CYCLIC CODE

TTI3J3 SISTEKM KOMUNIKASI II

CYCLIC CODE

- Cyclic code merupakan subklas dari block code. Suatu binary code dikatakan sebagai cyclic code bila memenuhi:
  - Sifat **Linearitas**: Penjumlahan dari dua buah codeword akan mengkasilkan codeword baru.
  - Sifat **cyclic**: Setiap pergeseran perputaran dari suatu code word akan menghasilkan codeword baru.
- Untuk proses encoding dan decoding , cyclic code dipermudah oleh sifat aljabar
- Untuk menggunakan sifat aljabar ini maka code cyclic direpresentasikan dalam bentuk Polynomial

v = (v0, v1, ,v2, ..., vn-1) → $V(X) = v_0 + v_1 X + v_2 X^2 + \ldots + v_{n-1} X^{n-1}$

CYCLIC CODE(7,4)

Information Message (m)	Codeword (U)	Code Polynomial U(X)
(0 0 0 0)	(0 0 0 0 0 0 0)	0
(1 0 0 0)	(1 1 0 1 0 0 0)	$1+X+X^3$
(0 1 0 0)	(0 1 1 0 1 0 0)	$X+X^2+X^4$
(1 1 0 0)	(1 0 1 1 1 0 0)	$1+X^2+X^3+X^4$
(0 0 1 0)	(0 0 1 1 0 1 0)	$X^2+X^3+X^5$
(1 0 1 0)	(1 1 1 0 0 1 0)	$1+X+X^2+X^5$
(0 1 1 0)	(0 1 0 1 1 1 0)	$X+X^3+X^4+X^5$
(1 1 1 0)	(1 0 0 0 1 1 0)	$1+X^4+X^5$
(0 0 0 1)	(0 0 0 1 1 0 1)	$X^3+X^4+X^6$
(1 0 0 1)	(1 1 0 0 1 0 1)	$1+X+X^4+X^6$
(0 1 0 1)	(0 1 1 1 0 0 1)	$X+X^2+X^3+X^6$
(1 1 0 1)	(1 0 1 0 0 0 1)	$1+X^2+X^6$
(0 0 1 1)	(0 0 1 0 1 1 1)	$X^2+X^4+X^5+X^6$
(1 0 1 1)	(1 1 1 1 1 1 1)	$1+X+X^2+X^3+X^4+X^5+X^6$
(0 1 1 1)	(0 1 0 0 0 1 1)	$X+X^5+X^6$
(1 1 1 1)	(1 0 0 1 0 1 1)	$1+X^3+X^5+X^6$

- Ekspresi codeword Cyclic code dalam bentuk polinomial

$$\mathbf{U}(X) = u_0 + u_1 X + u_2 X^2 + \ldots + u_{n-1} X^{n-1} \quad \text{degree } (n-1)$$

- Hubungan antara codeword dan pergeseran siklis:

$$\begin{aligned} X\mathbf{U}(X) &= u_0 X + u_1 X^2 + \ldots, u_{n-2} X^{n-1} + u_{n-1} X^n \\ &= \underbrace{u_{n-1} + u_0 X + u_1 X^2 + \ldots + u_{n-2} X^{n-1}}_{\mathbf{U}^{(1)}(X)} \\ &= \mathbf{U}^{(1)}(X) + u_{n-1}(X^n + 1) \end{aligned}$$

  - Oleh karena itu:

$$\mathbf{U}^{(1)}(X) = X\mathbf{U}(X) \text{ modulo } (X^n + 1)$$

By extension

$$\mathbf{U}^{(i)}(X) = X^i \mathbf{U}(X) \text{ modulo } (X^n + 1)$$

CYCLIC CODE

- **Basic properties of Cyclic codes:**
  - Let C be a binary (n,k) linear cyclic code
    1. Within the set of code polynomials in C, there is a unique monic polynomial $\mathbf{g}(X)$ with minimal degree $r < n$. $\mathbf{g}(X)$ is called the generator polynomials.

