SATBAYEV UNIVERSITY

Institute of automation and information technologies

Department Electronics, telecommunications and space technologies

Lecture 14
Cyclic Codes. Encoding and Decoding Algorithms

Lecturer Dosbayev Zh.

SATBAYEV UNIVERSITY

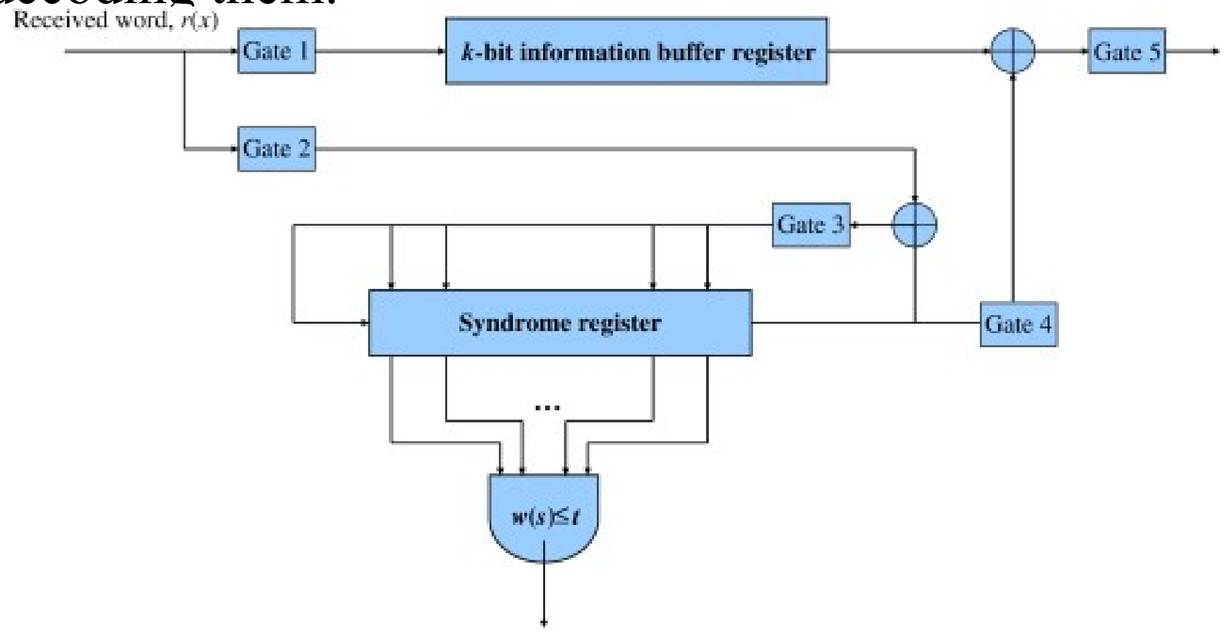
Content

- Introduction
- Description of Cyclic Codes
- Encoding of Cyclic Codes
- Decoding of Cyclic Codes

Introduction

Cyclic codes form an important subclass of linear codes. These codes are attractive for two reasons:

- Encoding and syndrome computation can be implemented easily by employing shift registers with feedback connections (or linear sequential circuits).
- Because they have considerable inherent algebraic structure, it is possible to find various practical methods for decoding them.



DESCRIPTION OF CYCLIC CODES

- If the n-tuple $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ are cyclic shifted one place to the right, we obtain another n-tuple
  - $\mathbf{v}^{(1)} = (v_{n-1}, v_0, v_1, \ldots, v_{n-2})$

  which is called a cyclic shift of v
- If the $\mathbf{v}$ are cyclically shifted i places to the right, we have
  - $\mathbf{v}^{(i)} = (v_{n-i}, v_{n-i+1}, \ldots, v_{n-1}, v_0, v_1, \ldots, v_{n-i-1})$

- Cyclically shifting $\mathbf{v}$ i places to the right is equivalent to cyclically shifting
- $\mathbf{v}$ $(n - i)$ place to the left

