Let V_1 be the cyclic code of length 9 generated by $X^6 + X^3 + 1$. The code word corresponding to the message word $a_1a_2a_3$ in this code is

$$\begin{aligned}&(a_1 + a_2X + a_3X^2)(1 + X^3 + X^6) + \langle X^9 - 1\rangle\\ &\quad = a_1 + a_2X + a_3X^2 + a_1X^3 + a_2X^4 + a_3X^5 + a_1X^6 + a_2X^7 + a_3X^8\\ &\qquad + \langle X^9 - 1\rangle\end{aligned}$$

or the word

$$a_1a_2a_3a_1a_2a_3a_1a_2a_3 = c_1c_2\text{---}c_9$$

(say). Consider the permutation σ of the set $\{1, 2, \ldots, 9\}$ defined by

$$\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 1 & 4 & 7 & 2 & 5 & 8 & 3 & 6 & 9\end{pmatrix}$$

Then

$$\sigma(c) = c_1c_4c_7c_2c_5c_8c_3c_6c_9 = a_1a_1a_1a_2a_2a_2a_3a_3a_3$$

Hence the code V_1 is equivalent to the code V. Generator matrix of the code V_1 is

$$\mathbf{G}_1 = \begin{pmatrix}1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1\end{pmatrix}$$

The permutation matrix $\mathbf{P}$ corresponding to σ is

$$\mathbf{P} = \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\end{pmatrix}$$

Therefore, the generator matrix of V is

$$\mathbf{G} = \mathbf{G}_1\mathbf{P} = \begin{pmatrix}1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1\end{pmatrix}$$

Case (ii)

A binary cyclic code of length 63 is generated by $X^5 + X^4 + 1$. Find the minimum distance of this code.

Solution
The polynomial $X^5 + X^4 + 1$ being a generator, there is a code word of weight 3. Therefore the minimum distance of the code is at most 3. The relation

$$a(X)(X^5 + X^4 + 1) \equiv X^i \pmod{X^{63} - 1}$$

is not possible for any $i \geq 0$ as

$$X^5 + X^4 + 1 = (X^2 + X + 1)(X^3 + X + 1)$$

is a divisor of $X^{63} - 1$.

Hence, there is no code word of weight 1.

$$X^3 + 1 | X^{21} + 1$$

and also

$$X^7 + 1 | X^{21} + 1$$

Therefore, $X^5 + X^4 + 1 | X^{21} + 1$ over $\mathbb{B}$. Taking

$$a(X) = \frac{(X^{21} + 1)}{(X^5 + X^4 + 1)}$$

we find that

$$a(X)(X^5 + X^4 + 1) \equiv X^{21} + 1 \pmod{X^{63} - 1}$$

Hence there are code words of weight 2 and the minimum distance of the code is 2.

Case (iii)
Consider the binary cyclic code $\mathscr{C}$ of length 7 generated by $1 + X^2 + X^3$. Any word of length 7 which is obtained from a code word in $\mathscr{C}$ by changing 0s into 1s and 1s into 0s is a linear combination over $\mathbb{B}$ of the polynomials $X + X^4 + X^5 + X^6$, $1 + X^2 + X^5 + X^6$, $1 + X + X^3 + X^6$ and $1 + X + X^2 + X^4$. Now

$$\begin{aligned}
X + X^4 + X^5 + X^6 &= X + X^3 + X^4 + X^3 + X^5 + X^6 \\
&= (X + X^3)(1 + X^2 + X^3) \\
1 + X^2 + X^5 + X^6 &= 1 + X^2 + X^3 + X^3 + X^5 + X^6 \\
&= (1 + X^3)(1 + X^2 + X^3) \\
1 + X + X^3 + X^6 &= 1 + X^2 + X^3 + X + X^2 + X^6 \\
&= 1 + X^2 + X^3 + X(1 + X^2 + X^3) + X^2 + X^3 + X^4 + X^6 \\
&= (1 + X^2 + X^3)(1 + X) + X^2(1 + X^2 + X^3) \\
&\quad + X^3(1 + X^2 + X^3) \\
&= (1 + X + X^2 + X^3)(1 + X^2 + X^3)
\end{aligned}$$

and

$$1 + X + X^2 + X^4 = 1 + X^2 + X^3 + X + X^3 + X^4$$
$$= (1 + X)(1 + X^2 + X^3)$$

Thus each one of these is in $\mathscr{C}$ and, hence, $\mathscr{C}$ is invariant under the operation of changing 0s into 1s and 1s into 0s in the code words.

Case (iv)
A similar argument can be used to prove that the binary cyclic code of length 7 generated by $1 + X + X^3$ is invariant under the operation of changing 0s into 1s and 1s into 0s in the code words.

We can make a general observation about the invariance of codes as mentioned in Cases (iii) and (iv) of Examples 6.4 above.

Definition 6.6
Let $a = a_0 a_1 \cdots a_{n-1}$ be a binary word of length n. Call the word obtained from a by changing 0s into 1s and 1s into 0s the **complement** of a and denote it by a'. Let the process of interchanging 0s and 1s be called **complementation**.

Let $\mathscr{C}$ be a binary linear code of length n and dimension k. Let $e^1, e^2, \ldots, e^k$ be a basis of $\mathscr{C}$. Then the set $\mathscr{C}' = \{a' | a \in \mathscr{C}\}$ is again a linear code generated by the complements of the basis elements. If $\mathscr{C}' = \mathscr{C}$, then we say that $\mathscr{C}$ is **invariant under complementation**.