$$\mathbf{g}(X) = g_0 + g_1 X + \ldots + g_r X^r$$

    2. Every code polynomial $\mathbf{U}(X)$ in C, can be expressed uniquely as

$$\mathbf{U}(X) = \mathbf{m}(X)\mathbf{g}(X)$$

    3. The generator polynomial $\mathbf{g}(X)$ is a factor of $X^n + 1$

CYCLIC CODE

- The orthogonality of **G** and **H** in polynomial form is expressed as $\mathbf{g}(X)\mathbf{h}(X) = X^n + 1$. This means $\mathbf{h}(X)$ is also a factor of $X^n + 1$

1. The row $i, i = 1, \ldots, k,$ of generator matrix is formed by the coefficients of the $"i-1"$ cyclic shift of the generator polynomial.

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}(X) \\ X\mathbf{g}(X) \\ \vdots \\ X^{k-1}\mathbf{g}(X) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & & & & \mathbf{0} \\ & g_0 & g_1 & \cdots & g_r & & & \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & g_0 & g_1 & \cdots & g_r & \\ \mathbf{0} & & & & g_0 & g_1 & \cdots & g_r \end{bmatrix}$$

CONTOH:

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{n-k} & 0 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{n-k} & 0 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{n-k} & 0 & \cdot & \cdot & 0 \\ \cdot \\ \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & g_{n-k} \end{pmatrix}$$

Example: (7,4) Cyclic Code with $g(X)=1+X+X^3$

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

Could be converted to systematic form with the help of row operations →

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

SYSTEMATIC CYCLIC CODE

- **Systematic encoding algorithm for an (n,k) Cyclic code:**

1. Multiply the message polynomial $\mathbf{m}(X)$ by X^{n-k}

2. Divide the result of Step 1 by the generator polynomial $\mathbf{g}(X)$. Let $\mathbf{p}(X)$ be the reminder.

3. Add $\mathbf{p}(X)$ to $X^{n-k}\mathbf{m}(X)$ to form the codeword $\mathbf{U}(X)$

CYCLIC CODE

- Example: For the systematic (7,4) Cyclic code with generator polynomial $\mathbf{g}(X) = 1 + X + X^3$
  1. Find the codeword for the message $\mathbf{m} = (1011)$

$$n = 7, \quad k = 4, \quad n - k = 3$$

$$\mathbf{m} = (1011) \Rightarrow \mathbf{m}(X) = 1 + X^2 + X^3$$

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

Divide $X^{n-k}\mathbf{m}(X)$ by $\mathbf{g}(X)$:

$$X^3 + X^5 + X^6 = \underbrace{(1 + X + X^2 + X^3)}_{\text{quotient } \mathbf{q}(X)}\underbrace{(1 + X + X^3)}_{\text{generator } \mathbf{g}(X)} + \underbrace{1}_{\text{remainder } \mathbf{p}(X)}$$

Form the codeword polynomial:

$$\mathbf{U}(X) = \mathbf{p}(X) + X^3\mathbf{m}(X) = 1 + X^3 + X^5 + X^6$$

$$\mathbf{U} = (\underbrace{1\ 0\ 0}_{\text{parity bits}}\ \underbrace{1\ 0\ 1\ 1}_{\text{message bits}})$$

CYCLIC CODE

- Find the generator and parity check matrices, **G** and **H**, respectively.

$$\mathbf{g}(X) = 1 + 1\cdot X + 0\cdot X^2 + 1\cdot X^3 \Rightarrow (g_0, g_1, g_2, g_3) = (1101)$$

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

Not in systematic form.
We do the following:

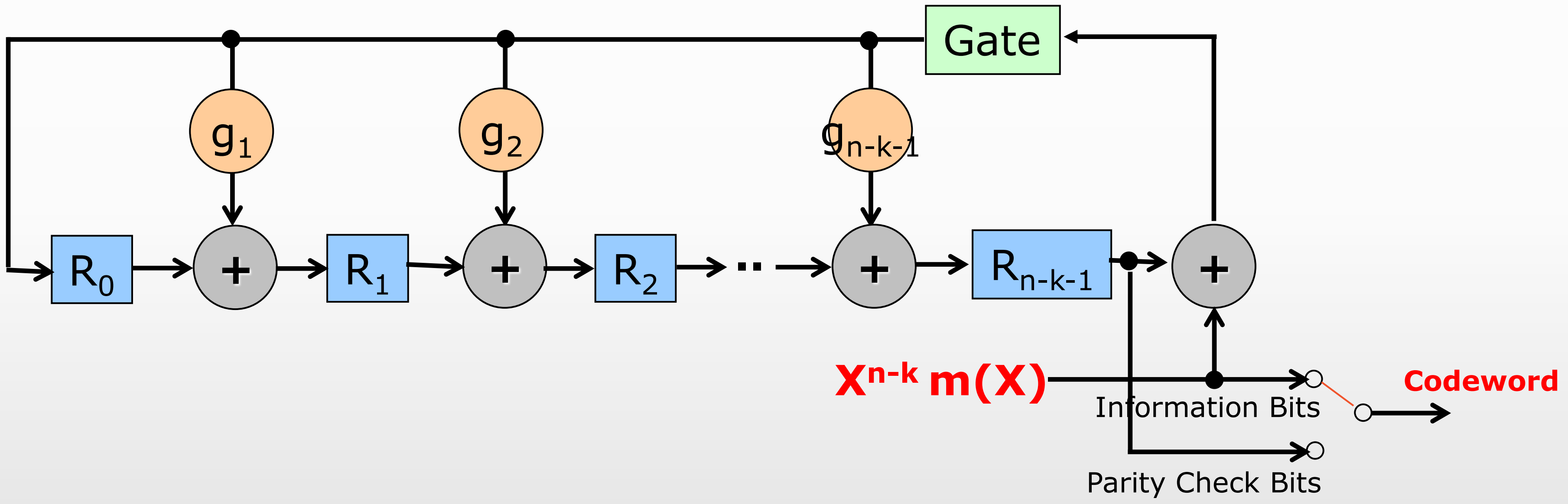
- $\text{row}(1) + \text{row}(3) \rightarrow \text{row}(3)$
- $\text{row}(1) + \text{row}(2) + \text{row}(4) \rightarrow \text{row}(4)$

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} = [\,\underbrace{\mathbf{P}}\;\vdots\;\underbrace{\mathbf{I}_{4\times4}}\,]$$

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} = [\,\underbrace{\mathbf{I}_{3\times3}}\;\vdots\;\underbrace{\mathbf{P}^T}\,]$$

