MODULE 4:

A Few Important Classes of Algebraic Codes:

Syllabus:

Cyclic codes. Polynomial and matrix description. Interrelation b/w polynomial and matrix view point. Systematic encoding. Decoding of cyclic codes.

Hamming codes, BCH codes, Reed-Solomon codes.

CYCLIC CODES

– In coding theory, a cyclic code is a block code, where the circular shifts of each codeword gives another word that belongs to the code.

– A code C is said is to be cyclic if:

(i) C is a linear code and

(ii) any cyclic shift of a codeword is also a codeword. i.e if the codeword $a_0 a_1 \ldots\ldots a_{n-1}$ is in C then $a_{n-1} a_0 \ldots a_{n-2}$ is also in C

eg) The binary code $C_1 = \{0000, 0101, 1010, 1111\}$ is a cyclic code.

However $C_2 = \{0000, 0110, 1001, 1111\}$ is not a cyclic code, but is equivalent to the first code. Interchanging the third and fourth components of C_2 yeild C_1.

The codeword $C_3 = \{00000, 01101, 11010, 10111\}$ is also not cyclic. The second codeword when cyclic-shifted to the left gives the third codeword. However, another left shift does not yield a valid codeword.

POLYNOMIALS:

– A polynomial is a mathematical expression:

$$f(x) = f_0 + f_1 x + \ldots f_m x^m$$

where the symbol x is called the indeterminate and the coefficients $f_0, f_1, \ldots f_m$ are the elements of $GF(q)$. The coefficient f_m is called leading co-efficient. If $f_m \neq 0$, then m is called the degree of the polynomial, and is denoted by $\deg f(x)$.

- A polynomial is a convinient way to represent a vector. Thus a codeword, c, of length n can be expressed as a polynomial $c(x)$ as following:

$$c = [c_0, c_1, c_2 \cdots c_{n-1}] \leftrightarrow c(x) = c_0 + c_1 x + c_2 x^2 + \dots c_{n-1} x^{n-1}$$

eg) The binary word $[1\ 0\ 0\ 1\ 1] \leftrightarrow$

$$1 + 0x + 0x^2 + 1x^3 + 1x^4$$
$$= \underline{1 + x^3 + x^4}$$

- Polynomials play an important role in the study of cyclic codes. Consider a generator polynomial $g(x)$.

: Let $F(x)$ be the set of polynomials in x with co efficients in $GF(q)$. Different polynomials in $F[x]$ can be added, subtracted and multiplied in the usual manner.

: $F[x]$ is an example of an algebraic structure called a ring. $F[x]$ is not a field because polynomials of degree greater than zero do not have multiplicative inverse.

: It can be seen that if $f(x), g(x) \in F[x]$, then $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$. However, $\deg f(x) + \deg(g(x))$ is not necessarily $\max\{\deg f(x), \deg g(x)\}$

: Now let us denote $F[x]/f(x)$ as the set of polynomials in $F[x]$ of degree less than $\deg f(x)$, with addition and multiplication modulo $f(x)$, as follows:

(a) If $a(x)$ & $b(x)$ belong to $F[x]/f(x)$, then sum $a(x) + b(x)$ in $F[x]/f(x)$ is same as in $F[x]$.

(b) The product $a(x)b(x)$ is the unique polynomial of degree of less than $\deg f(x)$ to which $a(x)b(x)$ is congruent modulo $f(x)$.

: $F[x]/f(x)$ is called the ring of polynomials (over $F[x]$) modulo $f(x)$. A ring satisfies the first seven of 8 axioms that define a field.

PROPERTIES OF CYCLIC PROPERTIES:

1) For a (n, k) cyclic code there exists a generator polynomial of degree $(n-k)$ given by: $g(x) = g_0 + g_1 x + g_2 x^2 + \dots + g_{n-k} x^{n-k}$
The generator polynomial is unique, i.e it is the only code vector polynomial of minimum degree $(n-k)$.

