Cyclic Codes

Yunghsiang S. Han

Department of Electrical Engineering,
National Taiwan University of Science and Technology
Taiwan

E-mail: yshan@mail.ntust.edu.tw

Description of Cyclic Codes

- If the components of an n-tuple $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1})$ are cyclically shifted i places to the right, the resultant n-tuple would be

$$\boldsymbol{v}^{(i)} = (v_{n-i}, v_{n-i+1}, \ldots, v_{n-1}, v_0, v_1, \ldots, v_{n-i-1}).$$

- Cyclically shifting $\boldsymbol{v}$ i places to the right is equivalent to cyclically shifting $\boldsymbol{v}$ $n-i$ places to the left.
- 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 $\boldsymbol{C}$.
- Code polynomial $\boldsymbol{v}(x)$ of the code vector $\boldsymbol{v}$ is defined as

$$\boldsymbol{v}(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}.$$

- $\boldsymbol{v}^{(i)}(x) = x^i \boldsymbol{v}(x) \bmod x^n + 1$.

Proof: Multiplying $\boldsymbol{v}(x)$ by x^i, we obtain

$$x^i\boldsymbol{v}(x) = v_0x^i + v_1x^{i+1} + \cdots + v_{n-i-1}x^{n-1} + \cdots + v_{n-1}x^{n+i-1}.$$

Then we manipulate the equation into the following form:

$$\begin{aligned} x^i\boldsymbol{v}(x) &= v_{n-i} + v_{n-i+1}x + \cdots + v_{n-1}x^{i-1} + v_0x^i + \cdots \\ &\quad + v_{n-i-1}x^{n-1} + v_{n-i}(x^n+1) + v_{n-i+1}x(x^n+1) \\ &\quad + \cdots + v_{n-1}x^{i-1}(x^n+1) \\ &= \boldsymbol{q}(x)(x^n+1) + \boldsymbol{v}^{(i)}(x), \end{aligned}$$

where $\boldsymbol{q}(x) = v_{n-i} + v_{n-i+1}x + \cdots + v_{n-1}x^{i-1}$.

- The nonzero code polynomial of minimum degree in a cyclic code $\boldsymbol{C}$ is unique.
- Let $\boldsymbol{g}(x) = g_0 + g_1x + \cdots + g_{r-1}x^{r-1} + x^r$ be the nonzero code polynomial of minimum degree in an (n,k) cyclic code $\boldsymbol{C}$. Then the constant term g_0 must be equal to 1.

Proof: Suppose that $g_0 = 0$. Then

$$\begin{aligned} \boldsymbol{g}(x) &= g_1 x + g_2 x^2 + \cdots + g_{r-1} x^{r-1} + x^r \\ &= x(g_1 + g_2 x + \cdots + g_{r-1} x^{r-2} + x^{r-1}). \end{aligned}$$

If we shift $\boldsymbol{g}(x)$ cyclically $n-1$ places to the right (or one place to the left), we obtain a nonzero code polynomial, $g_1 + g_2 x + \cdots + g_{r-1} x^{r-2} + x^{r-1}$, which has a degree less than r. Contradiction.

A $(7, 4)$ Cyclic Code Generated by $\boldsymbol{g}(x) = 1 + x + x^3$

Messages	Code Vectors	Code Polynomials
(0 0 0 0)	0 0 0 0 0 0 0	$0 = 0 \cdot \boldsymbol{g}(x)$
(1 0 0 0)	1 1 0 1 0 0 0	$1 + x + x^3 = 1 \cdot \boldsymbol{g}(x)$
(0 1 0 0)	0 1 1 0 1 0 0	$x + x^2 + x^4 = x \cdot \boldsymbol{g}(x)$
(1 1 0 0)	1 0 1 1 1 0 0	$1 + x^2 + x^3 + x^4 = (1 + x) \cdot \boldsymbol{g}(x)$
(0 0 1 0)	0 0 1 1 0 1 0	$x^2 + x^3 + x^5 = x^2 \cdot \boldsymbol{g}(x)$
(1 0 1 0)	1 1 1 0 0 1 0	$1 + x + x^2 + x^5 = (1 + x^2) \cdot \boldsymbol{g}(x)$
(0 1 1 0)	0 1 0 1 1 1 0	$x + x^3 + x^4 + x^5 = (x + x^2) \cdot \boldsymbol{g}(x)$
(1 1 1 0)	1 0 0 0 1 1 0	$1 + x^4 + x^5 = (1 + x + x^2) \cdot \boldsymbol{g}(x)$
(0 0 0 1)	0 0 0 1 1 0 1	$x^3 + x^4 + x^6 = x^3 \cdot \boldsymbol{g}(x)$
(1 0 0 1)	1 1 0 0 1 0 1	$1 + x + x^4 + x^6 = (1 + x^3) \cdot \boldsymbol{g}(x)$
(0 1 0 1)	0 1 1 1 0 0 1	$x + x^2 + x^3 + x^6 = (x + x^3) \cdot \boldsymbol{g}(x)$
(1 1 0 1)	1 0 1 0 0 0 1	$1 + x^2 + x^6 = (1 + x + x^3) \cdot \boldsymbol{g}(x)$
(0 0 1 1)	0 0 1 0 1 1 1	$x^2 + x^4 + x^5 + x^6 = (x^2 + x^3) \cdot \boldsymbol{g}(x)$
(1 0 1 1)	1 1 1 1 1 1 1	$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = (1 + x^2 + x^3) \cdot \boldsymbol{g}(x)$
(1 1 1 1)	1 0 0 1 0 1 1	$1 + x^3 + x^5 + x^6 = (1 + x + x^2 + x^3) \cdot \boldsymbol{g}(x)$

- Consider the polynomial $x\boldsymbol{g}(x), x^2\boldsymbol{g}(x), \ldots, x^{n-r-1}\boldsymbol{g}(x)$. Clearly, they are cyclic shifts of $\boldsymbol{g}(x)$ and hence code polynomials in $\boldsymbol{C}$. Since $\boldsymbol{C}$ is linear, a linear combination of $\boldsymbol{g}(x), x\boldsymbol{g}(x), \ldots, x^{n-r-1}\boldsymbol{g}(x)$,

$$\begin{aligned}\boldsymbol{v}(x) &= u_0\boldsymbol{g}(x) + u_1 x\boldsymbol{g}(x) + \cdots + u_{n-r-1}x^{n-r-1}\boldsymbol{g}(x) \\ &= (u_0 + u_1 x + \cdots + u_{n-r-1}x^{n-r-1})\boldsymbol{g}(x),\end{aligned}$$

  is also a code polynomial where $u_i \in \{0, 1\}$.

- Let $\boldsymbol{g}(x) = 1 + g_1 x + \cdots + g_{r-1}x^{r-1} + x^r$ be the nonzero code polynomial of minimum degree in an (n, k) cyclic code $\boldsymbol{C}$. A binary polynomial of degree $n-1$ or less is a code polynomial *if and only if* it is a multiple of $\boldsymbol{g}(x)$.

  Proof: Let $\boldsymbol{v}(x)$ be a binary polynomial of degree $n-1$ or less. Suppose that $\boldsymbol{v}(x)$ is a multiple of $\boldsymbol{g}(x)$. Then

$$\boldsymbol{v}(x) = (a_0 + a_1 x + \cdots + a_{n-r-1}x^{n-r-1})\boldsymbol{g}(x)$$

$$= a_0\boldsymbol{g}(x) + a_1 x\boldsymbol{g}(x) + \cdots + a_{n-r-1}x^{n-r-1}\boldsymbol{g}(x).$$

Since $\boldsymbol{v}(x)$ is a linear combination of the code polynomials, $\boldsymbol{g}(x), x\boldsymbol{g}(x), \ldots, x^{n-r-1}\boldsymbol{g}(x)$, it is a code polynomial in $\boldsymbol{C}$. Now let $\boldsymbol{v}(x)$ be a code polynomial in $\boldsymbol{C}$. Dividing $\boldsymbol{v}(x)$ by $\boldsymbol{g}(x)$, we obtain

$$\boldsymbol{v}(x) = \boldsymbol{a}(x)\boldsymbol{g}(x) + \boldsymbol{b}(x),$$

where the degree of $\boldsymbol{b}(x)$ is less than the degree of $\boldsymbol{g}(x)$. Since $\boldsymbol{v}(x)$ and $\boldsymbol{a}(x)\boldsymbol{g}(x)$ are code polynomials, $\boldsymbol{b}(x)$ is also a code polynomial. Suppose $\boldsymbol{b}(x) \neq 0$. Then $\boldsymbol{b}(x)$ is a code polynomial with less degree than that of $\boldsymbol{g}(x)$. Contradiction.