DESCRIPTION OF CYCLIC CODES

Definition An (n, k) linear code $\boldsymbol{C}$ is called a cyclic code if every cyclic shift of a code vector in $\boldsymbol{C}$ is also a code vector in $\boldsymbol{C}$

The (7, 4) linear code given in Table is a cyclic code

To develop the algebraic properties of a cyclic code, we treat the components of a code vector $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ as the coefficients of a polynomial as follows:

$$\mathbf{v}(X) = v_0 + v_1 X + v_2 X^2 + \cdots + v_{n-1} X^{n-1}$$

If $v_{n-1} \neq 0$, the degree of $\mathbf{v}(X)$ is $n - 1$

If $v_{n-1} = 0$, the degree of $\mathbf{v}(X)$ is less than $n - 1$

The correspondence between the vector $\mathbf{v}$ and the polynomial $\mathbf{v}(X)$ is one-to-one

SATBAYEV UNIVERSITY

DESCRIPTION OF CYCLIC CODES

TABLE 4.1 A (7, 4) CYCLIC CODE GENERATED BY $g(X) = 1 + X + X^3$

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

DESCRIPTION OF CYCLIC CODES

The code polynomial that corresponds to the code vector $\mathbf{v}(i)$ is

$$\mathbf{v}^{(i)}(X) = v_{n-i} + v_{n-i+1}X + \cdots + v_{n-1}X^{i-1} + v_0X^i + v_1X^{i+1} + \cdots + v_{n-i-1}X^{n-1}$$

Multiplying $\mathbf{v}(X)$ by X^i, we obtain

$$X^i\mathbf{v}(X) = v_0X^i + v_1X^{i+1} + \cdots + v_{n-i-1}X^{n-1} + \cdots + v_{n-1}X^{n+i-1}$$

- The equation above can be manipulated into the following form :

$$\begin{aligned} X^i\mathbf{v}(X) &= v_{n-i} + v_{n-i+1}X + \cdots + v_{n-1}X^{i-1} + v_0X^i + \cdots + v_{n-i-1}X^{n-1} \\ &\quad + v_{n-i}(X^n+1) + v_{n-i+1}X(X^n+1) + \cdots + v_{n-1}X^{i-1}(X^n+1) \\ &= \mathbf{q}(X)\cdot(X^n + 1) + \mathbf{v}^{(i)}(X) \end{aligned}$$

ENCODING OF CYCLIC CODES

- Encoding of an (n, k) cyclic code in systematic form consists of three steps:
  - Multiply the message polynomial $\mathbf{u}(X)$ by X^{n-k} Divide $X^{n-k}\mathbf{u}(X)$ by $\mathbf{g}(X)$ to obtain the remainder $\mathbf{b}(X)$ Form the code word $\mathbf{b}(X) + X^{n-k}\mathbf{u}(X)$

- All these three steps can be accomplished with a division circuit which is a linear $(n–k)$-stage shift register with feedback connections based on the generator polynomial