2) The generator polynomial $g(x)$ of a (n, k) cyclic code is a factor of $x^n + 1$: $x^n + 1 = g(x) \cdot h(x)$, where $h(x)$ is another polynomial of degree k called "parity check polynomial.

3) If $g(x)$ is a polynomial of degree (n, k) and is a factor of $x^n + 1$, then it generates (n, k) cyclic code:

a) The coefficient vector polynomial $c[x]$ can be found using: $c[x] = d[x] \cdot g[x]$, where $d[x]$ is message vector polynomial degree $k / D(x)$.

$\therefore d[x] = d_0 + d_1 x + d_2 x^2 + \dots d_{k-1} x^{k-1}$. This method generates non systematic cyclic codes.

b) To generate a systematic cyclic code the remainder polynomial $b(x)$ is got from division of $x^{n-k} \cdot d(x)$ by $g(x)$. The co-efficient of $b(x)$ are placed in the beginning of code vectors followed by co-efficient of message ptolynomial $d(x)$ to get code vector.

$$\boxed{\text{n bit code vector}}$$
$\xleftarrow{k\ \text{co-eff of } b(x)} \ast \xrightarrow{\text{co-eff of } d(x)}$

SYSTEMATIC CYCLIC CODES:

- In systematic form, the first 3 bits are check bits and last 4 bits are message bits.
- Check bits are obtained from remainder polynomial $b(x)$.

$$b(x) = \frac{x^{n-k} \cdot D(x)}{g(x)} + \underbrace{Q(x)}_{\text{quotient term}}$$

Steps for encoding cyclic systematic codes:

Steps involved in encoding procedure for an (n, k) cyclic codes

1) Multiply message polynomial $m(x)$ by x^{n-k}.

2) Divide $x^{n-k}m(x)$ by $g(x)$ obtaining remainder $b(x)$.

3) Add $b(x)$ to $x^{n-k}m(x)$ obtaining code polynomial $c[x]$

eg] Let $D = [0\ 0\ 0\ 1]$

$D(x) = x^3 \quad [0\times x^0 + 0\times x^1 + 0\times x^2 + 1\times x^3]$

$\Rightarrow x^{n-k}D(x) \Rightarrow x^{7-4}\, x^3$

$= \underline{\underline{x^6}}$

$$
\begin{array}{r|l}
 & x^3 + x + 1 \\
\hline
x^3+x+1 & x^6 \\
 & \underline{-x^6 + x^4 + x^3} \\
 & x^4 + x^3 \\
 & \underline{x^4 + x^2 + x} \\
 & x^3 + x^2 + x \\
 & \underline{x^3 + x + 1} \\
 & x^2 + 1 \text{ (remainder).}
\end{array}
$$

$b(x) = x^2 + 1$

$= 1 + 0\times x + 1\times x^2$

$= \underline{\underline{101}}$

A METHOD FOR GENERATING CYCLIC CODES:

The following steps can be used to generate a cyclic code.

(i) Take a polynomial $f(x)$ in R_n.

(ii) Obtain a set of polynomials by multiplying $f(x)$ by all possible polynomials in R_n.

(iii) The set of polynomials obtained above corresponds to the set of codewords belonging to a cyclic code. The block length of the code is n.

- A generator polynomial can be used to construct the cyclic code.

eg) Consider a polynomial $f(x) = 1 + x^2$ in R_3 defined over GF(2). In general a polynomial in $R_3 (= F[x]/(x^3-1))$ can be operated as $r(x) = r_0 + r_1 x + r_2 x^2$ where the coefficients can take the values 0 or 1 (since defined over GF(2)).

Thus there can be a total of $2 \times 2 \times 2 = 8$ polynomials in R_3 defined over $GF(2)$, which are $0, 1, x, x^2, 1+x^2, x+x^2, 1+x+x^2$.

