## ELEC 6131: Error Detecting and Correcting Codes
## Lecture 6: Cyclic Codes

**Cyclic codes:**

**Definition:** a linear block code is cyclic if a cycle shift of any codeword is another codeword.

The $i$th shift of $\underline{v} = (v_0, v_1, \cdots, v_{n-1})$ is:

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

For example, $\underline{v}^{(1)} = (v_{n-1}, v_0, v_1, \cdots, v_{n-2})$ and $\underline{v}^{(2)} = (v_{n-2}, v_{n-1}, v_0, v_1, \cdots, v_{n-3})$.

**Example:**

A (7, 4) cyclic code generated by $\mathbf{g}(X) = 1 + X + X^3$.

| Messages | Code vectors | Code polynomials |
|---|---|---|
| (0000) | 0000000 | $0 = 0 \cdot \mathbf{g}(X)$ |
| (1000) | 1101000 | $1 + X + X^3 = 1 \cdot \mathbf{g}(X)$ |
| (0100) | 0110100 | $X + X^2 + X^4 = X \cdot \mathbf{g}(X)$ |
| (1100) | 1011100 | $1 + X^2 + X^3 + X^4 = (1 + X) \cdot \mathbf{g}(X)$ |
| (0010) | 0011010 | $X^2 + X^3 + X^5 = X^2 \cdot \mathbf{g}(X)$ |
| (1010) | 1110010 | $1 + X + X^2 + X^5 = (1 + X^2) \cdot \mathbf{g}(X)$ |
| (0110) | 0101110 | $X + X^3 + X^4 + X^5 = (X + X^2) \cdot \mathbf{g}(X)$ |
| (1110) | 1000110 | $1 + X^4 + X^5 = (1 + X + X^2) \cdot \mathbf{g}(X)$ |
| (0001) | 0001101 | $X^3 + X^4 + X^6 = X^3 \cdot \mathbf{g}(X)$ |
| (1001) | 1100101 | $1 + X + X^4 + X^6 = (1 + X^3) \cdot \mathbf{g}(X)$ |
| (0101) | 0111001 | $X + X^2 + X^3 + X^6 = (X + X^3) \cdot \mathbf{g}(X)$ |
| (1101) | 1010001 | $1 + X^2 + X^6 = (1 + X + X^3) \cdot \mathbf{g}(X)$ |
| (0011) | 0010111 | $X^2 + X^4 + X^5 + X^6 = (X^2 + X^3) \cdot \mathbf{g}(X)$ |
| (1011) | 1111111 | $1 + X + X^2 + X^3 + X^4 + X^5 + X^6 = (1 + X^2 + X^3) \cdot \mathbf{g}(X)$ |
| (0111) | 0100011 | $X + X^5 + X^6 = (X + X^2 + X^3) \cdot \mathbf{g}(X)$ |
| (1111) | 1001011 | $1 + X^3 + X^5 + X^6 = (1 + X + X^2 + X^3) \cdot \mathbf{g}(X)$ |

Let $v(X) = v_0 + v_1 X + v_2 X^2 + \cdots + v_{n-1} X^{n-1}$ be the polynomial representation of $\underline{v}$. Then,

$$v^{(i)}(X) = v_{n-i} + v_{n-i+1} X + \cdots + v_{n-1} X^{i-1} + \cancel{v_0 X^i} + \cancel{v_1 X^{i+1}} + \cdots + \cancel{v_{n-i-1} X^{n-1}}.$$

Multiply $X^i$ by $v(X)$, i.e., shift $\underline{v}$ $i$ times (linearly, not cyclically). Then,

$$X^i v(X) = \cancel{v_0 X^i} + \cancel{v_1 X^{i+1}} + \cdots + \cancel{v_{n-i-1} X^{n-1}} + \cdots + v_{n-1} X^{n+i-1}.$$

Add $X^i v(X)$ and $v^{(i)}(X)$:

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

or:

$$X^i v(X) + v^{(i)}(X) = [v_{n-i} + v_{n-i+1}X + \cdots + v_{n-1}X^{i-1}](X^n + 1).$$

So:

$$X^i v(X) = q(X)[X^n + 1] + v^{(i)}(X).$$

That is, the $i$th cyclic shift of $v(X)$ is generated by dividing $X^i v(X)$ by $X^n + 1$.

**Theorem 1:** the non-zero code polynomial with minimum degree in a cyclic code $C$ is unique.

**Proof:** let $g(X) = g_0 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r$ be the minimal degree code polynomial of $C$. Suppose there is another $g'(X) = g_0' + g_1'X + \cdots + g_{r-1}'X^{r-1} + X^r$. Then, $g(X) + g'(X)$ is another codeword in $C$ with degree less than $r$. $\Rightarrow$ contradiction.