$$\mathbf{g}(X) = 1 + g_1X + g_2X^2 + \ldots + g_{n-k-1}X^{n-k-1} + X^{n-k}$$

ENCODING OF CYCLIC CODES

- Such a circuit is shown below

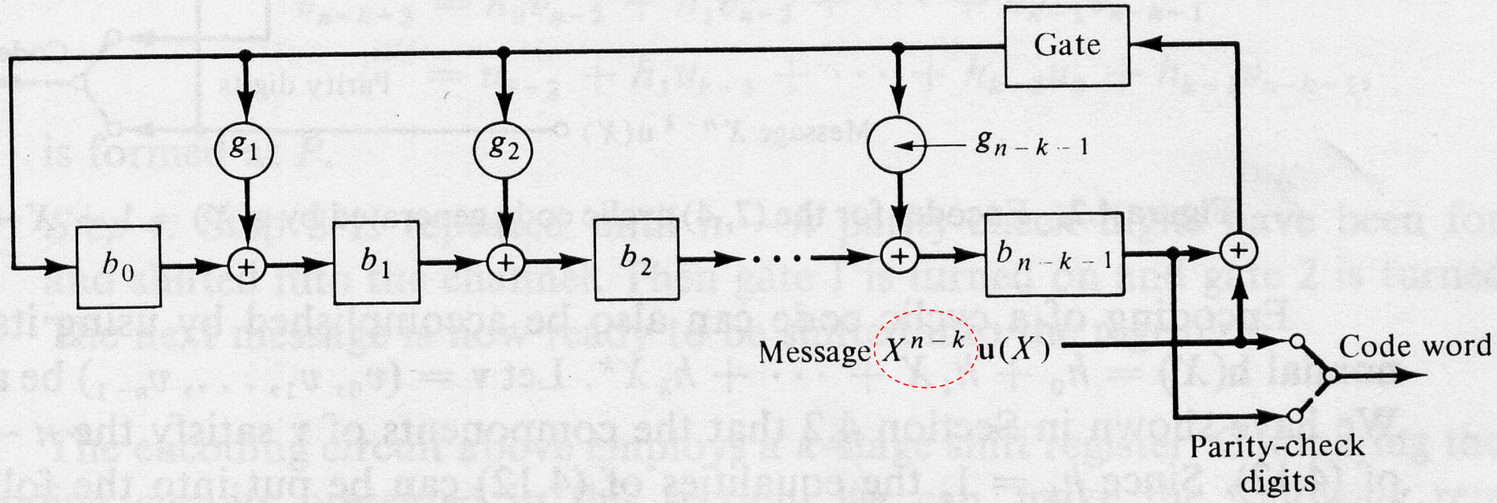


Figure 4.1 Encoding circuit for an (n, k) cyclic code with generator polynomial $\mathbf{g}(X) = 1 + g_1X + g_2X^2 + \cdots + g_{n-k-1}X^{n-k-1} + X^{n-k}$.

Example

- Consider the (7, 4) cyclic code generated by $\mathbf{g}(X) = 1 + X + X^3$ The encoding circuit based on $\mathbf{g}(X)$ is shown in Fig. Suppose that the message $\mathbf{u} = (1\ 0\ 1\ 1)$ is to be encoded
- As the message digits are shifted into the register, the contents in the register are as follows:
- After four shift, the contents of the register are (1 0 0)

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)

Example

- The complete vector is (1 0 0 1 0 1 1) and code polynomial is $1 + X^3 + X^5 + X^6$

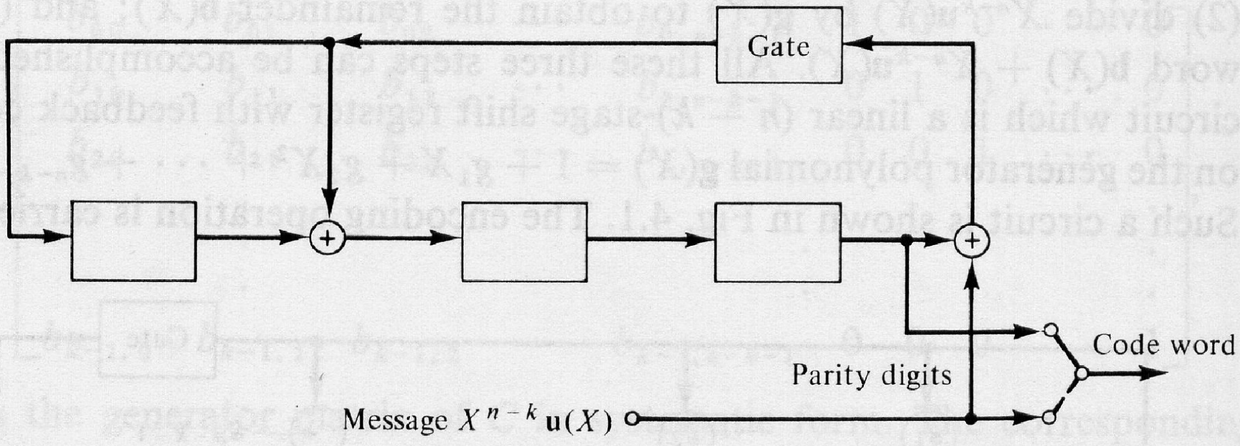


Figure 4.2 Encoder for the (7, 4) cyclic code generated by $\mathbf{g}(X) = 1 + X + X^3$.