To generate the cyclic code, we multiply $f(x)$ with these 8 possible elements of R_3, and then reduce the results modulo (x^3-1).

$(1+x^2)\cdot 0 = 0$, $\quad (1+x^2)(1+x) = x+x^2$,

$(1+x^2)\cdot 1 = 1+x^2$, $\quad (1+x^2)(1+x^2) = 1+x$

$(1+x^2)\cdot x = 1+x$, $\quad (1+x^2)(x+x^2) = 1+x^2$

$(1+x^2)x^2 = x+x^2$, $\quad (1+x^2)(1+x+x^2) = 0$.

Thus there are only four distinct codewords: $\{0, 1+x, 1+x^2, x+x^2\}$ which corresponds to $\{000, 011, 101, 110\}$.

Let C be a (n,k) non-zero cyclic code in R_n, then:

(i) There exists a unique monic polynomial $g(x)$ of the smallest degree in C.

(ii) The cyclic code C consists of all multiples of the generator polynomial $g(x)$ by polynomials of degree $k-1$ or less.

(iii) $g(x)$ is a factor of x^n-1.

The third point helps to obtain the generator polynomial for a cyclic code. All we have to do is to factorise x^n-1 into irreducible, monic polynomials. We can also find all the possible cyclic codewords of block length n simply by factorising x^n-1.

- A simple encoding rule to generate the codewords from the generator polynomial is:

$$c(x) = i(x)g(x).$$

$i(x)$: Information polynomial. $\quad c(x)$: codeword polynomial.

$g(x)$: Generator polynomial.

- The recieved word at the reciever, after passing through a noisy channel can be expressed as:

$$v(x) = c(x) + e(x). \quad e(x)\text{: error polynomial.}$$

- We define the Syndrome Polynomial $s(x)$ as the remainder of of $v(x)$ under division by $g(x)$

MATRIX DESCRIPTION OF CYCLIC CODES

Suppose C is a cyclic code with generator polynomial $g(x) = g_0 + g_1 x + g_2 x^2 + \dots + g_r x^r$ of degree r, then the generator matrix of C is given by:

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & 0 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ \vdots & \vdots & & & & & & & \vdots \\ 0 & 0 & 0 & 0 & 0 & g_0 & g_1 & \cdots & g_r \end{bmatrix}$$

n columns.

$k = (n-r)$ rows.

i.e the generator matrix is of the order $k \times n$.

– Polynomials $g(x)$, $x\,g(x)$, $x^2 g(x)$ and $x^3 g(x)$ represent code vector polynomial of the same cyclic code.

eg] $g(x) = 1 + x + x^3$, $(n, k) = (7, 4)$

$= 1 \times x^0 + 1 \times x^1 + 0 \times x^2 + 1 \times x^3 + 0 \times x^4 + 0 \times x^5 + 0 \times x^6$

The code corresponding to $g(x) = 1101000$

$x \cdot g(x) = x(1 + x + x^3)$

$= x + x^2 + x^4$

$\therefore$ the code vector corresponding to $x\,g(x) = 0110100$.

$x^2 g(x) = x^2(1 + x + x^3)$

$= x^2 + x^3 + x^5$

$\therefore$ Code vector corresponding to $x^2 g(x)$ is 0011010.

$x^3 g(x) = x^3(1 + x + x^3)$

$= x^3 + x^4 + x^6$

$\therefore$ code vector corresponding to $x^3 g(x)$ is 0001101

Thus writing the generator matrix using the above code vector we get:

$$[G]_{K\times n} = \begin{bmatrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{bmatrix} \quad \begin{matrix} g(x) \\ \vdots \\ \vdots \\ x^{k-1} g(x). \end{matrix}$$

- The generator matrix G is not in systematic form, i.e. it cannot be normalised in $[P_k \,|\, I_k] = [P \,|\, I_4]$ form.
- The last 4 elements of 1^{st} and 2^{nd} row of $[G]$ coincides with first and two rows of I_k, but not the last rows.
- It can be transformed into a systematic form by adding first row to 3^{rd} row and placing the result in third row.

