

--	--	--	--	--	--	--	--	--	--

Improvement Test - May 2017

Sub:	Information Theory and Coding						Code:	10TE65	
Date:	_/_/05/2017	Duration:	90 mins	Max Marks:	50	Sem:	6A&B	Branch:	TCE

Answer Any Five Full Questions

	Marks	OBE	
		CO	RB T
1 Write a short note on RS codes and GOLAY codes .	10	CO 5	L1

1. Reed Solomon codes

- RS codes are a class of maximum distance separable codes.
- Proposed by I.S. REED & G. SOLOMON in the year 1960.
- Non binary codes
- A class of non binary BCH codes.
- The developments in VLSI processing technology make these codes practically prominent in recent years, because of their low decoding computations.

2. To show that RS codes as special case of BCH codes

Let us consider the primitive q -ary BCH codes of length $n = q^m - 1$ and the extension of field of q elements invoked for locating roots of generator polynomial.

Let $m=1$, we get $n = q - 1$, which governs the RS codes.

For the primitive BCH codes, the generator polynomial is given by

$$g(x) = \text{LCM}[\phi_{\alpha^1}(x), \phi_{\alpha^2}(x), \dots, \phi_{\alpha^{t+1}}(x)]$$

Where $\phi_{\alpha^j}(\alpha) =$ minimal polynomial of element α^j
 $\alpha^j =$ powers of a primitive element α
 $\delta =$ desired value of d_{\min} .

Now with $m=1$, however, the minimal polynomials of elements in $GF(q)$ are first degree of the form $g(x)$ reduces to

$$g(x) = (x - \alpha^j)(x - \alpha^{j+1}) \dots (x - \alpha^{j+\delta-1})$$

This is a polynomial over $GF(q)$ of degree $\delta-1$. Thus $n-k = \delta-1$ for RS codes.

$$\therefore n-k = \delta-1 \rightarrow \textcircled{3}$$

Since these are BCH codes, the true minimum distance must be at least:

$$d_{\min} \geq \delta = n-k+1 \Rightarrow d_{\min} = n-k+1.$$

\therefore The RS codes are "Maximum distance separable" (MDS) codes, i.e., for any (n, k) MDS, the minimum distance $d_{\min} = n-k+1$. But, for a RS code, $d_{\min} = n-k+1$.

The values of k may be any integer $0 \leq k \leq n$. In eqⁿ $\textcircled{1}$ & $\textcircled{2}$ the starting exponent in the roots, is completely arbitrary and is commonly taken to be 1.

1. GOLAY CODES

Golay codes are $(23, 12)$ binary codes capable upto 3 errors in a block of 23 bit code word. It is a perfect code because it satisfies the equality sign in the Hamming bound for $t=3$.



2 Write a note on **Shortened cyclic codes** and **Burst error correcting codes**.

10

CO	L3
5	

Shortened Cyclic Codes

The cyclic codes have the generator polynomial as a factor of $x^n + 1$.

But, the polynomial $x^n + 1$ has relatively few divisors. Hence there are usually very few cyclic codes for

to overcome this difficulty & to increase the r (n, k) for which useful codes can be constructed, they are often used in shortened form.

In the shortened form, the last i information bits are always '0'. i.e., the last i bits of the code are zero. Hence the name zero padding codes.

These bits are not transmitted, the decoder for cyclic codes can decode the shortened code simply by padding the received $(n-i)$ tuples of

hence, for a given (n, k) cyclic code, it is always possible to construct a $(n-i, k-i)$ shortened cyclic code.

The shortened cyclic codes are a subset of the original code from which it is derived & hence its d_{min} & error correction capability is at least as great as the original code.

Advantages

- * The encoding circuit, syndrome circuit & error correction procedure for shortened cyclic codes are identical to the original cyclic codes.

- All shortened cyclic codes inherit nearly all of the advantages of cyclic codes.
- The mathematical structure of cyclic codes serve as shortened cyclic codes.

x. Burst error correcting codes

- The presence of impulse noise affects more than one bit to cause burst errors.
- Codes used for correcting random errors are efficient for correcting burst errors.
- Special codes have been developed to correct

x. Burst of length q: Is defined as a vector whose components are confined to q digit positions, the first q non-zero.

Eq: The vector $V = (00101001000)$ has a burst of length 9. A code which is capable of correcting all bursts of length q or less is called q -burst-error correcting and is said to be burst error correcting.