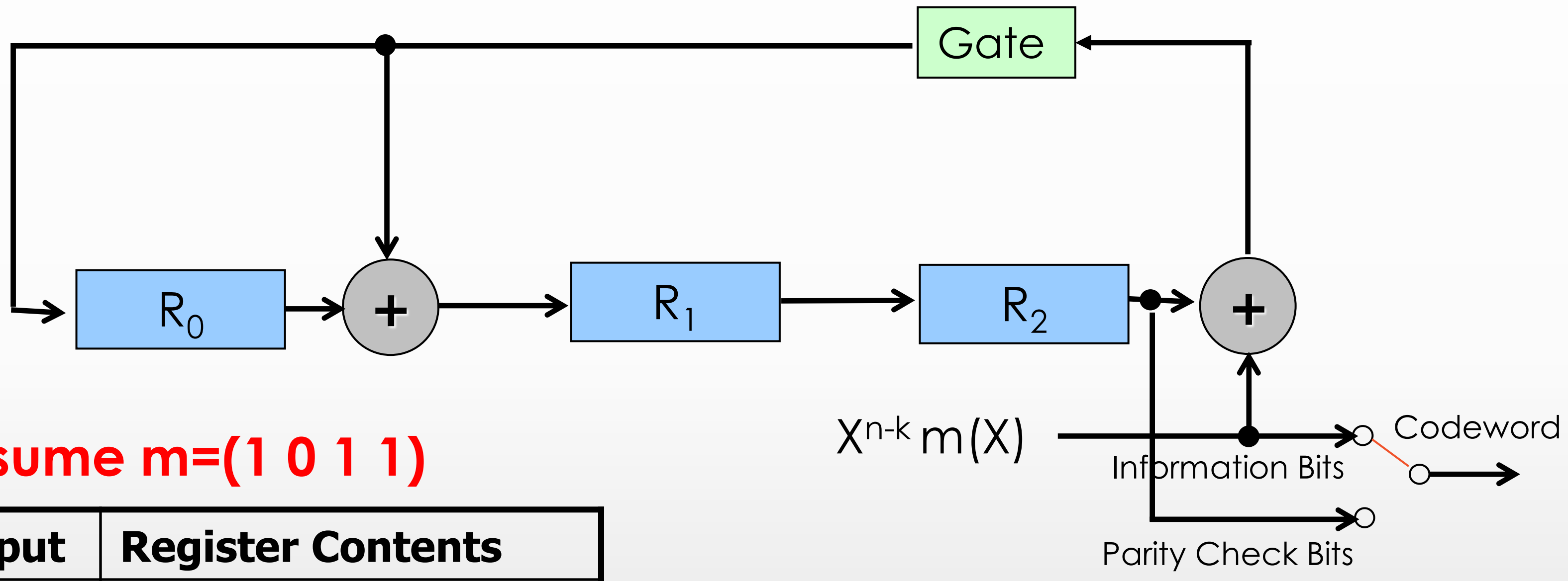
RANGKAIAN ENCODER KODE CYCLIC

Encoding Circuit is a Division Circuit



CONTOH

Encoding Circuit of (7,4) Cyclic Code with $g(X)=1+X+X^3$



Assume m=(1 0 1 1)

Input	Register Contents
	0 0 0 (Initial State)
1	1 1 0 (First Shift)
1	1 0 1 (Second Shift)
0	1 0 0 (Third Shift)
1	1 0 0 (Fourth Shift)

Codeword:
(1 0 0 1 0 1 1)

CONTOH: VERIFIKASI RANGKAIAN ENKODER

$m=(1\ 0\ 1\ 1) \rightarrow m(X) = 1+X^2+X^3$

1. $X^3m(X) = X^3+X^5+X^6$
2. $X^3m(X)/g(X) = (1+X+X^2+X^3) + 1/g(X) \rightarrow p(X) = 1$
