RSET

RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY

101001/EC600C INFORMATION THEORY & CODING

MODULE 4 - PART 1

Ms. Anila Kuriakose, Asst Professor, Dept. of ECE, RSET

Syllabus

Module 4: A Few Important Classes of Algebraic codes

Cyclic codes. Polynomial and matrix description. Interrelation between polynomial and matrix view point. Systematic encoding. Decoding of cyclic codes.

(Only description, no decoding algorithms) Hamming Codes, BCH codes, Reed-Solomon Codes.

Cyclic Codes

- An (n,k) linear block code is said to be cyclic if every cyclic shift of the code is also code vector of C.

- Eg: If $\boldsymbol{V_1 = 0101110,}$ then $\boldsymbol{V_2 = 0010111}$, $\boldsymbol{V_3 = 1001011}$, etc. will also be code vectors of V.

Cyclic codes

- It is a subclass of *linear block codes*.
- An advantage of cyclic codes over most other types of codes:

  1. Encoding & Syndrome calculating circuits can be easily implemented

  - Using simple shift registers with feed back connections.

  2. Well defined mathematical structure that permits the design of higher-order error correcting codes.

- Cyclic codes have algebraic structures which makes it possible to design codes with useful error correcting properties.
- An (n, k) linear block code is said to be cyclic if every cyclic shift of the code is also code vector of C.

Cyclic codes

- A binary code is said to be a *cyclic code* if it satisfies:
  a) **Linearity Property:** The sum of any two codewords in the code is also a codeword.
  b) **Cyclic Property:** Any cyclic shift (lateral shift) of a codeword in the code is also a codeword.

Messages	Code Vectors	Code polynomials
(0 0 0 0)	0 0 0 0 0 0 0	$0 = 0 \cdot \mathbf{g}(X)$
(1 0 0 0)	1 1 0 1 0 0 0	$1 + X + X^3 = 1 \cdot \mathbf{g}(X)$
(0 1 0 0)	0 1 1 0 1 0 0	$X + X^2 + X^4 = X \cdot \mathbf{g}(X)$
(1 1 0 0)	1 0 1 1 1 0 0	$1 + X^2 + X^3 + X^4 = (1 + X) \cdot \mathbf{g}(X)$
(0 0 1 0)	0 0 1 1 0 1 0	$X^2 + X^3 + X^5 = X^2 \cdot \mathbf{g}(X)$
(1 0 1 0)	1 1 1 0 0 1 0	$1 + X + X^2 + X^5 = (1 + X^2) \cdot \mathbf{g}(X)$
(0 1 1 0)	0 1 0 1 1 1 0	$X + X^3 + X^4 + X^5 = (X + X^2) \cdot \mathbf{g}(X)$
(1 1 1 0)	1 0 0 0 1 1 0	$1 + X^4 + X^5 = (1 + X + X^2) \cdot \mathbf{g}(X)$
(0 0 0 1)	0 0 0 1 1 0 1	$X^3 + X^4 + X^6 = X^3 \cdot \mathbf{g}(X)$
(1 0 0 1)	1 1 0 0 1 0 1	$1 + X + X^4 + X^6 = (1 + X^3) \cdot \mathbf{g}(X)$
(0 1 0 1)	0 1 1 1 0 0 1	$X + X^2 + X^3 + X^6 = (X + X^3) \cdot \mathbf{g}(X)$
(1 1 0 1)	1 0 1 0 0 0 1	$1 + X^2 + X^6 = (1 + X + X^3) \cdot \mathbf{g}(X)$
(0 0 1 1)	0 0 1 0 1 1 1	$X^2 + X^4 + X^5 + X^6 = (X^2 + X^3) \cdot \mathbf{g}(X)$
(1 0 1 1)	1 1 1 1 1 1 1	$1 + X + X^2 + X^3 + X^4 + X^5 + X^6 = (1 + X^2 + X^3) \cdot \mathbf{g}(X)$
(0 1 1 1)	0 1 0 0 0 1 1	$X + X^5 + X^6 = (X + X^2 + X^3) \cdot \mathbf{g}(X)$
(1 1 1 1)	1 0 0 1 0 1 1	$1 + X^3 + X^5 + X^6 = (1 + X + X^2 + X^3) \cdot \mathbf{g}(X)$