**Theorem 2:** let $g(X) = g_0 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r$ be the minimum degree polynomial of a cyclic code $C$. Then, $g_0 \neq 0$.

**Proof:** if $g_0 = 0$ then shifting $g(X)$ once to the left (or $n-1$ times to right) results in $g_1 + g_2X + \cdots + g_{r-1}X^{r-2} + X^{r-1}$ which has a degree $< r$ $\Rightarrow$ contradiction. So, $g(X) = 1 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r$.

Let $g(X)$ be the polynomial of minimum degree of a code $C$. Take $g(X), Xg(X), X^2g(X), \cdots, X^{n-r-1}g(X)$. These are shifts of $g(X)$ by $0, 1, \cdots, n-r-1$. So, they are codewords. Any linear combination of them is also a codeword. Therefore,

$$v(X) = u_0g(X) + u_1Xg(X) + \cdots + u_{n-r-1}X^{n-r-1}g(X)$$
$$= [u_0 + u_1X + \cdots + u_{n-r-1}X^{n-r-1}]g(X)$$

is also a code.

**Theorem 3:** let $g(X) = 1 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r$ be the non-zero code polynomial of minimum degree of an $(n, k)$ cyclic code $C$. A binary polynomial of degree $n-1$ or less is a code polynomial <u>if</u> and <u>only if</u> it is a multiple of $g(X)$.

**Proof:** let $v(X)$ be a polynomial of degree $n-1$ or less such that:

$$v(X) = (a_0 + a_1X + \cdots + a_{n-r-1}X^{n-r-1})g(X).$$

Then,

$$v(X) = a_0g(X) + a_1Xg(X) + \cdots + a_{n-r-1}X^{n-r-1}g(X).$$

Since $g(X), Xg(X), \cdots$ are each codeword of $C$ so is their sum $v(X)$.

Now assume $v(X)$ be a code polynomial in $C$. Then write:

$$v(X) = a(X)g(X) + b(X)$$

i.e., divide $v(X)$ by $g(X)$ and get remainder $b(X)$ and quotient $a(X)$.

$$b(X) = v(X) + a(X)g(X).$$

$v(X)$ is a codeword and so is $a(X)g(X)$. Therefore, $b(X)$ is also a codeword. But degree of $b(X)$ is less than $r \Rightarrow$ contradiction unless if $b(X) = 0$.

The number of polynomials of degree $n-1$ or less that are multiple of $g(X)$ is $2^{n-r}$. Due to 1-to-1 correspondence between these polynomials and the codewords (Theorem 3), we have $2^{n-r} = 2^k \Rightarrow r = n-k$.

**Theorem 4:** in an $(n,k)$ cyclic code, there is one and only one code polynomial of degree $n-k$,

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

Every code polynomial is a multiple of $g(X)$. Every binary polynomial of degree $n-1$ or less that is a multiple of $g(X)$ is a code polynomial. So,

$$v(X) = u(X)g(X)$$

is a code polynomial, however, not in a systematic form.

To make code systematic, multiply the information polynomial $u(X)$ by $X^{n-k}$. This means placing the $k$ information bits at the head of the shift register (in $k$ right-most Flip-Flops). Then,

$$u(X) = u_0 + u_1X + \cdots + u_{k-1}X^{k-1}$$

will result in:

$$X^{n-k}u(X) = u_0X^{n-k} + u_1X^{n-k+1} + \cdots + u_{k-1}X^{n-1}.$$

Now divide $X^{n-k}u(X)$ by $g(X)$ to get:

$$X^{n-k}u(X) = a(X)g(X) + b(X),$$

where $b(X)$ is a polynomial of degree $n-k-1$ or less:

$$b(X) = b_0 + b_1X + \cdots + b_{n-k-1}X^{n-k-1}$$

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

This means that $b(X) + X^{n-k}u(X)$ is the representation of a codeword in systematic form, i.e.,

$$\begin{aligned} b(X) + X^{n-k}u(X) = b_0 + b_1X + \cdots + b_{n-k-1}X^{n-k-1} \\ + u_0X^{n-k} + u_1X^{n-k+1} + \cdots + u_{k-1}X^{n-1} \end{aligned}$$