$$[G]_{K\times n} = \left[\begin{array}{ccc|cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right]$$

$R_3 \rightarrow R_1 + R_3$

$R_4 \rightarrow R_1 + R_2 + R_4.$

$$\Rightarrow G = \begin{bmatrix} 110 & 1000 \\ 011 & 0100 \\ 111 & 0010 \\ 101 & 0001 \end{bmatrix} \qquad \text{Now } G = [P \,|\, I_4]$$

Parity Check Matrix:

- The rows of H matrix are:

$$H = x^k h(x^{-1}) \; x^{k+1} h(x^{-1}) \ldots x^{n-1} h(x^{-1}).$$

We know that:

$$x^n + 1 = g(x) \cdot h(x).$$

- For (7, 4) cyclic code, we have $n = 7$.

$$x^7 + 1 = g(x) \cdot h(x).$$

- ∴ parity check polynomial $h(x) = \dfrac{x^7+1}{g(x)}.$

$$g(x) = x^3 + x + 1$$

$$
\begin{array}{r|l}
 & x^4+x^2+x+1 \\
\Rightarrow\ x^3+x+1 & x^7+1 \\
 & x^7+x^5+x^4 \\ \hline
 & x^5+x^4+1 \\
 & x^5+x^3+x^2 \\ \hline
 & x^4+x^3+x^2+1 \\
 & x^4+0+x^2+x \\ \hline
 & x^3+x^2+1 \\
 & x^3+x+1 \\ \hline
 & 0
\end{array}
$$

$\therefore\ h(x) = x^4+x^2+x+1$

- Reciprocal of $h(x)$ is defined as $x^k h(x^{-1})$. This polynomial is also a factor of $(1+x^n)$.
- Let us consider $x^4 h(x^{-1})$ for a (7, 4) cyclic code.

$\Rightarrow$

$$h(x) = 1+x^2+x+x^4$$

$$h(x^{-1}) = 1+\frac{1}{x}+\frac{1}{x^2}+\frac{1}{x^4}$$

$$\Rightarrow x^4 h(x^{-1}) = x^4\left(1+\frac{1}{x}+\frac{1}{x^2}+\frac{1}{x^4}\right) = x^4+x^3+x^2+1.$$

Hence the code is [1 0 1 1 1 0 0]

$$\Rightarrow x^5(h(x^{-1})) = x^5\left(1+\frac{1}{x}+\frac{1}{x^2}+\frac{1}{x^4}\right) = x^5+x^3+x^4+x.$$

Code = [0 1 0 1 1 1 0]

$$\Rightarrow x^6(h(x^{-1})) = x^6\left(1+\frac{1}{x}+\frac{1}{x^2}+\frac{1}{x^4}\right) = x^6+x^5+x^4+x^2$$

Code = [0 0 1 0 1 1 1].

$\because$ H is a $(n-k)\times n$ matrix

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

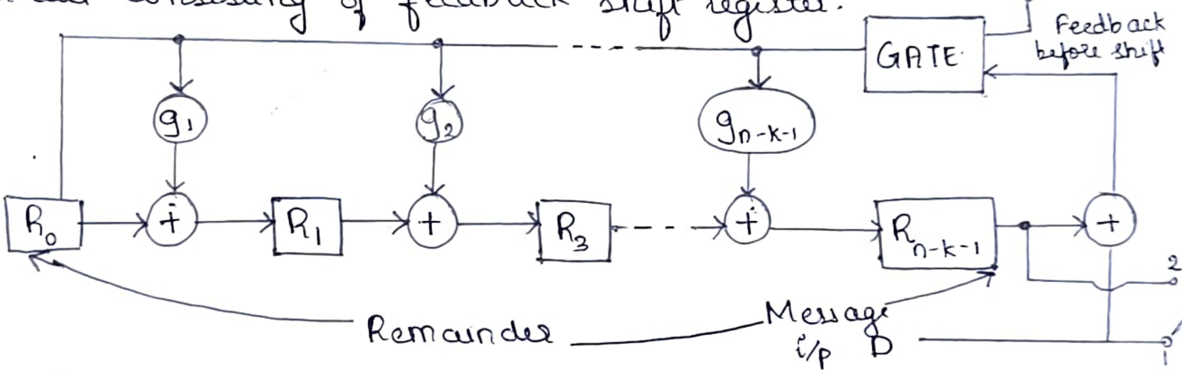
But this is not in the form of $[I_{n-k} \mid P^T]$

