Information Theory & Coding
(5CS3-01)

Unit-4 Notes

Vision of the Institute

To become a renowned center of outcome based learning and work towards academic, professional, cultural and social enrichment of the lives of individuals and communities.

Mission of the Institute

M1- Focus on evaluation of learning outcomes and motivate students to inculcate research aptitude by project based learning.

M2- Identify, based on informed perception of Indian, regional and global needs, the areas of focus and provide platform to gain knowledge and solutions.

M3- Offer opportunities for interaction between academia and industry.

M4- Develop human potential to its fullest extent so that intellectually capable and imaginatively gifted leaders can emerge in a range of professions.

Vision of the Department

To become renowned Centre of excellence in computer science and engineering and make competent engineers & professionals with high ethical values prepared for lifelong learning.

Mission of the Department

M1-To impart outcome based education for emerging technologies in the field of computer science and engineering.

M2-To provide opportunities for interaction between academia and industry.

M3- To provide platform for lifelong learning by accepting the change in technologies

M4- To develop aptitude of fulfilling social responsibilities.

Program Outcomes (PO)

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis**: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions**: Design solutions for complex engineering problemsand design system components or processes that meet thespecified needs with appropriate consideration for the public health and safety, andthe cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issuesand the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Program Educational Objectives (PEO)

1. To provide students with the fundamentals of Engineering Sciences with more emphasis in **Computer Science &Engineering** by way of analyzing and exploiting engineering challenges.
2. To train students with good scientific and engineering knowledge so as to comprehend, analyze, design, and create novel products and solutions for the real life problems.
3. To inculcate professional and ethical attitude, effective communication skills, teamwork skills, multidisciplinary approach, entrepreneurial thinking and an ability to relate engineering issues with social issues.
4. To provide students with an academic environment aware of excellence, leadership, written ethical codes and guidelines, and the self-motivated life-long learning needed for a successful professional career.
5. To prepare students to excel in Industry and Higher education by Educating Students along with High moral values and Knowledge

Program Specific Outcomes (PSO)

PSO1: Ability to interpret and analyze network specific and cyber security issues, automation in real word environment.

PSO2: Ability to Design and Develop Mobile and Web-based applications under realistic constraints.

Course Outcome:

CO1: Apply the fundamental concepts of information theory viz. entropy, mutual information and channel capacity in communication system.

CO2: Examine the principles of source coding and data transmission.

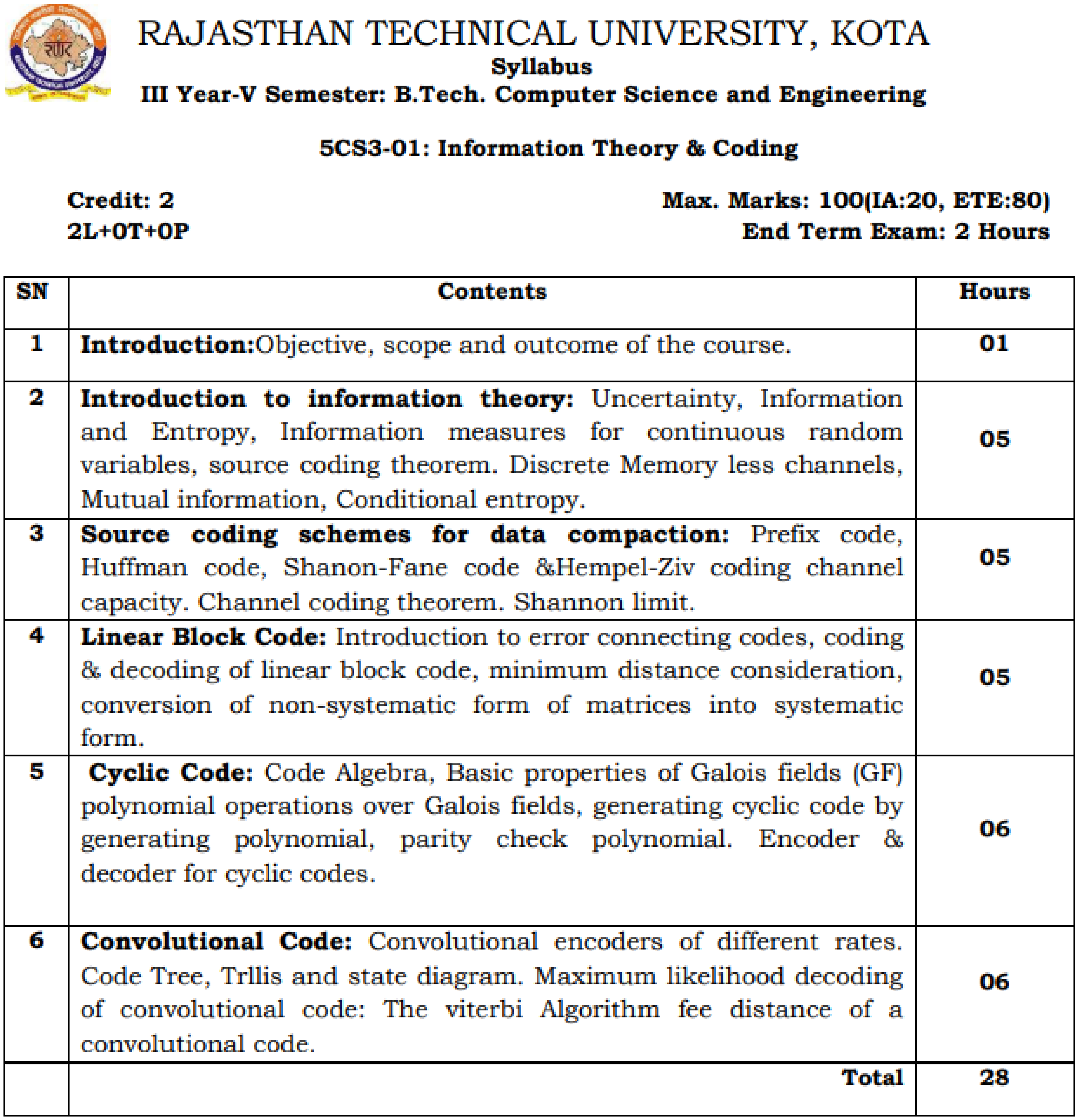
CO3: Analyze linear block code, cyclic code and Convolution code.

CO4: Evaluate information theoretic methods to novel settings of encoding and decoding techniques.