3. $U(X) = 1+X^3+X^5+X^6 \rightarrow U = (1\ 0\ 0\ 1\ 0\ 1\ 1)$

SYNDROME

- Syndrome decoding for Cyclic codes:
  - Received codeword in polynomial form is given by

$$\mathbf{r}(X) = \mathbf{U}(X) + \mathbf{e}(X)$$

Received codeword ← $\mathbf{r}(X)$; $\mathbf{e}(X)$ → Error patter n

  - The syndrome is the reminder obtained by dividing the received polynomial by the generator polynomial.

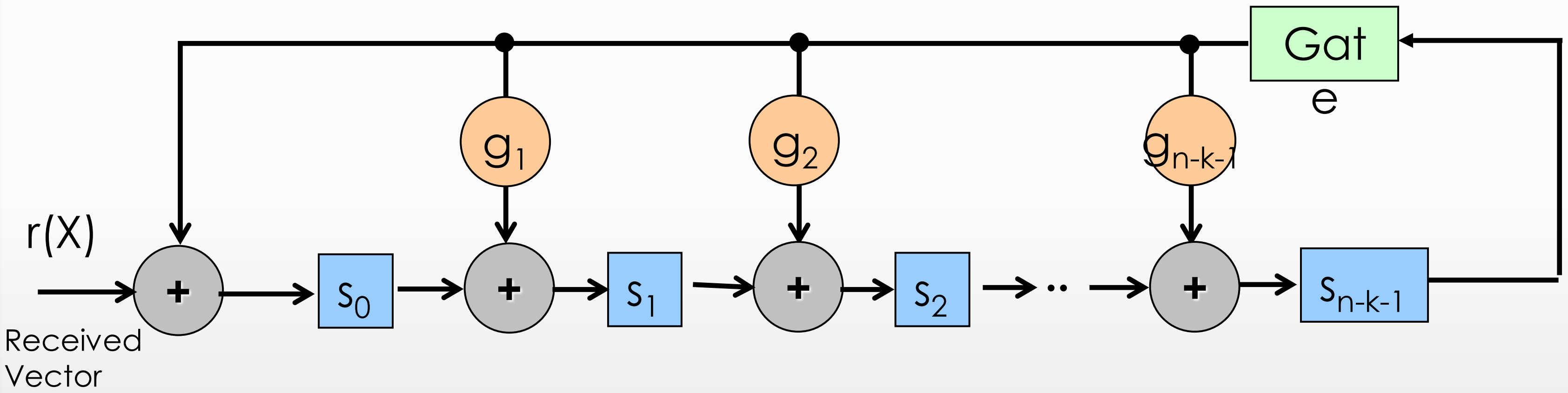
$$\mathbf{r}(X) = \mathbf{q}(X)\mathbf{g}(X) + \mathbf{S}(X)$$