Algebraic Structure of Cyclic Codes

- In general let the n tuple code vector be represented as

$$V = (\ v_0\ \ v_1\ \ v_2\ \ \dots\dots\dots v_{n-1})$$

- The code vectors can be represented in polynomial form of order (n-1) as

$$V(x) = v_0 + v_1x + v_2x^2 + \dots\dots\dots + v_{n-1}x^{n-1}$$

Properties of Cyclic Codes

1. For (n,k) cyclic code, the generator polynomial of degree (n-k) is given as

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

2. The generator polynomial g(x) of an (n,k) cyclic code is a factor of $X^n + 1$

$$X^n + 1 = g(x).h(x)$$

h(x) is another polynomial of degree k called the **parity check polynomial**

3. The code vector polynomial V(x) in non systematic form is given as

$V(x) = U(x).g(x)$, where U(x) is the message polynomial of degree k-1

$$U(x) = u_0 + u_1x + u_2x^2 + \dots\dots\dots + u_{k-1}x^{k-1}$$

Systematic Cyclic Codes

$$V = (\ v_0\ \ v_1\ \ v_2\ \ \ldots\ldots..v_{n-1})$$
$$= (\ p_0\ , p_1\ , p_2\ , \ldots p_{n-k-1}, u_o\ , u_1, \ldots..u_{k-1})$$

$$V(X) = P(X) + X^{n-k}u(X)$$

where P(X) is the remainder obtained by dividing $\frac{X^{n-k}\,u(X)}{g(x)}$

Example for (7,4) non systematic cyclic code:

n=7, k=4, n-k=3

- Let us take **g(x)=** $\mathbf{1 + X + X^3}$. [g(x) is a polynomial of order n-k=3]
- u(X) is the message polynomial with order k-1=3

u(X) = $\boldsymbol{u_o + u_1X + u_2X^2 + u_3X^3}$

- ∴The code polynomial is
- **v(X)=u(X).g(X)**

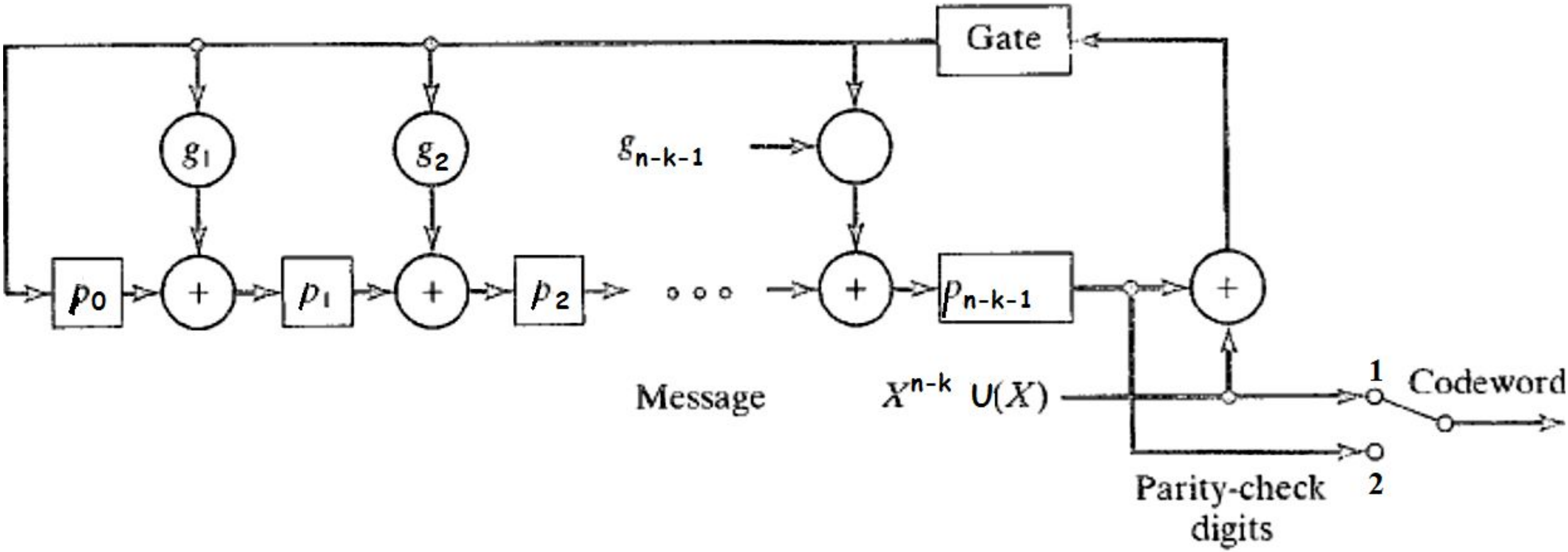
- **Find answer and verify**

Systematic Cyclic Codes

Steps to generate systematic cyclic code:

1. Generate g(X).
2. Pre-multiply message u(X) by $\boldsymbol{X^{n-k}}$ to shift the message bits to the last.
3. Obtain the remainder P(X) (parity polynomial) by $\dfrac{\boldsymbol{X^{n-k}.u(X)}}{\boldsymbol{g(X)}}$
4. $\boldsymbol{V(X) = p(X) + X^{n-k}u(X)}$

Encoding Circuit of (n,k) Cyclic Code using generator polynomial



Steps for Encoding

Steps for Encoding

Initially the contents of all shift registers are 0.