$\Rightarrow$ Adding 1st row to 3rd row and the result is placed in first row.

$$\Rightarrow H = \left[\begin{array}{ccc|cccc} 1&0&0&1&0&1&1 \\ 0&1&0&1&1&1&0 \\ 0&0&0&0&1&1&1 \end{array}\right] \qquad H^T = \begin{bmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \\ 1&1&0 \\ 0&1&1 \\ 1&1&1 \\ 1&0&1 \end{bmatrix}$$

ENCODING USING (n-k) BIT SHIFT REGISTER :

- In order to obtain remainder polynomial $b(x)$, we have to perform the division of $x^{n-k} D(x)$ by the generator polynomial $g(x)$.
- This division can be accomplished using dividing circuit consisting of feedback shift register.



Symbols :

- $\boxed{R}$ → Flipflops that make up a shift register.
- $\oplus$ → Modulo - 2 adders.
- (g_i) → A closed path if $g_i = 1$ and open if $g_i = 0$.
- $\boxed{\text{GATE}}$ → AND gate

Operations of an encoder :

- Function :

It is assumed that at the occurance of clock pulse, register i/p are shifted into register and appear at the end of the clock pulses.

i) With the gate turned ON and switch is positional the information digits ($d_0, d_1, d_2 \ldots d_{k-1}$) are shifted into register (with d_{k-1} first) and simultaneously into the channel. As soon as the k information digits have been shifted into the register, register contain parity check bits. (R_0, R_1 ... R_{n-k-1}).

2) With the gate turned OFF and the switch in position 2, the contents of the shift register are shifted into channel. Thus the code vector ($R_0, R_1 \dots R_{n-k-1}, d_0, d_1, \dots d_{k-1}$) is generated and sent over the channel.

Example:

Design an encoder for (7, 4) cyclic code generated by $g(x)$, $g(x) = 1+x+x^3$. Verify its operation using the message vectors: 1001 & 1011.

Ans:

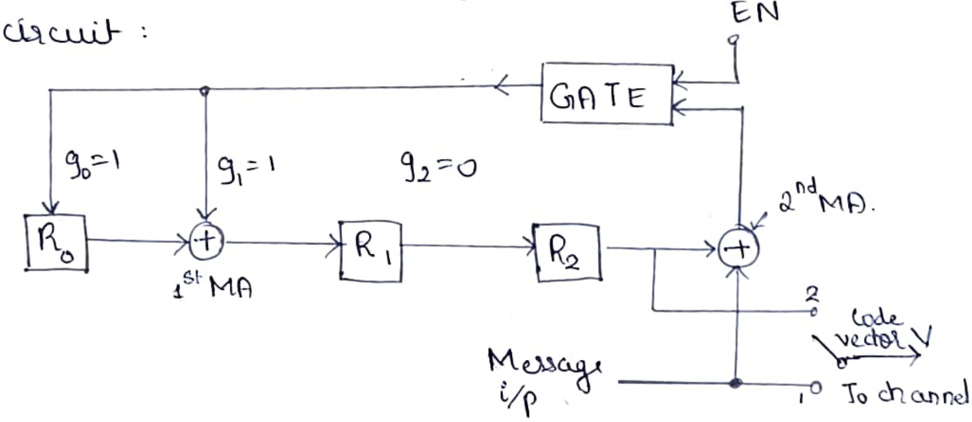
$$g(x) = g_0 + g_1 x + g_2 x^2 + \dots g_{n-k} x^{n-k}.$$
$$= 1 + g_1 x + g_2 x^2 + \dots x^{n-k}$$