$\mathbf{S}(X)$ → Syndrome

  - With syndrome and Standard array, error is estimated.
    - In Cyclic codes, the size of standard array is considerably reduced.

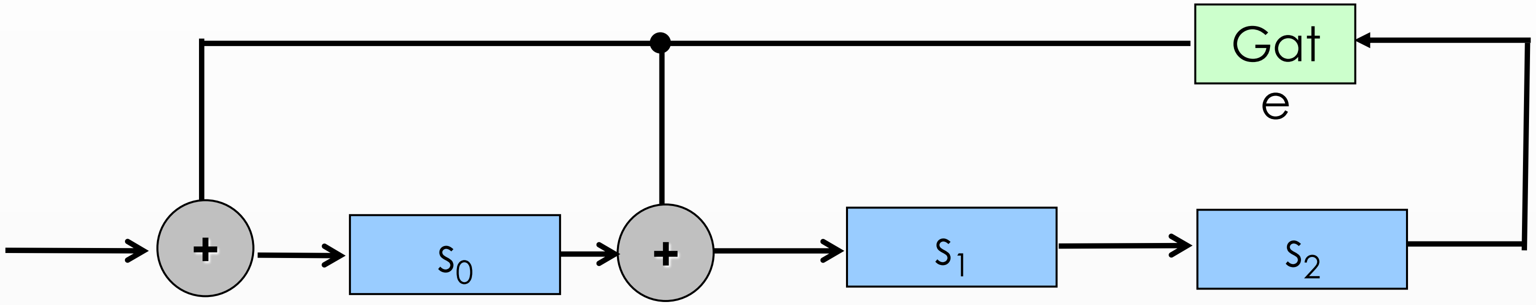
RANGKAIAN SYNDROME

Syndrome Circuit is a Division Circuit



CONTOH : RANGKAIAN SYNDROME

Syndrome Circuit of (7,4) Cyclic Code with $g(X)=1+X+X^3$

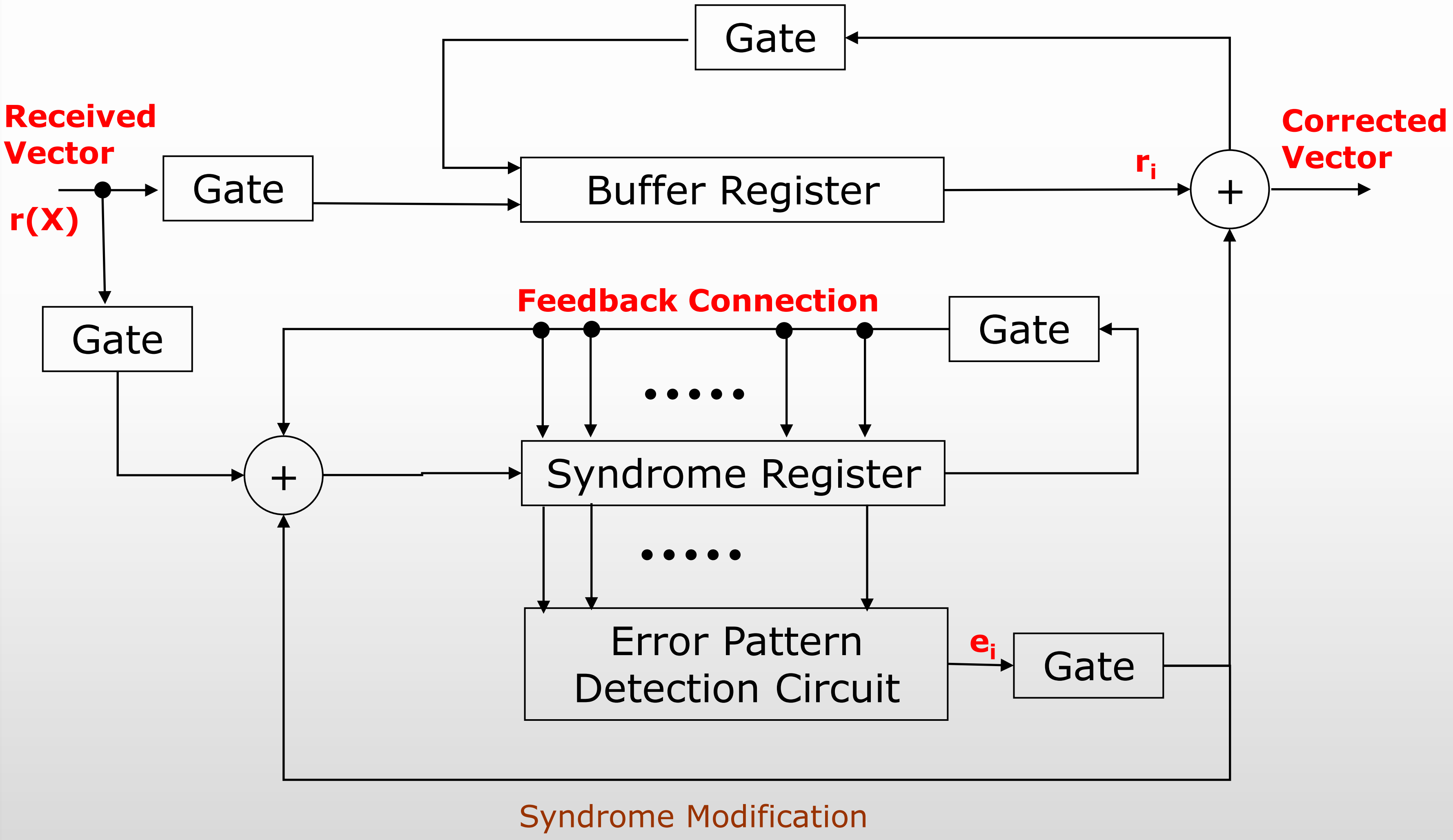


Assume r=(0 0 1 0 1 1 0)

