# Cyclic Codes

Definition:A linear code is called a cyclic code if every cyclic shift of a codeword is also a codeword. Thus, if , a=[$a_{n-1}$, $a_{n-2}$,……$a_0$] is the codeword of the cyclic code of length n, then the cyclic shift of this codeword =[$a_{n-2}$, $a_{n-3}$,……$a_0$, $a_{n-1}$] is the codeword of the same code. Shifting all bits to the left one position yield another codeword as [$a_{n-3}$, $a_{n-4}$,……$a_0$, $a_{n-1}$, $a_{n-2}$].

## Generation of Cyclic codes:

a. **Non-Systematic cyclic codes:** the output code word is generated using polynomial multiplication.

**Procedure:**

1. For [D]=[$a_1$, $a_2$, …… $a_k$] data word, write the data word in terms of a power of a dummy variable and with $a_1$ weighted as MSB (Most Significant Bit) and $a_k$ as LSB (Least Significant Bit).

   i.e. $D(X)=a_k+ a_{k-1}X+ a_{k-2}X^2+……….+a_1X^{k-1}$

   where (+) is mod-2 addition EX-OR

   for example if [D]=[11101] then
   $D(X)= 1+X^2+X^3+X^4$

   If $D(X)= 1+X^2+X^6$ then
   [D]=[1000101]

2. Multiplication: Multiply D(X) by what is called generator polynomial g(X) of order r.
   This g(X) is one of the factors of $X^n+1$.

   For example, if n=7, then $X^7+1=(X+1)(X^3+ X^2+1)(X^3+ X^2+1)$

   For n=7, r=3, we can choose either $g(X)= X^3+ X^2+1$ or $X^3+ X+1$.

3. The output code words will be C(X)=D(X)g(X) then C(X) is used to find the output code word [C].

***Ex: Write down the code table for the (7,4) non systematic cyclic code with generator polynomial g(X)= $X^3$+ X+1.***

**Sol:**

K=4, r=3 then D=[ $a_1$ $a_2$ $a_3$ $a_4$ ] so the code table will be:

| $a_1$ | $a_2$ | $a_3$ | $a_4$ | $c_1$ | $c_2$ | $c_3$ | $c_4$ | $c_5$ | $c_6$ | $c_7$ | $w_i$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | --- |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 3 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 3 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 4 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 3 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 4 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 4 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 3 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 3 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 4 |
| 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 4 |
| 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 3 |
| 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 4 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 7 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 3 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 4 |

[D]=[0 0 0 1] then D(X)=1
C(X)=D(X)g(X)=1.( $X^3$+ X+1)= $X^3$+ X+1 [C]=[0001011]

[D]=[0 0 1 0] then D(X)=X
C(X)= X.( $X^3$+ X+1)= $X^4$+ $X^2$+X [C]=[0010110]

[D]=[0 0 1 1] then D(X)=X+1
C(X)=(X+1).( $X^3$+ X+1)=
$X^3$+ X+1+ $X^4$+ $X^2$+X = $X^4$+ $X^3$+ $X^2$+1 [C]=[0011101]

And so on with the rest of the codes.

b. **Systematic cyclic codes:**
The polynomial representation may be used with the same generator polynomial g(X) used in **non-Systematic** codes.

**Procedure:**

1. Find D(X) from [D]
2. Select g(X) of order r from factorization of $X^n+1$
3. $C(X) = X^r.D(X) + (\mathrm{Re}\,m\frac{X^r D(X)}{g(X)})$ where **Rem** is the reminder of long division
4. Use C(X) to find [C].

Note that C(X) consists of two parts, the first is $X^r.D(X)$ which is the same information data shifted to left by r position, the second is the reminder $\mathrm{Re}\,m\frac{X^r D(X)}{g(X)}$ of order (r-1) which is the r LSBs of the output code word or parity bits, hence [C] will have the form:

$$[C]=[\ a_1, a_2, \ldots\ldots a_k\ c_1, c_2, \ldots .c_r]$$

***Ex: find the code table for (7,4) systematic cyclic code generated by g(X)= $X^3$+ $X^2$+1***

**Sol:**

| $a_1$ | $a_2$ | $a_3$ | $a_4$ | $c_1$ | $c_2$ | $c_3$ | $w_i$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | --- |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 3 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 4 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 3 |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 3 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 4 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 3 |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | 4 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 3 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 4 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 3 |
| 1 | 0 | 1 | 1 | 1 | 0 | 0 | 4 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 4 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 3 |
| 1 | 1 | 1 | 0 | 0 | 1 | 0 | 4 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 7 |

Here n=7, k=4, r=3

For [D]=[0001] , D(X)=1

$X^r.D(X) = X^3.1 = X^3$

$$\begin{array}{r} 1 \\ X^3+X^2+1\overline{\smash{)}X^3\phantom{+X^2+1}} \\ \underline{X^3+X^2+1} \\ X^2+1 \end{array}$$

$C(X)=X^rD(X)+\text{Reminder}$
$=X^3+X^2+1$ [C]=[0001 101]

- ❖ Note that the reminder gives directly the r-parity bits if written in binary form.