The condition for a burst- q -correcting code is that the no of parity bits must at least $\geq q$.

$$\text{i.e., } n-k \geq q$$

The upper bound on the burst error correcting of an (n, k) code is $\boxed{q \leq \frac{n-k}{2}}$ bits.

- 3 For the $(7,4)$ cyclic codes, $g(x) = 1 + x + x^3$ and $D(x) = d_0 + d_1x + d_2x^2 + d_3x^3$. Find all the 16 code vectors in **Systematic** and **Non systematic** form.

CO	L3
5	

Non-systematic Cyclic Code

(6)

It is defined by $V(x) = D(x)q(x)$.

Ex 1: For a (7,4) sec, the generator polynomial is

$q(x) = 1+x+x^3$, find all the valid possible

i) Non-systematic form

ii) systematic form.

Solⁿ: Given $(n, k) = (7, 4) \rightarrow (1)$

$$\Rightarrow x^n + 1 = x^7 + 1 \rightarrow (2)$$

$$q(x) = 1 + x + x^3 \rightarrow (3)$$

$$D(x) = d_0 + d_1x + d_2x^2 + d_3x^3 \rightarrow (4)$$

Valid possible code comb^s = $q^k = 2^4 = 16$.

\therefore The non-systematic cyclic codes are given by

$$V(x) = D(x)q(x) \rightarrow (5)$$

substituting eq^s (3) & (4) in (5) yields.

$$V(x) = (d_0 + d_1x + d_2x^2 + d_3x^3)(1 + x + x^3)$$

$$= d_0 + d_1x + d_2x^2 + d_3x^3$$

$$+ d_0x + d_1x^2 + d_2x^3 + d_3x^4$$

$$+ d_0x^3 + d_1x^4$$

$$V(x) = d_0x^0 + (d_0 + d_1)x + (d_1 + d_2)x^2 + (d_2 + d_3)$$

$$(d_1 + d_3)x^3 + d_2x^4 + d_3x^5$$

$$V(x) = v_0(x^0) + v_1x + v_2x^2 + v_3x^3 + v_4x^4 + v_5$$

Possible valid $2^k = 2^4 = 16$ combination inputs (d) & its
 Code vectors are ⑦

msg (d)				Code Vector						
d_0	d_1	d_2	d_3	v_0	v_1	v_2	v_3	v_4	v_5	v_6
d_0	d_1	d_2	d_3	d_0	(d_0, d_1)	(d_1, d_2)	(d_0, d_2)	(d_1, d_3)	d_2	d_3
0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1	1	0	1
0	0	1	0	0	0	1	1	0	1	0
0	0	1	1	0	0	1	0	1	1	1
0	1	0	0	0	1	1	1	0	0	1
0	1	0	1	0	1	1	1	1	1	0
0	1	1	0	0	1	0	0	0	1	1
0	1	1	1	0	1	0	1	0	0	0
1	0	0	0	1	1	0	1	1	0	1
1	0	0	1	1	1	0	0	1	0	1
1	0	1	0	1	1	1	1	1	1	1
1	0	1	1	1	1	1	0	1	1	0
1	1	0	0	1	0	1	0	0	0	1
1	1	0	1	1	0	0	0	1	1	0
1	1	1	0	1	0	0	1	0	1	1
1	1	1	1	1	0	0	1	0	1	1

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Systematic cyclic codes

(8)

x. In systematic cyclic codes - the left most check bits and - the rest rightmost k bits are

x. To derive this set let us derive the gene in standard form.

$$\text{i.e., } G = [P \mid I_k]_{k \times n}$$

$$\Rightarrow G = [P \mid I_4]_{4 \times 7}$$

The first row of a G matrix, g can be derived generator polynomial as.

$$\text{given } g(x) = 1 + x + x^3$$

$$\Rightarrow g(x) = 1 \cdot x^0 + 1 \cdot x^1 + 0 \cdot x^2 + 1 \cdot x^3 + 0 \cdot x^4 + 0$$

since $(n=7)$

\therefore The first row is 1101000

||| 3 more rows are obtained as follows

1st row is generated using

$$xg(x) = 0 \cdot x^0 + 1 \cdot x^1 + 1 \cdot x^2 + 0 \cdot x^3 + 1 \cdot x^4$$

\Rightarrow The 2nd row is 0110100 $\rightarrow x$

||| 3rd row is 0011010 $\rightarrow x^2$

4th row is 0001101 $\rightarrow x^3$

$$\Rightarrow G = \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array} \right]_{k \times n}$$

$\underbrace{\hspace{3em}}_P \quad \underbrace{\hspace{3em}}_{I_{n-k}}$

since the augmented matrix, identity matrix is standard form.