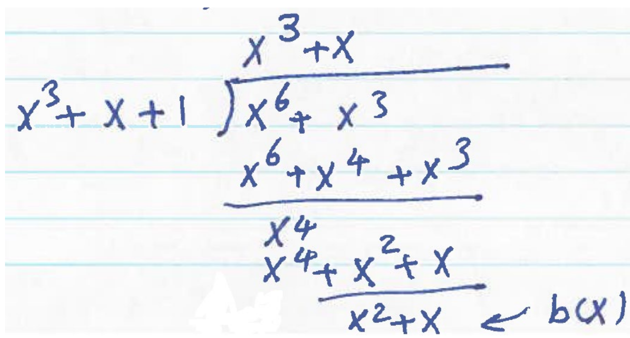
that represents

$$\underline{v} = (b_0, b_1, \cdots, b_{n-k-1}, u_0, u_1, \cdots, u_{k-1}).$$

**Example:** consider the $(7,4)$ cyclic code generated by $g(X) = 1 + X + X^3$. Let $u(X) = 1 + X^3$. Then,

1- $X^3 u(X) = X^3 + X^6$

2-




3- $v(X) = b(X) + X^3 u(X) = X + X^2 + X^3 + X^6$ or $\underline{v} = (0, 1, 1, 1, 0, 0, 1)$

**A (7, 4) cyclic code in systematic form generated by $\mathbf{g}(X) = 1 + X + X^3$.**

| Message | Codeword | |
|---|---|---|
| (0000) | (0000000) | $0 = 0 \cdot \mathbf{g}(X)$ |
| (1000) | (1101000) | $1 + X + X^3 = \mathbf{g}(X)$ |
| (0100) | (0110100) | $X + X^2 + X^4 = X\mathbf{g}(X)$ |
| (1100) | (1011100) | $1 + X^2 + X^3 + X^4 = (1 + X)\mathbf{g}(X)$ |
| (0010) | (1110010) | $1 + X + X^2 + X^5 = (1 + X^2)\mathbf{g}(X)$ |
| (1010) | (0011010) | $X^2 + X^3 + X^5 = X^2\mathbf{g}(X)$ |
| (0110) | (1000110) | $1 + X^4 + X^5 = (1 + X + X^2)\mathbf{g}(X)$ |
| (1110) | (0101110) | $X + X^3 + X^4 + X^5 = (X + X^2)\mathbf{g}(X)$ |
| (0001) | (1010001) | $1 + X^2 + X^6 = (1 + X + X^3)\mathbf{g}(X)$ |
| (1001) | (0111001) | $X + X^2 + X^3 + X^6 = (X + X^3)\mathbf{g}(X)$ |
| (0101) | (1100101) | $1 + X + X^4 + X^6 = (1 + X^3)\mathbf{g}(X)$ |
| (1101) | (0001101) | $X^3 + X^4 + X^6 = X^3\mathbf{g}(X)$ |
| (0011) | (0100011) | $X + X^5 + X^6 = (X + X^2 + X^3)\mathbf{g}(X)$ |
| (1011) | (1001011) | $1 + X^3 + X^5 + X^6 = (1 + X + X^2 + X^3)\mathbf{g}(X)$ |
| (0111) | (0010111) | $X^2 + X^4 + X^5 + X^6 = (X^2 + X^3)\mathbf{g}(X)$ |
| (1111) | (1111111) | $1 + X + X^2 + X^3 + X^4 + X^5 + X^6 = (1 + X^2 + X^5)\mathbf{g}(X)$ |

**Theorem 5:** the generator polynomial of an $(n, k)$ code is a factor of $X^n + 1$.

**Proof:** divide $X^k g(X)$ by $X^n + 1$.

$$X^k g(X) = (X^n + 1) + g^{(k)}(X) \quad \text{or} \quad X^n + 1 = X^k g(X) + g^{(k)}(X)$$

$g^{(k)}(X)$ is a code polynomial. So, $g^{(k)}(X) = a(X)b(X)$ for some $a(X)$. So,

$$X^n + 1 = [X^k + a(X)]g(X). \qquad QED$$

**Theorem 6:** if $g(X)$ is a polynomial of degree $n-k$ and is a factor of $X^n+1$. Then $g(X)$ generates an $(n,k)$ cyclic code.

**Proof:** let $g(X), Xg(X), \cdots, X^{k-1}g(X)$. They are all polynomials of degree $n-1$ or less. A linear combination of them:

$$v(X) = u_0 g(X) + u_1 X g(X) + \cdots + u_{k-1} X^{k-1} g(X)$$
$$= [u_0 + u_1 X + \cdots + u_{k-1} X^{k-1}] g(X)$$

is a code polynomial since $u_i \in \{0,1\}$. Then $v(X)$ will have $2^k$ possibilities. These $2^k$ polynomials form the $2^k$ codewords of the $(n,k)$ code.

**Generator polynomial of a cyclic code:**

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

For example, for $(7,4)$ code with $g(X) = 1 + X + X^3$, $g_0 = g_1 = g_3 = 1$ and $g_i = 0$ otherwise.