For [D]=[0010] , D(X)=X

$X^r.D(X) = X^3.X = X^4$

$$\begin{array}{r} X+1 \\ X^3+X^2+1\overline{\smash{)}X^4\phantom{+X^3+X}} \\ \underline{X^4+X^3+X} \\ X^3+X \\ \underline{X^3+X^2+1} \\ X^2+X+1 \end{array}$$

$C(X)= X^4+X^2+X+1$ [C]=[0010 111]

For [D]=[0011] , D(X)=X+1

$X^r.D(X) = X^3.(X+1) = X^4+X^3$

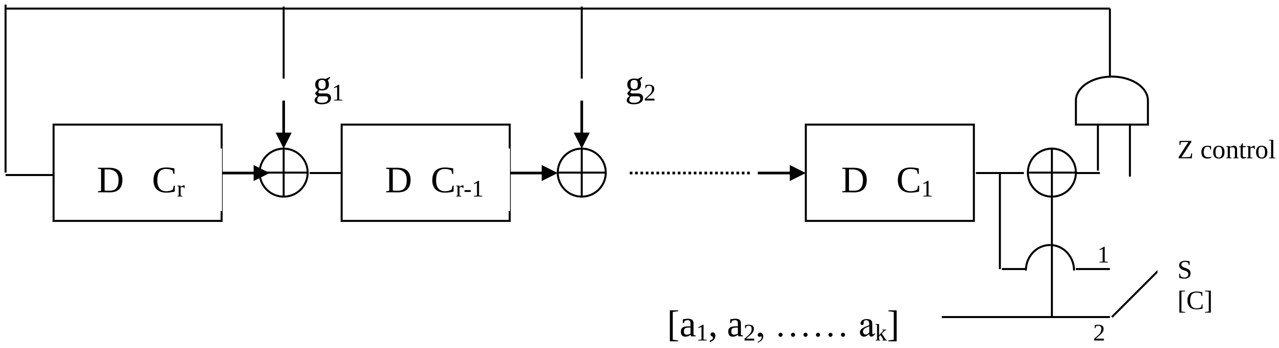
$$\begin{array}{r} X+1 \\ X^3+X^2+1\overline{\smash{)}X^4+X^3\phantom{+X}} \\ \underline{X^4+X^3+X} \\ X \end{array}$$

$C(X)= X^4+X^3+X$ [C]=[0011 010]

And so on with the rest of the codes

## Implementation of Cyclic Encoder:

Practically, the long division required in encoding is done using logic circuit. That implements the division by g(X) polynomial. In general :
$g(X)=g_0+ g_1X+ g_2X^2+\ldots\ldots\ldots.+g_rX^r$, then $g_0=g_r=1$ always for any factorization of $X^n+1$. Hence only $g_1$, $g_2\ldots..,g_{r-1}$ is shown in the implementation circuit:



- ❖ This logic circuit is called Modular.
- ❖ Feedback shift register implemented using D-flip flop with synchronized clock.

**Circuit Operation :-**

Switch S is at position 1 giving the data bit to [C] output and at the same time for k clock pulses, the control Z is enabled "Z=1" to feedback the content to the registers to produce $c_1$, $c_2$, ….. $c_r$ bits at the end of last clock.

Switch S is at position 2, the Z disabled to get these r parity bits to [C] and at the same time r 0's will be fed back to the register to initialize the register to the next data block.

**NOTE**

Previous encoding procedure for systematic cyclic code can be done faster without polynomial representation if instead of g(X) is converted into binary form called the "divisor" of the cyclic code.

***Ex:***

***Using g(X)=$X^3$+$X^2$+1, find the output codeword for [D]=[0011] and [D]=[0010]***

**Sol:**

1. Convert from polynomial into binary form
   g(X) =$X^3$+$X^2$+1        [G]=[1101]
2. Add r 0's as LSB to data=[$a_1$, $a_2$, ….  $a_k$] to get [$a_1$, $a_2$, …. $a_k$ 0 0 0 ]
   for [D]=[0011] we will have [0011000]
3. Divide it by [G]

```
           1
1101)0011000
       001101
       000001    0

          r-parity
```

