Ⅲ Cyclic Code

- shift registers with feedback connections
  inherent algebraic structure → Algorithmic technique
- random-error correction & burst-error correction spurred by algebraic coding theorists
- particularly efficient for error detection

Def : Cyclic Code (i) one linear code (subset of $GF(q)[x]/x^n-1$)
(n, k) (ii) $x \bullet c(x) \bmod x^n-1 \in C(x)$ if $c(x) \in C(x)$

$$c(x) = \sum_{i=0}^{n-1} c_i x^i$$

Shift right *i* ≈
Shift left *n-i*

- $v = (v_0, v_1, ..., v_{n-1})$: code vector
  $v^{(1)} = (v_{n-1}, v_0, v_1, \ldots, v_{n-2})$
  $v^{(i)} = (v_{n-i}, v_{n-i+1}, \ldots, v_{n-1}, v_0, v_1, \ldots, v_{n-i-1})$
- $v(x) = v_0 + v_1x + \ldots + v_{n-1}x^{n-1}$: code polynomial
- $v^{(i)}(x) = v_{n-i} + v_{n-i+1}x + \ldots + v_{n-i-1}x^{n-1} = x^iv(x)/x^n-1$

Def : generator polynomial : The nonzero monic code polynomial of minimum degree in a cyclic code *C*

$g(x) = g_0 + g_1x + \ldots + g_{r-1}x^{r-1} + x^r$

(note : multiply by a field element to make it monic)

- g(x) is unique
- In GF(2), $g_0 = 1$

claim : r = n - k

i.e. 下一頁Thm (i) 之證明

For (n, k) cyclic code

Consider : $g(x), xg(x), x^2g(x), \ldots, x^{n-r-1}g(x)$

$$\begin{array}{ccc} \shortparallel & \shortparallel & \shortparallel \\ g^{(1)}(x) & g^{(2)}(x) & g^{(n-r-1)}(x) \end{array} \longleftarrow \text{code polynomials}$$

$v(x) = u_0g(x) + u_1xg(x) + u_2x^2g(x) + \ldots + u_{n-r-1}x^{n-r-1}g(x)$
$= (u_0 + u_1x + u_2x^2 + \ldots + u_{n-r-1}x^{n-r-1})g(x)$
$= u(x)g(x)$ is also a code polynomial

Note If r = n–k, deg u(x) = k-1 u(x) : information polynomial

Thm : Let $g(x) = 1 + g_1(x) + \ldots + g_{r-1}x^{r-1} + x^r$ be the generator polynomial in an (n, k) cyclic code. A binary polynomial of degree n-1 or less is a code polynomial iff it is a multiple of g(x).

Proof:

(i)← $v(x) = (a_0+a_1x+\ldots+a_{n-r-1}x^{n-r-1})g(x) = a_0g(x)+a_1xg(x)+\ldots+a_{n-r-1}x^{n-r-1}g(x)$

(ii) → $v(x) = a(x)g(x) + b(x)$ ∴ $b(x) = v(x) + a(x)g(x)$

# of binary polynomial with degree ≤ n-1 that are multiples of $g(x) = 2^{n-r}$

$2^{n-r} = 2^k \Rightarrow r = n-k$

Thm : In an (n,k) cyclic code, there exists one and only one code polynomial of degree n-k

$$g(x) = 1 + g_1x + g_2x^2 + \ldots + g_{n-k-1}x^{n-k-1} + x^{n-k}$$

Every code polynomial is a multiple of g(x) and every binary polynomial of degree n-1 or less that is a multiple of g(x) is a code polynomial.

Q: $g(x), xg(x), x^2g(x), \ldots, x^{k-1}g(x)$ are linear independent ? Yes, and they can span the k-dimension (n,k) linear code

Thm : $g(x) \mid x^n+1 \ (x^n-1)$

pf: $x^n - 1 = Q(x)g(x) + s(x)$ ← 兩邊 mod x^n-1

$\Rightarrow 0 = \underline{Q(x)g(x)/x^n-1} + s(x)$

$\equiv c(x) \in C(x)$

$s(x) = 0 - c(x) \in$ code polynomial $\therefore s(x) = 0$

Q: $\forall n,k$, Does there exist an (n, k) cyclic code?

Thm : If g(x) is a polynomial of degree n-k and is a factor of $x^n+1(x^n-1)$, then g(x) generate an (n, k) cyclic code

pf: (1) $v(x) = u_0\,g(x) + u_1xg(x) + \ldots + u_{k-1}x^{k-1}g(x)$

$= (u_0 + u_1x + \ldots + u_{k-1}x^{k-1})g(x) = v_0+v_1x+\ldots+v_{n-1}x^{n-1}$

there exists 2^k code polynomials ⇒ (n,k) linear code

(2) If v(x) is a code polynomial, to prove that $v^{(1)}(x)$ is also a code polynomial

since $xv(x) = v_{n-1}(x^n-1)+v^{(1)}(x)$

⇒ $v^{(1)}(x)$ is a multiple of g(x) & $\deg[v^{(1)}(x)] \le n-1$

∴ $v^{(1)}(x)$ is also a code polynomial

Q: For large n, x^n+1 may have many factors of degree n-k.
How to select g(x)?

Non-Systematic Encoding

$\Rightarrow v(x) = u(x)g(x)$

$x^{n-k}u(x) = a(x)g(x) + t(x)$

$\Rightarrow t(x) + x^{n-k}u(x) = a(x)g(x)$

& $\deg[t(x) + x^{n-k}u(x)] \le n-1$

$\therefore$ It's a code polynomial

Systematic Encoding

$v(x) = x^{n-k}u(x) + t(x)$

where t(x) is chosen st. (i) deg t(x) < n-k

(ii) v(x)/g(x) = 0

$\therefore t(x) = -x^{n-k}u(x)/g(x)$

$\equiv t_0 + t_1x + \ldots + t_{n-k-1}x^{n-k-1}$

$v = (t_0, t_1, \ldots, t_{n-k-1}, u_0, u_1, \ldots, u_{k-1})$

Q: t(x) physical mean?

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

non-systematic

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)	1 1 1 0 0 1 0	$1+x+x^2+x^5 = (1+x^2) \cdot g(x)$
(1 0 1 0)	$\boxed{0\ 0\ 1}\boxed{1\ 0\ 1\ 0}$	$x^2+ x^3+x^5 = x^2 \cdot g(x)$
(0 1 1 0)	1 0 0 0 1 1 0	$1+x^4+x^5 = (1+x+x^2) \cdot g(x)$
(1 1 1 0)	0 1 0 1 1 1 0	$x+x^3+x^4+x^5 = (x+x^2) \cdot g(x)$
(0 0 0 1)	1 0 1 0 0 0 1	$1+x^2+x^6 = (1+x+x^3) \cdot g(x)$
(1 0 0 1)	0 1 1 1 0 0 1	$x+x^2+x^3+x^6 = (x+x^3) \cdot g(x)$
(0 1 0 1)	1 1 0 0 1 0 1	$1+x+x^4+x^6 = (1+x^3) \cdot g(x)$
(1 1 0 1)	0 0 0 1 1 0 1	$x^3+x^4+x^6 = x^3 \cdot g(x)$
(0 0 1 1)	0 1 0 0 0 1 1	$x+x^5+x^6 = (x+x^2+x^3) \cdot g(x)$
(1 0 1 1)	1 0 0 1 0 1 1	$1+x^3+x^5+x^6 = (1+x+x^2+x^3) \cdot g(x)$
(0 1 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 1 1 1)	1 1 1 1 1 1 1	$1+x+x^2+x^3+x^4+x^5+x^6 = (1+x^2+x^5) \cdot g(x)$

systematic $\rightarrow$ (1 0 1 0)

$$\frac{X^3(x^2+1)}{X^3+x+1} = x^2$$

Generator & Parity-check Matrices

(一)