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

This is not always in systematic form. We can make it into systematic form by row and column operations. For example, for the $(7,4)$ code:

$$G' = \begin{bmatrix} \underline{g}_0 \\ \underline{g}_1 \\ \underline{g}_0 + \underline{g}_2 \\ \underline{g}_0 + \underline{g}_1 + \underline{g}_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

**Parity check matrix of cyclic codes:**

We saw that $g(X)$ divides $X^n + 1$. Write

$$X^n + 1 = g(X)h(X),$$

where $h(X)$ is a polynomial of degree $k$

$$h(X) = h_0 + h_1 X + \cdots + h_k X^k.$$

Consider a code polynomial $v(X)$

$$
\begin{aligned}
v(X)h(X) &= u(X)g(X)h(X) \\
&= u(X)(X^n + 1) \\
&= u(X)X^n + u(X).
\end{aligned}
$$

Since $u(X)$ has degree less than or equal $k-1$, so $u(X)X^n + u(X)$ does not have $X^k, X^{k+1}, \cdots, X^{n-1}$. That is coefficients of these powers of $X$ are zero. So, we get $n-k$ equalities:

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

So, we have $H$ as:

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

**Theorem 7:** let $g(X)$ be the generator polynomial of the $(n,k)$ cyclic code $C$. The dual code of $C$ is generated by $X^k h(X^{-1})$ where $h(X) = \frac{X^n+1}{g(X)}$.

**Example:** consider $(7,4)$ code $C$ with $g(X) = 1 + X + X^3$. The generator polynomial of $C^t$ is $X^4 h(X^{-1})$ where

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

That is, the generator of $C^t$ is:

$$
\begin{aligned}
X^4 h(X^{-1}) &= X^4(1 + X^{-1} + X^{-2} + X^{-4}) \\
&= 1 + X^2 + X^3 + X^4.
\end{aligned}
$$

So, $C^t$ is a $(7,3)$ code with $d_{min} = 4$. Therefore, it can correct any single error and detect any combination of double errors.

**Encoding of cyclic codes:**

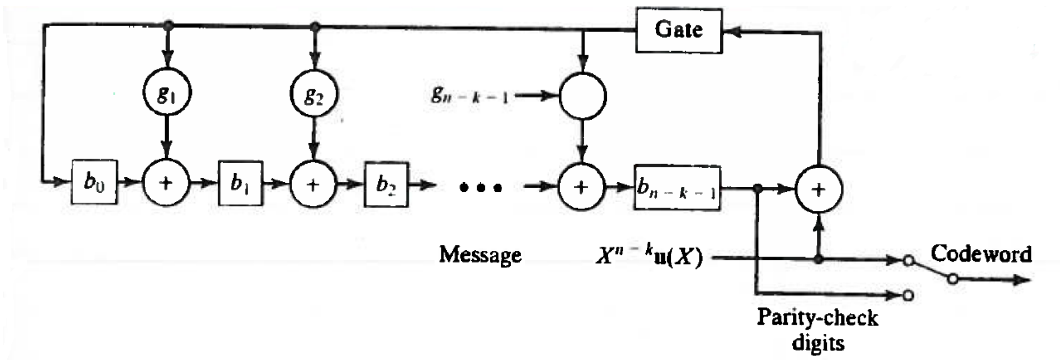
We saw that if we multiply the information polynomial by $X^{n-k}$ and divide by $g(X)$, we get:

$$
X^{n-1}u(X) = a(X)g(X) + b(X)
$$

and

$$
a(X)g(X) = b(X) + X^{n-1}u(X)
$$

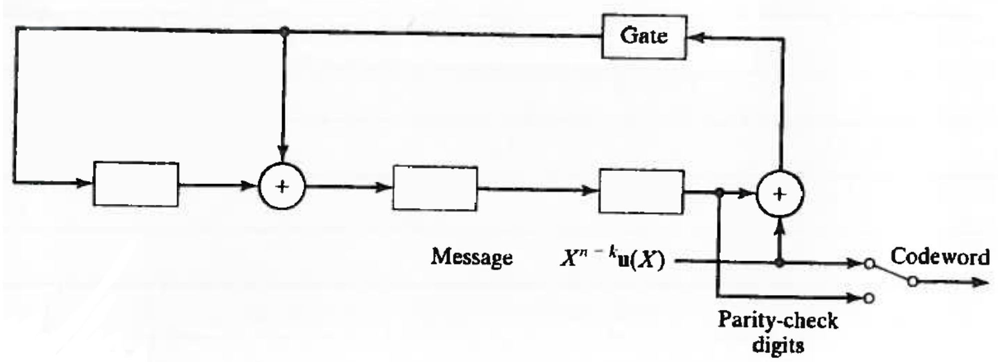
is a codeword in systematic form. The following circuit encodes $u(X)$ based on the above discussion.