Performing Elementary row transformation

$$\begin{aligned} \text{i.e., } R_3 &\rightarrow R_3 + R_1 \\ R_4 &\rightarrow R_4 + R_2 + R_1 \end{aligned}$$

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

$\underbrace{\hspace{10em}}_{I_4}$

$$\Rightarrow P = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}_{4 \times 3}$$

Now since the 'G' matrix is in standard form, code can be obtained as follows.

$$\begin{aligned} V &= DG \\ &= [d_0 \ d_1 \ d_2 \ d_3] \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \end{aligned}$$

$$= \begin{matrix} v_0 & v_1 & v_2 & v_3 \\ (d_0 + d_2 + d_3) & (d_0 + d_1 + d_2) & (d_1 + d_2 + d_3) & (d_1) \end{matrix}$$

The valid codes and their msg vectors are as follows

$d_0 \ d_1 \ d_2 \ d_3$	v_0	v_1	v_2	v_3	v_4	v_5	v_6	$d_0 \ d_1 \ d_2 \ d_3$	$v_0 \ v_1$
0 0 0 0	0	0	0	0	0	0	0	1 0 1 1	0 0
0 0 0 1	1	0	1	0	0	0	1	1 1 0 0	1 0
0 0 1 0	1	1	1	0	0	1	0	1 1 0 1	0 0
0 0 1 1	0	1	0	0	0	1	1	1 1 1 0	0 1
1 0 0 0	1	1	0	1	0	0	0	1 1 1 1	1 1
1 0 0 1	0	1	1	1	0	0	1		
1 0 1 0	0	0	1	1	0	1	0		

- 4 Design an encoder for (7,4) binary cyclic code generated by $g(x) = 1 + x + x^3$ and verify its operation using the message vector (1001) and (1011). 10

solⁿ: In general we have generator polynomial as

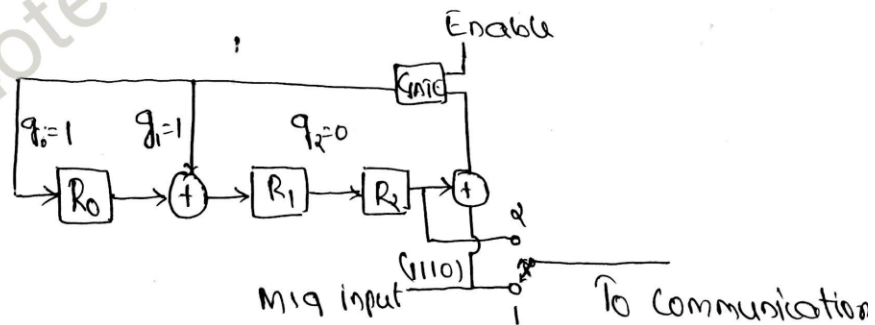
$$g(x) = g_0 + g_1x + g_2x^2 + \dots + g_{n-k}x^{n-k}$$

in the given data we have

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

$$\Rightarrow g_0 = 1, g_1 = 1, g_2 = 0 \text{ \& } g_3 = 1$$

The encoding circuit for the given generator is



Encoding circuit for (7,4) CRC with

For the input msg vector $D=[1110]$ the operation in the table below.

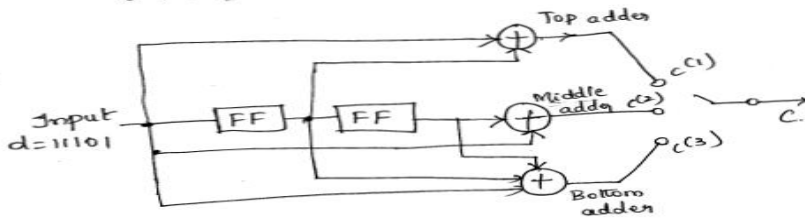
No of shifts	Input D	Shift Register Contents			Rema
		R_0	R_1	R_2	
	switch position 1 Gate Enable				
		0	0	0	← power
1	0	0	0	0	-
2	1	1	1	0	-
3	1	1	0	1	-
4	1	0	1	0	-
	switch position 2 Gate Disable				
5	X	0	0	1	→ 0
6	X	0	0	0	→ 1
7	X	0	0	0	→ 0

Explanation - for the same in simple words if we

- 5 Consider a (3,1,2) convolution code with $g^{(1)} = (110)$, $g^{(2)} = (101)$ and $g^{(3)} = (111)$. Draw the **Encoding Circuit** and obtain the **Generator Matrix** 10

CO	L4
5	

(3,1,2) convolution encoder .