$v = u \cdot G$

$v(x) = (u_0 + u_1x + \ldots + u_{k-1}x^{k-1})g(x)$

Q: $GH^T=0$

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

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

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

$= x^{n-k} g(\frac{1}{x}) x^k h(\frac{1}{x})$

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

where $h(x) = h_0 + h_1x + \ldots + h_kx^k$: parity polynomial

$\rightarrow x^kh(x^{-1}) = h_k + h_{k-1}x + \ldots + h_0x^k$

Q: $\because$ $x^kh(x^{-1}) \mid x^n+1$ $\therefore$ $x^kh(x^{-1})$ can also generate an (n, n-k) cyclic code

$\sum_{i=0} g_i h_{k-i}$ k-th coefficient

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & . & . & . & . & . & h_0 & 0 & 0 & 0 & . & . & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & . & . & . & . & . & h_0 & 0 & 0 & . & . & 0 \\ 0 & 0 & h_k & h_{k-1} & h_{k-2} & . & . & . & . & . & h_0 & 0 & . & . & 0 \\ . \\ . \\ . \\ 0 & 0 & . & . & . & 0 & h_k & h_{k-1} & h_{k-2} & . & . & . & . & . & h_0 \end{pmatrix}_{(n-k) \times n}$$

Note If $v(x) = a(x)g(x)$

$v(x)h(x) = a(x)g(x)h(x) = a(x)(x^n+1) = a(x) + x^n a(x)$

$\because \deg a(x) \le k-1$

0 1 …k-1 ———— n n+1 …n+k-1

$$\therefore \sum_{i=0}^{k} h_i v_{j-i} = 0,\ k \le j < n-1. \quad \approx \quad v \cdot H^T = 0$$

deg = j 項係數

$$\left[\sum_{i=0}^{k} h_i v_{n-i-j} = 0 \quad 1 \le j \le n-k \right]$$

(二)

consider each i corresponding to an information place

$x^{n-k+i} = a_i(x)g(x) + b_i(x) \quad 0 \le i \le k-1$

$x^{n-k}, x^{n-k+1}, \ldots, x^{n-1}$

where $b_i(x) = b_{i0} + b_{i1}x + \ldots + b_{i,n-k-1}x^{n-k-1}$

➔ $b_i(x) + x^{n-k+i}$ are code polynomials

Q: $GH^T=0$

$$G = \begin{pmatrix} b_{00} & b_{01} & b_{02} & . & . & . & b_{0,n-k-1} & 1 & 0 & 0 & . & . & . & 0 \\ b_{10} & b_{11} & b_{12} & & & & b_{1,n-k-1} & 0 & 1 & 0 & . & . & . & 0 \\ b_{20} & b_{21} & b_{22} & & & & b_{2,n-k-1} & 0 & 0 & 1 & . & . & . & 0 \\ & & . \\ & & . \\ & & . \\ b_{k-1,0} & b_{k-1,1} & b_{k-1,2} & & & & b_{k-1,n-k-1} & 0 & 0 & 0 & . & . & . & 1 \end{pmatrix}_{k \times n}$$

Q:
(1) linear independent?
(2) 與 $x^{n-k}u(x)/g(x)$之關係?

$$H = \begin{pmatrix} 1 & 0 & 0 & . & . & . & 0 & b_{00} & b_{10} & b_{20} & . & . & . & b_{k-1,0} \\ 0 & 1 & 0 & . & . & . & 0 & b_{01} & b_{11} & b_{21} & . & . & . & b_{k-1,1} \\ 0 & 0 & 1 & . & . & . & 0 & b_{02} & b_{12} & b_{22} & . & . & . & b_{k-1,2} \\ & . \\ & . \\ & . \\ 0 & 0 & 0 & . & . & . & 1 & b_{0,n-k-1} & b_{1,n-k-1} & b_{2,n-k-1} & . & . & . & b_{k-1,n-k-1} \end{pmatrix}_{(n-k) \times n}$$

(3) check $VH^T=0$

(4) (一)G與(二)G之關係?

Ans (2)

$$\frac{x^{n-k}u(x)}{g(x)} = \frac{u_0x^{n-k} + u_1x^{n-k+1} + \dots + u_{k-1}x^{n-1}}{g(x)}$$
$$= u_0b_0(x) + u_1b_1(x) + \dots + u_{k-1}b_{k-1}(x)$$
$$= t_0 + t_1x + \dots + t_{n-k-1}x^{n-k-1}$$

Ans (3)

$$V = (v_0,v_1,\dots,v_{n-k-1},v_{n-k},v_{n-k+1},\dots,v_{n-1})$$
$$= (t_0,t_1,\dots,t_{n-k-1},u_0,u_1,\dots,u_{k-1})$$

$$V(H^T)_{\text{1st column}} = v_0 + v_{n-k}b_{00} + v_{n-k+1}b_{10} + \dots + v_{n-1}b_{k-1,0}$$
$$= \underline{t_0} + \underline{u_0b_{00} + u_1b_{10} + \dots + u_{k-1}b_{k-1,0}}$$

$$= 0$$

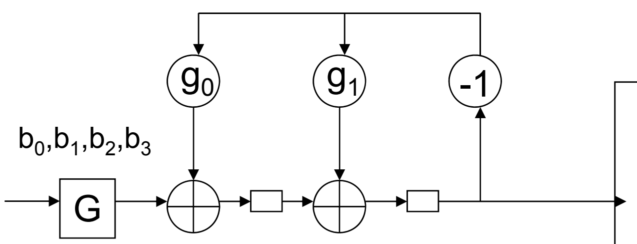
(一). b(x) mod g(x)

$$g(x) = x^2 + g_1x + g_0$$
$$b(x) = b_3x^3 + b_2x^2 + b_1x + b_0$$

$$\boxed{n\text{-}k = \deg[g(x)] = 2}$$

$$\begin{array}{r l}
 & b_3x + (b_2 - g_1b_3) \\
x^2 + g_1x + g_0 \,\big) & b_3x^3 + b_2x^2 + b_1x + b_0 \\
 & \underline{b_3x^3 + g_1b_3x^2 + g_0b_3x} \\
 & (b_2 - g_1b_3)x^2 + (b_1 - g_0b_3)x + b_0 \\
 & \underline{(b_2 - g_1b_3)x^2 + g_1(b_2 - g_1b_3)x + g_0(b_2 - g_1b_3)} \\
 & Ax + B \; (=s(x))
\end{array}$$

在 Finite field 運算



0	0
b_3	0
b_2	b_3
$b_1 - g_0b_3$	$b_2 - g_1b_3$
$b_0 - g_0(b_2 - g_1b_3)$	$(b_1 - g_0b_3) - g_1(b_2 - g_1b_3)$
‖	‖
B	A

$$b_3x^3 \bmod g(x) = (-g_0b_3 + g_1^2b_3)x + g_0g_1b_3$$
$$b_2x^2 \bmod g(x) = -g_1b_2x - g_0b_2$$
$$b_1x \bmod g(x) = b_1x$$
$$b_0 \bmod g(x) = b_0$$

b_3x^3 mod g(x)

⇒ 就b_3x^3 單獨而言, 需要 4 clock,完成計算 b_3x^3 mod g(x).

b_2x^2 mod g(x)

⇒ 就b_2x^2 單獨而言, 需要 3 clock,完成計算 b_2x^2 mod g(x).