DECODING OF CYCLIC CODES

Decoding of cyclic code consists of the same three steps as for decoding linear codes:

- Syndrome computation
- Association of the syndrome to an error pattern
- Error correction

The syndrome computation for cyclic codes can be accomplished with a division circuit whose complexity is linearly proportional to the number of parity-check digits (i.e., $n - k$)

A straightforward approach to the design of a decoding circuit is via a combinational logic circuit that implements the table-lookup procedure

DECODING OF CYCLIC CODES

- The limit to this approach is that the complexity of the decoding circuit tends to grow exponentially with the code length and the number of errors that we intend to correct
- The cyclic structure of a cyclic code allows us to decode a received vector $\mathbf{r}(X)=r_0+r_1X+r_2X^2+\ldots+r_{n-1}X^{n-1}$ in a serial manner.
- The received digits are decoded one at a time and each digit is decoded with the same circuitry.
- As soon as the syndrome has been computed, the decoding circuit checks whether the syndrome $\mathbf{s}(X)$ corresponds to a correctable error pattern $\mathbf{e}(X)= e_0+ e_1X+\ldots+e_{n-1}X^{n-1}$ with an error at the highest-order position X^{n-1} (i.e., $e_{n-1}=1$).

DECODING OF CYCLIC CODES

- If $\mathbf{s}(X)$ does not correspond to an error pattern with $e_{n-1}=1$, the received polynomial and the syndrome register are cyclically shifted once simultaneously.

By doing so, we obtain $\mathbf{r}^{(1)}(X)=r_{n-1}+r_0X+r_1X^2+\ldots+r_{n-2}X^{n-1}$ and the new contents in the syndrome register form the syndrome $\mathbf{s}^{(1)}(X)$ of $\mathbf{r}^{(1)}(X)$.

- The same decoding circuit will check whether $\mathbf{s}^{(1)}(X)$ corresponds to an error pattern with an error at location X^{n-1}. If the syndrome $\mathbf{s}(X)$ does correspond to an error pattern with $e_{n-1}=1$, the first received digit r_{n-1} is an erroneous digit and it must be corrected.
- This correction is carried out by $r_{n-1} \dot{+} e_{n-1}$.

DECODING OF CYCLIC CODES

To remove the effect of an error digit on the syndrome, we simply feed the error digit into the shift register from the left end through an EXCLUSIVE-OR gate

The decoding operation is described as follows:

Step 1

- The syndrome is formed by shifting the entire received vector into the syndrome register
- At the same time the received vector is stored into the buffer register

Step 2

- The syndrome is read into the detector and is tested for the corresponding error pattern

DECODING OF CYCLIC CODES

Step 2 (cont.)

The detector is a combinational logic circuit which is designed in such a way that its output is 1 if the syndrome in the syndrome register corresponds to a correctable error pattern with an error at the highrst-order position X^{n-1}

- if a "1" appears at the output of the detector, the received symbol in the rightmost stage of the buffer register is assumed to be erroneous and must be corrected
- If a "0" appears at the output of the detector, the received symbol at the rightmost stage of the buffer register is assumed to be correct and no correction necessary

The output of the detector is the estimated error value for the symbol to come out of the buffer

DECODING OF CYCLIC CODES

Step 3

- The first received symbol is read out of the buffer
- If the first received symbol is detected to be an erroreous symbol, it is corrected by the output of the detector
- The output of the detector is fed back to the syndrome register to modify the syndrome
- This results in a new syndrome, which corresponds to the altered received vector shifted one place to the right

Step 4

- The new syndrome formed in step 3 is used to detect whether or not the second received symbol is an erroneous symbol
- The decoder repeats step 2 and 3

Step 5

- The decoder decodes the received vector symbol by symbol in the manner outlined above until the entire received vector is read out of the buffer register

•The decoder above is known as *Meggitt decoder*

Example

- Consider the decoding of the (7, 4) cyclic code generated by

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

- This code has minimum distance 3 and is capable of correcting any single error over a block of seven digits
- There are seven single-error patterns
- These seven error patterns and the all-zero vector form all the coset leader of the decoding table