- The number of binary polynomials of degree $n-1$ or less that are multiples of $\boldsymbol{g}(x)$ is 2^{n-r}.
- There are total of 2^k code polynomials in $\boldsymbol{C}$, $2^{n-r} = 2^k$, i.e., $r = n - k$.

- The polynomial $\boldsymbol{g}(x)$ is called the *generator polynomial* of the code.
- The degree of $\boldsymbol{g}(x)$ is equal to the number of parity-check digits of the code.
- The generator polynomial $\boldsymbol{g}(x)$ of an (n, k) cyclic code is a factor of $x^n + 1$.

  Proof: We have

  $$x^k \boldsymbol{g}(x) = (x^n + 1) + \boldsymbol{g}^{(k)}(x).$$

  Since $\boldsymbol{g}^{(k)}(x)$ is the code polynomial obtained by shifting $\boldsymbol{g}(x)$ to the right cyclically k times, $\boldsymbol{g}^{(k)}(x)$ is a multiple of $\boldsymbol{g}(x)$. Hence,

  $$x^n + 1 = \{x^k + \boldsymbol{a}(x)\}\boldsymbol{g}(x).$$
- If $\boldsymbol{g}(x)$ is a polynomial of degree $n - k$ and is a factor of $x^n + 1$, then $\boldsymbol{g}(x)$ generates an (n, k) cyclic code.

Proof: A linear combination of $\boldsymbol{g}(x), x\boldsymbol{g}(x), \ldots, x^{k-1}\boldsymbol{g}(x)$,

$$\begin{aligned}\boldsymbol{v}(x) &= a_0\boldsymbol{g}(x) + a_1 x\boldsymbol{g}(x) + \cdots + a_{k-1}x^{k-1}\boldsymbol{g}(x) \\ &= (a_0 + a_1 x + \cdots + a_{k-1}x^{k-1})\boldsymbol{g}(x),\end{aligned}$$

is a polynomial of degree $n-1$ or less and is a multiple of $\boldsymbol{g}(x)$. There are a total of 2^k such polynomial and they form an (n,k) linear code.

Let $\boldsymbol{v}(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$ be a code polynomial in this code. We have

$$\begin{aligned}x\boldsymbol{v}(x) &= v_0 x + v_1 x^2 + \cdots + v_{n-1}x^n \\ &= v_{n-1}(x^n + 1) + (v_{n-1} + v_0 x + \cdots + v_{n-2}x^{n-1}) \\ &= v_{n-1}(x^n + 1) + \boldsymbol{v}^{(1)}(x).\end{aligned}$$

Since both $x\boldsymbol{v}(x)$ and $x^n + 1$ are divisible by $\boldsymbol{g}(x)$, $\boldsymbol{v}^{(1)}$ must be divisible by $\boldsymbol{g}(x)$. Hence, $\boldsymbol{v}^{(1)}(x)$ is a code polynomial and the code generated by $\boldsymbol{g}(x)$ is a cyclic code.

- Suppose that the message to be encoded is $\boldsymbol{u} = (u_0, u_1, \ldots, u_{k-1})$. Then

$$x^{n-k}\boldsymbol{u}(x) = u_0 x^{n-k} + u_1 x^{n-k+1} + \cdots + u_{k-1} x^{n-1}.$$

Dividing $x^{n-k}\boldsymbol{u}(x)$ by $\boldsymbol{g}(x)$, we have

$$x^{n-k}\boldsymbol{u}(x) = \boldsymbol{a}(x)\boldsymbol{g}(x) + \boldsymbol{b}(x).$$

Since the degree of $\boldsymbol{g}(x)$ is $n-k$, the degree of $\boldsymbol{b}(x)$ must be $n-k-1$ or less. Then

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

is a multiple of $\boldsymbol{g}(x)$ and therefore it is a code polynomial.

$$\begin{aligned}\boldsymbol{b}(x) + x^{n-k}\boldsymbol{u}(x) &= b_0 + b_1 x + \cdots + b_{n-k-1}x^{n-k-1} \\ &\quad + u_0 x^{n-k} + u_1 x^{n-k+1} + \cdots + u_{k-1}x^{n-1}\end{aligned}$$

then corresponds to the code vector

$$(b_0, b_1, \ldots, b_{n-k-1}, u_0, u_1, \ldots, u_{k-1}).$$

A $(7,4)$ Cyclic Code Gnerated by $\boldsymbol{g}(x) = 1 + x + x^3$

Messages	Code Vectors	Code Polynomials
(0 0 0 0)	0 0 0 0 0 0 0	$0 = 0 \cdot \boldsymbol{g}(x)$
(1 0 0 0)	1 1 0 1 0 0 0	$1 + x + x^3 = 1 \cdot \boldsymbol{g}(x)$
(0 1 0 0)	0 1 1 0 1 0 0	$x + x^2 + x^4 = x \cdot \boldsymbol{g}(x)$
(1 1 0 0)	1 0 1 1 1 0 0	$1 + x^2 + x^3 + x^4 = (1 + x) \cdot \boldsymbol{g}(x)$
(0 0 1 0)	0 0 1 1 0 1 0	$x^2 + x^3 + x^5 = x^2 \cdot \boldsymbol{g}(x)$
(1 0 1 0)	1 1 1 0 0 1 0	$1 + x + x^2 + x^5 = (1 + x^2) \cdot \boldsymbol{g}(x)$
(0 1 1 0)	0 1 0 1 1 1 0	$x + x^3 + x^4 + x^5 = (x + x^2) \cdot \boldsymbol{g}(x)$
(1 1 1 0)	1 0 0 0 1 1 0	$1 + x^4 + x^5 = (1 + x + x^2) \cdot \boldsymbol{g}(x)$
(0 0 0 1)	0 0 0 1 1 0 1	$x^3 + x^4 + x^6 = x^3 \cdot \boldsymbol{g}(x)$
(1 0 0 1)	1 1 0 0 1 0 1	$1 + x + x^4 + x^6 = (1 + x^3) \cdot \boldsymbol{g}(x)$
(0 1 0 1)	0 1 1 1 0 0 1	$x + x^2 + x^3 + x^6 = (x + x^3) \cdot \boldsymbol{g}(x)$
(1 1 0 1)	1 0 1 0 0 0 1	$1 + x^2 + x^6 = (1 + x + x^3) \cdot \boldsymbol{g}(x)$
(0 0 1 1)	0 0 1 0 1 1 1	$x^2 + x^4 + x^5 + x^6 = (x^2 + x^3) \cdot \boldsymbol{g}(x)$
(1 0 1 1)	1 1 1 1 1 1 1	$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = (1 + x^2 + x^3) \cdot \boldsymbol{g}(x)$
(1 1 1 1)	1 0 0 1 0 1 1	$1 + x^3 + x^5 + x^6 = (1 + x + x^2 + x^3) \cdot \boldsymbol{g}(x)$

Generator and Parity-Check Matrices

- The generator matrix of an (n, k) code $\boldsymbol{C}$ is as follows:

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

- In general, $\boldsymbol{G}$ is not in systematic form. However, it can be put into systematic form with row operation.

- Let

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

where the polynomial $\boldsymbol{h}(x)$ has the degree k and is of the following form:

$$\boldsymbol{h}(x) = h_0 + h_1 x + \cdots + h_k x^k$$

with $h_0 = h_k = 1$.