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

1) Close the gate and enter information bits in and also send them over channel. This does multiplication by $X^{n-k}$ as well as parity bit generation.
2) Open the gate (break the feedback).
3) Output the $n - k$ parity bits.

**Example:** $(7, 4)$ code with $g(X) = 1 + X + X^3$.




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

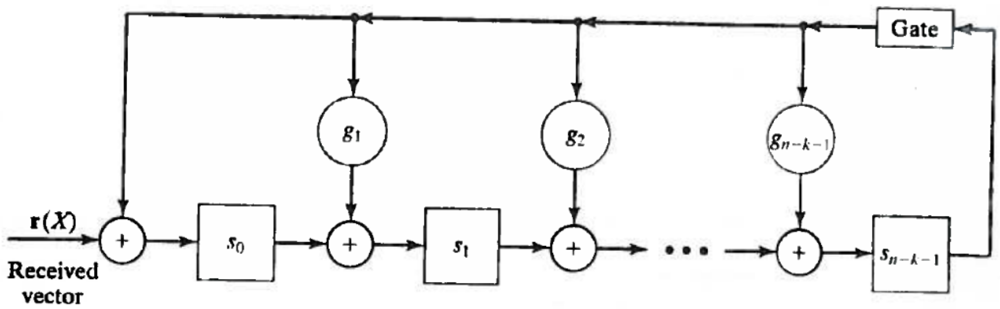
**Syndrome:**

Assume $r(X) = r_0 + r_1X + r_2X^2 + \cdots + r_{n-1}X^{n-1}$ is the polynomial representing received bits. Divide $r(X)$ by $g(X)$ to get:

$$r(X) = a(X)g(X) + s(X).$$

$s(X)$ is a polynomial of degree $n - k - 1$ or less. The $n - k$ coefficients of $s(X)$ are the syndromes.

**Theorem 8:** let $s(X)$ be the syndrome of $r(X) = r_0 + r_1X + \cdots + r_{n-1}X^{n-1}$. Then, $s^{(i)}(X)$ resulting from dividing $X^i s(X)$ by $g(X)$ is the syndrome of $r^{(i)}(X)$.




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

Example of $(7, 4)$ code:

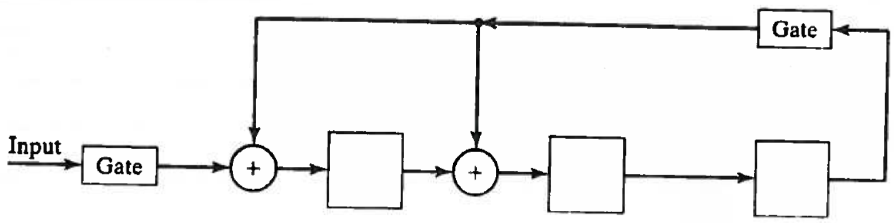
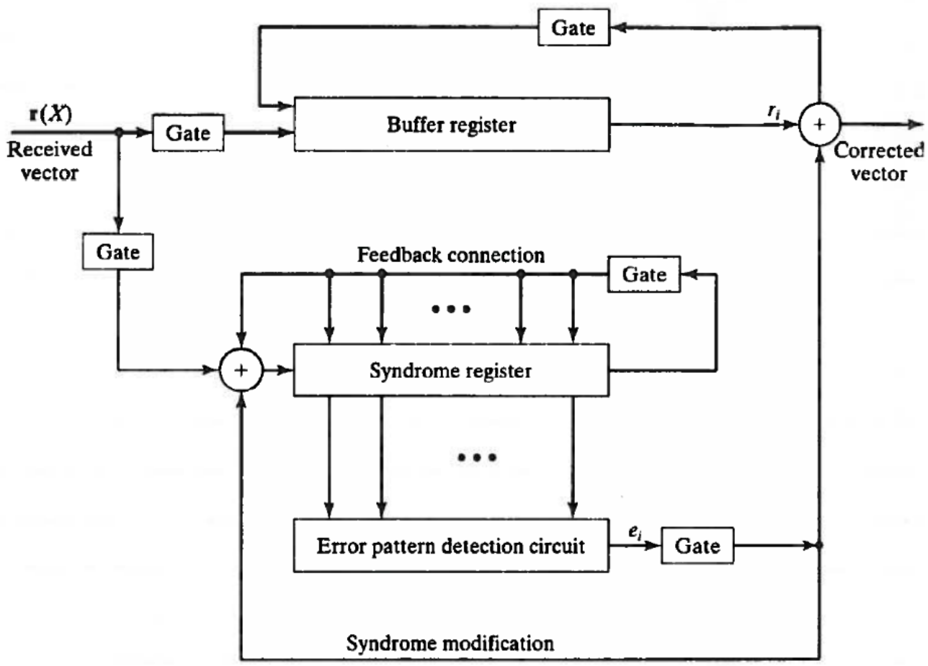



FIGURE 5.6: Syndrome circuit for the (7, 4) cyclic code generated by $\mathbf{g}(X) = 1 + X + X^3$.