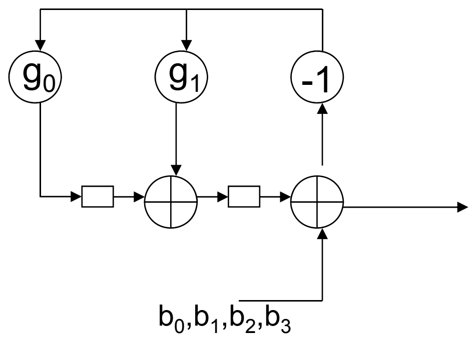
b_1x mod g(x)

⇒ 就b_1x 單獨而言, 需要 2 clock,完成計算 b_1x mod g(x).

b_0 mod g(x)

⇒ 就b_0 單獨而言, 需要 1 clock,完成計算 b_0 mod g(x).

(二). $x^2b(x)$ mod g(x)



(i) 就b_3x^3 單獨而言, 在第4 clock 結束後, syndrome內容為b_3x^5 mod g(x). i.e. 相當於 (一), b_3由左方輸入但需 6個clock.

i.e. 0, 0, 0, 0, 0 , b_3

(i) 同理 for b_2x^2, b_1x, b_0

Q: implementation by (一)

(1) xb(x)/g(x)

(i) while complete the computation $b(x)/g(x) \equiv s(x)$

(ii) $\boxed{G}$ disable

(iii) one right shift

(iv) result = xs(x)/g(x)

$\because$ xb(x) ≈ input 0, b_0, b_1, b_2 , b_3

(2) $x^2b(x)/g(x)$

input 0, 0, b_0, b_1, b_2 , b_3

Encoding

< Method Ⅰ >

step (i) $x^{n-k}u(x)$

(ii) $x^{n-k}u(x)/g(x) = b(x)$

(iii) $b(x) + x^{n-k}u(x)$

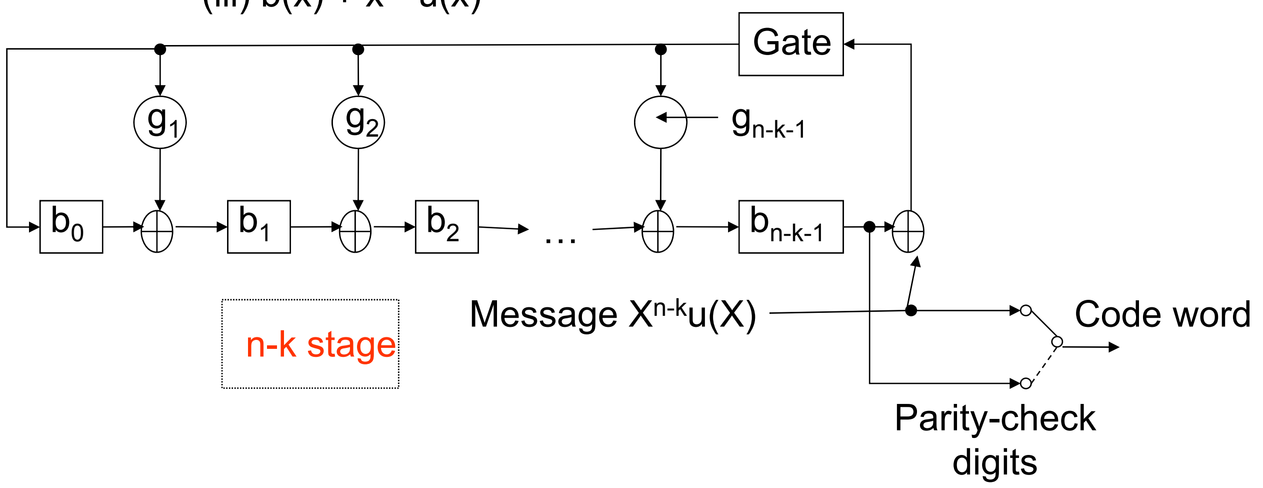


Figure 4.1 Encoding circuit for an (n, k) cyclic code with generator polynomial $g(X) = 1 + g_1X + g_2X^2 + \ldots + g_{n-k-1}X^{n-k-1} + X^{n-k}$

Example 4.5

Consider the (7, 4) cyclic code generated by $g(X) = 1 + X + X^3$. The encoding circuit based on g(X) is shown in Figure 4.2. Suppose that the message **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:

	Input	Register contents
		0 0 0 (initial state)
	1	1 1 0 (first shift)
	1	1 0 1 (second shift)
= k	0	1 0 0 (third shift)
	1	1 0 0 (fourth shift)

After four shifts, the contents of the register are (1 0 0). Thus, the complete code vector is (1 0 0 1 0 1 1) and the code polynomial is $1 + X^3 + X^5 + X^6$.

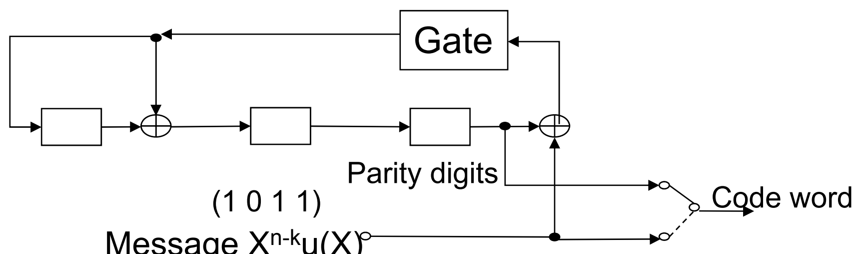


Figure 4.2 Encoder for the (7, 4) cyclic code generated by $g(X) = 1 + X + X^3$

< Method Ⅱ >

$$v_{n-k-j} = \sum_{i=0}^{k-1} h_i v_{n-i-j} \qquad 1 \le j \le n-k \quad \text{--- (1)}$$

$\Rightarrow$ given k information digits $(v_{n-k}, v_{n-k+1}, \ldots, v_{n-1}) = (u_0, u_1, \ldots, u_{k-1})$
By (1), to determine the n-k parity-check digits $(v_0, v_1, \ldots, v_{n-k-1})$