$$g_0 = g_{n-k}$$

Given $g(x) = 1+x+x^3$ for (7, 4) cyclic code.
Comparing co-efficients we have

$$g_0 = 1, \quad g_1 = 1, \quad g_2 = 0.$$

Encoder circuit:



Mechanism of operation:

1) Initialisation → clear $R_0\ R_1\ R_2$ i.e $R_0\ R_1\ R_2 = 0\,0\,0$.

2) Input data $d_0\ d_1\ d_2\ d_3 = 1001$. Moving D_3 first to 2^{nd} MA, $R_2 = 0$. o/p of second MA = 1.

3) O/p of gate is moved to $R_0 = 0$ was now shifted to MA 1 & $R_1 = 0 \oplus 1 = 1$. i.e $R_1 = 1$.

Previous value of R_1 is moved to R_2 directly i.e $R_2 = 0$.
So second sequence becomes $R_0 R_1 R_2 = 110$.

4) Next i/p is $d_2 = 0$. Move d_2 to second MA. $\Rightarrow 0 \oplus 0 = 0$.
Gate $= 0 \longrightarrow$ moves to $R_0 = 0$.

$1 \oplus 0 = 1 \Rightarrow R_1 = 1$

$R_2 =$ previous $R_1 = 0$.

Thus the third sequence is 011.

5) Next i/p is 0, gate is $0 \oplus 1 = 1$.

$\Rightarrow R_0 = 1$

$R_1 = 0 \oplus 1 = 1$

$R_2 =$ Prev value of $R_1 = 1$

Hence the fourth sequence is 111.

6) Last i/p is $d_0 = 1$. Modulo adder 2 will have i/p 1, gate is zero $\Rightarrow R_0 = 0$, $R_1 = 1 \oplus 0 = 1$, $R_2 = 1$.

Last sequence is 011.

- When all the data bits are removed into the register final contents of shift register is 011. These are co-efficients of polynomial $R(x)$.

- Now switch S is shifted from 1 to position 2 and gate is turned OFF (EN=0) and contents of shift register are shifted into channel using 3 more shifts. The code vector is then

0111001.

The code vector generated is sent over the channel.

SYNDROME CALCULATION:

- Error detection and correction

- When a transmitted code vector C is passed through a noisy channel, the code vector R is recieved, R may not be the same as that of C.

- R has 2^k code vectors similar to that of C.

Decoder:

Function of a decoder:

- To determine the transmitted code vector C based on the recieved vector R.

- The decoder first tests whether or not the recieved vector R, is a valid code vector by calculating the syndrome of the recieved vector.

- If the syndrome is zero, the recieved vector polynomial is divisible by the generator polynomial and recieved vector is a valid code vector. The decoder accepts this recieved vector R(x) as transmitted code vector.

- A non zero syndrome indicated error present:

- The recieved word be represented by a polynomial of degree (n-1) or less.

$$r(x) = r_0 + r_1 x + r_2 x^2 + r_3 x^3 + \dots r_{n-1} x^{n-1}$$

i.e $$\frac{R(x)}{g(x)} = Q(x) + \frac{S(x)}{g(x)} \quad \text{—— ①}$$

quotient polynomial of the division.