CO-PO Mapping:

CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO12
Apply the fundamental concepts of information theory viz. entropy, mutual information and channel capacity in communication system.	3	2	2	2	1	1	1	1	1	1	1	3
Examine the principles of source coding and data transmission.	3	3	3	3	2	1	1	1	1	1	1	3
Analyze linear block code, cyclic code and Convolution code.	3	3	3	2	1	1	1	1	1	1	1	3
Evaluate information theoretic methods to novel settings of encoding and decoding techniques.	3	3	3	2	1	1	1	1	1	1	1	3

SYLLABUS:



RAJASTHAN TECHNICAL UNIVERSITY, KOTA

Syllabus

III Year-V Semester: B.Tech. Computer Science and Engineering

5CS3-01: Information Theory & Coding

Credit: 2
2L+0T+0P

Max. Marks: 100(IA:20, ETE:80)
End Term Exam: 2 Hours

SN	Contents	Hours
1	**Introduction:**Objective, scope and outcome of the course.	01
2	**Introduction to information theory:** Uncertainty, Information and Entropy, Information measures for continuous random variables, source coding theorem. Discrete Memory less channels, Mutual information, Conditional entropy.	05
3	**Source coding schemes for data compaction:** Prefix code, Huffman code, Shanon-Fane code &Hempel-Ziv coding channel capacity. Channel coding theorem. Shannon limit.	05
4	**Linear Block Code:** Introduction to error connecting codes, coding & decoding of linear block code, minimum distance consideration, conversion of non-systematic form of matrices into systematic form.	05
5	**Cyclic Code:** Code Algebra, Basic properties of Galois fields (GF) polynomial operations over Galois fields, generating cyclic code by generating polynomial, parity check polynomial. Encoder & decoder for cyclic codes.	06
6	**Convolutional Code:** Convolutional encoders of different rates. Code Tree, Trllis and state diagram. Maximum likelihood decoding of convolutional code: The viterbi Algorithm fee distance of a convolutional code.	06
	Total	**28**

LECTURE PLAN:

Unit No./ Total lec. Req.	Topics	Lect. Req.
	Objective, Scope & Outcome of the Course	1
Unit-1	Introduction to information theory, Uncertainty, Entropy	1
	Information measures for continuous random variables	1
	Numerical problem on entropy	1
	Source coding theorem, Discrete memory less channels	1
	Mutual information, Conditional entropy	1
Unit-2	Prefix code, Huffman coding	1
	Shannon – fanon coding	1
	Numerical on haffman and shanon fano coding	1
	Hempel-Ziv coding	1
	Channel capacity, Channel coding theorem, Shannon limit	1
Unit-3	Introduction to error correcting codes	1
	Coding and decoding of linear block code	1
	Numerical problem on Linear block code	1
	Error correcting codes, Minimum distance consideration	1
	Conversion of non symmetric form of matrix into symmetric form	1
Unit-4	Code algebra	1
	Basic properties of Galois Field(GF)	1
	Polynomial operation over Galois field	1
	Generating cyclic code by generating polynomial	1
	Numerical Problems on generator polynomial	1
	Parity check polynomial , Encoder and decoder for cyclic codes	1
Unit-5	Convolutional encoders of different rates	1
	Code tree	1
	Trellis diagram	1
	state diagram	1
	Maximum likelihood decoding of convolution code	1
	Viterbi algorithm, Free distance of convolution codes	1

UNIT-4

Anoop

Binary cyclic codes!- Binary cyclic code are an important Subclass of linear block codes. These code can be easily implemented using feedback shift registers.

The advantages of Binary cyclic codes over linear block codes are:-

1. Encoding & Syndrome calculation can be easily implement using simple shift registers with feedback connections.
2. BCC have a fair amount of mathematical structure that usefull to design codes with useful error correcting Properties.

An (n,k) linear code is called a cyclic code if it can be described by the following properties:

(a) linear
(b) cyclic

· If the n tuple $V = (v_0, v_1, v_2 --- v_{n-1})$ is a codeword in the subspace S, than

$$v^{(1)} = (v_{n-1}, v_0, v_1, v_2 --- v_{n-2})$$

obtain by an end around shift, is also a codeword in S.

The component of a codeword $V = (v_0, v_1 --- v_{n-1})$ can be written as, in the form of Polynomial

$$V(x) = v_0 + v_1 x + v_2 x^2 + --- v_{n-1} x^{n-1}$$

Q: A cyclic (7,3) code has the generator polynomial

$$g(x) = x^4 + x^2 + x + 1$$

find the generator matrix for this code. further find the minimum distance for this code.

Soln The generator matrix for the given (7,3) cyclic code with the generator Polynomial

$$g(x) = x^4 + x^2 + x + 1$$ is given by

$$G = \begin{bmatrix} x^{K-1} g(x) \\ x^{K-2} g(x) \\ \vdots \\ g(x) \end{bmatrix} = \begin{bmatrix} x^{3-1} g(x) \\ x^{3-2} g(x) \\ x^{3-3} g(x) \end{bmatrix} = \begin{bmatrix} x^2 g(x) \\ x\, g(x) \\ g(x) \end{bmatrix}$$

$$\Rightarrow G = \begin{bmatrix} x^6 + x^4 + x^3 + x^2 \\ x^5 + x^3 + x^2 + x \\ x^4 + x^2 + x + 1 \end{bmatrix}$$

$$\Rightarrow G = \left[\begin{array}{ccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] \qquad G = [I_K | P]$$

the above matrix is not in it's Systematic form. So we use elementary row transformations as

$R_1 \rightarrow R_1 + R_3$

Not column transfer bcoz $P \neq I$

$$\Rightarrow G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \quad \text{———} \quad ①$$

The above matrix can be written as -

$$G = [I_K | P] \Rightarrow [I_3 | P]$$

where $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $P = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$

Since $K=3$ then $2^K = 2^3 = 8$ Messages.

So data words are

(000) (001) (010) (011) (100) (101) (110) (111).

The corresponding codewords are obtained by using the relation $c = DG$ as follows.

$$m = (000) \Rightarrow c = [000]\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] = (000\,\underline{0000}) \quad 0$$

$$m = (001) \Rightarrow c = [001]\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] = [001\,\underline{0111}]$$

$$m = [010] \Rightarrow c = [010]\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] = [0101110]$$

$$m = [011] \Rightarrow c = [011]\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] = [0111001]$$

$$m = [100] \Rightarrow c = [100]\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] = [1001011]$$

$$m = [101] \Rightarrow c = [101]\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] = [1011100]$$

$$m = [110] \Rightarrow c = [110]\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] = [1100101]$$

$$m = [111] \Rightarrow c = [111]\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] = [1110010]$$

Since the minimum distance between any two codewords is 4, therefore the minimum distance of this code is 4.