- A parity-check matrix of $\boldsymbol{C}$ may be obtained from $\boldsymbol{h}(x)$.
- Let $\boldsymbol{v}$ be a code vector in $\boldsymbol{C}$ and $\boldsymbol{v}(x) = \boldsymbol{a}(x)\boldsymbol{g}(x)$. Then

$$\begin{aligned} \boldsymbol{v}(x)\boldsymbol{h}(x) &= \boldsymbol{a}(x)\boldsymbol{g}(x)\boldsymbol{h}(x) \\ &= \boldsymbol{a}(x)(x^n + 1) \\ &= \boldsymbol{a}(x) + x^n\boldsymbol{a}(x). \end{aligned}$$

Since the degree of $\boldsymbol{a}(x)$ is $k-1$ or less, the powers $x^k, x^{k+1}, \ldots, x^{n-1}$ do not appear in $\boldsymbol{a}(x) + x^n\boldsymbol{a}(x)$. Therefore,

$$\sum_{i=0}^{k} h_i v_{n-i-j} = 0 \text{ for } 1 \leq j \leq n-k.$$

We take the *reciprocal* of $\boldsymbol{h}(x)$,

$$x^k\boldsymbol{h}(x^{-1}) = h_k + h_{k-1}x + h_{k-2}x^2 + \cdots + h_0x^k,$$

and can see that $x^k\boldsymbol{h}(x^{-1})$ is also a factor of x^n+1. $x^k\boldsymbol{h}(x^{-1})$ then generates an $(n, n-k)$ cyclic code with the following $(n-k)\times n$ matrix as a generator matrix:

$$\boldsymbol{H} = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdot & \cdot & \cdot & \cdot & h_0 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \cdot & \cdot & \cdot & \cdot & h_0 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & h_k & h_{k-1} & \cdot & \cdot & \cdot & \cdot & \cdot & h_0 & \cdot & \cdot & 0 \\ \cdot & & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & & \cdot \\ 0 & 0 & \cdot & \cdot & 0 & h_k & h_{k-1} & h_{k-2} & \cdot & \cdot & \cdot & \cdot & h_0 \end{bmatrix}$$

Then $\boldsymbol{H}$ is a parity-check matrix of the cyclic code $\boldsymbol{C}$. We call $\boldsymbol{h}(x)$ the *parity polynomial* of $\boldsymbol{C}$.

- Let $\boldsymbol{C}$ be an (n, k) cyclic code with generator polynomial $\boldsymbol{g}(x)$. The dual code of $\boldsymbol{C}$ is also cyclic and is generated by the polynomial $x^k\boldsymbol{h}(x^{-1})$, where $\boldsymbol{h}(x) = (x^n+1)/\boldsymbol{g}(x)$.
- Let

$$x^{n-k+i} = \boldsymbol{a}_i(x)\boldsymbol{g}(x) + \boldsymbol{b}_i(x) \text{ for } 0 \le i \le k-1,$$

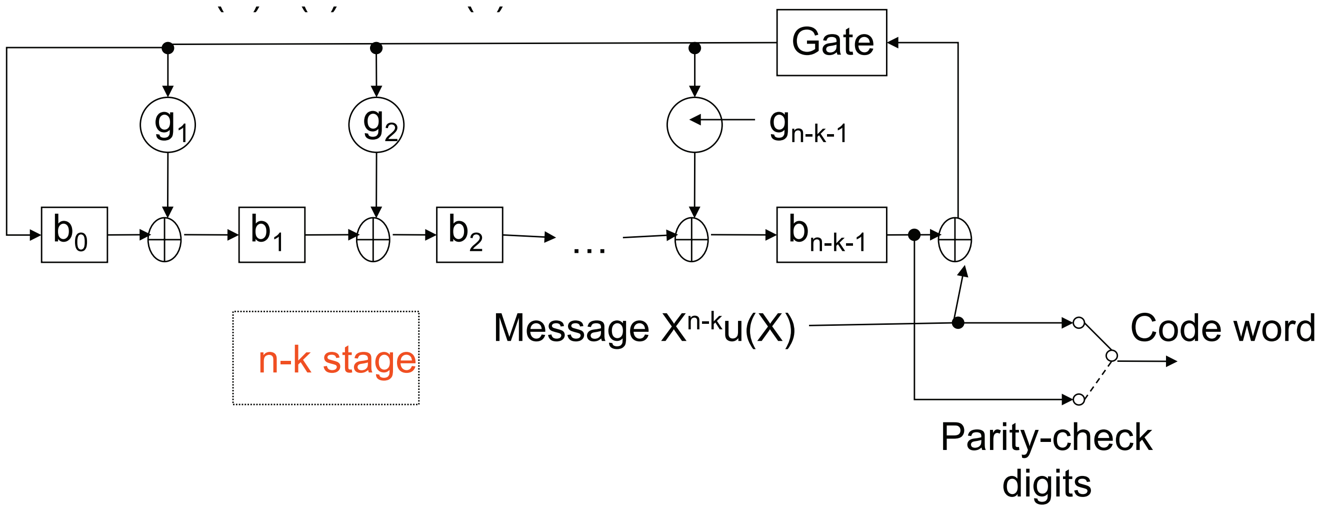
where $\boldsymbol{b}_i(x) = b_{i0} + b_{i1} + \cdots + b_{i(n-k-1)}$. Since $\boldsymbol{b}_i(x) + x^{n-k+i}$ are multiples of $\boldsymbol{g}(x)$, they are code polynomials. Then

$$\boldsymbol{G} = \begin{bmatrix} b_{00} & b_{01} & b_{02} & \cdots & b_{0(n-k-1)} & 1 & 0 & 0 & \cdots & 0 \\ b_{10} & b_{11} & b_{12} & \cdots & b_{1(n-k-1)} & 0 & 1 & 0 & \cdots & 0 \\ b_{20} & b_{21} & b_{22} & \cdots & b_{2(n-k-1)} & 0 & & 1 & \cdots & 0 \\ & \vdots & & & & \vdots & & & & \vdots \\ b_{(k-1)0} & b_{(k-1)1} & b_{(k-1)2} & \cdots & b_{(k-1)(n-k-1)} & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

- The corresponding parity-check matrix for $\boldsymbol{C}$ is

$$\boldsymbol{H} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & b_{00} & b_{10} & b_{20} & \cdots & b_{(k-1)0} \\ 0 & 1 & 0 & \cdots & 0 & b_{01} & b_{11} & b_{21} & \cdots & b_{(k-1)1} \\ 0 & 0 & 1 & \cdots & 0 & b_{02} & b_{12} & b_{22} & \cdots & b_{(k-1)2} \\ & \vdots & & & & \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_{0(n-k-1)} & b_{1(n-k-1)} & b_{2(n-k-1)} & \cdots & b_{(k-1)(n-k-1)} \end{bmatrix}.$$

Encoding of Cyclic Codes

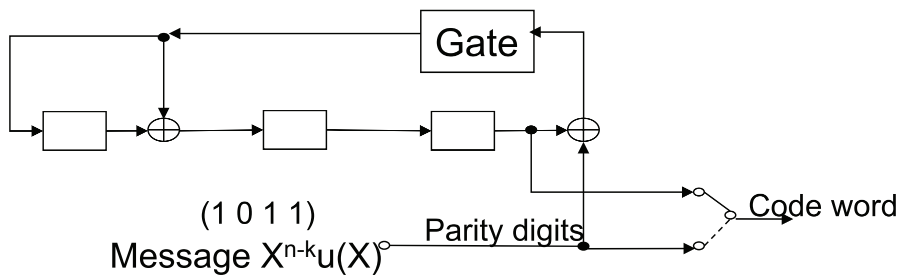
- Encoding process: (1) Multiply $\boldsymbol{u}(x)$ by x^{n-k}; (2) divide $x^{n-k}\boldsymbol{u}(x)$ by $\boldsymbol{g}(x)$; (3) form the code word $\boldsymbol{b}(x) + x^{n-k}\boldsymbol{u}(x)$.
- 

Example

- Consider the $(7, 4)$ cyclic code generated by $\boldsymbol{g}(x) = 1 + x + x^3$. Suppose that the message $\boldsymbol{u} = (1\ 0\ 1\ 1)$ is to be encoded. 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)
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 $(1\ 0\ 0\ 1\ 0\ 1\ 1)$.



Encoding by Parity Polynomial

- Since $h_k = 1$, we have

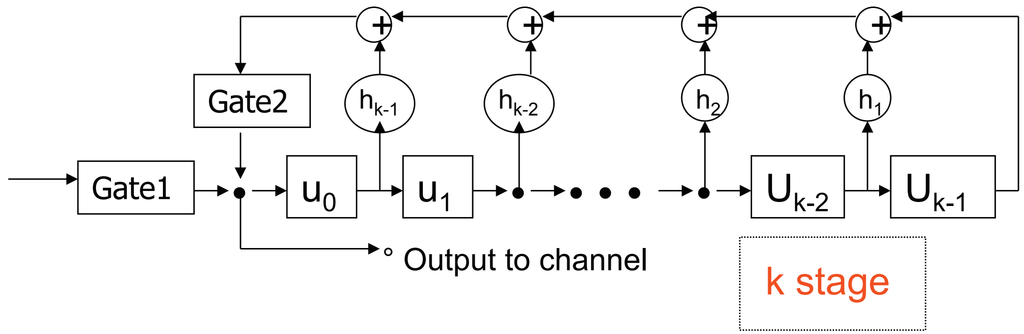
$$v_{n-k-j} = \sum_{i=0}^{k-1} h_i v_{n-i-j} \text{ for } 1 \leq j \leq n-k,$$

which is known as a *difference equation.*

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

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

- Encoding circuit:

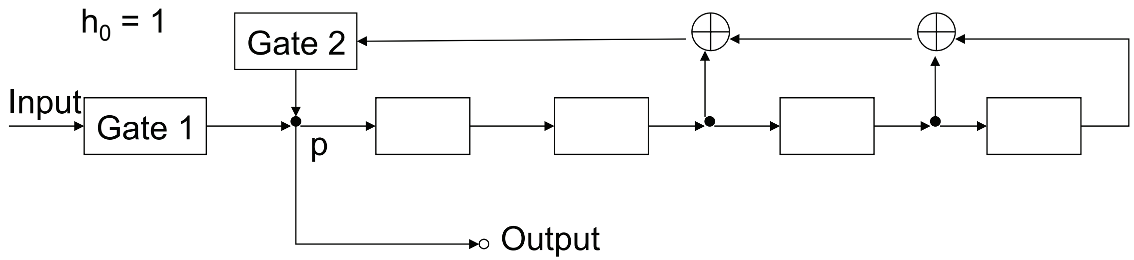


Example

- The parity polynomial of the $(7,4)$ cyclic code generated by $\boldsymbol{g}(x) = 1 + x + x^3$ is

$$\boldsymbol{h}(x) = \frac{x^7+1}{1+x+x^3} = 1 + x + x^2 + x^4.$$

The encoding circuit:



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 parity-check digits are

$$\begin{aligned} v_2 &= v_6 + v_3 + v_4 = 1 + 1 + 0 = 0 \\ v_1 &= v_5 + v_4 + v_3 = 1 + 0 + 1 = 0 \\ v_0 &= v_4 + v_3 + v_2 = 0 + 1 + 0 = 1. \end{aligned}$$

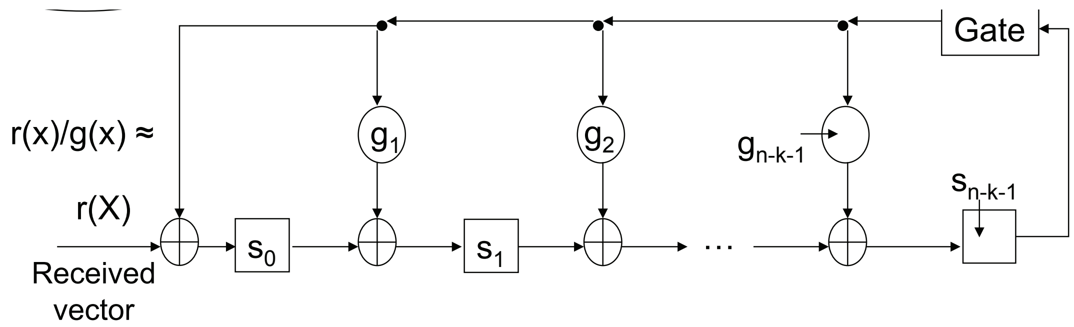
The code vector that corresponds to the message (1 0 1 1) is (1 0 0 1 0 1 1).

Syndrome Computation

- Let $\boldsymbol{r} = (r_0, r_1, \ldots, r_{n-1})$ be the received vector. The *syndrome* is calculated as $\boldsymbol{s} = \boldsymbol{r} \cdot \boldsymbol{H}^T$, where $\boldsymbol{H}$ is the parity-check matrix.
- If syndrome is not identical to zero, $\boldsymbol{r}$ is not a code vector and the presence of errors has been detected.
- Dividing $\boldsymbol{r}(x)$ by the generator polynomial $\boldsymbol{g}(x)$, we obtain

$$\boldsymbol{r}(x) = \boldsymbol{a}(x)\boldsymbol{g}(x) + \boldsymbol{s}(x).$$

- The $n-k$ coefficients of $\boldsymbol{s}(x)$ form the syndrome $\boldsymbol{s}$. We call $\boldsymbol{s}(x)$ the *syndrome*.



- If $\boldsymbol{C}$ is a systematic code, then the syndrome is simply the vector sum of the received parity digits and the parity-check digits recomputed from the received information digits.
- Let $\boldsymbol{s}(x)$ be the syndrome of a received polynomial $\boldsymbol{r}(x)$. Then the remainder $\boldsymbol{s}^{(1)}(x)$ resulting from dividing $x\boldsymbol{s}(x)$ by the generator polynomial $\boldsymbol{g}(x)$ is the syndrome of $\boldsymbol{r}^{(1)}(x)$, which is a cyclic shift of $\boldsymbol{r}(x)$.

  Proof: We have

$$x\boldsymbol{r}(x) = r_{n-1}(x^n + 1) + \boldsymbol{r}^{(1)}(x).$$

  Then

$$\boldsymbol{c}(x)\boldsymbol{g}(x) + \boldsymbol{\rho}(x) = r_{n-1}\boldsymbol{g}(x)\boldsymbol{h}(x) + x[\boldsymbol{a}(x)\boldsymbol{g}(x) + \boldsymbol{s}(x)],$$

  where $\boldsymbol{\rho}(x)$ is the remainder resulting from dividing $\boldsymbol{r}^{(1)}(x)$ by $\boldsymbol{g}(x)$. Then $\boldsymbol{\rho}(x)$ is the syndrome of $\boldsymbol{r}^{(1)}(x)$. Rearranging the above equation, we have

$$x\boldsymbol{s}(x) = [\boldsymbol{c}(x) + r_{n-1}\boldsymbol{h}(x) + x\boldsymbol{a}(x)]\boldsymbol{g}(x) + \boldsymbol{\rho}(x).$$

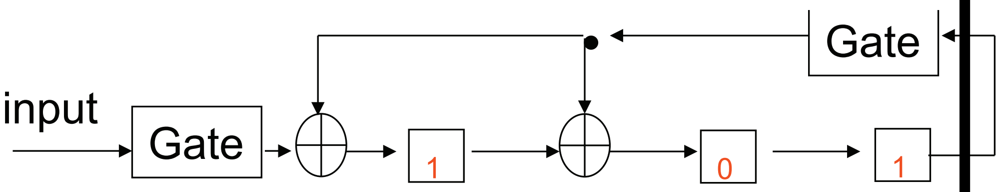
It is clearly that $\boldsymbol{\rho}(x)$ is also the remainder resulting from dividing $x\boldsymbol{s}(x)$ by $\boldsymbol{g}(x)$. Therefore, $\boldsymbol{\rho}(x) = \boldsymbol{s}^{(1)}(x)$.

- The remainder $\boldsymbol{s}^{(i)}(x)$ resulting from dividing $x^i\boldsymbol{s}(x)$ be the generator polynomial $\boldsymbol{g}(x)$ is the syndrome of $\boldsymbol{r}^{(i)}(x)$, which is the ith cyclic shift of $\boldsymbol{r}(x)$.

Example

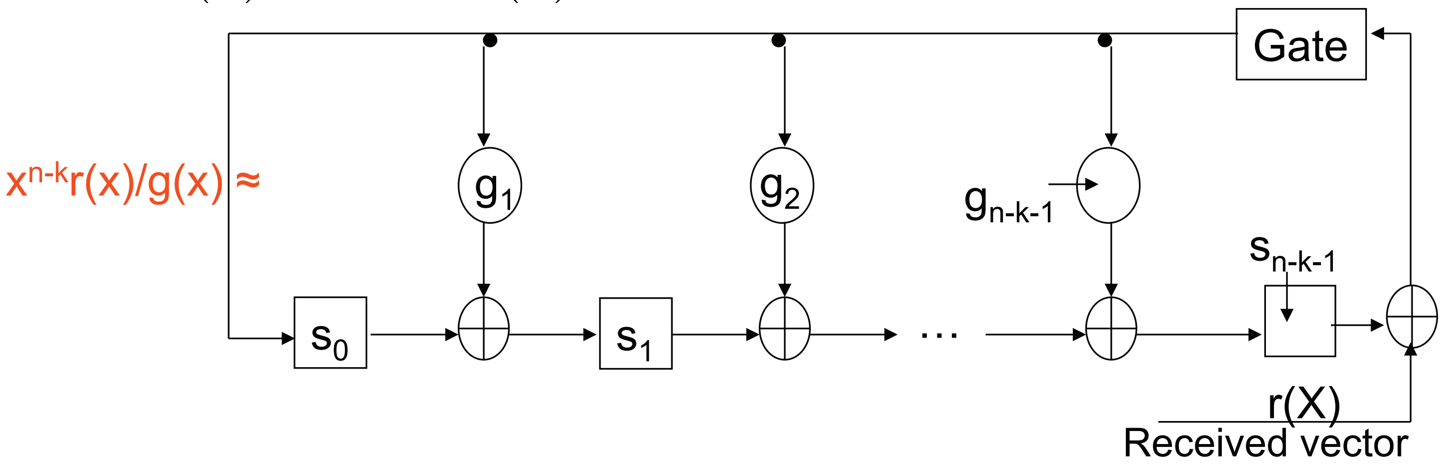
Consider the $(7, 4)$ cyclic code generated by $\boldsymbol{g}(x) = 1 + x + x^3$. Suppose that the received vector is $\boldsymbol{r} = (0\ 0\ 1\ 0\ 1\ 1\ 0)$. The syndrome of $\boldsymbol{r}$ is $\boldsymbol{s} = (1\ 0\ 1)$. As the received vector is shifted into the circuit, the contents in the register are as follows:

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 $s^{(2)}$)



If the register is shifted once more with the input gate disabled, the new contents will be $\boldsymbol{s}^{(1)} = (1\ 0\ 0)$, which is the syndrome of $\boldsymbol{r}^{(1)} = (0\ 0\ 0\ 1\ 0\ 1\ 1)$.