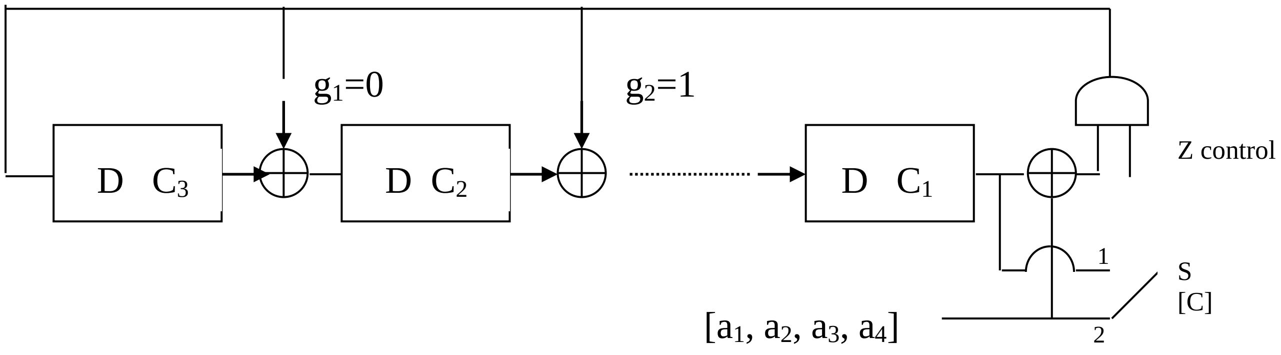
Then [C]=[0011010]

For [D]=[0010]

The out put should be [C]=[0010111].. how??

***Ex:***

***Using the encoder logic circuit to find the o/p codeword for systematic cyclic code with g(x)= $X^3$+$X^2$+1     and for [D]=[0101], [0010]***



**Sol:**

First we write the transition equations for $c_1$, $c_2$, $c_3$ (we write the next state of them in terms of the present state and the input, this is done when Z=1 then:

$c_3^{n+1}=c_1^n+a_i$
$c_2^{n+1}=c_3^n$
$c_1^{n+1}=c_2^n+ c_1^n +a_i= c_2^n+ c_3^{n+1}$

For [D]=[0101]

| $a_i$ |
|---|
| 0 |
| 1 |
| 0 |
| 1 |

| $c_3$ | $c_2$ | $c_1$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 0 | 0 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |
| 0 | 0 | 0 |
| 0 | 0 | 0 |

Then $c_1\ c_2\ c_3$ =110 and [C]=[0101110]

For [D]=[0010]

| $a_i$ |
|---|
| 0 |
| 0 |
| 1 |
| 0 |

| $c_3$ | $c_2$ | $c_1$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 0 | 0 |
| 0 | 0 | 0 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |
| 0 | 0 | 0 |

Then $c_1\ c_2\ c_3$ =111 and [C]=[0010111]

# Decoding of Systematic Cyclic Code:-

At the receiver
[R]=[C]+[E] where [E] is the error word
Or
R(X)=C(X)+E(X) , E(X) is the error polynomial

Now if we divide above equation by g(X) taking the reminder :-

$$\mathrm{Re}\,m\left[\frac{R(X)}{g(X)}\right]=\mathrm{Re}\,m\left[\frac{C(X)}{g(X)}\right]+\mathrm{Re}\,m\left[\frac{E(X)}{g(X)}\right]$$

And since $\mathrm{Re}\,m\left[\frac{C(X)}{g(X)}\right]=0$ as shown before, then :-

$\mathrm{Re}\,m\left[\frac{R(X)}{g(X)}\right]=\mathrm{Re}\,m\left[\frac{E(X)}{g(X)}\right]=S(X)$ =syndrome polynomial of order (r-1).

1. If S(X) = 0 then no error occurs.
2. If S(X) # 0 then error occurs

To find the locations of these errors, the receiver may prepare a syndrome table, store it in its memory, use it to find [E] from [S] starting with less number of errors.

***Ex: Prepare the syndrome table for (7,4) systematic cyclic code with g(X)=$X^3$+$X^2$+1 and for single error. Check the syndrome when double error at first and last positions occur.***

**Sol:-**

| Error Word [E] | | | | | | | $S_1$ | $S_2$ | $S_3$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |

Each [S] is found from [E] by long division by g(X). for example if [E]=[0100000] error at second position from the left then:-

```
          _____________
1 1 0 1 | 0 1 0 0 0 0 0
            1 1 0 1
          -------------
            0 1 0 1 0
              1 1 0 1
          -------------
              0 1 1 1 0
                1 1 0 1
          -------------
                0 0 1 1
                    ---
                    [S]
```

- Note that no repeated [S] for all possible single error. This is expected since $w_{i(min)}$=3 and the given (7,4) code is a single error correction. Note also for double error [E]=[0000011], then [S]=[011] which is single error at the second position (from the left), there by these errors cannot be corrected.