$v_{n-k-1} = h_0 v_{n-1} + h_1 v_{n-2} + \ldots + h_{k-1} v_{n-k} = u_{k-1} + h_1 u_{k-2} + \ldots + h_{k-1} u_0$
$v_{n-k-2} = h_0 v_{n-2} + h_1 v_{n-3} + \ldots + h_{k-1} v_{n-k-1} = u_{k-2} + h_1 u_{k-3} + \ldots + h_{k-2} u_0 + h_{k-1} v_{n-k-1}$

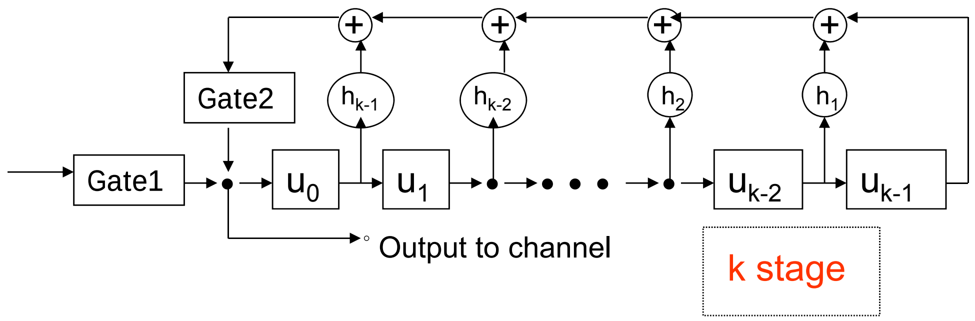


Figure 4.3 Encoding circuit for an (n, k) cyclic code based on the parity polynomial $h(x) = 1 + h_1 X + h_2 X^2 + \ldots + h_{k-1} X^{k-1} + X^k$

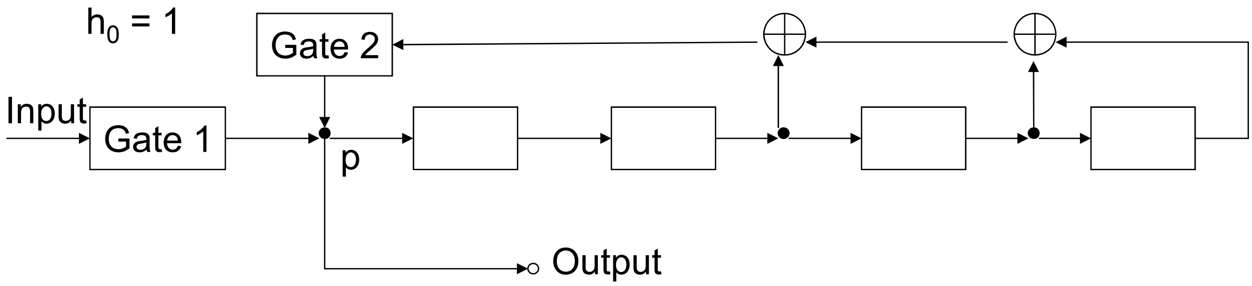


Figure 4.4 Encoding circuit for the (7, 4) cyclic code based on its parity polynomial $h(x) = 1 + X + X^2 + X^4$

Suppose that the message to be encoded is (1 0 1 1).
Then $v_3 = 1$, $v_4 = 0$, $v_5 = 1$, $v_6 = 1$. The first parity-check digit is

$v_2 = v_6 + v_5 + v_4 = 1 + 1 + 0 = 0$

The second parity-check digit is

$v_1 = v_5 + v_4 + v_3 = 1 + 0 + 1 = 0$

Q: 觀察 Method Ⅰ, Ⅱ 結果相同

The third parity-check digit is

$v_0 = v_4 + v_3 + v_2 = 0 + 1 + 0 = 1$

Thus, the code vector that corresponds to the message (1 0 1 1) is
($\underline{1\ 0\ 0}$ 1 0 1 1).

Syndrome Computation & Error Detection

< Type Ⅰ >

$r(x) = r_0 + r_1x + \dots + r_{n-1}x^{n-1}$

$\quad = a(x)\bullet g(x) + s(x) \qquad \deg s(x) \le n-k-1$

$$\boxed{Q : s(x) \leftrightarrow rH^T}$$

$s(x) = 0 \iff r(x)$ is a code polynomial

syndrome

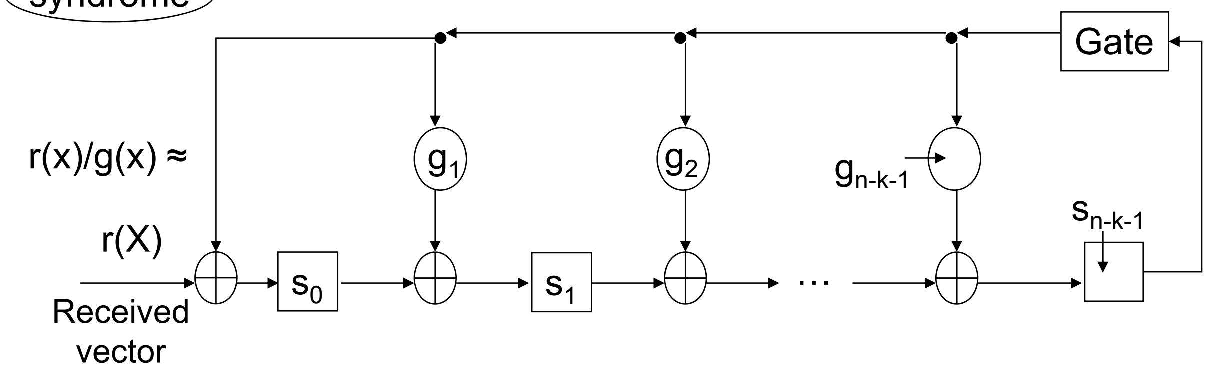


Figure 4.5 An (n-k)-stage syndrome circuit with input from the left end.

Thm : Let s(x) be the syndrome of a received polynomial r(x)
Then $s^{(1)}(x)$ ($= x\bullet s(x)/g(x)$) is the syndrome of
$r^{(1)}(x)$ ($= x \bullet r(x)/x^n+1$)

Ref. pp.14

pf:

$$s(x) = r(x)/g(x)$$

$$\Rightarrow x\cdot s(x)/g(x) = [x\cdot r(x)/g(x)]/g(x) \overset{?}{=} x\cdot r(x)/g(x)$$

$$= \left[x\cdot r(x)/x^n+1\right]/g(x)$$

$$= r^{(1)}(x)/g(x) \triangleq s^{(1)}(x)$$

$$\left[x\cdot\left[p(x)g(x)+s(x)\right]/g(x)\right]/g(x) = x\cdot s(x)/g(x)$$

$$\left[x\cdot\left[p(x)g(x)+s(x)\right]\right]/g(x) = x\cdot s(x)/g(x)$$

r(x) --- s(x)

$r^{(1)}(x)$ --- $s^{(1)}(x)$

=?