- We may shift the received vector $\boldsymbol{r}(x)$ into the syndrome register from the right end. However, after the entire $\boldsymbol{r}(x)$ has been shifted into the register, the contents in the register do not form the sybdrome of $\boldsymbol{r}(x)$; rather, they form the syndrome $\boldsymbol{s}^{(n-k)}(x)$ of $\boldsymbol{r}^{(n-k)}(x)$.



Proof: We have

$$x^{n-k}\boldsymbol{r}(x) = \boldsymbol{a}(x)\boldsymbol{g}(x) + \boldsymbol{\rho}(x).$$

It is known that

$$x^{n-k}\boldsymbol{r}(x) = \boldsymbol{b}(x)(x^n + 1) + \boldsymbol{r}^{(n-k)}(x).$$

Hence,

$$\boldsymbol{r}^{(n-k)}(x) = [\boldsymbol{b}(x)\boldsymbol{h}(x) + \boldsymbol{a}(x)]\boldsymbol{g}(x) + \boldsymbol{\rho}(x).$$

When $\boldsymbol{r}^{(n-k)}(x)$ is divided by $\boldsymbol{g}(x)$, $\boldsymbol{\rho}(x)$ is also the remainder. Therefore, $\boldsymbol{\rho}(x)$ is indeed the syndrome of $\boldsymbol{r}^{(n-k)}(x)$.

Error Detection

- Let $\boldsymbol{v}(x)$ be the transmitted code word and $\boldsymbol{e}(x) = e_0 + e_1 x + \cdots + e_{n-1}x^{n-1}$ be the error pattern. Then

$$\boldsymbol{r}(x) = \boldsymbol{v}(x) + \boldsymbol{e}(x) = \boldsymbol{b}(x)\boldsymbol{g}(x) + \boldsymbol{e}(x).$$

- Following the definition of syndrome, we have

$$\boldsymbol{e}(x) = [\boldsymbol{a}(x) + \boldsymbol{b}(x)]\boldsymbol{g}(x) + \boldsymbol{s}(x).$$

  This shows that the syndrome is actually equal to the remainder resulting from dividing the error pattern by the generator polynomial.

- The decoder has to estimate $\boldsymbol{e}(x)$ based on the syndrome $\boldsymbol{s}(x)$.
- If $\boldsymbol{e}(x)$ is identical to a code vector, $\boldsymbol{e}(x)$ is an undetectable error pattern.
- The error-detection circuit is simply a syndrome circuit with an

OR gate with the syndrome digits as inputs.

- For a cyclic code, an error pattern with errors confined to i high-order positions and $\ell - i$ low-order positions is also regarded as a burst of length ℓ or less. such a burst is called *end-around* burst.
- An (n, k) cyclic code is capable of detecting any error burst of length $n - k$ or less, including the end-around bursts.

  Proof: Suppose that the error pattern is a burst of length of $n - k$ or less. Then

  $$\boldsymbol{e}(x) = x^j \boldsymbol{B}(x),$$

  where $0 \leq j \leq n - 1$ and $\boldsymbol{B}(x)$ is a polynomial of degree $n - k - 1$ or less. Since the degree of $\boldsymbol{B}(x)$ is less than that of $\boldsymbol{g}(x)$, $\boldsymbol{B}(x)$ is not divisible by $\boldsymbol{g}(x)$. Since $\boldsymbol{g}(x)$ is a factor of $x^n + 1$ and x is not a factor of $\boldsymbol{g}(x)$, $\boldsymbol{g}(x)$ and x^j must be relatively prime. Therefore, $\boldsymbol{e}(x)$ is not divisible by $\boldsymbol{g}(x)$. The last part of the above statement is left as an exercise.

- The fraction of undetectable bursts of length $n-k+1$ is $2^{-(n-k-1)}$.

  Proof: Consider the bursts of length $n-k+1$ starting from the ith digit position and ending at the $(i+n-k)$th digit position. There are 2^{n-k-1} such burst. Among these bursts, the only one that cannot be detected is

  $$\boldsymbol{e}(x) = x^i \boldsymbol{g}(x).$$

  Therefore, the fraction of undetectable bursts of length $n-k+1$ starting from the ith digit position is $2^{-(n-k-1)}$.

- For $\ell > n-k+1$, the fraction of undetectable error bursts of length ℓ is $2^{-(n-k)}$. The proof is left as an exercise.

Decoding of Cyclic Codes

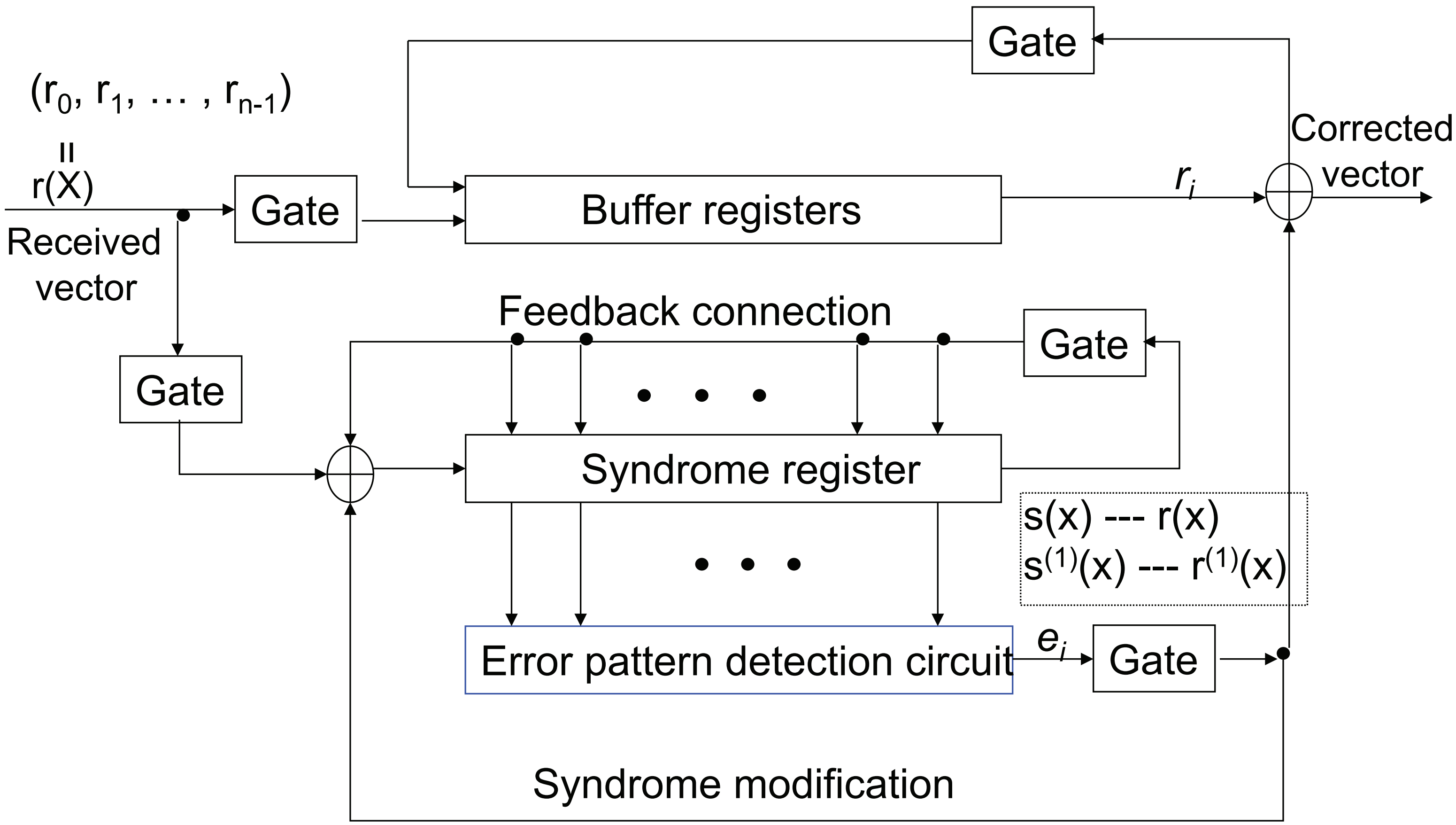
- Decoding of linear codes consists of three steps: (1) syndrome computation; (2) association of the syndrome to an error pattern; (3) error correction.
- The cyclic structure of a cyclic code allows us to decode a received vector $\boldsymbol{r}(x)$ in serial manner.
- The received digits are decoded one at a time and each digit is decoded with the same circuitry.
- The decoding circuit checks whether the syndrome $\boldsymbol{s}(x)$ corresponds to a correctable error pattern $\boldsymbol{e}(x)$ with an error at the highest-order position x^{n-1} (i.e., $e_{n-1} = 1$).
- If $\boldsymbol{s}(x)$ 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 this, we have $\boldsymbol{r}^{(1)}(x)$ and $\boldsymbol{s}^{(1)}(x)$.