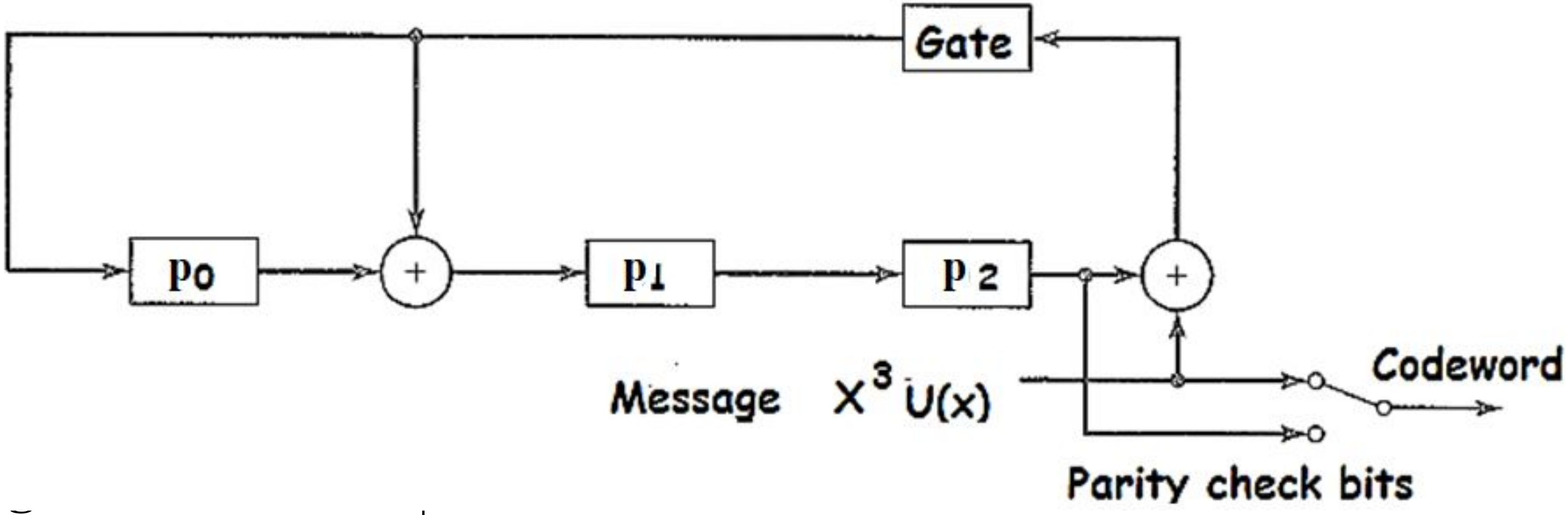
Step 1 :With the gate turned on and the switch at ‘1’, the k information digits $\boldsymbol{u_0, u_1 \ldots . u_{k-1}}$ (or $\boldsymbol{u(X) = u_0 + u_1 X + \ldots\ldots + u_{k-1} X^{k-1}}$ in the polynomial form) are shifted into the circuit and simultaneously into the communication channel. Shifting the message u(X) into the circuit from the front end is equivalent to pre-multiplying u(X) by $\boldsymbol{X^{n-k}}$. As soon as the complete message has entered the circuit, the n – k digits in the register form the remainder and thus they are the parity-check digits.

Step 2 : Break the feedback connection by turning off the gate and the switch position is moved to ‘2’.

Step 3 : Shift the parity-check digits out and send them into the channel. These (n-k) parity digits $\boldsymbol{p_0, p_1 \ldots . p_{n-k-1}}$, together with the message bits form the code word

Q. Draw the encoding circuit for a (7,4) systematic cyclic code with generator matrix $\mathbf{g}(X) = 1 + X + X^3$ and find the codeword for message U=[1011]

$g_0 = 1, g_1 = 1,$
$g_2 = 0, g_3 = 1$



Input	R
1	
1	
0	
1	

Code word =[p u]

=**Answer**

Q. For a systematic (n,k) cyclic code with $\mathbf{g}(\boldsymbol{X}) = \mathbf{1} + \boldsymbol{X} + \boldsymbol{X}^{\mathbf{3}}$, find the codeword for message U=[1011], U=[1001] & U=[0101]

u=[1 0 1 1], u(X)=1 $+X^2 + X^3$

$$P(X) = remainder\ of\ \left\{\frac{X^{n-k}\,u(X)}{\mathrm{g(X)}}\right\} = \boldsymbol{answer}$$

Codeword V(X) = $p(X) + X^{n-k}u(X) = p(X) + X^3u(X)$

$= \boldsymbol{answer}$

Generator & Parity check matices of (n,k) Cyclic code

- The generator polynomial is given by

$$g(X) = g_0 + g_1X + g_2X^2 + \ldots\ldots + g_{n-k}X^{n-k}$$

where $g_0 = g_{n-k} = 1$

- The **generator matrix** of size k×n is formed with g(X) as the first row, $\mathbf{X}g(X)$ as the second row, $X^2g(X)$ as the third row ……and $X^{k-1}g(X)$ as the last row.
- The generator matrix formed will be in the non systematic form which can be transformed to systematic form by row manipulations.

- To form the parity check matrix, H of size (n-k)×n ,we find the parity check polynomial h(X)

$$\boldsymbol{X^n + 1 = g(X).h(X)}$$

$$\boldsymbol{h(X) = \frac{X^n + 1}{g(X)}}$$

- $\boldsymbol{X^k h(X^{-1}),\ X^{k+1} h(X^{-1}), X^{k+2} h(X^{-1})}$ is computed and is used to form the first, second,………$\boldsymbol{(n-k)^{th}}$ row the of H matrix respectively.

- The H matrix so formed is in the non systematic form.
- The systematic H matrix can be obtained by row manipulations.

Q. Construct the generator matrix and parity check matrix for a (7,4) cyclic code with generator polynomial $\mathbf{g}(X) = 1 + X + X^3$.

Soln:

n=7, k=4, n-k=3

Size of G = k×n = 4×7

$$\mathbf{g}(X) = 1 + X + X^3$$

$$Xg(X) = X + X^2 + X^4$$

$$X^2 g(X) = X^2 + X^3 + X^5$$

$$X^3 g(X) = X^3 + X^4 + X^6$$

$$G = [answer]$$

$$G\ in\ systematic\ form = [P|\ \ I_k] = [P|\ \ I_4]$$

Systematic Form

$$G = [\quad]$$

$$X^n + 1 = X^7 + 1 = g(X).h(X)$$

$$h(X) = \frac{X^7 + 1}{g(x)} = \frac{X^7 + 1}{1 + X + X^3}$$

Size of H = (n-k)×n = 3×7

$$h(X) = 1 + X + X^2 + X^4$$

$$h(X^{-1}) = 1 + X^{-1} + X^{-2} + X^{-4}$$

$$X^k h(X^{-1}) = X^4 h(X^{-1}) = X^4 + X^3 + X^2 + 1$$

$$X^5 h(X^{-1}) = X^5 + X^4 + X^3 + X$$

$$X^6 h(X^{-1}) = X^6 + X^5 + X^4 + X^2$$

$$H = [\quad]$$

In systematic form

$$H = [I_{n-k} \mid P^T] = [I_3 \mid P^T]$$

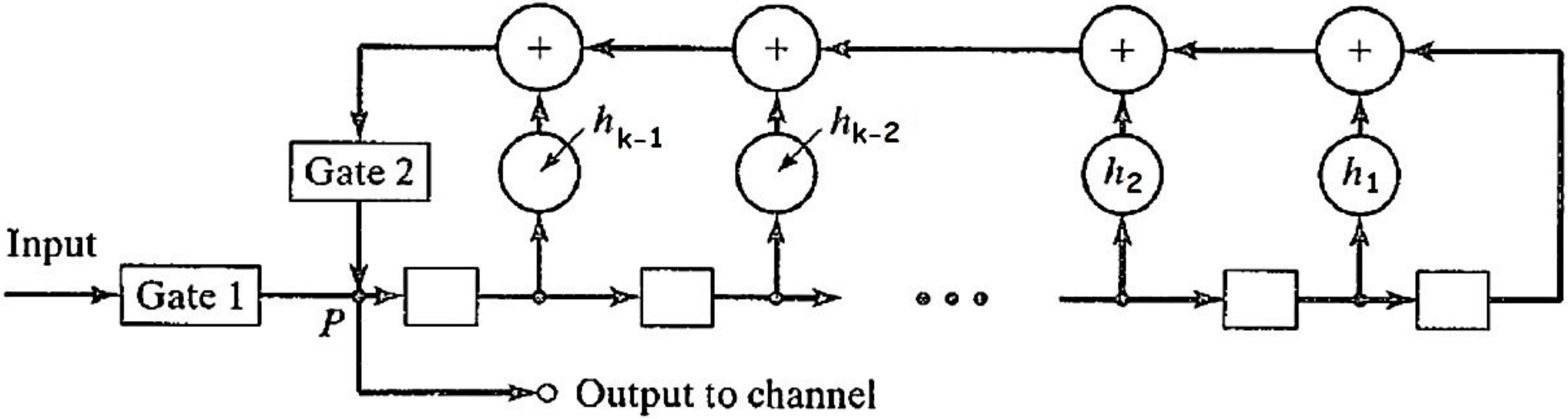
$$H = [answer]$$

Encoding of Cyclic Codes using Parity Check Polynomial

- Encoding of a cyclic code can also be done using parity check polynomial of degree k

$$\boldsymbol{h(X) = h_0 + h_1 X + h_2 X^2 + \ldots\ldots\ldots + h_k X^k}$$

where $\boldsymbol{h_k} = \boldsymbol{h_0} = 1$



Steps for Encoding

Step 1 : Initially gate 1 is turned on and gate 2 is turned off. The k information digits $u_0, u_1 \dots\dots u_{k-1}$ (or $u(X) = u_0 + u_1X + \dots\dots + u_{k-1}X^{k-1}$ in the polynomial form) are shifted into the register and the communication channel simultaneously.

Step 2 :As soon as the k information digits have entered the shift register, gate 1 is turned off and gate 2 is turned on. The first parity-check digit $v_{n-k-1} = u_{k-1} + h_1u_{k-2} + \dots\dots + h_{k-1}u_0$ is formed and appears at point P.

Step 3 : The first parity -check digits is shifted into the channel and is also shifted into the register. The second parity-check digits $v_{n-k-2} = u_{k-2} + h_1u_{k-3} + \dots\dots + h_{k-2}u_0 + h_{k-1}v_{n-k-1}$ is formed at P

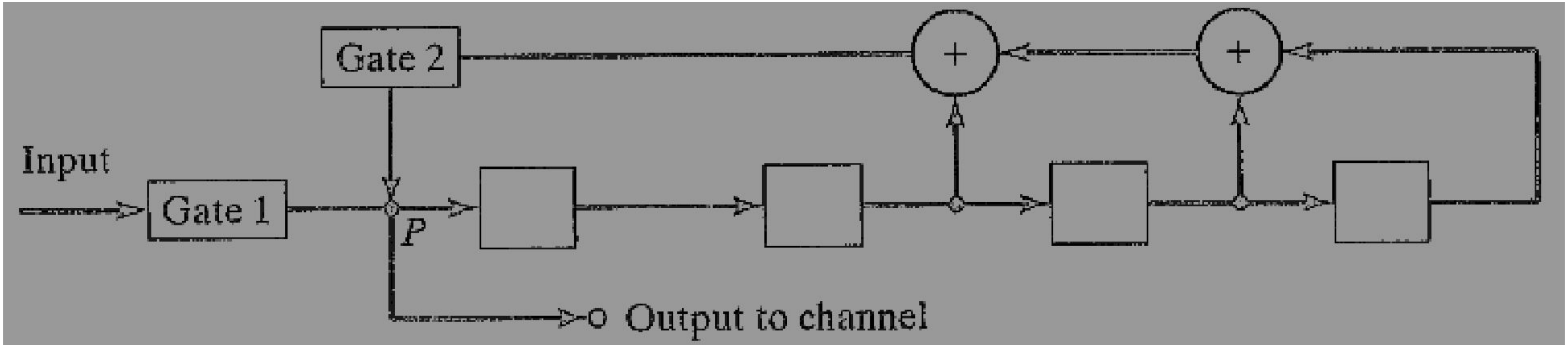
Step 4 :Step 3 is repeated until n – k parity-check digits have been formed and shifted into the channel.

Q: Draw the encoding circuit for a (7,4) systematic cyclic code with generator polynomial $g(X) = 1 + X + X^3$ for message U=[1011] using h(X).

$$X^n + 1 = X^7 + 1 = g(X).h(X)$$

$$h(X) = \frac{X^7 + 1}{g(X)} = \frac{X^7 + 1}{1 + X + X^3} = 1 + X + X^2 + X^4$$

$$h_1 = 1, h_2 = 1, h_{k-1} = h_3 = 0$$



U=[1011] $\boldsymbol{u_0 = 1, u_1 = 0, u_2 = 1, u_3 = 1}$

The first parity-check digits is

$$\boldsymbol{v_{n-k-1} = v_2 = u_{k-1} + h_1 u_{k-2} + \ldots\ldots + h_{k-1} u_0 = u_3 + h_1 u_2 + h_2 u_1 + h_3 u_0}$$

$$\boldsymbol{= 1 + 1 + 0 + 0 = 0}$$

The second parity-check digits is

$$\boldsymbol{v_{n-k-2} = v_1 = u_{k-2} + h_1 u_{k-3} + \ldots\ldots + h_{k-2} u_0 + h_{k-1} v_{n-k-1}}$$

$$\boldsymbol{= u_2 + h_1 u_1 + h_2 u_0 + h_3 v_2 = 1 + 0 + 1 + 0 = 0}$$

The third parity-check digits is

$$\boldsymbol{v_{n-k-3} = v_0 = u_{k-3} + \ldots\ldots + h_{k-3} u_0 + h_{k-2} v_{n-k-1} + h_{k-1} v_{n-k-2}}$$

$$\boldsymbol{= u_1 + h_1 u_0 + h_2 v_2 + h_3 v_1 = 0 + 1 + 0 + 0 = 1}$$

Thus, the code vector that corresponds to the message (1 0 1 1) is (1 0 0 1 0 1 1)

- To form the H matrix of size (n-k)×n ,we find the parity check polynomial h(X) by

$$\boldsymbol{X^n + 1 = g(X).h(X)}$$

- $\boldsymbol{X^k h(X^{-1}), X^{k+1} h(X^{-1}), X^{k+2} h(X^{-1})}$ ….. $\boldsymbol{X^{k+(n-k-1)} h(X^{-1})}$ is computed and is used to form the first, second,………$\boldsymbol{(n-k)^{th}}$ row the of H matrix respectively.

- The H matrix so formed is in the <u>non systematic form.</u>
- The systematic H matrix can be obtained by row manipulations.

Generator Polynomial for Cyclic Codes

- An ***(n, k)*** cyclic code for set of code polynomials of degree ≤ ***(n–1)*** and contains a polynomial ***g(X)***, of degree ***(n – k)*** as a factor, called the "***generator polynomial***" of the code.
- Polynomial is equivalent to the generator matrix ***G***, of block codes.
- Since degree of g(X) is (n – k), $g_0 = g_{n-1} = 1$.
- $g(X) = 1 + \sum_{i=1}^{n-k-1} g_i X^i + X^{n-k}$

  As $g(X) = g_0 + g_1 X + g_2 X^2 + \ldots\ldots\ldots + g_{n-k} X^{n-k}$
- It is the only polynomial of minimum degree and is unique.

Generator & Parity Check Matrices of Cyclic Codes

- The generator polynomial is given by

  $$g(X) = g_0 + g_1X + g_2X^2 + \ldots\ldots\ldots + g_{n-k}X^{n-k}$$

  where $g_0 = g_{n-k} = 1$
- The polynomials $Xg(X)$, $X^2 g(X)$, $X^3 g(X), \ldots, X^{k-1} g(X)$ also represent the code vector polynomials in the same code.
- The **generator matrix** of size $k \times n$ is formed with
  - **$g(X)$** as the first row,
  - $Xg(X)$ as the second row,
  - $X^2 g(X)$ as the third row, and
  - $X^{k-1} g(X)$ as the last row.

$$G = [P|\ I_k]$$

Generator & Parity Check Matrices of Cyclic Codes

- The generator matrix formed will be in the non systematic form which can be ***transformed to systematic form by row manipulations***. $G = [P|\ I_k]$
- To form the H matrix of size $(n-k) \times n$,we find the parity check polynomial h(X) by $\boldsymbol{X^n + 1 = g(X).h(X)}$
  - To construct H matrix, reciprocal of parity check polynomial defined by $X^k h(X^{-1})$, $X^k h(X^{-1})$ is also a factor of polynomial X^n+1.

Generator & Parity Check Matrices of Cyclic Codes

- $X^k h(X^{-1})$ → 1st row,
- $X^{k+1} h(X^{-1})$ → 2nd row,
- $X^{k+2} h(X^{-1})$ → 3rd row , …,
- $X^{k+(n-k-1)} h(X^{-1})$ → $(n-k)^{th}$ row the of H matrix respectively.
- The H matrix so formed is in the non systematic form.
- The ***systematic H matrix can be obtained by row manipulations***.

$$H = [I_{n-k} \mid P^T]$$

Problem 5.1

Q. Construct the generator matrix and parity check matrix for a *(7, 4)* cyclic code with generator polynomial $g(X) = X^3 + X + 1$.

Solution:

- Given n = 7, k = 4, n – k = 3
- Start with generator polynomial & its three cyclic shift versions are:

$$\mathbf{g}(\boldsymbol{X}) = \mathbf{1} + \boldsymbol{X} + \boldsymbol{X}^3$$
$$\boldsymbol{X}\boldsymbol{g}(\boldsymbol{X}) = \boldsymbol{X} + \boldsymbol{X}^2 + \boldsymbol{X}^4$$
$$\boldsymbol{X}^2\boldsymbol{g}(\boldsymbol{X}) = \boldsymbol{X}^2 + \boldsymbol{X}^3 + \boldsymbol{X}^5$$
$$\boldsymbol{X}^3\boldsymbol{g}(\boldsymbol{X}) = \boldsymbol{X}^3 + \boldsymbol{X}^4 + \boldsymbol{X}^6$$

Problem 5.1

- Now co-efficient of these polynomials are used as elements of 4 rows of a (4 x 7) matrix to get generator matrix as:

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

- Since generator matrix constructed is not in a systematic format, using *Row manipulation transform into systematic format.*
- $G = [P|\ I_k] = [P|\ I_4]$

Problem 5.1

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

- 1^{st} row & 2^{nd} row-no change
- 3^{rd} row $=3^{rd}$ row $+ 1^{st}$ row
- 4^{th} row $=4^{th} + 1^{st} + 2^{nd}$ row
- Thus, $G = \left[\begin{array}{ccc|cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right] = [P \vdots I_4]$
- Using this generator matrix, in systematic form code word for u= (1011) is v = (1001011) {obtained as sum of 1^{st} row $+3^{rd}$ row $+ 4^{th}$ row of G-matrix}

Problem 5.1

- To construct H-matrix, reciprocal of parity check polynomial defined by $X^k h(X^{-1})$. Polynomial $X^k h(X^{-1})$ is also a factor of polynomial X^n+1.
- $X^n + 1 = X^7 + 1 = g(X).h(X)$
- $h(X) = \frac{X^7+1}{g(x)} = \frac{X^7+1}{X^3+X+1} = X^4 + X^2 + X + 1$

$\therefore h(X) = 1 + X + X^2 + X^4$

- $h(X^{-1}) = 1 + X^{-1} + X^{-2} + X^{-4}$
- $X^k h(X^{-1}) = X^4 h(X^{-1}) = X^4 + X^3 + X^2 + 1$

Problem 5.1

1st row $X^4h(X^{-1}) = X^4 + X^3 + X^2 + 1$

2nd row $X^5h(X^{-1}) = X^5 + X^4 + X^3 + X$

3rd row $X^6h(X^{-1}) = X^6 + X^5 + X^4 + X^2$

The two cyclic shifted versions are

- Using the co-efficient of these polynomials, we have:

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

- This matrix is in non systematic form.
- In systematic form; $H = [I_{n-k} \mid P^T] = [I_3 \mid P^T]$

Problem 5.1

- *By Row Manipulation*; 1st row = 1st + 3rd row
- 2nd & 3rd row-no change

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

- Thus systematic format is obtained for $G = [P \;\vdots\; I_k]$ & $H = [I_{n-k} \;\vdots\; P^T]$.

Cyclic codes

A Cyclic Code is represented as (n, k) Code:

- 'n' → total number of bits in the codeword
- 'k' → total number of bits in the message
- 'n – k' = 'q' → total number of check bits or parity bits added to the message bits

Generator Polynomial is used to generate Cyclic Codes:

- For (n, k) cyclic code the Generator Polynomial is given by:

$$g(X) = X^q \oplus g_{q-1}X^{q-1} \oplus \ldots \oplus g_1X^1 \oplus 1$$

- The highest degree of generator polynomial is 'q'.

Q. Construct the generator matrix and parity check matrix for a (7,4) systematic cyclic code with generator polynomial $\mathbf{g}(X) = 1 + X + X^3$.

-

1st row & 2nd row-no change

3rd row =3rd row + 1st row

4th row =4th +1st + 2nd row

$$h(X) = 1 + X + X^2 + X^4$$

$$h(X^{-1}) = 1 + X^{-1} + X^{-2} + X^{-4}$$

$$X^k h(X^{-1}) = X^4 h(X^{-1}) = X^4 + X^3 + X^2 + 1$$

$$X^5 h(X^{-1}) = X^5 + X^4 + X^3 + X$$

$$X^6 h(X^{-1}) = X^6 + X^5 + X^4 + X^2$$

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

In systematic form

$$H = [I_{n-k} \mid P^T] = [I_3 \mid P^T]$$

1st row = 1st + 3rd row

2nd & 3rd row-no change

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

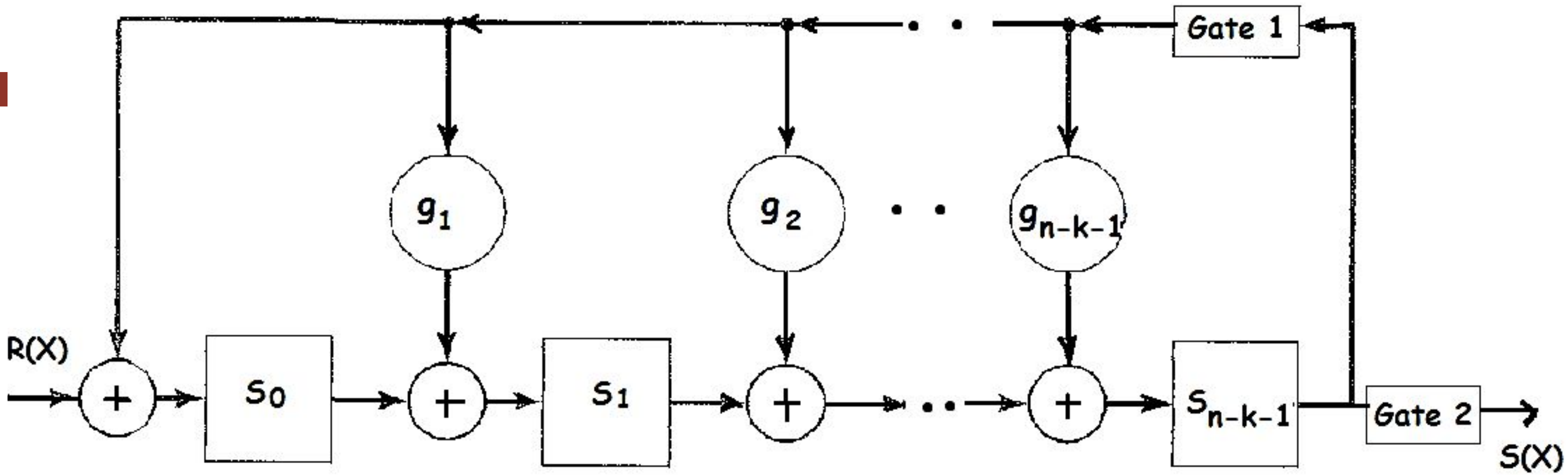
Syndrome Calculation for Error Detection and Correction