Ref : pp. 10 & 11

$r = (r_0, r_1, \ldots, r_{n-k-1}, r_{n-k}, \ldots, r_{n-1}) = (t_0, t_1, \ldots, t_{n-k-1}, u_0, u_1, \ldots, u_{k-1})$

$r \bullet H^T = (s_0, s_1, \ldots, s_{n-k-1})$

$s_0 = r_0 + \underline{r_{n-k}b_{00} + r_{n-k+1}b_{10} + \ldots + r_{n-1}b_{k-1,0}} = r_0 + \underline{t_0}$

$s_1 = r_1 + r_{n-k}b_{01} + r_{n-k+1}b_{11} + \ldots + r_{n-1}b_{k-1,1} = r_1 + t_1$

$\vdots$

$s_{n-k-1} = r_{n-k-1} + r_{n-k}b_{0,\,n-k-1} + r_{n-k+1}b_{1,\,n-k-1} + \ldots + r_{n-1}b_{k-1,\,n-k-1} = r_{n-k-1} + t_{n-k-1}$

Syndrome is simply the vector sum of the received parity digits and the parity-check digits recomputed from the received information digits

$\because\ r(x) = r_0 + r_1x + \ldots + r_{n-k-1}x^{n-k-1} + x^{n-k} \bullet u(x)$

$u(x) = u_0 + u_1x + \ldots + u_{k-1}x^{k-1}$

$\therefore\ r(x)/g(x) = r_0 + r_1x + \ldots + r_{n-k-1}x^{n-k-1} + \underline{x^{n-k} \bullet u(x)/g(x)}$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \| $

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad t_0 + t_1x + \ldots + t_{n-k-1}x^{n-k-1}$

$\boxed{(r_{n-k}, r_{n-k+1}, \ldots, r_{n-1})G = (t_0, t_1, \ldots, t_{n-k-1}, r_{n-k}, r_{n-k+1}, r_{n-1})}$

Example 4.7

A syndrome circuit for the (7, 4) cyclic code generated by $g(X) = 1 + X + X^3$ is shown in Figure 4.6. Suppose that the receive vector is **r** = (0 0 1 0 1 1 0). The syndrome of **r** is s = (1 0 1). As the received vector is shifted into the circuit, the contents in the register are given in Table 4.3.

$H(x)/g(x)$

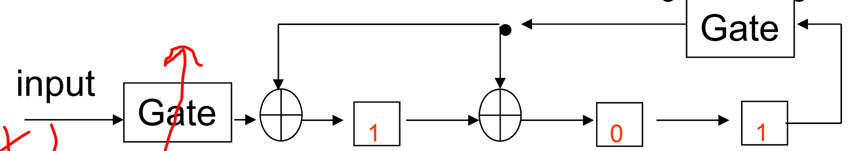


Figure 4.6 Syndrome circuit for the (7, 4) cyclic code generated by $g(X) = 1 + X + X^3$.

$S^{(1)}(x)$

$\|$

$\|$

$S(x)$

Shift	Input	Register contents
		0 0 0 (initial state)
1	0	0 0 0
2	1	1 0 0
3	1	1 1 0
4	0	0 1 1
5	1	0 1 1
6	0	1 1 1
~~7~~	0	1 0 1 (syndrome s)
8	-	1 0 0 (syndrome $s^{(1)}$)
9	-	0 1 0 (syndrome $s^{(2)}$)

$r^{(1)}(x)/g(x)$

$r^{(2)}(x)$

Table 4.3 CONTENTS OF THE SYNDROME REGISTER SHOWN IN FIGURE 4.6 WITH r = (0 0 1 0 1 1 0) AS INPUT

< Type II >

$x^{n-k}r(x)/g(x) \approx$

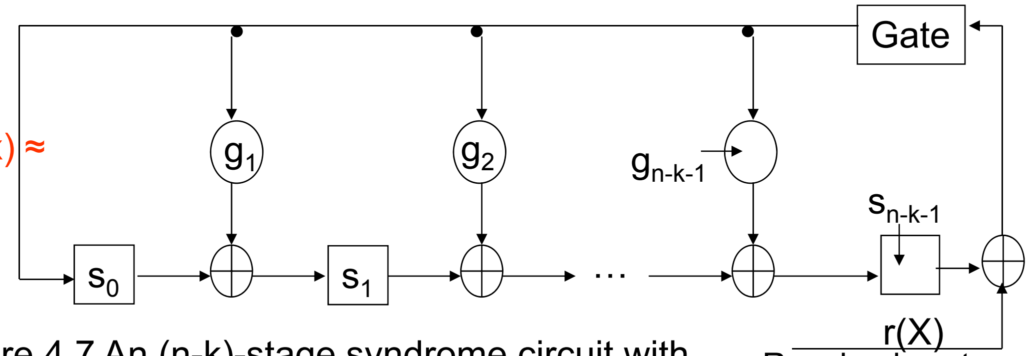


Figure 4.7 An (n-k)-stage syndrome circuit with input from the right end.

Cor : The contents of the registers form the syndrome $s^{(n-k)}(x)$ of $r^{(n-k)}(x)$, which is the (n-k)-th cyclic shift of r(x)

Note :

1. $x^{n-k}r(x)/g(x) = [x^{n-k}r(x)/x^n+1]/g(x) = r^{(n-k)}(x)/g(x) = s^{(n-k)}(x)$
2. $r(x) = v(x) + e(x)$

   $\therefore\ s(x) = r(x)/g(x) = e(x)/g(x)$

$x^{n-k}r(x)$
$= Q(x)(x^n+1) + R(x)$
$= Q(x)p(x)g(x) + q(x)g(x) + s(x)$
$= [Q(x)p(x) + q(x)]g(x) + s(x)$

Decoding

1. syndrome
2. error pattern
3. correct

Meggitt decoder → received digits are decoded one at a time and each digit is decoded with the same circuitry

<see next page>

Note : If Syndrome register ≠ 0's at the end of decoding (n shifts) uncorrectable error pattern

(i) $r_1(x) = r(x) + x^{n-1}$
(ii) $s_1(X) = s(x) + x^{n-1}/g(x)$
(iii) $s_1^{(1)}(x) = x \cdot s_1(x)/g(x)$
$= xs(x)/g(x) + [x \cdot x^{n-1}/g(x)]/g(x)$
$= xs(x)/g(x) + x^n/g(x) = s^{(1)}(x) + 1$

	syndrome	
$r(x)$		$s(x)$
$r^{(1)}(x)$		$s^{(1)}(x)$
$r_1(x)$		$s_1(x)$
$r_1^{(1)}(x)$		$s_1^{(1)}(x)$

$x^n - 1 = Q(x)g(x)$
$\rightarrow x^n = Q(x)g(x) + 1$

< Type Ⅰ >

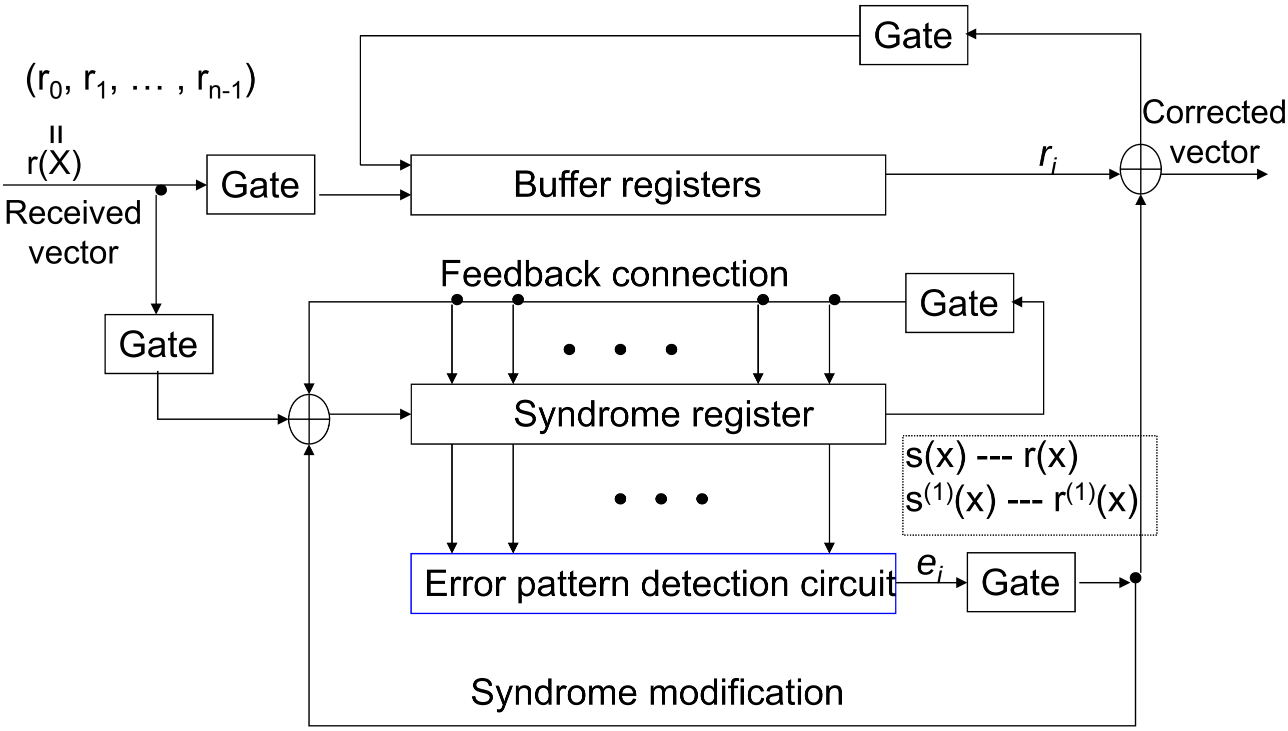


Figure 4.8 General cyclic code decoder with received polynomial r(X) shifted into the syndrome register from the left end

Example 4.9

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 leaders of the decoding table. Thus, they form all the correctable error patterns. Suppose that the received polynomial $\mathbf{r}(X) = r_0 + r_1X + r_2X^2 + r_3X^3 + r_4X^4 + r_5X_5 + r_6X^6$ is shifted into the syndrome register from the left end. The seven single-error patterns and their corresponding syndromes are listed in Table 4.4.

TABLE 4.4 ERROR PATTERNS AND THEIR SYNDROMES WITH THE RECEIVED POLYNOMIAL **r**(x) SHIFTED INTO THE SYNDROME REGISTER FROM THE LEFT END

r(x) = v(x) + e(x)

Error pattern e(X)	Syndrome s(X)	Syndrome vector (s_0, s_1, s_2)
$e_6(X) = X^6$	$s(X) = 1 + X^2$	(1 0 1)
$e_5(X) = X^5$	$s(X) = 1 + X + X^2$	(1 1 1)
$e_4(X) = X^4$	$s(X) = X + X^2$	(0 1 1)
$e_3(X) = X^3$	$s(X) = 1 + X$	(1 1 0)
$e_2(X) = X^2$	$s(X) = X^2$	(0 0 1)
$e_1(X) = X^1$	$s(X) = X$	(0 1 0)
$e_0(X) = X^0$	$s(X) = 1$	(1 0 0)

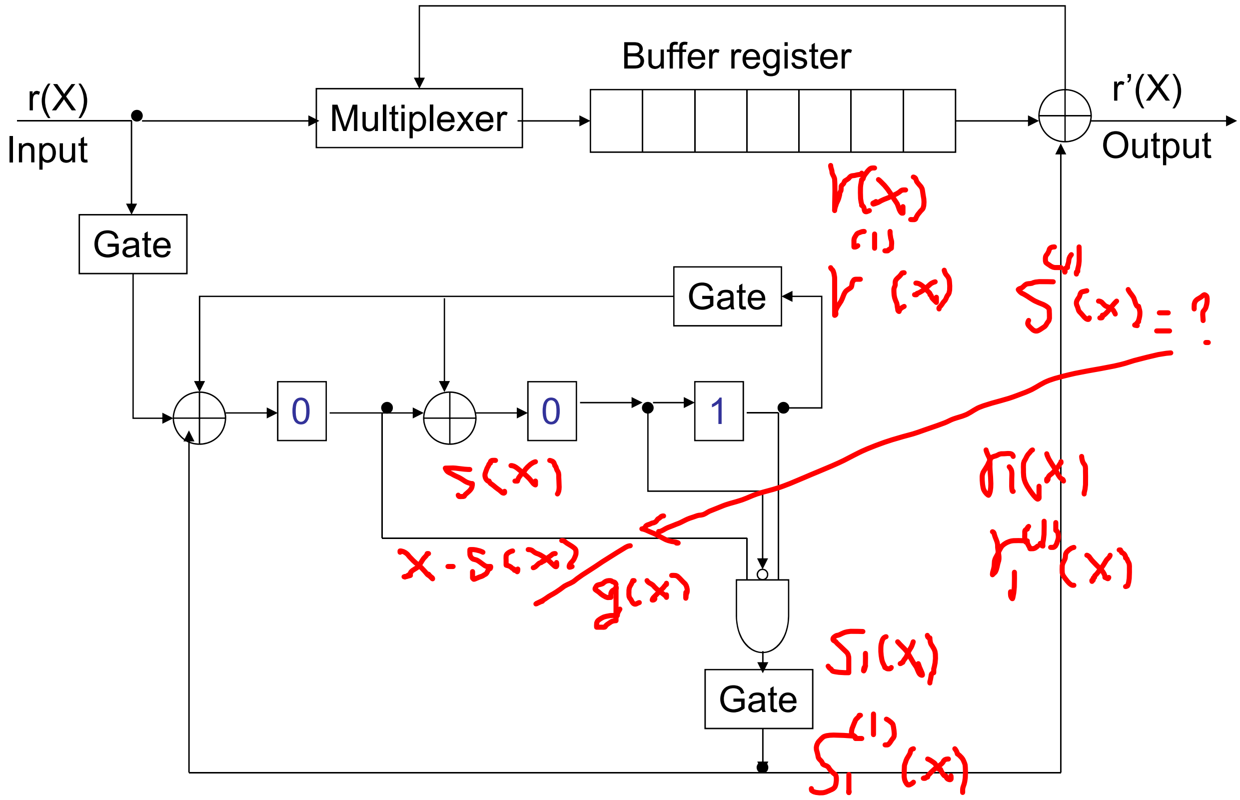
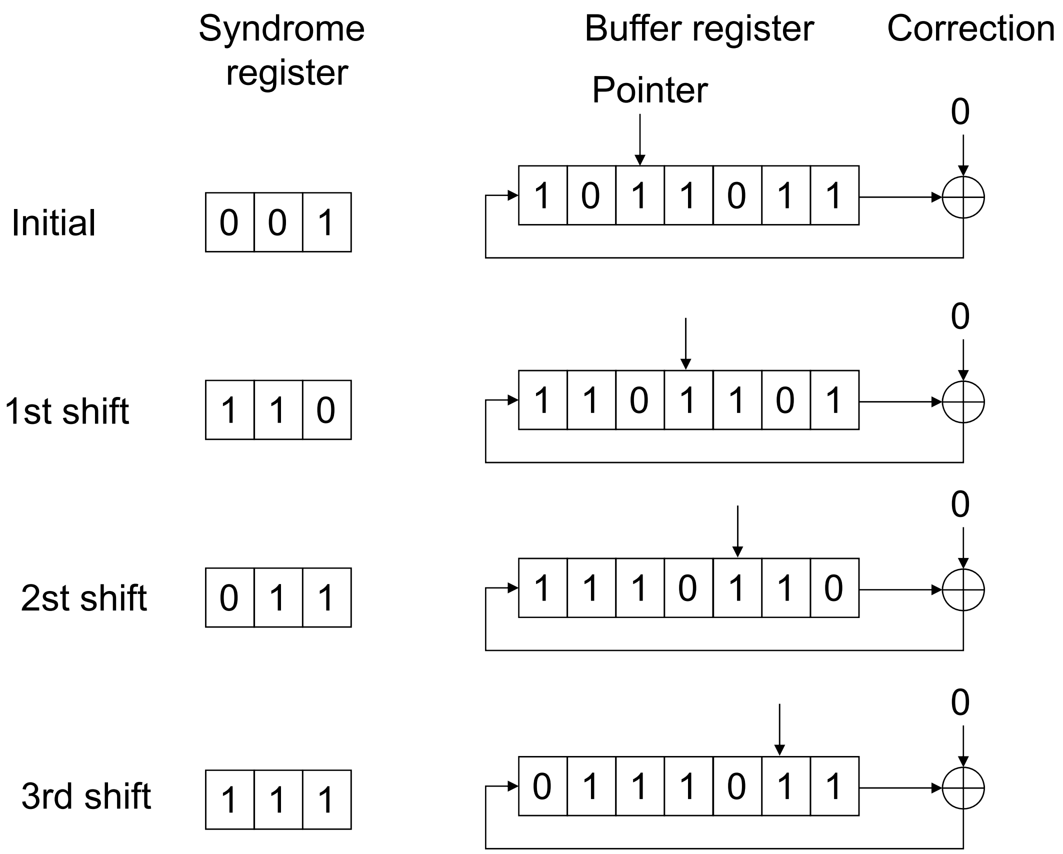