- The second digit r_{n-2} of $\boldsymbol{r}(x)$ becomes the first digit of $\boldsymbol{r}^{(1)}(x)$. The same decoding processes.
- If the syndrome $\boldsymbol{s}(x)$ of $\boldsymbol{r}(x)$ does correspond to an error pattern with an error at the location x^{n-1}, the first received digit r_{n-1} is an erroneous digit and it must be corrected by taking the sum $r_{n-1} \oplus e_{n-1}$.
- This correction results in a modified received polynomial, denoted by
  $\boldsymbol{r}_1(x) = r_0 + r_1 x + \cdots + r_{n-2}x^{n-2} + (r_{n-1} \oplus e_{n-1})x^{n-1}$.
- The effect of the error digit e_{n-1} on the syndrome can be achieved by adding the syndrome of $\boldsymbol{e}'(x) = x^{n-1}$ to $\boldsymbol{s}(x)$.
- The syndrome $\boldsymbol{s}_1^{(1)}$ of $\boldsymbol{r}_1^{(1)}(x)$ is the remainder resulting from dividing $x[\boldsymbol{s}(x) + x^{n-1}]$ by the generator polynomial $\boldsymbol{g}(x)$.
- Since the remainders resulting from dividing $x\boldsymbol{s}(x)$ and x^n by