Now going back to the example for double error [E]=[1000001]

```
          _____________
1 1 0 1 | 1 0 0 0 0 0 1
          1 1 0 1
          -------------
          0 1 0 1 0
            1 1 0 1
          -------------
            0 1 1 1 0
              1 1 0 1
          -------------
              0 0 1 1 1
                    ---
                    [S]
```

[S]=[111] which is the same [S] as if single error occurs at third position from the left.

***Ex: using previous syndrome table, find the corrected word for the received word [R]=[1010011].***

**Sol:-**

First, the receiver will find [S] from the reminder of R(X)/g(X)

$$\begin{array}{cccc|ccccccc}
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ \cline{1-4}
 & & & & 1 & 1 & 0 & 1 & & & \\ \cline{5-11}
 & & & & 0 & 1 & 1 & 1 & 0 & & \\
 & & & & & 1 & 1 & 0 & 1 & & \\ \cline{6-11}
 & & & & & 0 & 0 & 1 & 1 & 1 & 1 \\
 & & & & & & & 1 & 1 & 0 & 1 \\ \cline{6-11}
 & & & & & & 0 & 0 & 0 & 1 & 0 \\ \cline{9-11}
 & & & & & & & & & [S] &
\end{array}$$

Hence, [S]=[010], using syndrome table and for this syndrome, [E]=[0000010]

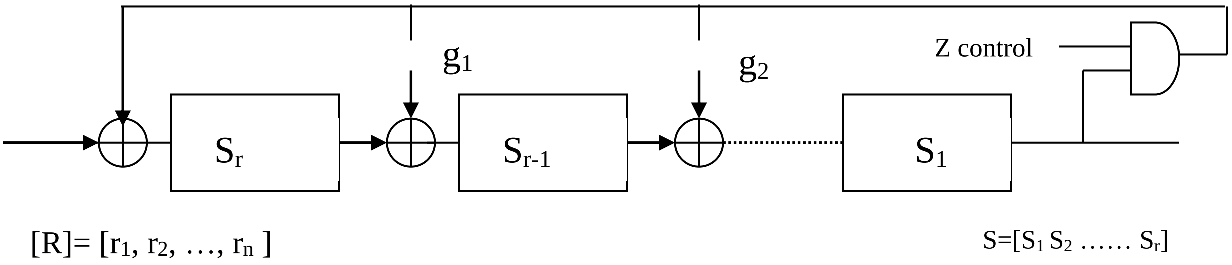
Then the corrected codeword

[C]=[R]+[E]

$$\begin{array}{rr}
 & 1010011 \\
 & \underline{0000010} \\
[C] = & 1010001
\end{array}$$

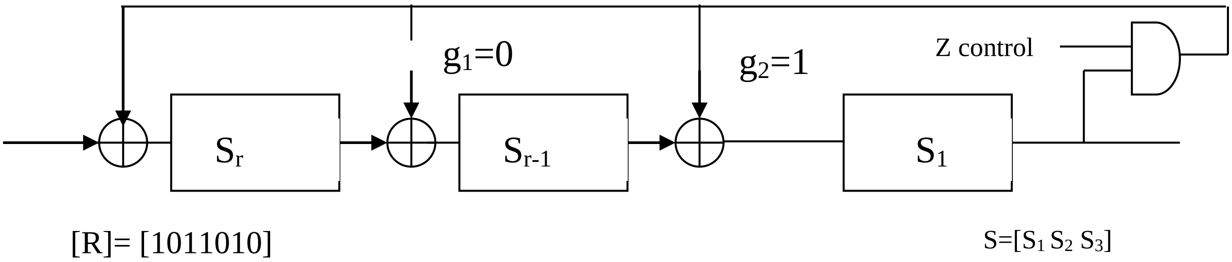
**Implementation of Cyclic Decoder:**

The long division of [R] by [G] to obtain the reminder is implemented is using logic circuit as shown for the generator g(X). The control Z is enabled for "n" clock pulses and then disabled for "r" clock pulses.



***Ex: use the decoder circuit to find the syndrome and the corrected word for the received word [R]=[1011010] , if g(X)=*** $X^3+X^2+1$

**Sol:-**



First we write the transition equations for $S_1\, S_2\, S_3$ when Z=1 :-

$S_3^{n+1}=S_1^n+r_i$
$S_2^{n+1}=S_3^n$
$S_1^{n+1}=S_2^n+ S_1^n$

| $r_i$ |
|---|
| --- |
| 1 |
| 0 |
| 1 |
| 1 |
| 0 |
| 1 |
| 0 |

| $S_3$ | $S_2$ | $S_1$ |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 0 |
| 1 | 1 | 0 |
| 0 | 1 | 1 |

Then [S]=[110], using the syndrome table then [E]=[1000000].
The corrected code word

$$\begin{array}{r} 1011010 \\ \underline{1000000} \\ [C] \; = \; 0011010 \end{array}$$