TABLE 5.3: Contents of the syndrome register shown in Figure 5.6 with $\mathbf{r} =$ (0010110) as input.

| Shift | Input | Register contents |
|---|---|---|
| | | 000 (initial state) |
| 1 | 0 | 000 |
| 2 | 1 | 100 |
| 3 | 1 | 110 |
| 4 | 0 | 011 |
| 5 | 1 | 011 |
| 6 | 0 | 111 |
| 7 | 0 | 101 (syndrome $\mathbf{s}$) |
| 8 | — | 100 (syndrome $\mathbf{s}^{(1)}$) |
| 9 | — | 010 (syndrome $\mathbf{s}^{(2)}$) |

**Decoding:**

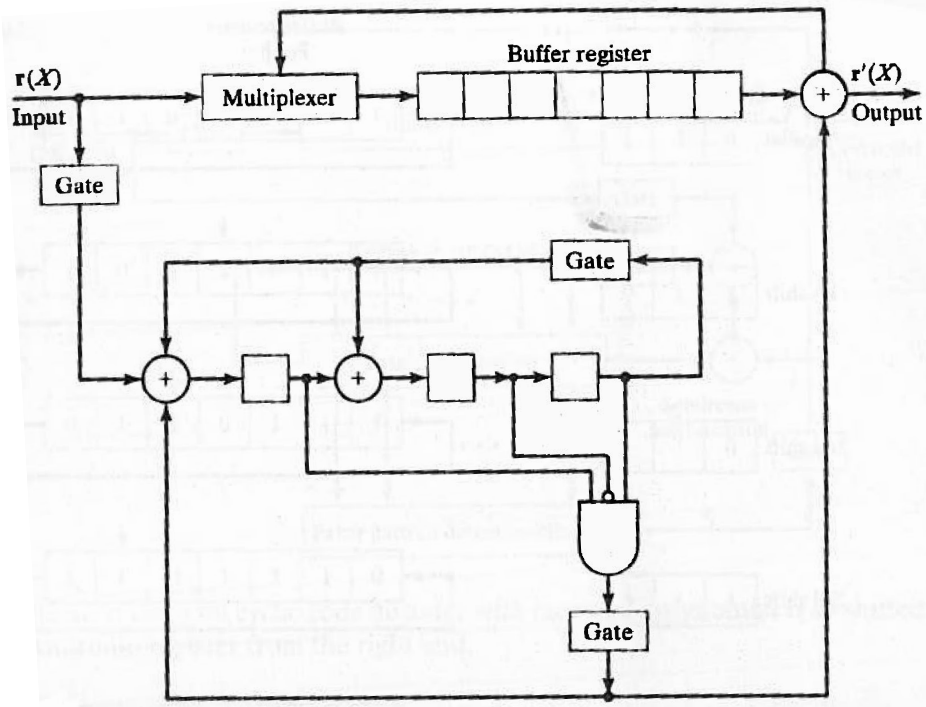



General cyclic code decoder with received polynomial $\mathbf{r}(X)$ shifted into the syndrome register from the left end.

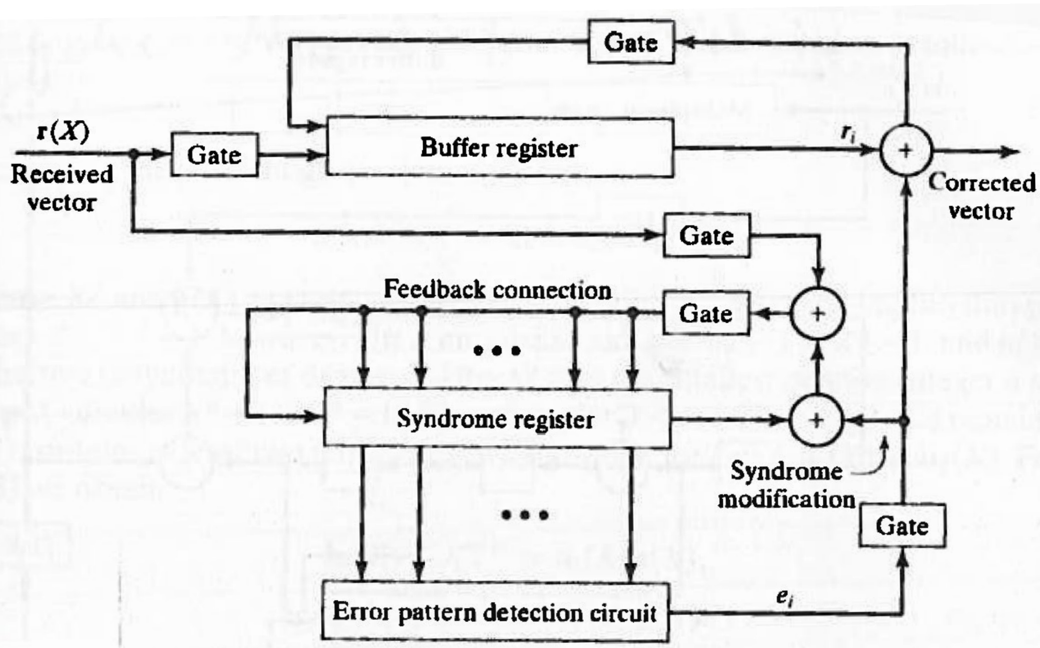
Example of (7, 4) code:

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** $(s_0, s_1, s_2)$ |
|---|---|---|
| $\mathbf{e}_6(X) = X^6$ | $\mathbf{s}(X) = 1 + X^2$ | (101) |
| $\mathbf{e}_5(X) = X^5$ | $\mathbf{s}(X) = 1 + X + X^2$ | (111) |
| $\mathbf{e}_4(X) = X^4$ | $\mathbf{s}(X) = X + X^2$ | (011) |
| $\mathbf{e}_3(X) = X^3$ | $\mathbf{s}(X) = 1 + X$ | (110) |
| $\mathbf{e}_2(X) = X^2$ | $\mathbf{s}(X) = X^2$ | (001) |
| $\mathbf{e}_1(X) = X^1$ | $\mathbf{s}(X) = X$ | (010) |
| $\mathbf{e}_0(X) = X^0$ | $\mathbf{s}(X) = 1$ | (100) |




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



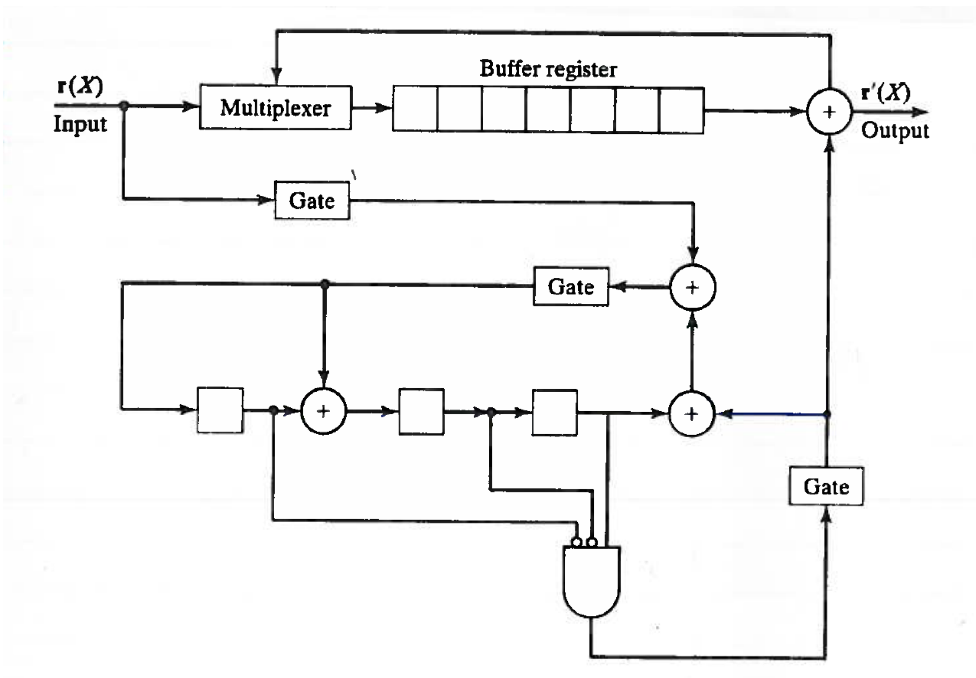

General cyclic code decoder with received polynomial $r(X)$ shifted into the syndrome register from the right end.