$\boldsymbol{g}(x)$ are $\boldsymbol{s}^{(1)}(x)$ and 1, respectively, we have

$$\boldsymbol{s}_1^{(1)}(x) = \boldsymbol{s}^{(1)}(x) + 1.$$

Meggitt Decoder I

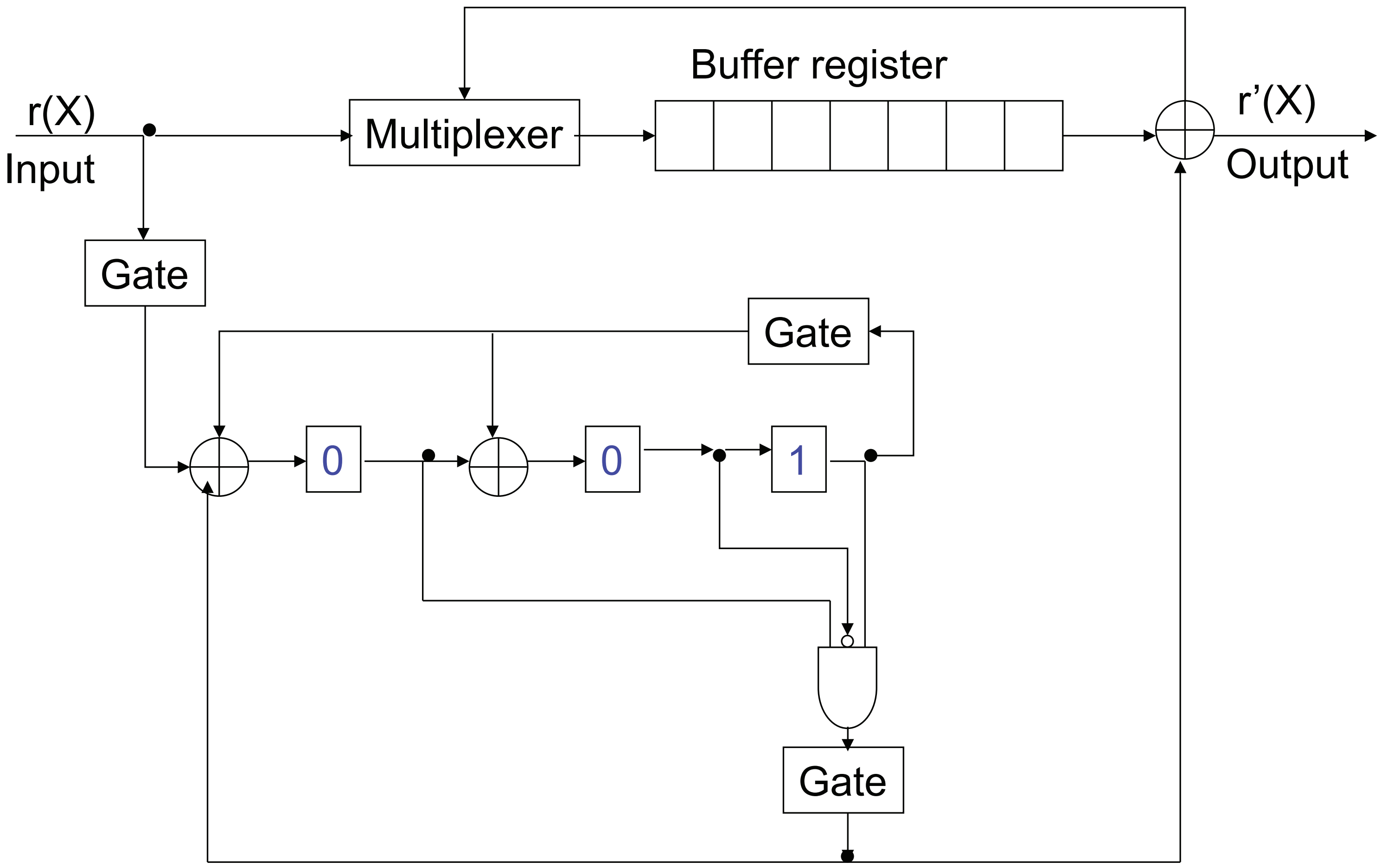


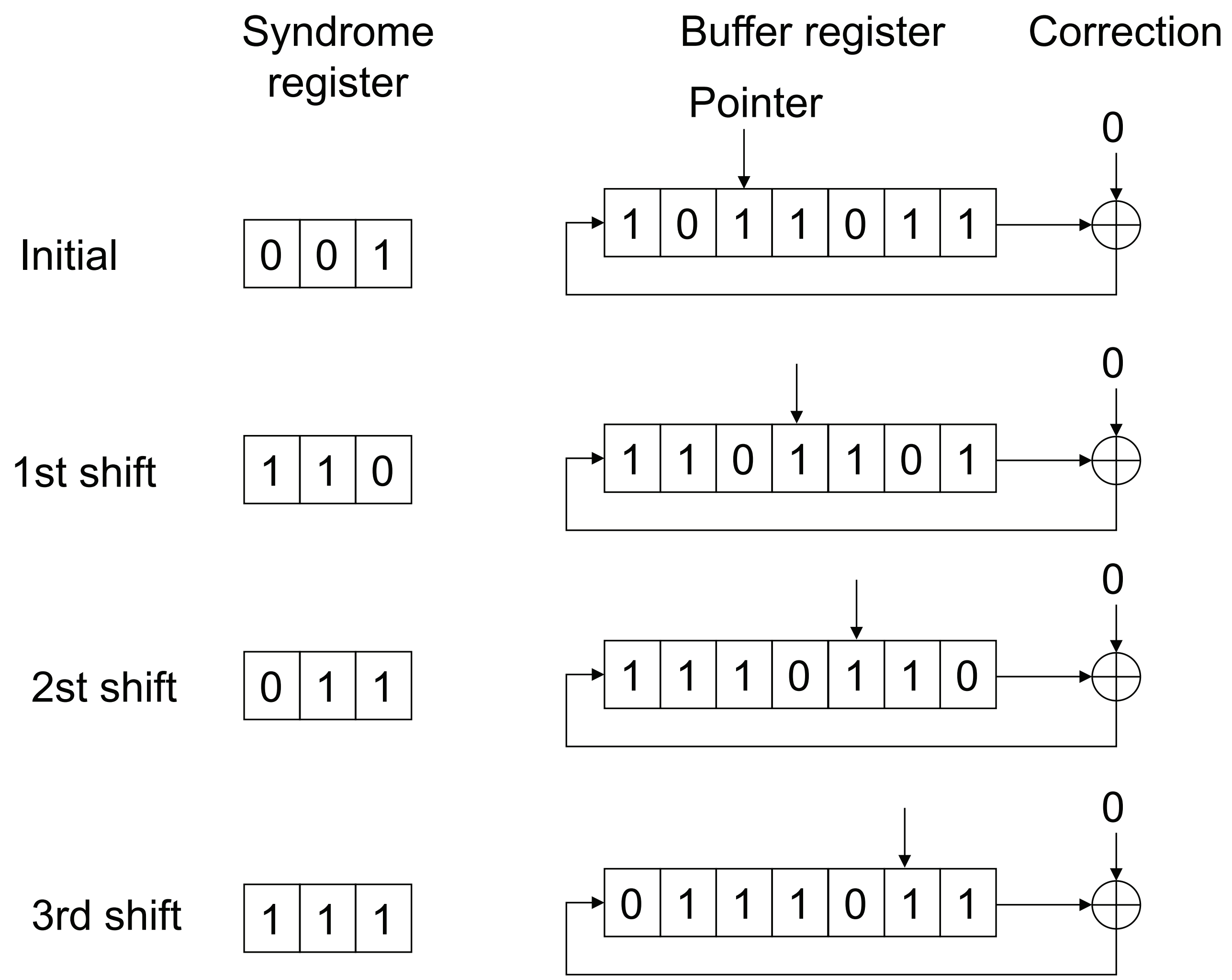
Example

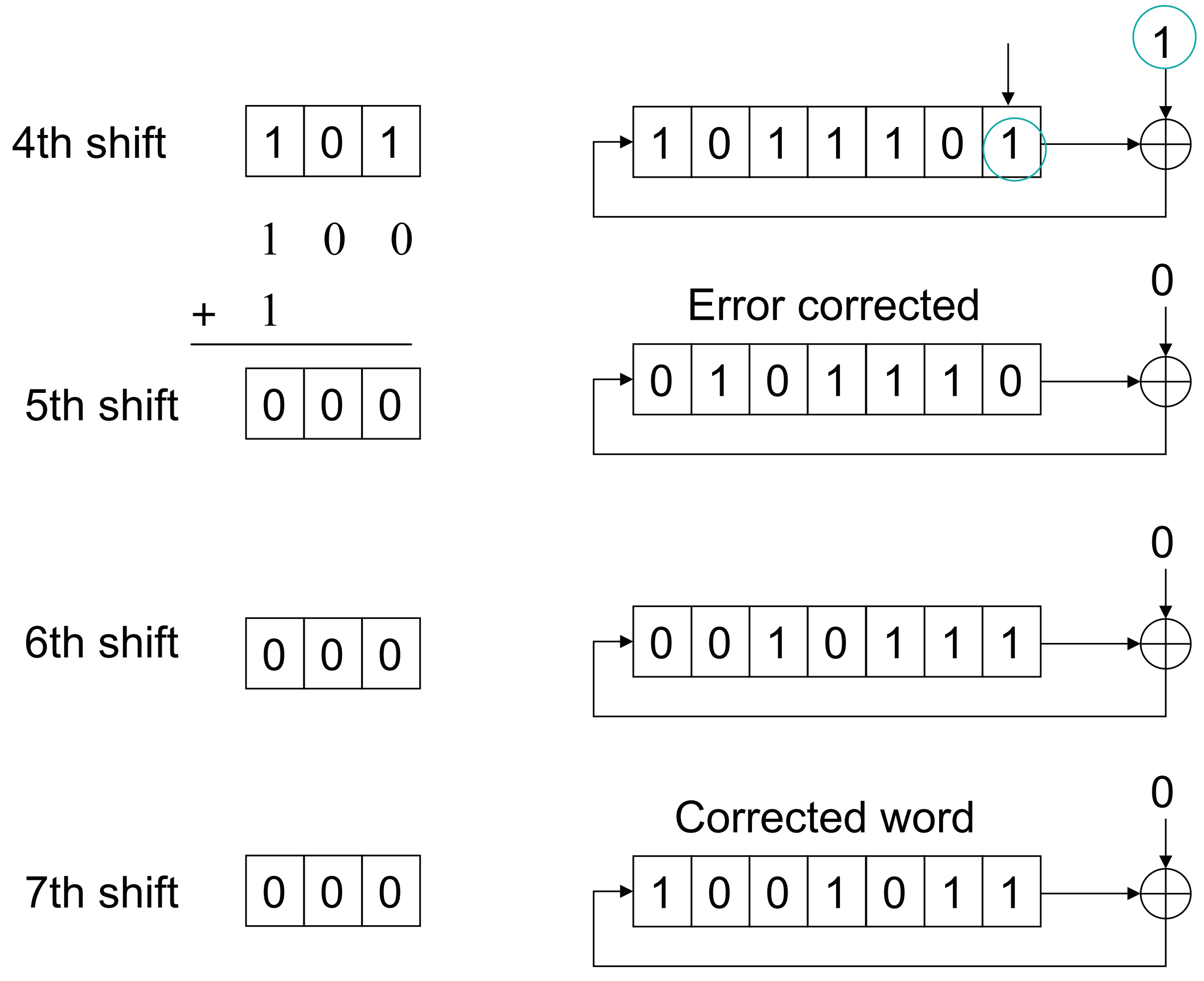
Consider the decoding of the $(7, 4)$ cyclic code generated by $\boldsymbol{g}(x) = 1 + x + x^3$. This code has minimum distance 3 and is capable of correcting any single error. The seven single-error patterns and their corresponding syndromes are as follows:

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)

Suppose that the code vector $\boldsymbol{v} = (1\ 0\ 0\ 1\ 0\ 1\ 1)$ is transmitted and $\boldsymbol{r} = (1\ 0\ 1\ 1\ 0\ 1\ 1)$.


Buffer register
r(X)
Input
Multiplexer
r'(X)
Output
Gate
Gate
0
0
1
Gate


Syndrome register
Buffer register
Correction
Pointer
Initial
0 0 1
1 0 1 1 0 1 1
0
1st shift
1 1 0
1 1 0 1 1 0 1
0
2st shift
0 1 1
1 1 1 0 1 1 0
0
3rd shift
1 1 1
0 1 1 1 0 1 1
0