Example

- They form all the correctable error patterns Suppose that the received polynomial
  - $\mathbf{r}(X) = r_0 + r_1 X + r_2 X^2 + \ldots + r_6 X^6$

•is shifted into the syndrome register from the left end The seven single-error patterns and their corresponding syndromes are listed in Table

TABLE 4.4 ERROR PATTERNS AND THEIR SYNDROMES WITH THE RECEIVED POLYNOMIAL $\mathbf{r}(X)$ SHIFTED INTO THE SYNDROME REGISTER FROM THE LEFT END

Error pattern $\mathbf{e}(X)$	Syndrome $\mathbf{s}(X)$	Syndrome vector (s_0, s_1, s_2)
$\mathbf{e}_6(X) = X^6$	$\mathbf{s}(X) = 1 + X^2$	(1 0 1)
$\mathbf{e}_5(X) = X^5$	$\mathbf{s}(X) = 1 + X + X^2$	(1 1 1)
$\mathbf{e}_4(X) = X^4$	$\mathbf{s}(X) = X + X^2$	(0 1 1)
$\mathbf{e}_3(X) = X^3$	$\mathbf{s}(X) = 1 + X$	(1 1 0)
$\mathbf{e}_2(X) = X^2$	$\mathbf{s}(X) = X^2$	(0 0 1)
$\mathbf{e}_1(X) = X^1$	$\mathbf{s}(X) = X$	(0 1 0)
$\mathbf{e}_0(X) = X^0$	$\mathbf{s}(X) = 1$	(1 0 0)

