3.1) The polynomial $1+X+X^3+X^4$ is a generator polynomial of a binary linear cyclic block code with code length $n \le 7$ if this polynomial is a factor of X^n+1, with $n = 5,6,7$. The number of redundant bits is $r = 4$

$n = 7$

$$\begin{array}{ll} X^7+1 & ! \quad X^4+X^3+X+1 \\ X^7+X^6+X^4+X^3 & \quad X^3+X^2+X \\ \hline X^6+X^4+X^3+X+1 & \\ X^6+X^5+X^3+X^2 & \\ \hline X^5+X^4+X^2+1 & \\ X^5+X^4+X^2+X & \\ \hline X+1 & \end{array}$$

This polynomial can not generate a cyclic code $C_{cyc}(7,3)$

$n = 6$

$$\begin{array}{ll} X^6+1 & ! \quad X^4+X^3+X+1 \\ X^6+X^5+X^3+X^2 & \quad X^2+X+1 \\ \hline X^5+X^3+X^2+1 & \\ X^5+X^4+X^3+X & \\ \hline X^4+X^3+X+1 & \\ X^4+X^3+X+1 & \\ \hline 0 & \end{array}$$

This polynomial can generate a cyclic code $C_{cyc}(6,2)$

$n = 5$

$$
\begin{array}{lll}
X^5+1 & ! & X^4+X^3+X+1 \\
X^5+X^4+X^2+X & & X+1 \\
\hline
X^4+X^2+X+1 & & \\
X^4+X^3+X+1 & & \\
\hline
X^3+X^3 & &
\end{array}
$$

This polynomial can not generate a cyclic code $C_{cyc}(5,1)$

3.2) Cyclic code $C_{cyc}(8,5)$

$$
\begin{array}{lll}
X^8+1 & ! & X^3+X^2+X+1 \\
X^8+X^7+X^6+X^5 & & X^5+X^4+X+1 \\
\hline
X^7+X^6+X^5+1 & & \\
X^7+X^6+X^5+X^4 & & \\
\hline
X^4+1 & & \\
X^4+X^3+X^2+X & & \\
\hline
X^3+X^2+X+1 & & \\
X^3+X^2+X+1 & & \\
\hline
0 & &
\end{array}
$$

The polynomial $g(X)=1+X+X^2+X^3$ is a generator polynomial of a cyclic code $C_{cyc}(8,5)$

If the message is $\boldsymbol{m}=(10101)$, that is, $m(X)=1+X^2+X^4$

$X^{n-k}m(X)=X^3m(X)=X^3+X^5+X^7$

$$
\begin{array}{ll}
X^7 + X^5 + x^3 & ! \quad X^3 + X^2 + X + 1 \\
X^7 + X^6 + X^5 + X^4 & X^4 + X^3 + X^2 + X \\
\hline
X^6 + X^4 + X^3 & \\
X^6 + X^5 + X^4 + X^3 & \\
\hline
X^5 & \\
X^5 + X^4 + X^3 + X^2 & \\
\hline
X^4 + X^3 + X^2 & \\
X^4 + X^3 + X^2 + X & \\
\hline
p(X) = X &
\end{array}
$$

Then

$c(X) = X + X^3 + X^5 + X^7$, $\quad \boldsymbol{c} = (01010101)$

3.3)

a) Since $r = 4 = n - k$, $\Rightarrow \; k = 3$

Code rate is equal to $R_c = 3/7 = 0.43$

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

rows 1+2 replaces row 2 $\quad \boldsymbol{G}' = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$

rows 1+2+3 replaces row 3 $\quad \boldsymbol{G}'' = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

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

Code table:

	m						***c***					w
0	0	0		0	0	0	0	0	0	0		4
0	0	1		0	1	1	1	0	0	1		4
0	1	0		1	1	1	0	0	1	0		4
0	1	1		1	0	0	1	0	1	1		4
1	0	0		1	0	1	1	1	0	0		4
1	0	1		1	1	0	0	1	0	1		4
1	1	0		0	1	0	1	1	1	0		4
1	1	1		0	0	1	0	1	1	1		4

Minimum distance $d_{min} = w_{min} = 4$, then

$t = 1,\ l = 3$

b) Code vector for the all ones message is $\boldsymbol{c} = (0010111)$ in systematic form, obtained by adding the three rows of the generator matrix ***G"***

c) The syndrome corresponding to an error in the first information symbol corresponds to an error pattern $\boldsymbol{e} = (1000000)$, or $e(X) = 1$. The corresponding syndrome is calculated as $S(X) = e(X) \bmod g(X)$:

$1 \qquad / X^4 + X^3 + X^2 + 1$

$1 \qquad\qquad 0$

This can be also determined multiplying $\boldsymbol{e} = (1000000)$ by the transpose of the parity check matrix $\boldsymbol{H}^T$, which results $\boldsymbol{S} = (1000)$. As an example, the received vector $\boldsymbol{r} = (1111001)$ is the second code vector in the above table, containing one error in the first bit. Thus, $r(X) = 1 + X + X^2 + X^3 + X^6$, and:

$$X^6 + X^3 + x^2 + X + 1 \quad ! \quad X^4 + X^3 + X^2 + 1$$
$$X^6 + X^5 + X^4 + X^2 \qquad\qquad X^2 + X$$

$$X^5 + X^4 + X^3 + X + 1$$
$$X^5 + X^4 + X^3 + X$$

$$S(X) = 1$$

Since $S(X) = r(X) \bmod g(X) = 1$, then the error is at the first position. By inspection of the transpose of the parity check matrix $\boldsymbol{H}^T$, we can see that there are seven different syndrome vector to be used for correcting any error pattern of size $t = 1$

3.4) Define what is meant by a cyclic error control code

3.5) A binary linear cyclic block code $C_{cyc}(n,k)$ has code length $n = 14$ and generator polynomial $g(X) = 1 + X^3 + X^4 + X^5$:

a) Since $r = n - k = 5, \quad k = 9$

For the all ones input vector

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

$$X^{n-k} m(X) = X^5 m(X) = X^5 + X^6 + X^7 + X^8 + X^9 + X^{10} + X^{11} + X^{12} + X^{13}$$

$$X^{13}+X^{12}+x^{11}+X^{10}+X^{9}+X^{8}+X^{7}+X^{6}+x^{5} \quad ! \quad X^{5}+X^{4}+X^{3}+1$$
$$X^{13}+X^{12}+X^{11}\qquad\qquad +X^{8}\qquad\qquad\qquad X^{8}+X^{5}+X^{3}$$

$$\_\_\_\_\_$$
$$X^{10}+X^{9}+X^{7}+X^{6}+X^{5}$$
$$X^{10}+X^{9}+X^{8}\qquad +X^{5}$$

$$\_\_\_\_\_$$
$$X^{8}+X^{7}+X^{6}$$
$$X^{8}+X^{7}+X^{6}+X^{3}$$

$$\_\_\_\_\_$$
$$p(X)=X^{3}$$

Then, $c(X)=X^{3}+X^{5}+X^{6}+X^{7}+X^{8}+X^{9}+X^{10}+X^{11}+X^{12}+X^{13}$, or

$$\boldsymbol{c}=(00010111111111)$$

b)

An error in the last bit is represented by the error pattern polynomial $e(X)=X^{13}$. The syndrome calculation consists on taking the remainder of the following polynomial division:

$$X^{13} \quad ! \quad X^5 + X^4 + X^3 + 1$$

$$X^{13} + X^{12} + X^{11} + X^8 \qquad X^8 + X^7 + X^5 + X^4 + X^3 + X^2$$

$$\_\_\_\_\_$$

$$X^{12} + X^{11} + X^8$$

$$X^{12} + X^{11} + X^{10} + X^7$$

$$\_\_\_\_\_$$

$$X^{10} + X^8 + X^7$$

$$X^{10} + X^9 + X^8 + X^5$$

$$\_\_\_\_\_$$

$$X^9 + X^7 + X^5$$

$$X^9 + X^8 + X^7 + X^4$$

$$\_\_\_\_\_$$

$$X^8 + X^5 + X^4$$

$$X^8 + X^7 + X^6 + X^3$$

$$\_\_\_\_\_$$

$$X^7 + X^6 + X^5 + X^4 + X^3$$

$$X^7 + X^6 + X^5 + X^2$$

$$\_\_\_\_\_$$

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

This code can correct this error pattern. If for instance we have the received vector $r(X) = X^3 + X^5 + X^6 + X^7 + X^8 + X^9 + X^{10} + X^{11} + X^{12}$, which is the code vector for the all ones input message containing an error in the last bit, the calculated syndrome polynomial is $S(X) = X^4 + X^3 + X^2$.

c) Can cyclic codes be non-linear?

Cyclic codes can be non-linear. This condition is verified when the addition of two code vectors of the code does not belong to the code. The code however will lose all the characteristics of a linear block code.