Encoding (Systemetic form) of Binary cyclic code:-

By using some algebric properties of the cyclic codes, it is possible to establish a Systematic encoding Procedure. The message vector in the Polynomial form is given by:-

$$M(X) = M_0 + M_1 X + M_2 X^2 + \cdots + M_{K-1} X^{K-1} \quad \text{—①}$$

in Systematic form, the message digits are utilized as a part of the codeword. The message polynomial can be manipulate algebraically by shifting the message digits into the rightmost K stages of a codeword Register, and then adding the parity digits by placing them in the leftmost n-K stages. multiply M(X) by X^{n-K}, the right shifted message polynomial is

$$X^{n-K} M(X) = M_0 X^{n-K} + M_1 X^{n-K+1} + \cdots + M_{K-1} X^{n-1} \quad \text{—②}$$

divide eq^n ② by g(X)

$$X^{n-K} m(X) = \underset{\text{Quotient}}{q(X)}\, g(X) + \underset{\text{Remainder}}{r(X)} \quad \text{—③}$$

where remainder can be expressed as

$$r(X) = r_0 + r_1 X + r_2 X^2 + \cdots + r_{n-K-1} X^{n-K-1}$$

or

$$r(X) = X^{n-K} m(X) \text{ modulo } g(X)$$

by using eq^n ③

$$r(X) + X^{n-K} m(X) = q(X)\, g(X) = V(X) \quad \text{—④}$$

the left hand side of eq^n ④ is a valid codeword of degree ~~n-K~~ n-1 or less, and when its polynomial is divided by g(X) there is a zero reminder. This codeword can be expanded into its polynomial as follows:-

$$r(X) + X^{n-K} m(X) = r_0 + r_1 X + r_2 X^2 + \cdots + r_{n-K-1} X^{n-K-1} + m_0 X^{n-K} + m_1 X^{n-K+1} + m_{K-1} X^{n-1}$$

The codeword polynomial corresponds to code vector

$$V = \underbrace{r_0, r_1 --- r_{n-K-1}}_{(n-K)\text{ Parity check bits}},\ \underbrace{m_0, m_1, --- m_{K-1}}_{K\text{ message bits}} \quad — ⑤$$

Q: The generator Polynomial of a (7,4) cyclic code is $g(x) = 1 + X + X^3$. find codeword for message vector 1011 in the following ways:-

a) by forming the code Polynomial using

$$V(X) = g(X)\, m(X)$$

where $m(X)$ = message Polynomial

b) by using systematic encoding method.

Soln a) message vector $= M = (m_0\, m_1\, m_2\, m_3) = 1011$

so message polynomial

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

Now codepolynomial

$$V(X) = m(X)\, g(X)$$

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

$$= 1+X+\underline{X^3}+X^2+\underline{X^3}+X^5+\underline{X^3}+X^4+X^6$$

$$\Rightarrow 1+X+X^2+\underline{X^3}+X^4+X^5+X^6 \qquad [\text{using } X \oplus X = 0]$$

and $V = (\underline{111}\ \underline{0111})$

b) in systematic form

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

$n = 7$, $K = 4$.

$n - K = 7 - 4 = 3$.

$$X^{n-K} m(X) = X^3(1+X^2+X^3) = X^3 + X^5 + X^6$$

Divide $X^{n-K} m(X)$ by $g(X)$ using Polynomial division,

we can write

$$\frac{\text{Data polynomial} \rightarrow X^3+X^5+X^6}{\rightarrow 1+X+X^3} = \underbrace{(1+X+X^2+X^3)}_{\text{Quotient } q(X)} + \underbrace{1}_{\text{Remainder } r(X)}$$

$$x^3+x+1 \overline{\big) x^6+x^5+x^3} \big(x^3+x^2+x+1$$

$$x^6+x^4+x^3$$

$$x^5+x^4$$

$$x^5+x^3+x^2$$

$$x^4+x^3+x^2$$

$$x^4+x^2+x$$

$$x^3+x$$

$$x^3+x+1$$

$$1$$

So Code Polynomial

$$V(x) = r(x) + x^3 m(x)$$

$$V(x) = r(x) + x^{n-k} m(x)$$

$$= 1 + x^3 + x^5 + x^6$$

and code $v = \underbrace{100}_{\text{parity}}\underbrace{1011}_{\text{Message bit}}$

Q. Construct a Systematic (7,4) cyclic code using the generator Polynomial $k=4$

$$g(x) = x^3+x^2+1$$

Sol^n we have to construct a cyclic code in which the numbers of data ~~words~~ bits are 4 and numbers of check numbers of data bits are 4 and numbers of code bits are 7 i.e. bits are 3, so that the number of code bits are 7 i.e.

$$n = 7 \text{ and } K=4$$

The generator polynomial is $g(x) = x^3+x^2+1$. The total number of data words possible are $2^4=16$. we consider the following data word

$$M = [1010]$$

The corresponding data Polynomial is

$$M(x) = x^3 + 0x^2 + x + 0(1) = x^3+x$$

further $x^{n-k} m(x) = x^{7-4}(x^3+x)$

$= x^3(x^3+x)$

$= \underline{x^6+x^4}$

Hence ~~$V(X)=$~~

$$\begin{array}{r|l|l}
x^3+x^2+1 & x^6+x^4 & x^3+x^2+1 \leftarrow q(x) \\
 & x^6+x^5+x^3 & \\
\hline
 & x^5+x^4+x^3 & \\
 & x^5+x^4+x^2 & \\
\hline
 & x^3+x^2 & \\
 & x^3+x^2+1 & \\
\hline
 & 1 \leftarrow r(x) &
\end{array}$$

Therefore the code polynomial corresponding to the data Polynomial $m(x) = x^3+x$ is given by,

$$V(X) = x^{n-k} m(X) + r(X)$$

where $r(X)$ is the remainder obtained by dividing $x^{n-k} m(X)$ by generator polynomial $g(X)$.

$\therefore V(X) = x^3(x^3+x)+1 = x^6+x^4+1$

the code polynomial can also be obtain by using

$$\boxed{V(X) = g(X)\, q(X)}$$

where $g(x)$ is the generator Polynomial and $q(x)$ is the quotient obtained on dividing $x^{n-k} m(x)$ by $g(x)$.