G is of order $L \times [n(L+m)]$
 $5 \times (3(5+2)) = 5 \text{ rows} \times 21 \text{ columns} .$

given $g^{(1)} = 110$
 $g^{(2)} = 101$
 $g^{(3)} = 111$

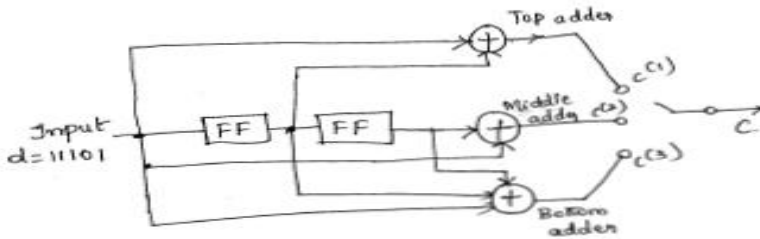
$$\therefore G = \begin{bmatrix} 111 & 101 & 011 & 000 & 000 & 000 & 000 \\ 000 & 111 & 101 & 011 & 000 & 000 & 000 \\ 000 & 000 & 111 & 101 & 011 & 000 & 000 \\ 000 & 000 & 000 & 111 & 101 & 011 & 000 \\ 000 & 000 & 000 & 000 & 111 & 101 & 011 \end{bmatrix}_{5 \times 21}$$

- 6 Consider a (3,1,2) convolution code with $g^{(1)} = (110)$, $g^{(2)} = (101)$ and $g^{(3)} = (111)$. Find the code-word corresponding to the information sequence (11101) in **Time Domain** approach and **Transform Domain** approach

10

CO L4
5

(3,1,2) convolution encoder .



G is of order $L \times [n(L+m)]$
 $5 \times (3(5+2)) = 5 \text{ rows} \times 21 \text{ columns} .$

given $g^{(1)} = 110$
 $g^{(2)} = 101$
 $g^{(3)} = 111$

$$\therefore G = \begin{bmatrix} 111 & 101 & 011 & 000 & 000 & 000 & 000 \\ 000 & 111 & 101 & 011 & 000 & 000 & 000 \\ 000 & 000 & 111 & 101 & 011 & 000 & 000 \\ 000 & 000 & 000 & 111 & 101 & 011 & 000 \\ 000 & 000 & 000 & 000 & 111 & 101 & 011 \end{bmatrix}_{5 \times 21}$$

$$\therefore [C] = [D] [G]$$

$$= [11101]$$

$$\begin{bmatrix} 111 & 101 & 011 & 000 & 000 & 000 & 000 \\ 000 & 111 & 101 & 011 & 000 & 000 & 000 \\ 000 & 000 & 111 & 101 & 011 & 000 & 000 \\ 000 & 000 & 000 & 111 & 101 & 011 & 000 \\ 000 & 000 & 000 & 000 & 111 & 101 & 011 \end{bmatrix}_{5 \times 21}$$

$$\therefore [c] = [111 \ 010 \ 001 \ 110 \ 100 \ 101 \ 011]$$

Transfer Domain Method.

Given : $[d] = [11101] \Rightarrow d(x) = 1 + x + x^2 + x^4$

$g^{(1)} = (10) \rightarrow g^{(1)}(x) = 1 + x$

$g^{(2)} = (101) \rightarrow g^{(2)}(x) = 1 + x^2$

$g^{(3)} = (111) \rightarrow g^{(3)}(x) = 1 + x + x^2$

\therefore we have the equnⁿ

$$C(x) = c^{(1)} x^{(n)} + x c^{(2)}(x^n) + x^2 c^{(3)}(x^n)$$

Before that we find $[C] = [D] [G]$ or

For top adder $\Rightarrow c^{(1)}(x) = d(x) g^{(1)}(x)$
 $= 1 + x + x^2 + x^4 (1 + x)$

$c^{(1)}(x) = 1 + x + x^2 + x^3 + x^4 + x^5$

$c^{(1)}(x) = 1 + x^3 + x^4 + x^5$

For middle adder $\Rightarrow c^{(2)}(x) = d(x) g^{(2)}(x)$
 $= 1 + x + x^2 + x^4 (1 + x^2)$

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

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

$c^{(2)}(x) = 1 + x + x^3 + x^6$

For bottom adder $\Rightarrow c^{(3)}(x) = d(x) g^{(3)}(x)$
 $= 1 + x + x^2 + x^4 (1 + x + x^2)$