3.6)

a) The code table is obtained by polynomial division

$\boldsymbol{m} = (01)$, $m(X) = X$, $X^{n-k} m(X) = X^4 m(X) = X^5$

X^5 ! $X^4 + X^3 + X + 1$

$X^5 + X^4 + X^2 + X$ $X + 1$

$X^4 + X^2 + X$

$X^4 + X^3 + X + 1$

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

then , $c(X) = X^5 + X^3 + X^2 + 1$, $\boldsymbol{c} = (101101)$

$\boldsymbol{m} = (10)$, $m(X) = 1$, $X^{n-k} m(X) = X^4 m(X) = X^4$

X^4 ! $X^4 + X^3 + X + 1$

$X^4 + X^3 + X + 1$ 1

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

then , $c(X) = X^4 + X^3 + X + 1$, $\boldsymbol{c} = (110110)$

$\boldsymbol{m} = (11)$, $m(X) = 1 + X$, $X^{n-k} m(X) = X^4 m(X) = X^4 + X^5$

$X^5 + X^4$! $X^4 + X^3 + X + 1$

$X^5 + X^4 + X^2 + X$ X

$p(X) = X^2 + X$

then , $c(X) = X^5 + X^4 + X^2 + X$, $\boldsymbol{c} = (011011)$

m					***c***				w
0	0		0	0	0	0	0	0	0
0	1		1	0	1	1	0	1	4
1	0		1	1	0	1	1	0	4
1	1		0	1	1	0	1	1	4

b)

$d_{min} = 4, \quad t = 1, \quad l = 3$

3.7)

a)

$r = 6$, $\qquad n - k = r = 6$, $\qquad k = 8$

b)

number of code vectors $2^k = 2^8 = 256$

c) The generator matrix is

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

By using Gaussian elimination, the generator matrix in systematic form is:

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

$$\boldsymbol{H}^{T} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{matrix} \\ \\ \\ (*) \\ \\ \\ \\ \\ \\ \\ \\ (*) \\ \\ (*) \end{matrix}$$

d) Rows of $\boldsymbol{H}^{T}$ indicated with a $(*)$ are three rows that added, results into the all zero vector, and thus, the minimum Hamming distance of this code is $d_{min} = 3$

e) For an error pattern of $(n-k)$ or less consecutive error positions, $e(X) = X^{j}B(X)$, where $1 \le X^{j} \le X^{n-1}$. Then,

$$deg\,ree(B(X)) \le n-k-1$$

Since $deg\,ree(g(X)) = n-k$, then $g(X)$ can not divide $B(X)$.

On the other hand $g(X).\alpha(X) = X^{n}+1$ and X is not a factor of $g(X)$, so that X^{j} is neither a factor of $g(X)$, and thus X^{j} and $g(X)$ are co-prime polynomials. Therefore $g(X)$ can not divide $e(X)$ and the corresponding syndrome is zero. This means that an error pattern of $(n-k)$ or less consecutive error positions is correctable. In this case $n-k=6$.

3.8)

a) The code vector in systematic form of the message vector $\boldsymbol{m} = (11001101011)$ is evaluated as follows:

$$m(X) = 1 + X + X^4 + X^5 + X^7 + X^9 + X^{10}$$

$$X^{n-k} m(X) = X^4 m(X) = X^4 + X^5 + X^8 + X^9 + X^{11} + X^{13} + X^{14}$$

$$\begin{array}{ll} X^{14} + X^{13} + x^{11} + X^9 + X^8 + X^5 + X^4 & ! \quad X^4 + X + 1 \\ X^{14} \quad + X^{11} + X^{10} & X^{10} + X^9 + X^4 \\ \hline X^{13} + X^{10} + X^9 + X^8 + X^5 + X^4 & \\ X^{13} + X^{10} + X^9 & \\ \hline X^8 + X^5 + X^4 & \\ X^8 + X^5 + X^4 & \\ \hline p(X) = 0 & \end{array}$$

$$c(X) = X^4 + X^5 + X^8 + X^9 + X^{11} + X^{13} + X^{14}$$

b) The received vector $\boldsymbol{r} = (000010001101011)$ is the code vector of item a) affected by an error in the fifth position

$$r(X) = X^4 + X^8 + X^9 + X^{11} + X^{13} + X^{14}$$

We calculate the syndrome as:

$$X^{14} + X^{13} + x^{11} + X^9 + X^8 + X^4 \quad ! \quad X^4 + X + 1$$
$$X^{14} + X^{11} + X^{10} \qquad\qquad X^{10} + X^9 + X^4 + X$$

$$X^{13} + X^{10} + X^9 + X^8 + X^4$$
$$X^{13} + X^{10} + X^9$$

$$X^8 + X^4$$
$$X^8 + X^5 + X^4$$

$$X^5$$
$$X^5 + X^2 + X$$

$$S(X) = X^2 + X$$

And the syndrome polynomial $S(X) = X^2 + X$ is the same as that corresponding to the error pattern $e(X) = X^5$, which identifies an error at the fifth position.