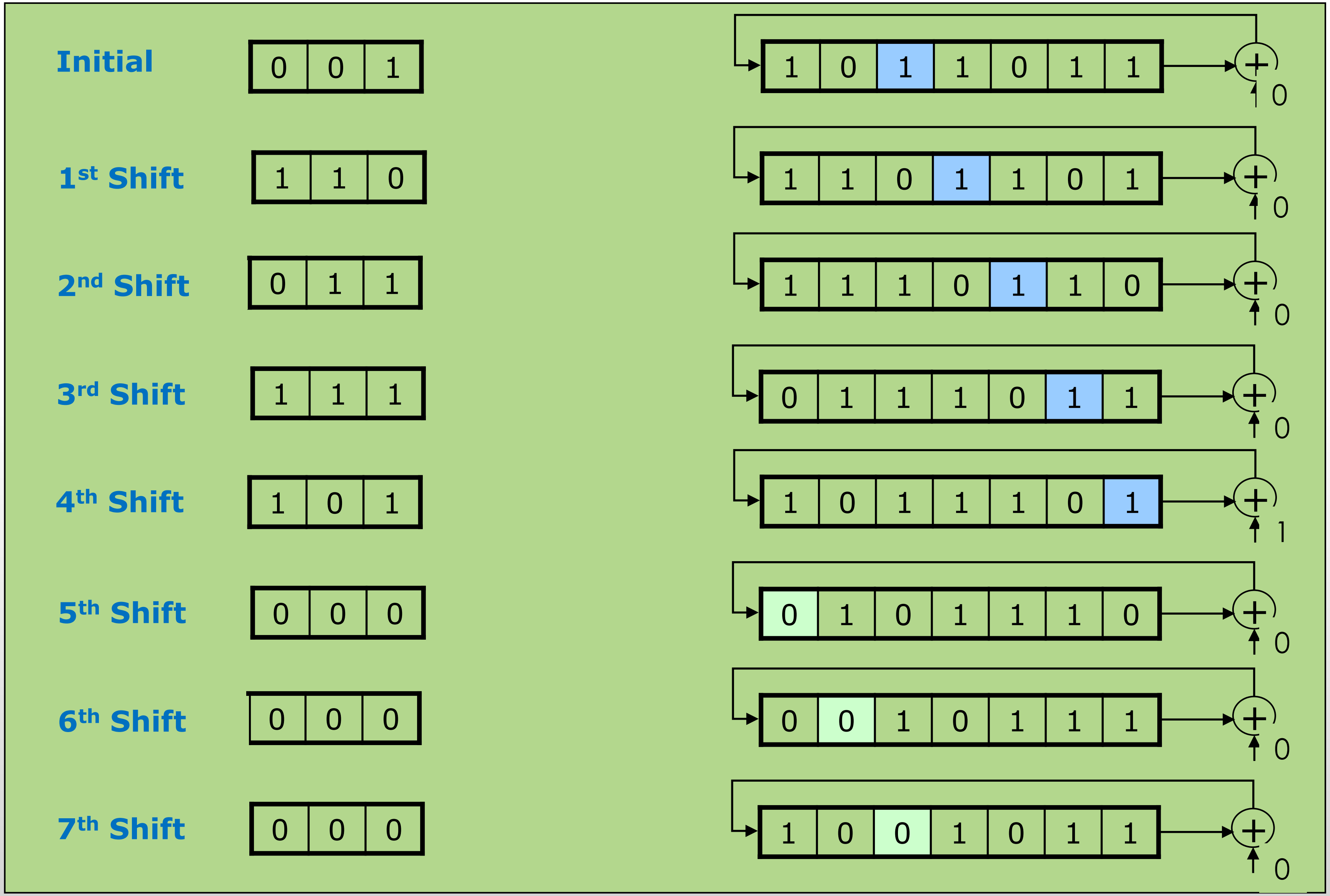
Input	Register Contents
	0 0 0 (Initial State)
0	0 0 0
1	1 0 0
1	1 1 0
0	0 1 1
1	0 1 1
0	1 1 1
0	1 0 1

Syndrome:
(1 0 1)

CYCLIC CODE DECODER



EXAMPLE DECODING OF (7,4) CYCLIC CODE $G(X)=1+X+X^3$: DECODER STEPS, $E(X)=X^2$



LATIHAN SOAL

- **Problem 5.21 (Bernard Sklar 1st edition) or Problem 6.21 (Bernard Sklar 2nd edition)**

A (15,5) cyclic code has a generator polynomial as follows:
$g(X) = 1 + X + X^2 + X^5 + X^8 + X^{10}$.

1. Find the code polynomial (in systematic form) for the message $m(X) = 1 + X^2 + X^4$.
2. Is $V(X) = 1 + X^4 + X^6 + X^8 + X^{14}$ a code polynomial in this system? Justify your answer.

TUGAS

- Cyclic code (7,4) Memiliki generator polinomial $g(x)= 1+X+X^3$

a. Tentukan generator matrix **G** dan parity-check matrix **H** untuk code tersebut., kemudian buktikan bahwa $HG^T=0$

b. Tentukan rangkaian encoder dan sindrome, menggunakan kode yang sistematik

- Sinyal transmisi diterima oleh demodulator di receiver, **r** = [0 1 0 1 0 0 1], tentukan syndrome polynomial S(X) yang kemudian diproses oleh error decoder. Berikan sequence yang merupakan output dari error decoder (estimasi dari codeword yang sebenarnya dikirim).