- Transmitted code vector v=$(\boldsymbol{v_0}\ \ \boldsymbol{v_1}\ \ \boldsymbol{v_2} \dots \dots \dots \dots \boldsymbol{v_{n-1}})$
- Received Code vector r= $(\boldsymbol{r_0}\ \ \boldsymbol{r_1}\ \boldsymbol{r_2} \dots \dots \dots \dots \boldsymbol{r_{n-1}})$
- Received Code vector in polynomial form
- $\boldsymbol{r(X) = r_0 + r_1X + r_2X^2 + \dots\dots\dots + r_{n-1}X^{n-1}}$
- If e(X) is the polynomial representing the error pattern caused by the channel
- $\mathbf{r}(\boldsymbol{X}) = \boldsymbol{v}(\boldsymbol{X}) + \boldsymbol{e}(\boldsymbol{X})$
- v(X) = u(X).g(X) $\rightarrow$ $\boldsymbol{r(X) = u(X).\,g(X) + e(X) --------- -(1)}$
- The syndrome s(X) of degree (n-k-1) is obtained as remainder by division of r(X) by the generator polynomial g(X)

$$\mathbf{r}(\boldsymbol{X}) = \boldsymbol{a(X).\,g(X) + s(X) --- -(2)}$$

- From (1) and (2) $\rightarrow$ $\boldsymbol{e(X) = [a(X) + u(X)].\,g(X) + s(X)}$

Syndrome Calculation Circuit



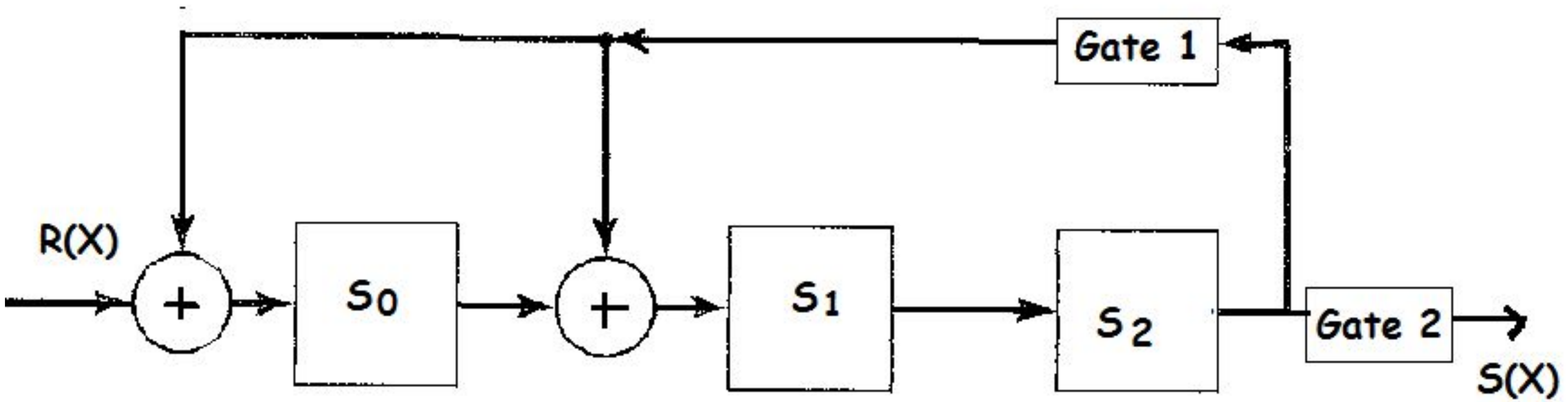
Step 1: The registers are first initialized to zero. With Gate 1 “ON” & Gate 2 “OFF”, the received vector is entered into the register.

Step 2: After the entire received vector is shifted into the register, the contents of the register will be the syndrome. The syndrome is shifted out of the register by turning Gate 2 ON and Gate 1 OFF.

Q. Draw the syndrome circuit for a (7,4) cyclic code with generator matrix $g(X) = 1 + X + X^3$.Compute the syndrome if the received code is r=[0010110]

$$g_0 = g_1 = 1, g_2 = 0, g_3 = 1$$

$$r(X) = X^2 + X^4 + X^5$$



0010110

Syndrome =answer

$s(X) =$

r	Register Contents
0	
1	
1	
0	
1	
0	
0	

END OF MODULE-4 PART-1

THANK YOU!!!!