Binary Cyclic codes

- Binary cyclic codes form a sub class of Linear Block codes
- They have two distinct **advantages** over others

1. Encoding and syndrome calculating circuits can be easily implemented with simple shift register with feedback connections and some basic gates

2. Cyclic codes have a mathematical structure(algebraic structure)that makes it easy to design

Algebraic structure of Cyclic codes

- Definition
- A (n,k) Linear block code is said to be cyclic if it exhibits the 2 properties

1. Cyclic property - every cyclic shifts of the code is also a code vector of C
2. Linearity – The sum of any 2 code words is also a code word

For example : Let C_1 = 0111001 be a code-vector of C. If C_2 = 1011100 [the last '1' of C_1 has moved into the first position] is also a code-vector of C, then it is called as *"Cyclic Code"*.

Similarly C_3 = 0101110, C_4 = 0010111 etc. will also be code vectors of C

In general, let the n-tuple be represented by

$$V = (v_0\ v_1\ v_2 \ldots\ldots\ldots v_{n-1}) \qquad \ldots\ldots (5.60)$$

If v belongs to a cyclic code, then

$$\left.\begin{aligned} V^{(1)} &= (v_{n-1}\ v_0\ v_1\ v_2 \ldots\ldots\ldots v_{n-2}) \\ \text{and} \quad V^{(2)} &= (v_{n-2}\ v_{n-1}\ v_0\ v_1\ v_2 \ldots\ldots\ldots v_{n-3}) \\ &\ \vdots \\ V^{(i)} &= (v_{n-i}\ v_{n-i+1} \ldots\ldots v_0\ v_1\ v_2 \ldots\ldots\ldots v_{n-i-1}) \end{aligned}\right\} \qquad \ldots\ldots (5.61)$$

obtained by shifting V cyclically successively, are also code-vectors of C.

This property of cyclic codes allows us to treat the elements of each code-vector as the coefficients of a polynomial of degree $(n - 1)$.

Equation (5.60) can now be represented as a polynomial given by

$$V(x) = v_0 + v_1 x + v_2 x^2 + \ldots\ldots + v_{n-1} x^{n-1} \quad \ldots\ldots (5.62)$$

Similarly, set of equations (5.61) are also represented as polynomials given by

$$\left.\begin{aligned} V^{(1)}(x) &= v_{n-1} + v_0 x + v_1 x^2 + \ldots\ldots\ldots\ldots + v_{n-2} x^{n-1} \\ V^{(2)}(x) &= v_{n-2} + v_{n-1} x + v_0 x^2 + \ldots\ldots\ldots\ldots + v_{n-3} x^{n-1} \\ &\vdots \qquad \vdots \qquad \vdots \\ V^{(i)}(x) &= v_{n-i} + v_{n-i+1} x + v_{n-i+2} x^2 + \ldots\ldots + v_{n-i-1} x^{n-1} \end{aligned}\right\} \quad \ldots\ldots (5.63)$$

field with the following rules of addition

Modulo 2 Algebra

$$0 + 0 = 0$$
$$0 + 1 = 1$$
$$1 + 0 = 0$$
$$1 + 1 = 0$$

Modulo-2 addition

$$0 . 0 = 0$$
$$0 . 1 = 0$$
$$1 . 0 = 0$$
$$1 . 1 = 1$$

Modulo-2 Multiplication

Modulo-2 Algebra:

Let us discuss addition, subtraction (same as addition in modulo-2 arithmetic), multiplication and division of polynomials with suitable examples.

Addition : The quantity $x + x$ can be written as

$$x + x = x(1+1) = x.0 = 0 \qquad \text{...... (5.64)}$$

since $1 + 1 = 0$ in modulo-2 addition

Similarly $x^2 + x^2 = x^2(1+1) = x^2.0 = 0$

and $x^3 + x^3 = x^3(1+1) = x^3.0 = 0$ and so on.

Subtraction of polynomials is same as addition in modulo-2 algebra.

Multiplication : The quantity $x.x = x^2$, $x^2.x = x^3$ and so on. Let us now consider multiplication of two polynomials.

Example 5.19 : Find the product of polynomials $f_1(x) = (x + 1)$ and $f_2(x) = x^3 + x + 1$ using modulo-2 algebra.

Solution

$$
\begin{aligned}
f_1(x).f_2(x) &= (x + 1)(x^3 + x + 1) \\
&= x^4 + x^2 + x + x^3 + x + 1 \\
&= x^4 + x^3 + x^2 + x + x + 1 \\
&= x^4 + x^3 + x^2 + x(1 + 1) + 1 \\
&= x^4 + x^3 + x^2 + 1 \quad \text{using equation (5.64).}
\end{aligned}
$$

Example 5.20 : Multiply $f_1(x) = 1 + x + x^3$ and $f_2(x) = (1 + x + x^2 + x^4)$ using modulo-2 algebra.

Solution

$$
\begin{aligned}
f_1(x).f_2(x) &= (1 + x + x^3)(1 + x + x^2 + x^4) \\
&= 1 + x + x^2 \qquad + x^4 \\
&= \quad + x + x^2 + x^3 \qquad + x^5 \\
&= \qquad\qquad + x^3 + x^4 + x^5 + x^7 \\
&= 1 + x^7 \quad \text{using equation (5.64)}
\end{aligned}
$$

Example 5.21 : Divide $f_2(x) = x^6 + x^5 + x^2$ by $f_1(x) = x^3 + x + 1$ using modulo-2 algebra.

Solution

$x^3 + x + 1)\ x^6 + x^5 + x^2\ (x^3 + x^2 + x \leftarrow Q(x)$

$\underline{x^6 + x^4 + x^3}$

$x^5 + x^4 + x^3 + x^2$ since subtraction is same as addition

$\underline{x^5 \quad\quad + x^3 + x^2}$

x^4

$\underline{x^4 + x^2 + x}$

$x^2 + x \leftarrow R(x)$