- Syndrome S(x) is a polynomial of degree n-k-1 or less. If e(x) is the error pattern caused by the channel, then

$$R(x) = C(x) + e(x).$$

$$\frac{R(x)}{g(x)} = \frac{C(x)}{g(x)} + \frac{e(x)}{g(x)}$$

We know that $c(x) = D(x) \cdot g(x)$.

$$\frac{R(x)}{g(x)} = D(x) + \frac{e(x)}{g(x)} \quad \text{—— ②}$$

Equating ① & ②.

$$D(x) + \frac{e(x)}{g(x)} = Q(x) + \frac{S(x)}{g(x)}.$$

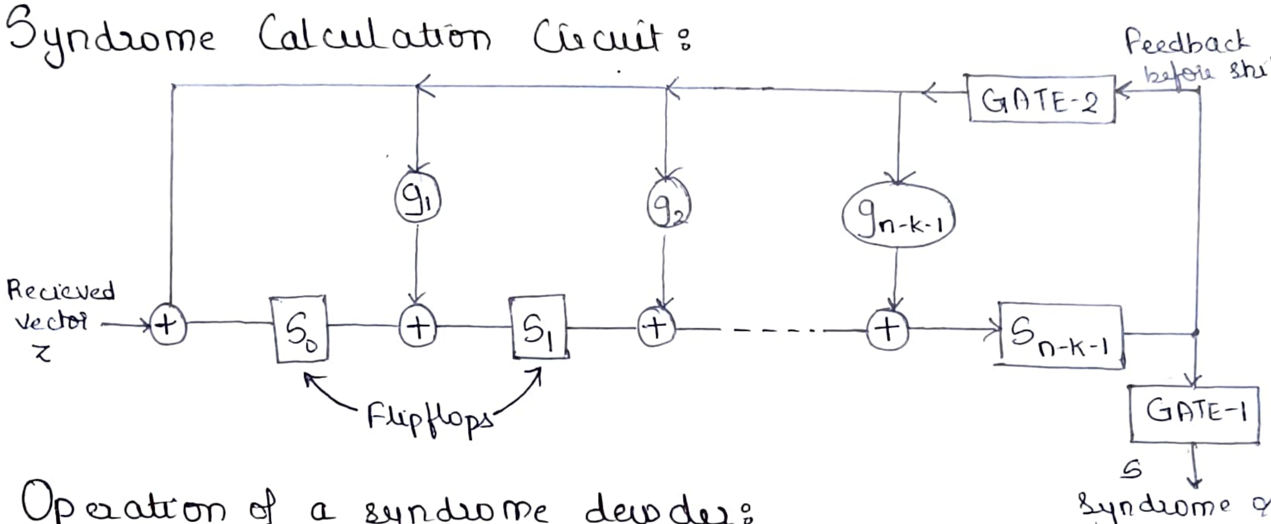
$$\frac{e(x)}{g(x)} = [Q(x) + D(x)] + \frac{S(x)}{g(x)}.$$

$$e(x) = [Q(x) + D(x)] \cdot g(x) + \frac{s(x)}{g(x)} \cdot g(x)$$

$$\Rightarrow e(x) = [Q(x) + D(x)] + s(x).$$

Hence the syndrome of $R(x)$ is equal to the remainder resulting from dividing the error pattern by generator polynomial. The syndrome contains information about the error pattern that can be used for error correction.

Syndrome Calculation Circuit:



Operation of a syndrome decoder:

– The syndrome carried as below:

1) The register is first initialised. The with gate 2 turned ON and gate 1 off, the recieved vector Z is entered into shift register.