Figure 4.9 Decoding circuit for the (7, 4) cyclic code generated by **g**(X) = 1 + X + X^3.



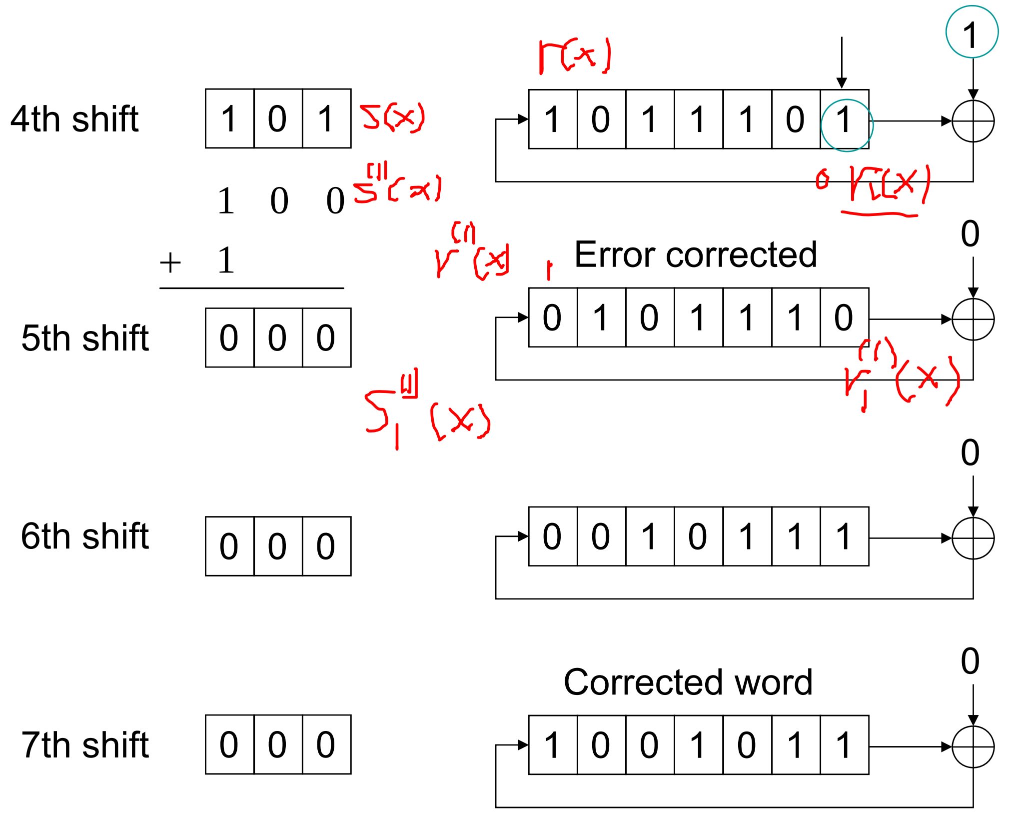


Figure 4.10 Error-correction process of the circuit shown in Figure 4.9

< Type Ⅱ >

(i) $s^{(n-k)}(x)$: syndrome of $r^{(n-k)}(x)$

(ii) If $e_{n-1} = 1$ In $r^{(n-k)}(x)$, the digit r_{n-1} is at the location x^{n-k-1}