$\therefore V(X) = (x^3+x^2+1)(x^3+x^2+1)$

$= x^6+x^5+x^3+x^5+x^4+x^2+x^3+x^2+1$

$= x^6+(x^5+x^5)+x^4+(x^3+x^3)+(x^2+x^2)+1$

$= x^6+x^4+1$

Now the code Polynomial converted into corresponding code vector is $V(X) = x^6+x^4+1 = x^6+0x^5+x^4+0x^3+0x^2+0x+1$ ~~is~~ $= (1\,0\,1\,0\,0\,0\,1)$

As an alternative we can construct the entire code by the use of generator Matrix G. the generator matrix G for a (n, K) cyclic code is given by

$$G=\begin{bmatrix} x^{K-1}g(x) \\ x^{K-2}g(x) \\ \vdots \\ g(x) \end{bmatrix} = \begin{bmatrix} g_0 g_1 \cdots\cdots g_{n-k} & 0 \; 0 \cdots\cdots 0 \\ 0 g_0 g_1 \cdots\cdots g_{n-k} & 0 \cdots\cdots 0 \\ \cdots\cdots & \cdots\cdots \\ 0 0 0 \cdots\cdots g_0 g_1 & \cdots\cdots g_{n-k} \end{bmatrix}$$

there $g(x) = x^3+x^2+1$ and $K=4$, therefore

$$\Rightarrow G = \begin{bmatrix} x^3g(x) \\ x^2g(x) \\ x\,g(x) \\ g(x) \end{bmatrix} = \begin{bmatrix} x^3(x^3+x^2+1) \\ x^2(x^3+x^2+1) \\ x(x^3+x^2+1) \\ x^3+x^2+1 \end{bmatrix} = \begin{bmatrix} x^6+x^5+x^3 \\ x^5+x^4+x^2 \\ x^4+x^3+x \\ x^3+x^2+1 \end{bmatrix}$$

$$\Rightarrow G = \begin{bmatrix} x^6+x^5+0x^4+x^3+0x^2+0x+0 \\ 0x^6+x^5+x^4+0x^3+x^2+0x+0 \\ 0x^6+0x^5+x^4+x^3+0x^2+x+0 \\ 0x^6+0x^5+0x^4+x^3+x^2+0x+1 \end{bmatrix}$$

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

The above matrix not in systematic form. to convert it into the standard form. we Perform the following operations

$R_1 \rightarrow R_1+R_2+R_3$

$R_2 \rightarrow R_2+R_3+R_4$

$R_3 \rightarrow R_3+R_4$

Now G will be

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right]$$

Now all the code vectors can be obtain using the relation $C = DG$ as follow:-

$$M_1 = (0000) \Rightarrow C = (0000)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = (0000000)$$

$$M_2 = (0001) \Rightarrow C = (0001)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = (0001101)$$

$$M_3 = (0010) \Rightarrow C = (0010)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = (0010111)$$

$$4 = (0011) \Rightarrow C = (0011)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow (0011010)$$

$$M_5 = (0100) \Rightarrow C = (0100)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow (0100011)$$

$$M_6 = (0101) \Rightarrow C = (0101)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow (0101110)$$

$$M_7 = (0110) \Rightarrow C = (0110)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow (0110100)$$

$$M_8 = (0111) \Rightarrow C = (0111)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow (0111001)$$

$$M_9 = (1000) \Rightarrow C = (1000)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow [1000110]$$

$$M_{10} = (1001) \Rightarrow C = (1001)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow [1001011]$$

$$\eta_{11} = (1010) \Rightarrow C = (1010)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow [1010001]$$

$$M_{12} = (1011) \Rightarrow C = (1011)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow [1011100]$$

$$M_{13} = [1100] \Rightarrow C = (1100)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow [1100101]$$

$$M_{14} = [1101] \Rightarrow C = (1101)\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow [1101000]$$

$$M_{15} = [1110] \Rightarrow C = [1110]\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow [1110010]$$

$$M_{16} = [1111] \Rightarrow C = [1111]\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow [1111111]$$

The minimum distance b/w any two codeword is 3. Hence this is a single error correcting and 14 of these codewords can be obtain by successive cyclic shift of two codewords 1110010 and 1101000. The remaing two codewords 1111111 and 0000000 remain unchange under cyclic shift.

Types of Cyclic codes! -

① Golay codes!- Golay code is capable of correcting any combination of three or fewer random errors in a block of 23 bits. The code has minimum distance of - The (23,12) Golay code is generated by either of the two generated polynomials.

$g_1(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$

$g_2(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$

which are factors of ~~x~~ $x^{23}+1$.

$x^{23} + 1 = (x+1)\, g_1(x)\, g_2(x)$

② Bose Chaudhari Hocquenghem (BCH) Codes!-

BCH ~~is~~ code can be treated as a generalization of the Hamming code for multiple error correction. for any Positive integers m (equal to or greater then 3) and t [Less than $(2^m - 1)/2$] there exists a binary BCH code with the following Parameter.

Block length ⇒ $n = 2^m - 1$

No of message bits $K \geq n - mt$

minimum distance $d_{min} \geq 2t + 1$

Each BCH code is a t-error correcting code in that it can ~~be~~ detect and correct upto t random errors per code word.

③ Galois field!-

A Galois field is a finite field with a finitefield order (i.e number of elements). The order of a finite fields is always a Prime or a power of Prime. for each prime power there exists exactly one finite field.

Every existed field of finite order s may be represented as Galois field of order $s - p^n$. The GF (p^n) is defined uniquelly by its order. A field is an algebric structure in which the operations of addition, subtraction, multiplication and division ~~to~~ can be performed and they satisfy the usual rules.

Properties of Galois fields! -

we have some property of the $GF(p^{nm})$ with respect to the included field, the $GF[p^n]$.

1. if two function $f(x)$ and $P(x)$ belonging to the $GF[p^n]$ have in the field no common divisor containing x, we can determine two function $f'(x)$ and $P'(x)$ belonging to the $GF[p^n]$ such that

$$f'(x).f(x) - P'(x).P(x) - 1$$

Q. factorize the Polynomial x^3-1 over $GF(2)$ and $GF(3)$.

Sol^n over any field, the factorization

$$x^3-1 = (x-1)(x^2+x+1)$$

The factor $(x-1)$ can not be reduced further. Now let us try to factorize the second term $p(x) = x^2+x+1$ in the Galois field $GF(2)$ which contain two elements 0 and 1 satisfying the addition and multiplication shown in table

Addition

+	0	1
0	0	1
1	1	0

multiplication

·	0	1
0	0	0
1	0	1

then $p(0) = 0+0+1 = 1 \neq 0$ over $GF(2)$

$p(1) = 1+1+1 = 1 \neq 0$ over $GF(2)$

therefore $p(x)$ can not be factorized further in $GF(2)$ and therefore in Galois field $GF(2)$ we have $x^3-1 = (x-1)(x^2+x+1)$.

Again $GF(3)$ contain three elements 0, 1 and 2 which satisfy the addition and multiplication shown in table.

Addition

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Multiplications

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

table 2

91

61

0122

1
2
3

④

01201

0120012

012

$P(0) = 0+0+1 = 0+1 = 1 \neq 0$ over $GF(3)$

$P(1) = 1+1+1 = 2+1 = 0$ over $GF(3)$

$P(2) = 2^2 + 2 + 1 \Rightarrow 2 \cdot 2 + 2 + 1 \Rightarrow 1+2+1 = 0+1 = 1 \neq 0$ over G

Since only $P(1) = 0$ therefore $(x-1)$ is the only factor of $P(x)$ possible in $GF(3)$ therefore in the Galois field GF(3.

$$x^3 - 1 = (x-1)(x^2+x+1) = (x-1)(x-1)(x-1)$$

Q. The following Polynomials $f(x)$ and $g(x)$ are defined over GF(3).

$f(x) = 2 + x + x^2 + 2x^4$

$g(x) = 1 + 2x^2 + 2x^4 + x^5$

Calculate addition and multiplication of the above two polynomials.

Soln in the Galois field GF(3), the addition and multiplication procedures are shown in the table 2.

$f(x) + g(x) = (2 + x + x^2 + 2x^4) + (1 + 2x^2 + 2x^4 + x^5)$

$= (2+1) + x + (1+2)x^2 + (2+2)x^4 + x^5$

$\Rightarrow 0 + x + 0x^2 + 1x^4 + x^5$

$\Rightarrow x + x^4 + x^5$

$f(x) \cdot g(x) = (2 + x + x^2 + 2x^4)(1 + 2x^2 + 2x^4 + x^5)$

$\Rightarrow 2 + x^2 + x^4 + 2x^5 + x + 2x^3 + 2x^5 + x^6 + x^2 + 2x^4 + 2x^6 +$

x^7 [illegible] $2x^4 + x^6 + x^8 + 2x^9$

$\Rightarrow 2 + x + 2x^2 + 2x^3 + (1+2+2)x^4 + (2+2)x^5 + (1+2+1)x^6 +$

$2x^7 + x^8 + 2x^9$

⇒ $2+x+2x^2+2x^3+2x^4+x^5+x^6+x^7+x^8+2x^9$

8. Construct a Galois field $GF(2^4)$ or $GF(16)$ as an extension
⑧ of the galois field $GF(2)$.

Ans By definition the Galois field $GF(2^4)$ is the field of Polynomial over $GF(2)$ modulo an irreducible Polynomial of degree 4 in Galois field $GF(2)$.

first we have to find an irreducible polynomial of degree 4 in Galois field $GF(2)$.
Now consider the Polynomial

add

+	0	1
0	0	1
1	1	0

Mult

·	0	1
0	0	0
1	0	1

$$P(x) = x^4+x+1$$

$P(0) = 0+0+1 = 1 \neq 0$ over $GF(2)$

$P(1) = 1+1+1 = 0+1 = 1 \neq 0$ over $GF(2)$

Therefore the polynomial $p(x) = x^4+x+1$ is irreducible over the galois field $GF(2)$.

Therefore the galois field $GF(2^4)$ of $2^4=16$ eleme may be formed as the field of Polynomials over $GF(2)$ modulo x^4+x+1.

Since $p(x)$ is of degree 4, therefore it must ~~be~~ have roots somewhere. Let α be the root of $p(x)$ then we have

$$p(\alpha) = 0$$

$$\alpha^4+\alpha+1 = 0$$

This element α is Known as the primitive element of GF(16). Every non-zero element of GF(16) can be expressed as some power of α. Since GF(16) contains 16 elements and 0 will be an element of GF(16), being the additive identity, therefore the elements of GF(16) are

$\{\alpha^0, \alpha^1, \alpha^2 --- \alpha^{14}\}$, 0 is not included.

where α is given by table 3. The Power, Polynomial, and vector representation of elements of $GF(2^4) =$ GF(16) are as follows

Power Representation	Polynomial Representation	Vector Representation
α^0 =	1	= (0001)
α^1 =	α^2	= (0010)
~~α^2 =~~	~~α^3~~	
α^3 =	$\alpha^3\cancel{+1}$	= (1000)
α^4 =	$\cancel{\alpha^2}+\alpha+1$	= (0011)
α^5 =	$\cancel{\alpha^3+}\alpha^2+\alpha$	= (0110)
α^6 =	$\alpha^3+\alpha^2$	= (1100)
α^7 =	$\alpha^3+\alpha+1$	= (1011)
α^8 =	α^2+1	= (0101)
α^9 =	$\alpha^3+\alpha$	= (1010)
α^{10} =	$\alpha^3+\alpha^2+\alpha$	= (0111)
α^{11} =	$\alpha^3+\alpha^2+\alpha$	= (1110)
α^{12} =	$\alpha^3+\alpha^2+\alpha+1$	= (1111)
α^{13} =	$\alpha^3+\alpha^2+1$	= (1101)
α^{14} =	α^3+1	= (1101)
α^{15} =	1	= α^0

0 will be the additive identy in GF(16) while evaluatin the elements, it should be remembered that

$$\alpha^4+\alpha+1=0$$

$$\Rightarrow \alpha^4=-\alpha-1=\alpha+1$$

Similarly $\alpha^5=\alpha^4.\alpha=(\alpha+1).\alpha=\alpha^2+\alpha$

$$\alpha^{12}=\alpha^6+\alpha^6=(\alpha^3+\alpha^2)(\alpha^3+\alpha^2)$$

$$=\alpha^6+\alpha^5+\alpha^4$$

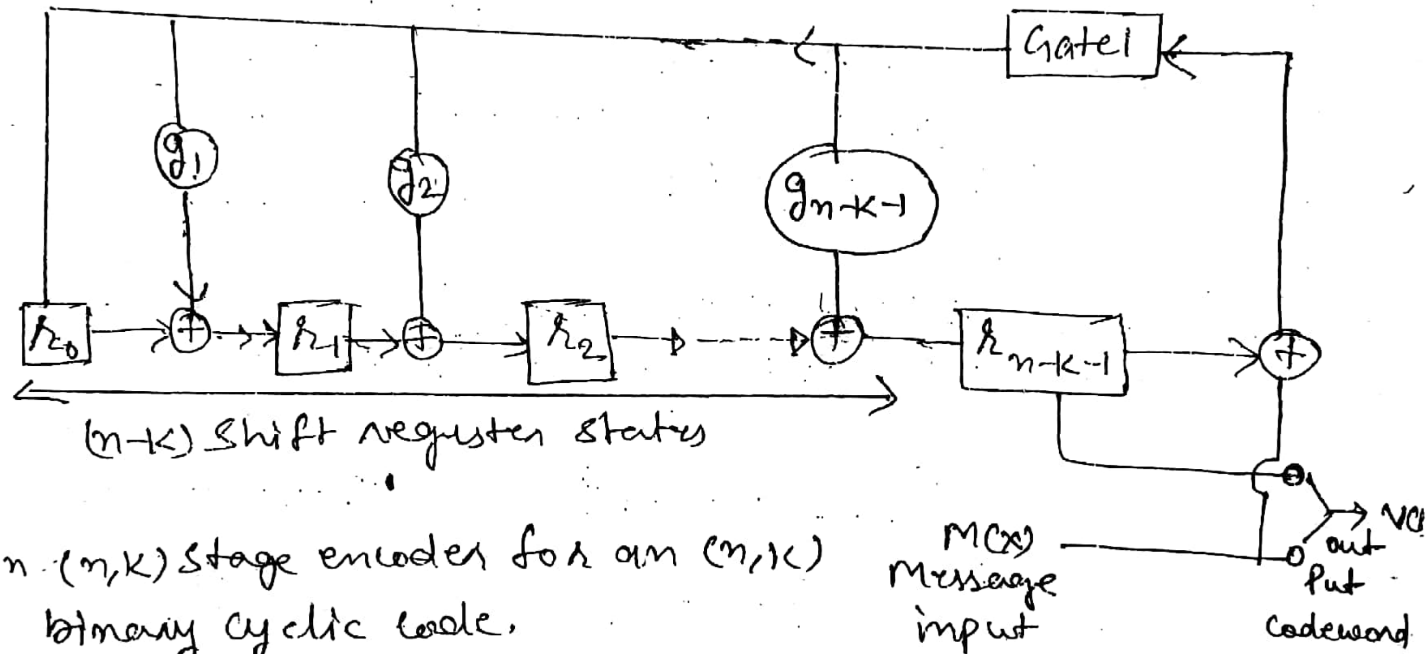
$$=\alpha^6+\alpha^4 \Rightarrow \alpha^3+\alpha^2+\alpha+1$$

SYSTEMATIC ENCODING USING (n-K) BIT SHIFT REGISTER:-

The stages of Register are first initialized by being filled with zeros. After the shifting of bits into the shift register, the quotient has been serially Presented at the output and the remainder resides in the registers.

The circuit feedback connections corresponds to the coefficients of the generator polynomial, which is written as

$$g(x) = 1 + g_1(x) + g_2(x)^2 + --- g_{n-k-1} x^{n-k-1} + x^{n-k}$$



An (n,K) stage encoder for an (n,K) binary cyclic code.

1. In circuit Symbol ☐ is used to denotes flip flop that makes up shift register.
2. at the occurrence of clock Pulse, the register inputs are Shifted into register and appear at output when the clock Pulse end.

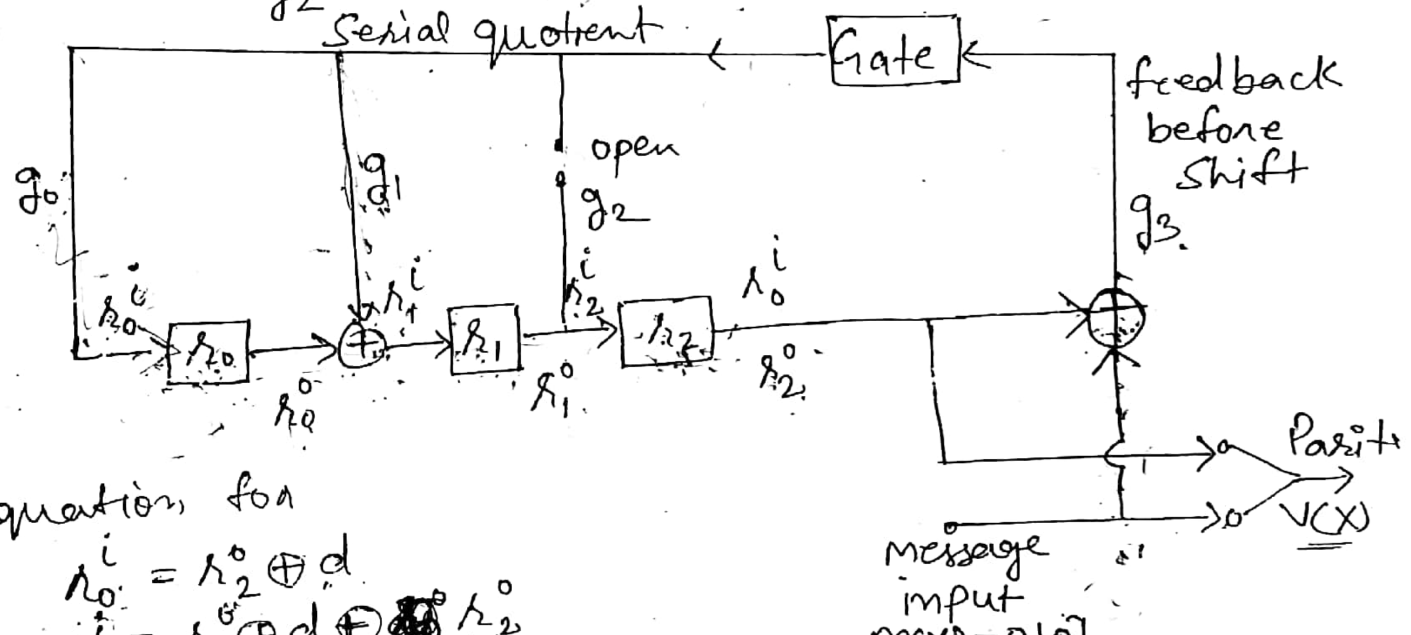
Q. Design an encoder for (7, 4) BCC generated by $g(x) = 1+x+x^3$ and varify its operation using message vector 0101.

Soln Here $g(x) = 1 + x + x^3$

So $g_0 = 1 \rightarrow$ close circuit

$g_1 = 1 \rightarrow$ closed path

$g_2 = 0 \rightarrow$ open Path $\quad g_3 = 1$



equation for

$$r_0^i = r_2^o \oplus d$$
$$r_1^i = r_0^o \oplus d \oplus r_2^o$$
$$r_2^i = r_1^o$$

input bit m	Register Inputs r_0^i	r_1^i	r_2^i	Register output r_0^o	r_1^o	r_2^o
–	0	0	0	0	0	0
1	1	1	0	1	1	0
0	0	1	1	0	1	1
1	0	0	1	0	0	1
0	1	1	0	1	1	0

the code vector for (0101) is $\underline{110}0101$

SYNDROME CALCULATION :-

Suppose that a code vector V is transmitted over a noisy channel. The received vector R may or may not be transmitted code vector. The function of decoder is to determine the transmitted code vector based on received vector.

The decoder first test whether or not the received vector is a valid code vector by calculating the syndrome of received word. if Sym = 0, the received vector is divisible by generator Polynomial. if S ≠ 0 indicates errors have occurred.

Syndrome S(X) of received vector R(X) is remainder s resulting from dividing R(X) by g(X).

$$\frac{R(X)}{g(X)} = q(X) + \frac{S(X)}{g(X)} \quad \text{———} \quad \textcircled{1}$$

$$q(X) = \text{quotient}$$

Syn S(X) is a Polynomial of degree $n-K-1$. if E(X) is Error Pattern caused by channel

$$R(X) = V(X) + E(X) \quad \text{———} \quad \textcircled{2}$$

divide eqn ② by g(X)

$$\frac{R(X)}{g(X)} = \frac{V(X)}{g(X)} + \frac{E(X)}{g(X)} \quad \text{———} \quad \textcircled{3}$$

$$V(X) = M(X)\, g(X)$$

by eqn ③

$$\frac{R(X)}{g(X)} = \frac{M(X)\, g(X)}{g(X)} + \frac{E(X)}{g(X)}$$

$$\frac{R(X)}{g(X)} = M(X) + \frac{E(X)}{g(X)} \quad \text{——} \quad \textcircled{4}$$

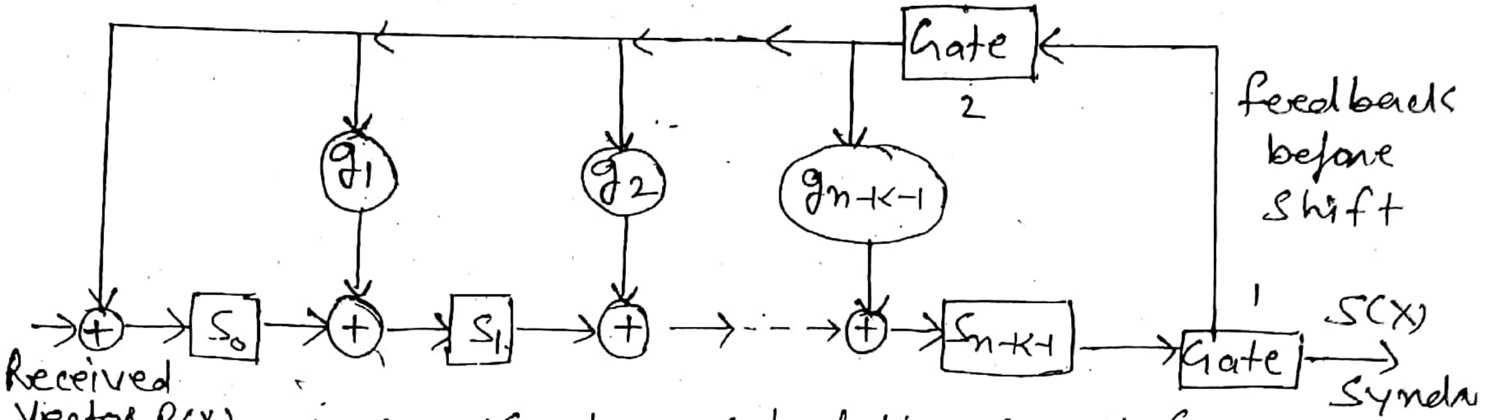
adding eqn ④ and ①

$$0 = [M(X) + q(X)] + \frac{E(X)}{g(X)} + \frac{S(X)}{g(X)}$$

$-E(X) = S(X) + [D(X) + q(X)]\, g(X)$

or

$E(X) = [M(X) + q(X)]\, g(X) + S(X)$ — ⑤



An (n-k) Syndrome calculation Circuit for an (n-k) cyclic code.

initialy register's are cleared. Then with gate2 turned on & gate1 turned OFF, the received vector R(X) is entered into shift register.

After entire received vector is shifted into register, the contents of Register will be syndrome. Now gate 2 turned off & gate 1 ON & syndrome vector is shifted out of register. The circuit is ready for Processing next received word.

Q. Consider a (5,1) repetition code. Page 3.54 UNIT3

a) Evaluate the Syndrome S for all five Possible single error Patterns.

b) Repeat ⓐ for all ten possible double error patterns.

c) Show that the (5,1) Repetition code is capable of correc-ing up to two errors.

Solⁿ a) $S = EH^T$

$$G = [\underset{I}{1}\ \underset{P}{1\,1\,1\,1}]$$

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

$S = EH^T$

0 0000 [illegible]

1 1 111

Where E is Error Vector, Let e = [10000] then

$$S = [10000]\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \Rightarrow [11111]$$

in Similar way other Syndromes can be evaluated.

So

e	S
1 0 0 0 0	1 1 1 1
0 1 0 0 0	1 0 0 0
0 0 1 0 0	0 1 0 0
0 0 0 1 0	0 0 1 0
0 0 0 0 1	0 0 0 1

ⓑ Let e = [11000] then

$$S = [11000]\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \Rightarrow [0111]$$

in Similar way other Syndromes are

e	S
1 1 0 0 0	0 1 1 1
1 0 1 0 0	1 0 1 1
1 0 0 1 0	1 1 0 1
1 0 0 0 1	1 1 1 0
0 1 1 0 0	1 1 0 0
0 1 0 1 0	1 0 1 0
0 1 0 0 1	1 0 0 1
0 0 1 1 0	0 1 1 0
0 0 1 0 1	0 1 0 1
0 0 0 1 1	0 0 1 1

ⓒ Since the Syndromes for all Single error and double error pattern are distinct. the (5, 1) repetition code is capable of correcting up to two errors.

Q design a Syndrome calculator for a (7,4) cyclic Hamming code generated by the polynomial $g(x) = x^3+x+1$. Evaluate the Syndrome for $y = (1001101)$.

Sol

$n = 7, \quad K = 4$

$q = n - K = 7 - 4 = 3$

The given generator Polynomial is

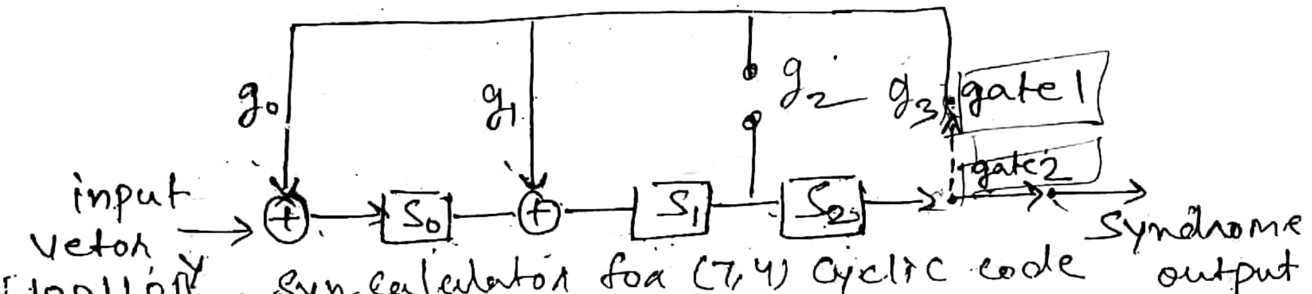
$G(x) = x^3 + 0.x^2 + x + 1$ ——①

$G(x) = x^3 + g_2 x^2 + g_1 x + 1$ (generalized eqn) —②

Comparing eqn ① & ②

$g_0 = 1 \quad g_1 = 1 \quad g_2 = 0$

So Syndrome calculator will be



Syn. calculator for (7,4) Cyclic code with $g(x) = x^3+x+1$

The ~~gate~~ switch 1 is kept in position ~~off~~ until all the 7 bit of Received Vector are shifted into the shift register. The switch is then closed to position 2 and clock pulses are applied to shift register. This gives syndrome vector at the output.

The received vector $y = (1001101)$

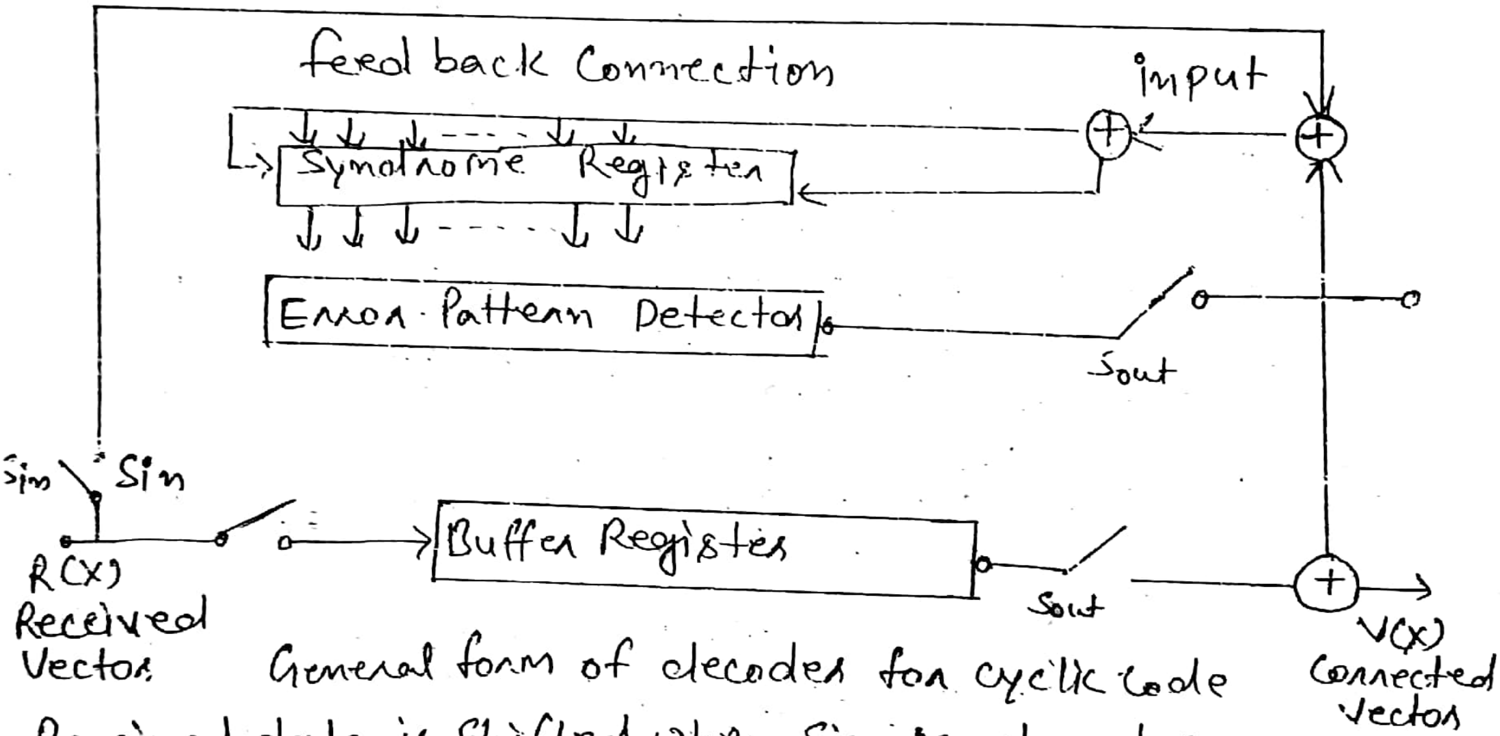
Shift	Received vector i.e bit of y	Contents of flip-flop in shift Registers		
		$S_0 = y \oplus S_2^0$	$S_1 = S_2^0 + S_0^0$	$S_2 = S_1^0$
–	–	0	0	0
1	1	1	0	0
2	0	0	1	0
3	0	0	0	1
4	1	0	1	0
5	1	1	0	1
6	0	1	0	0
7	1	1	1	0

The table show that at end of last shift the registers contents are $(S_0, S_1, S_2) = (110)$ Hence the calculated Syndrome will b $S = (S_2, S_1, S_0) = (011)$ Ans.

ERROR ~~COR~~ DETECTION AND ERROR CORRECTION :-

Error Detection:- It can be implemented by simply adding an additional flip flop to Syndrome calculation. if $S \neq 0$ flip flop sets & an indication of error is provided.

Error Correction:- Decoder task is to determine correctable error pattern E(X) from Syndrome S(X). Then add to R(X) to determine transmitted code vector V(X).



General form of decoder for cyclic code

Received data is shifted when Sin is closed & Sout is open. Error correction is performed when Sout is closed & Sin open.

2. The decoder for a class of Single error correcting cyclic Codes (Hamming codes)