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

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

$c^{(3)}(x) = 1 + x^2 + x^5 + x^6$

\therefore for encoder equnⁿ

$C(x) = c^{(1)} x^3 + x c^{(2)}(x^3) + x^2 c^{(3)}(x^3)$

$= 1 + x^3 + x^6 + x^9 + x(1 + x^3 + x^6 + x^9) + x^2(1 + x^2 + x^5 + x^8)$

$= 1 + x^3 + x^6 + x^9 + x + x^4 + x^{10} + x^{12} + x^2 + x^5 + x^{17} + x^{20}$

$= 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^9 + x^{10} + x^{12} + x^{15} + x^{17} + x^{19} + x^{20}$

$C(x) \Rightarrow$ q.p of encoder is $[111\ 010\ 001\ 110\ 100\ 101\ 011]$

\therefore Transfer Domain & Time Domain Codevectors are same.

- 7 Consider the binary convolution encoder shown in Fig. 7. Draw the state table, state transition table, state diagram and corresponding code tree. Using the code tree find the encoded sequence for (10111).

10

CO 5 L4

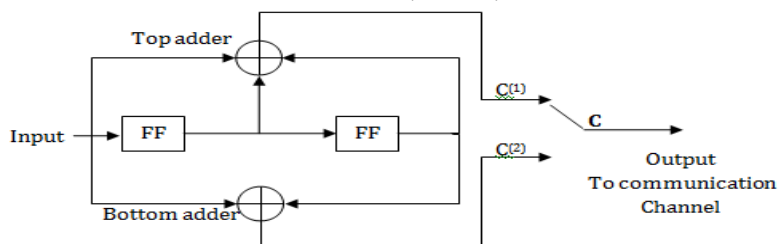
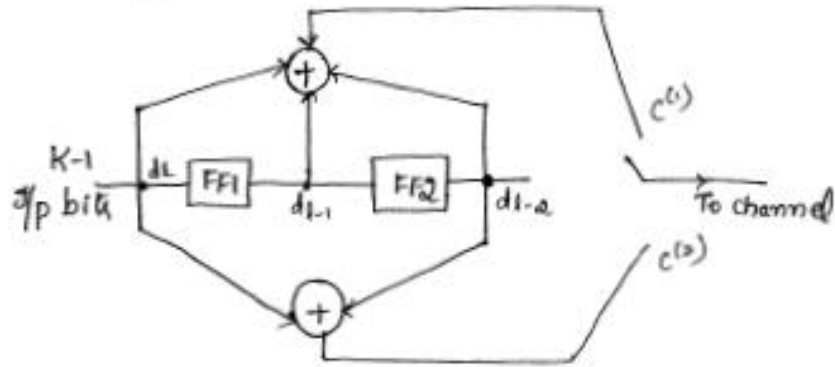


Fig. 7. (2, 1, 2) Convolution encoder.

State table, State transition table, State diagram, Code tree.

1. Draw the state transition table, state diagram & code tree for (2, 1, 2) convolution encoder with impulse response $g^{(1)} = 111$, $g^{(2)} = 101$ & input $D = [10111]$

Solⁿ



① State table

There are 2 flip flops in the shift register i.e 2
 \therefore there are $2^2 = 4$ states with binary data, that
 represented in the table below

State	S_0	S_1	S_2	S_3
Binary Description	00	10	01	11

② State Transition Table.

It is a table indicating the transition between 4 states and also the corresponding code bits output during each transition.

The output of the mod-2 adders can be represented as

$$c^{(1)} = d_1 + d_{1-1} + d_{1-2}$$

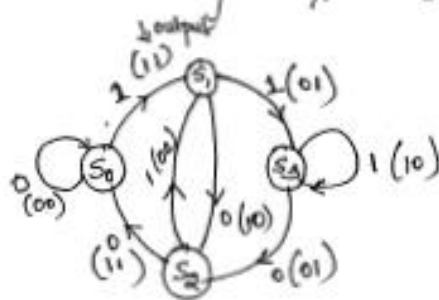
$$c^{(2)} = d_1 + d_{1-2}$$

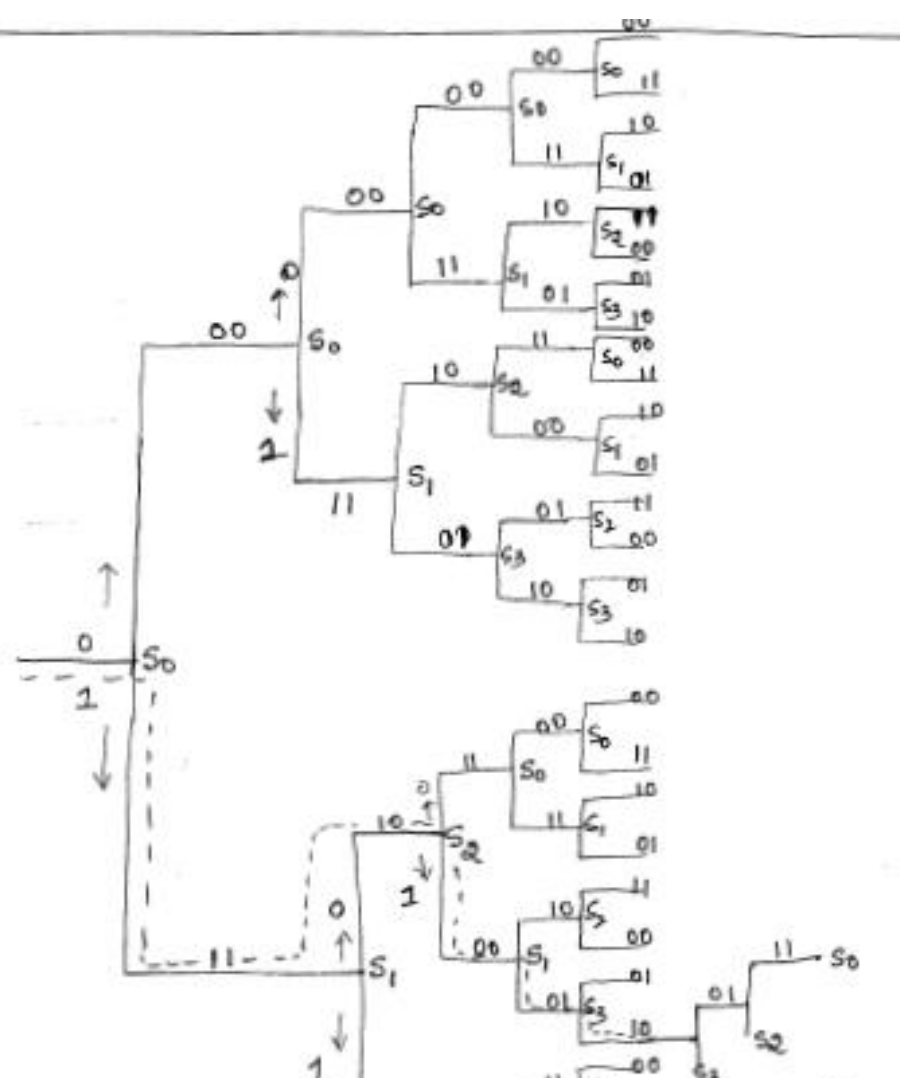
Present state	Input bit	Next state	d_1	d_{1-1}	d_{1-2}	Output $c^{(1)}$ $c^{(2)}$
$S_0 = 00$	0	$S_0 = 00$	0	0	0	0 0
	1	$S_1 = 10$	1	0	0	1 1
$S_1 = 10$	0	$S_2 = 01$	0	1	0	1 0
	1	$S_3 = 11$	1	1	0	0 1
$S_2 = 01$	0	$S_0 = 00$	0	0	1	1 1
	1	$S_1 = 10$	1	0	1	0 0
$S_3 = 11$	0	$S_2 = 01$	0	1	1	0 1
	1	$S_3 = 11$	1	1	1	1 0

Construction: Initially, let the flip flops be cleared i.e. '00'.

- If $i/p = 0 \Rightarrow$ shift register at '00' $\rightarrow S_0$, \therefore o/p of add $c^{(1)} c^{(2)} = 00$
- If $i/p = 1$ the flip FF, changes state from 0 to 1 the contents of FF, (which was '0') get shifted to FF₀. \therefore The new shift register contents are '10' $\rightarrow S_1$ this transition is caused by a $i/p = 1 \& d_1 d_{1-1} d_{1-2} = 11$ & $c^{(1)} c^{(2)} = 11$.

③ State diagram.





The no of flipflops in encoder = $m=2$
 \therefore 2 more bits are needed to reset the encodes.

To obtain the complete code corresponding to a i/p data of length KL , the tree graph has to be extended by $n(m-3)$ time units & this extended part is called 'tail of the tree'

← Tail of tree