SATBAYEV UNIVERSITY

Example

- The complete decoding circuit is shown in Fig

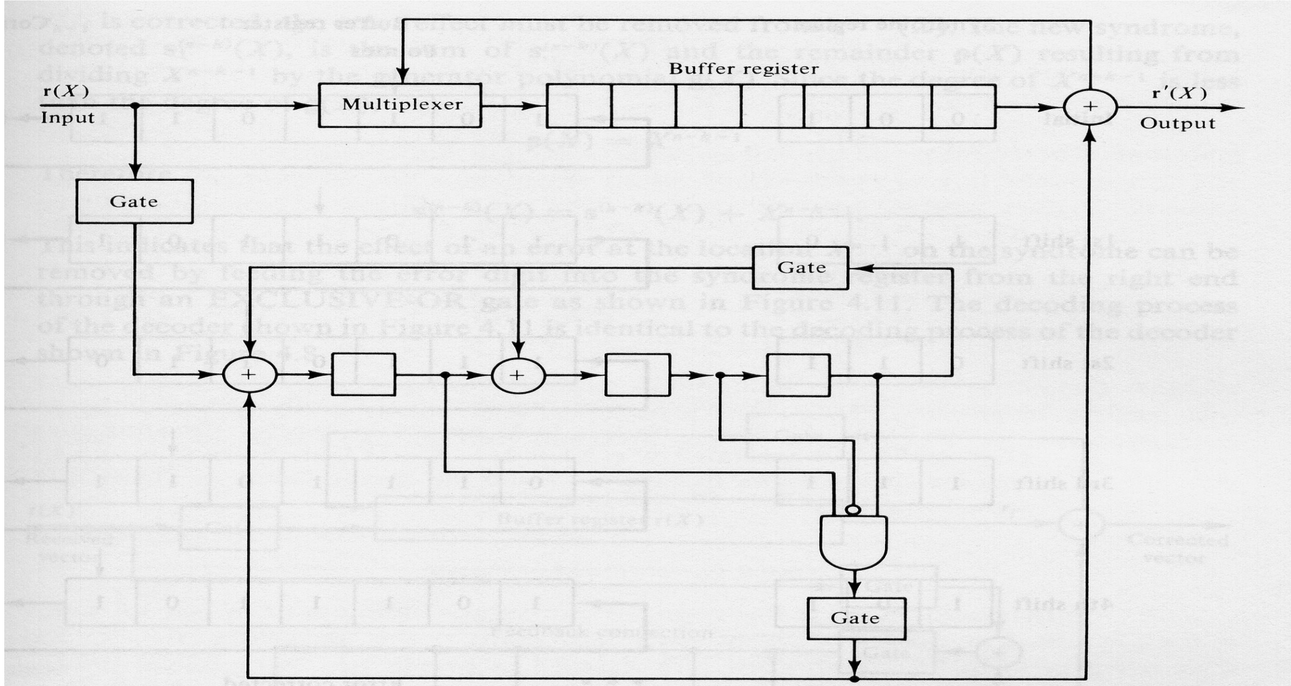
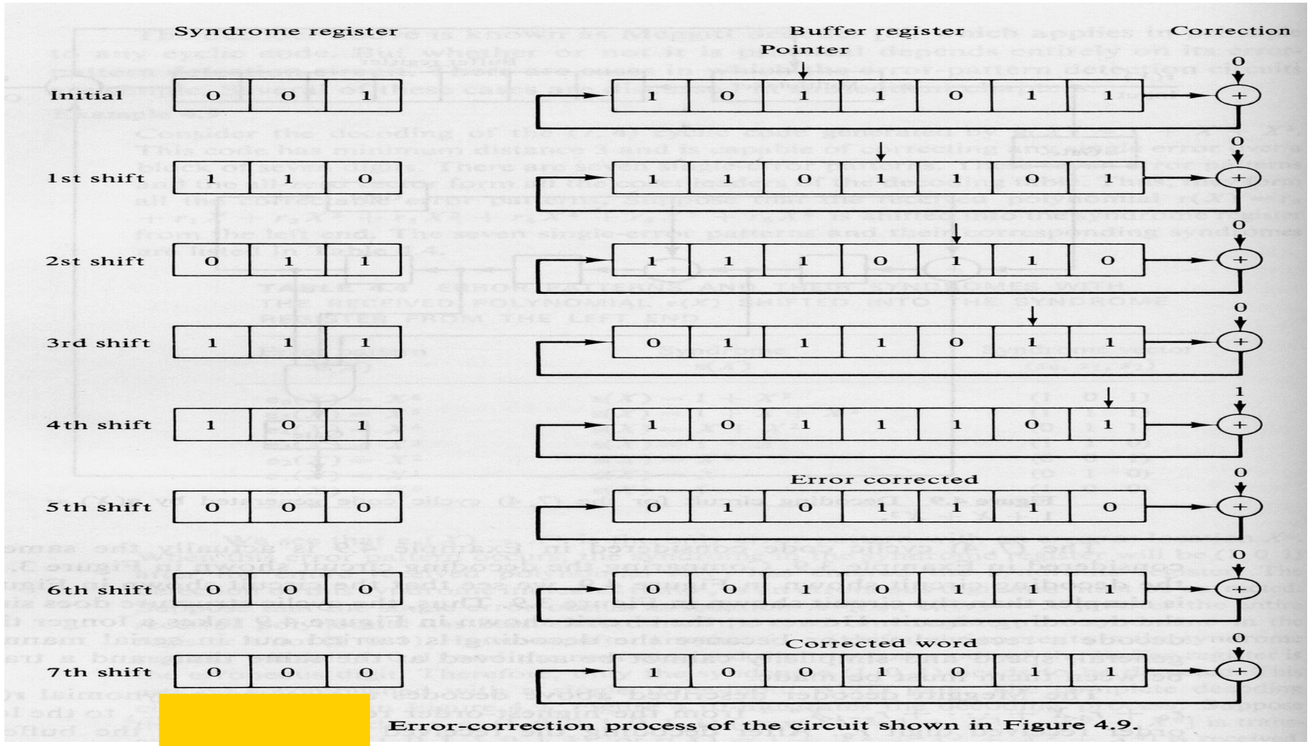


Figure 4.9 Decoding circuit for the (7, 4) cyclic code generated by $g(X) = 1 + X + X^3$.

SATBAYEV UNIVERSITY

Example

- The decoding process is illustrated



Error-correction process of the circuit shown in Figure 4.9.