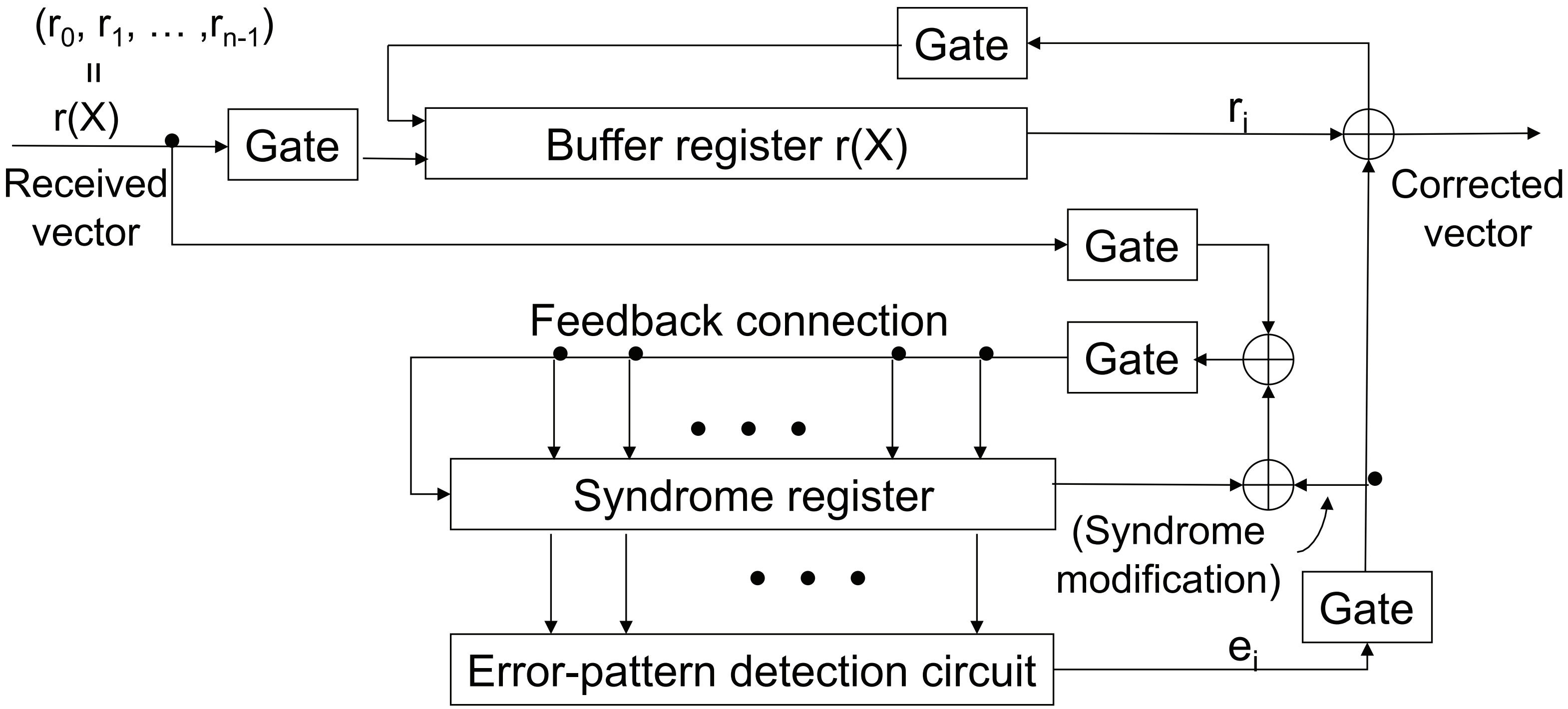

4th shift
1 0 1
1 0 0
+ 1
5th shift
0 0 0
6th shift
0 0 0
7th shift
0 0 0
1
1 0 1 1 1 0 1
Error corrected
0
0 1 0 1 1 1 0
0
0 0 1 0 1 1 1
Corrected word
0
1 0 0 1 0 1 1

Meggitt Decoder II

- To decode a cyclic code, the received polynomial $\boldsymbol{r}(x)$ may be shifted into the syndrome register from the right end for computing the syndrome.
- When $\boldsymbol{r}(x)$ has been shifted into the syndrome register, the register contains $\boldsymbol{s}^{(n-k)}(x)$, which is the syndrome of $\boldsymbol{r}^{(n-k)}(x)$. If $\boldsymbol{s}^{(n-k)}(x)$ corresponds to an error pattern $\boldsymbol{e}(x)$ with $e_{n-1} = 1$, the highest-order digit r_{n-1} of $\boldsymbol{r}(x)$ is erroneous and must be corrected.
- In $\boldsymbol{r}^{(n-k)}(x)$, the digit r_{n-1} is at the location x^{n-k-1}. When r_{n-1} is corrected, the error effect must be removed from $\boldsymbol{s}^{(n-k)}(x)$.
- The new syndrome $\boldsymbol{s}_1^{(n-k)}(x)$ is the sum of $\boldsymbol{s}^{(n-k)}(x)$ and the remainder $\boldsymbol{\rho}(x)$ resulting from dividing x^{n-k-1} by $\boldsymbol{g}(x)$. Since

the degree of x^{n-k-1} is less than the degree of $\boldsymbol{g}(x)$,

$$\boldsymbol{s}_1^{(n-k)}(x) = \boldsymbol{s}^{(n-k)}(x) + x^{n-k-1}.$$

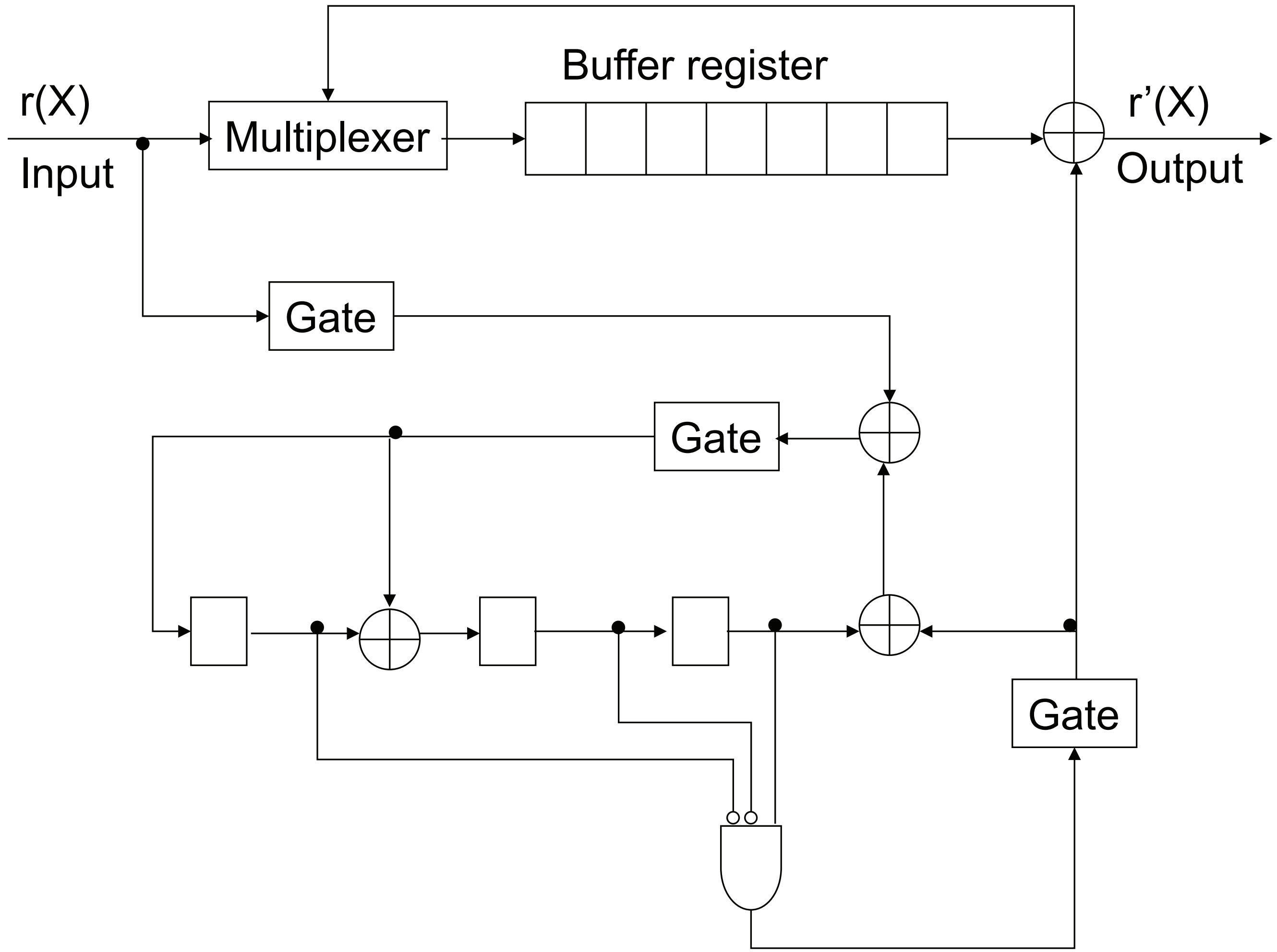


Example

Again, we consider the decoding of the $(7, 4)$ cyclic code generated by $\boldsymbol{g}(X) = 1 + X + X^3$. Suppose that the received polynomial $\boldsymbol{r}(X)$ is shifted into the syndrome register from the right end. The seven single-error patterns and their corresponding syndromes are as follows:

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)

We see that only when $\boldsymbol{e}(X) = X^6$ occurs, the syndrome is $(0\ 0\ 1)$ after the entire received polynomial $\boldsymbol{r}(X)$ 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 $\boldsymbol{r}(X)$ 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 $\boldsymbol{g}(X) = 1 + X + X^3$.


Buffer register
r(X)
Multiplexer
r'(X)
Input
Output
Gate
Gate
Gate