Another implementation of syndrome calculator

Syndrome decoding of $(7,4)$ code using syndrome decoder fed from right:

Error patterns and their syndromes with the received polynomial $\mathbf{r}(X)$ shifted into the syndrome register from the right end.

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




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

**Cyclic Hamming codes:**

A Hamming code of length $n = 2^m - 1$ with $m \geq 3$ is generated by a primitive polynomial of degree $m$. let's see how we can put the Hamming code with defined in last lecture in cyclic form:

Divide $X^{m+i}$ by $p(X)$ to get $X^{m+i} = a_i(X)p(X) + b_i(X)$.

1) Since $p(X)$ is primitive, $X$ is not a factor of $p(X)$ so $p(X)$ does not divide $X^{m+i} \Rightarrow b_i(X) \neq 0$.

2) $b_i(X)$ has at least <u>two terms</u>. If it had one term:

$$X^{m+i} = a_i(X)p(X) + X^j$$
$$\Rightarrow X^j\left(X^{m+i-j} + 1\right) = a_i(X)p(X)$$
$$\Rightarrow p(X) \text{ divides } X^{m+i-j} + 1 \text{ but } m + i - j < 2^m - 1$$
$$\Rightarrow \text{contradiction.}$$

3) If $i \neq j$, then $b_i(X) \neq b_j(X)$. Let

$$X^{m+i} = b_i(X) + a_i(X)p(X)$$
$$X^{m+j} = b_j(X) + a_j(X)p(X).$$

If $b_i(X) = b_j(X)$, then

$$X^{m+i}\left(X^{j-i} + 1\right) = \left[a_i(X) + a_j(X)\right]p(X),$$

i.e., $p(X)$ divides $X^{j-i} + 1 \Rightarrow$ contradiction.

Let $H = [I_m : Q]$ be the parity check matrix of this code. $I_m$ is an $m \times m$ identity matrix with $Q$ an $m \times (2^m - m - 1)$ matrix with $\underline{b_i} = (b_{i0}, b_{i1}, \cdots, b_{i,m-1})$ as its columns. Since no two columns of $Q$ are the same and each have at least two 1's, then $H$ is indeed a parity-check matrix of a Hamming code.

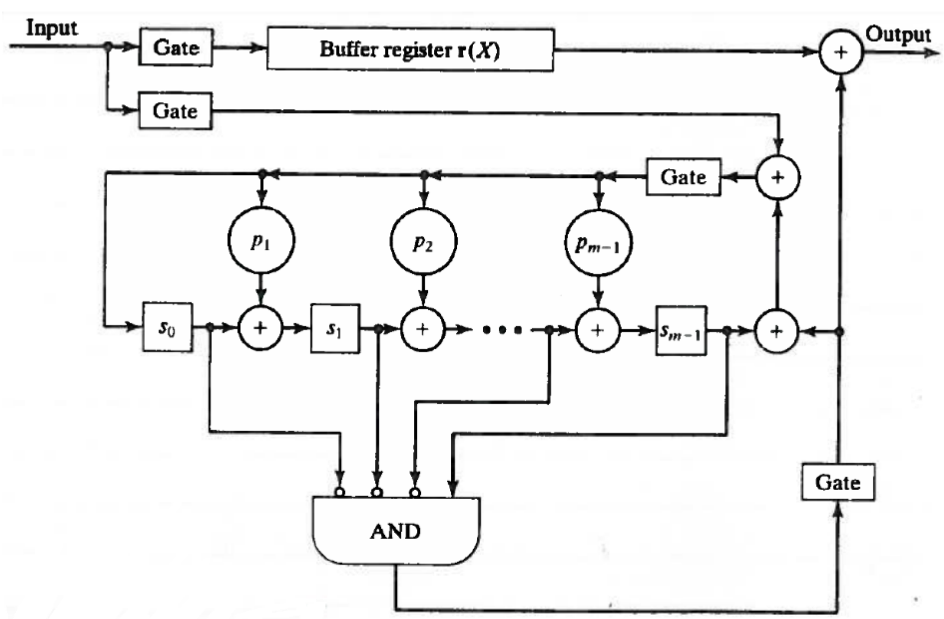
**Syndrome decoding of Hamming codes:**

Assume that error is in location with highest order, i.e.,

$$e(X) = X^{2^m - 2}.$$

Then, feeding $r(X)$ from right to syndrome calculator is equivalent to dividing $X^m \cdot X^{2^m-2}$ by the generator polynomial $p(X)$. Since $p(X)$ divides $X^{2^m-1} + 1$ then

$$s(X) = X^{m-1} \text{ or } \underline{s} = (0, 0, \cdots, 0, 1).$$




Decoder for a cyclic Hamming code.