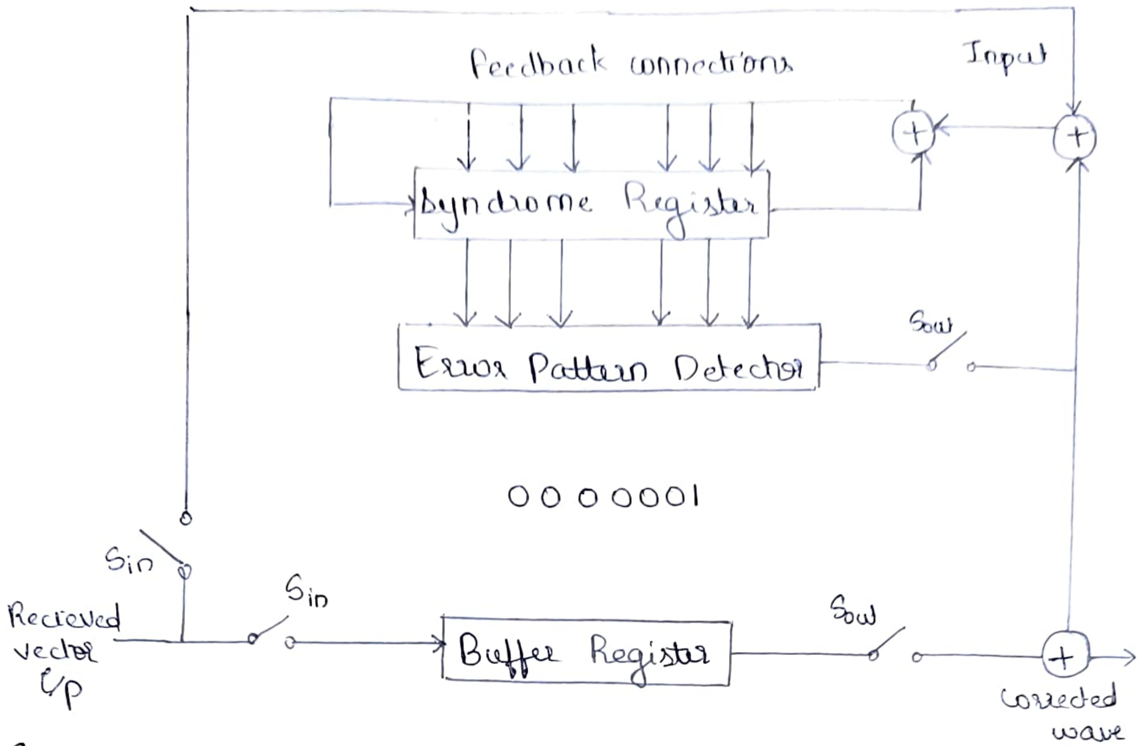
2) After the entire recieved vector is shifted into the register, the contents of the register will be syndrome. Now gate-2 is turned off, gate-1 on, and the syndrome vector is shifted out of register. The circuit is ready for processing the next recieved vector.

Advantages of Cyclic Codes:

– Extremely well selected for error detection. Error detection can be implemented by simply adding an additional Flipflop to the syndrome calculation.

If syndrome is non zero, FF are set and error is noted. For error detection only cyclic codes are normally preferable.

GENERAL FORM OF DECODER
(with error correction)



Steps for decoding :

1) The recieved signal vector is shifted into the buffer register and the syndrome register.

2) After the syndrome for recieved vector is calculated and placed in syndrom register, the contents of syndrome register is read into the detector.

— Detector is a combinational circuit designed to o/p a 1 if the syndrome in syndrome corresponds to a correctable error pattern with an error @ the highest order position x^{n-1}

— If detector o/p is 1, recieved digit at the right most stage of the buffer register is erroneous and hence is corrected.

— If detected o/p is 0, right most stage of buffer reg is assumed to be correct. Thus the detector o/p is the estimated error value for digit coming out of the buffer register.

If the first recieved digit is in error, detector o/p is 1; which is used for corresponding the first recieved digit. The o/p of detector is also fed into the syndrome register, to modify the syndrome.

This results in a new syndrome corresponding to recieved vector shifted to right by one place.

The new syndrome is now used to check whether or not, the second recieved digit, now at the right most stage of buff in an erroneous digit. If so it is corrected, a new syndrome is calculated as in step 3 and procedure is repeated.

The decoder operates on the recieved vector digit by digit until entire recieved vector is shifted out of the buffer.

At the end of the decoding operations, the syndrome registers will contain all 0's.

HAMMING CODES

- Single Error correcting hamming codes: