scheme in the following manner, which is based on the concept of the erasure channel: The first decoder only detects errors, and in case of detecting a non-zero syndrome, erasures all the received elements of the received vector and indicates to the second decoder where are the errors. This second decoder now can use its system of 4 equations to determine 4 values of errors, because it knows their positions. Thus, the error event that makes the scheme collapse is an error event of 5 elements per word. For this to happen, and due to the action of the interleaver seen in the figure below, a burst of 33 elements in error makes the second decoder be not able to correct that pattern. Therefore the scheme is able to correct a burst of up to 32 elements, in this case, a burst of 128 bits.