$$r_1(x) = r(x) + x^{n-1}$$

$$\Rightarrow r_1^{(n-k)}(x) = r^{(n-k)}(x) + x^{n-k-1}$$

$$\Rightarrow s_1^{(n-k)}(x) = s^{(n-k)}(x) + x^{n-k-1}$$

$\cancel{x^6 \cdot x^3}$ $g(x)$

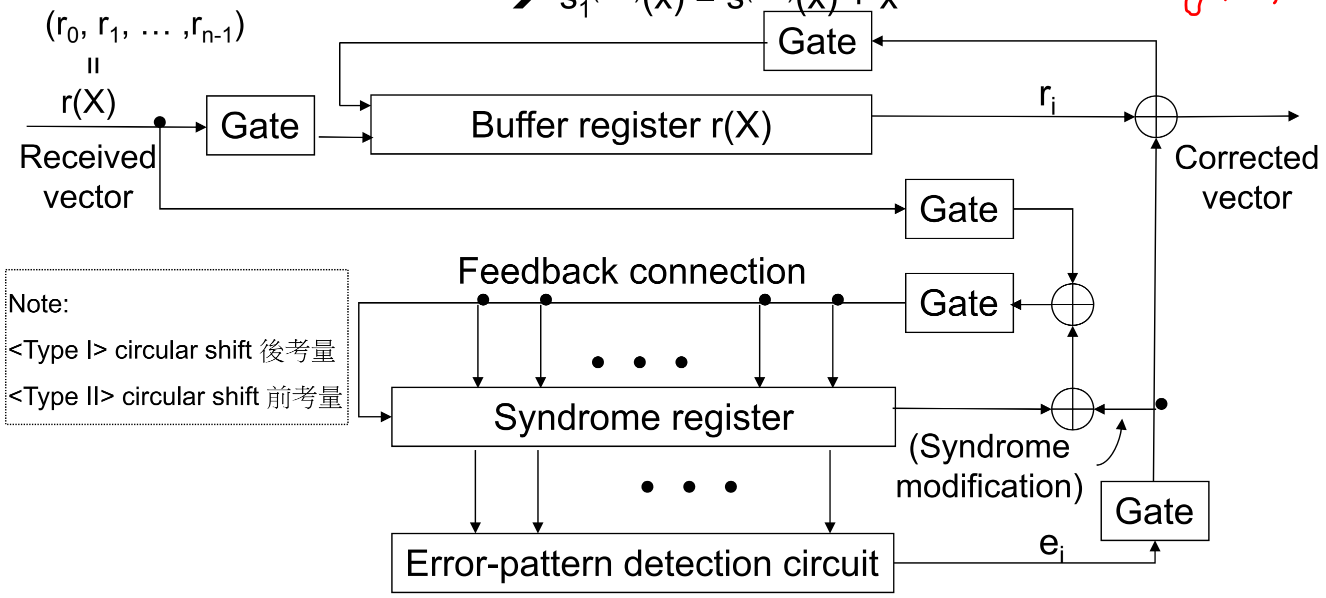


Figure 4.11 General cyclic code decoder with received polynomial **r**(X) shifted into the syndrome register from the right end.

Example 4.10

Again, we consider the decoding of the (7, 4) cyclic code generated by **g**(X) = 1 + X + X^3. Suppose that the received polynomial **r**(X) is shifted into the syndrome register from the right end. The seven single-error patterns and their corresponding syndromes are listed in Table 4.5.

We see that only when **e**(X) = X^6 occurs, the syndrome is (0 0 1) after the entire received polynomial **r**(X) has been shifted into the syndrome register. If the single error occurs at the location X^i with $i \neq 6$, the syndrome in the register will not be (0 0 1) after the entire received polynomial **r**(X) has been shifted into the syndrome register. However, another 6 – i shifts, the syndrome register will contain (0 0 1). Based on this fact, we obtain another decoding circuit for the (7, 4) cyclic code generated by **g**(X) = 1 + X + X^3, as shown in Figure 4.12. We see that the circuit shown in Figure 4.9 and the circuit shown in Figure 4.12 have the same complexity.

TABLE 4.5 ERROR PATTERNS AND THEIR SYNDROMES WITH THE RECEIVED POLYNOMIAL **r**(x) SHIFTED INTO THE SYNDROME REGISTER FROM THE RIGHT END

Error pattern e(X)	Syndrome $s^{(3)}(X)$	Syndrome vector (s_0, s_1, s_2)
e(X) = X^6	$s^{(3)}(X) = X^2$	(0 0 1)
e(X) = X^5	$s^{(3)}(X) = X$	(0 1 0)
e(X) = X^4	$s^{(3)}(X) = 1$	(1 0 0)
e(X) = X^3	$s^{(3)}(X) = 1 + X^2$	(1 0 1)
e(X) = X^2	$s^{(3)}(X) = 1 + X + X^2$	(1 1 1)
e(X) = X^1	$s^{(3)}(X) = X + X^2$	(0 1 1)
e(X) = X^0	$s^{(3)}(X) = 1 + X$	(1 1 0)

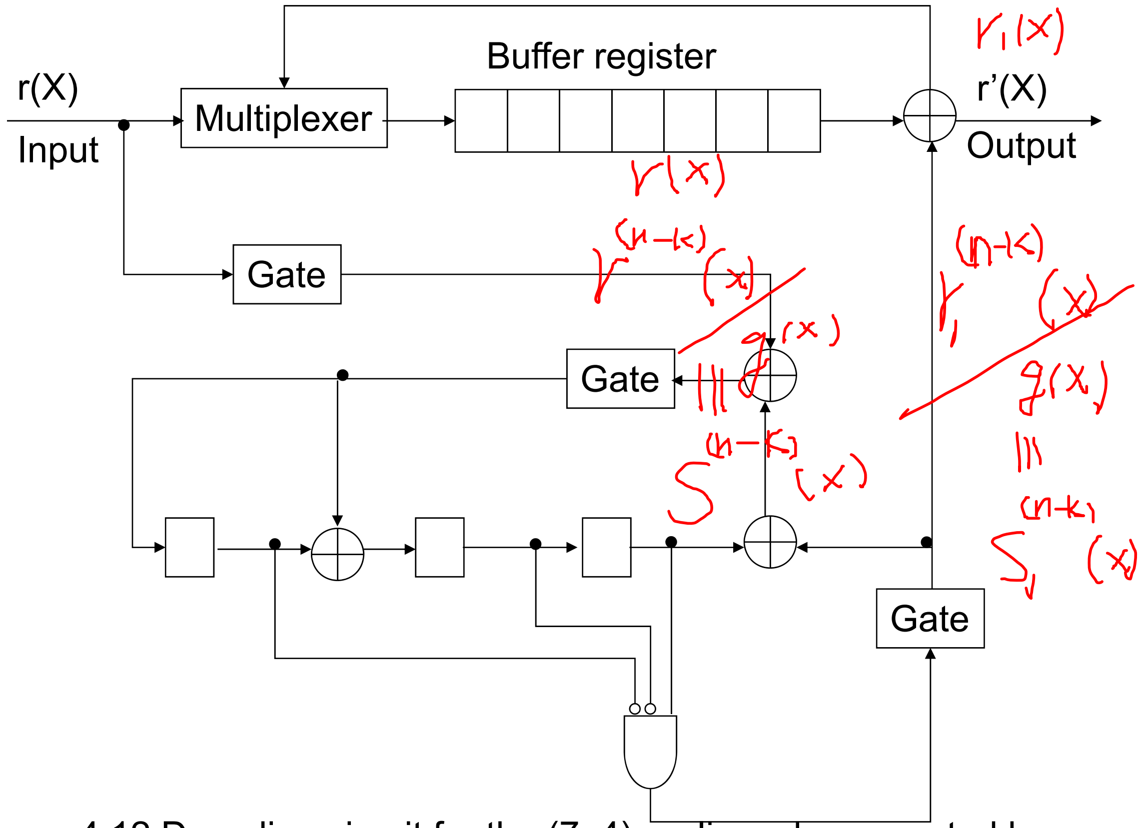


Figure 4.12 Decoding circuit for the (7, 4) cyclic code generated by **g**(X) = 1 + X + X^3.