Theorem 6.9
Let $\mathscr{C}$ be a binary cyclic code of length n with generator polynomial

$$g(X) = 1 + g_1 X + \cdots + g_{r-1} X^{r-1} + X^r$$

Then the code $\mathscr{C}$ is invariant under complementation iff $1 + X + X^2 + \cdots + X^{n-1}$ is divisible by $g(X)$. Equivalently, a binary cyclic code is invariant under complementation iff it contains the all 1 word.

Proof
Every code polynomial in $\mathscr{C}$ is a linear combination of the polynomials $g(X)$, $Xg(X), \ldots, X^{n-r-1} g(X)$. Let $k(X)$ denote the complement

$$(g_1 + 1)X + \cdots + (g_{r-1} + 1)X^{r-1} + X^{r+1} + \cdots + X^{n-1}$$

of the generator polynomial $g(X)$.

Then

$$k(X) = g(X) + (1 + X + \cdots + X^{n-1})$$

Modulo $X^n - 1$

$$X^i k(X) = X^i g(X) + (1 + X + \cdots + X^{n-1}) \; \forall i \geq 1$$

Therefore, the complement of any code polynomial is a linear combination of the polynomials

$$X^i g(X) + (1 + X + \cdots + X^{n-1}) \quad 0 \leq i \leq n - r - 1$$

Any such linear combination is divisible by $g(X)$ iff

$$g(X) | (1 + X + \cdots + X^{n-1})$$

and the result follows.

Corollary
A binary cyclic code of odd length n with generator polynomial $g(X)$ is invariant under interchange of 0s and 1s iff $1 + X$ does not divide $g(X)$.

We know that

$$X^{15} + 1 = (X + 1)(X^4 + X^3 + 1)(X^4 + X + 1)(X^2 + X + 1) \times (X^4 + X^3 + X^2 + X + 1)$$

Also

$$X^{15} + 1 = (X + 1)(1 + X + \cdots + X^{14})$$

Therefore the binary cyclic codes of length 15 generated by

(i) $X^4 + X^3 + 1$
(ii) $X^4 + X + 1$
(iii) $X^4 + X^3 + X^2 + X + 1$
(iv) $(X^2 + X + 1)(X^4 + X + 1)$
(v) $(X^2 + X + 1)(X^4 + X^3 + 1)$

are invariant under interchange of 0s and 1s.

Exercise 6.5

1. A (4, 12) binary linear code $\mathscr{C}$ is defined by $(a_1, a_2, \ldots, a_{12}) \in \mathscr{C}$ iff $a_1 = a_2 = a_3 = a_4$, $a_5 = a_6 = a_7 = a_8$, $a_9 = a_{10} = a_{11} = a_{12}$. Is the code $\mathscr{C}$ equivalent to a cyclic code?
2. A (5, 15) binary linear code $\mathscr{C}$ is defined by $(a_1, a_2, \ldots, a_{15}) \in \mathscr{C}$ iff $a_1 = a_2 = \cdots = a_5$, $a_6 = a_7 = \cdots = a_{10}$, $a_{11} = a_{12} = \cdots = a_{15}$. Is $\mathscr{C}$ equivalent to a cyclic code?
3. Determine m and k if the (m, mk) binary linear code $\mathscr{C}$ defined by $(a_1, \ldots, a_{mk}) \in \mathscr{C}$ iff $a_1 = \cdots = a_m$, $a_{m+1} = \cdots = a_{2m}, \ldots, a_{m(k-1)+1} = \cdots = a_{mk}$ is equivalent to a cyclic code.

6.7 CYCLIC CODES AND GROUP ALGEBRAS

Let A be a group and F a field. Let FA denote the set of all finite formal sums of the form

$$\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_n a_n$$

where $\alpha_i \in F$, $a_i \in A$. Two elements $\sum \alpha_i a_i$, $\sum \beta_i a_i$ in FA are equal iff $\alpha_i = \beta_i \forall i$. For two elements $\sum \alpha_i a_i$, $\sum \beta_i a_i$, define

$$\sum \alpha_i a_i + \sum \beta_i a_i = \sum (\alpha_i + \beta_i) a_i$$

In FA, we define multiplication distributively using the group multiplication in A. Explicitly

$$(\sum \alpha_i a_i)(\sum \beta_j b_j) = \sum (\alpha_i \beta_j) a_i b_j$$

With the addition and multiplication defined above, FA becomes an algebra over F. Also, it is a free F-module with the elements of A as a basis.

Theorem 6.10
If $A = \langle a \rangle$ is a finite cyclic group of order n, then FA and $F[X]/I$, I the ideal $\langle X^n - 1 \rangle$ of $F[X]$ generated by $X^n - 1$, are isomorphic F-algebras.

Proof
Define a map $\theta: F[X] \to FA$ by

$$\theta(\sum \alpha_i X^i) = \sum \alpha_i a^i \quad \alpha_i \in F$$

which is clearly an onto F-algebra homomorphism. The homomorphism θ maps the ideal I of $F[X]$ onto 0 and so θ induces an epimorphism $\theta: F[X]/I \to FA$,

$$\theta(\sum \alpha_i X^i + I) = \sum \alpha_i a^i \quad \alpha_i \in F$$

Any element of $F[X]/I$ is of the form $\sum \alpha_i X^i + I$, where $\alpha_i = 0$ for $i \geq n$. Therefore, if

$$\theta\left(\sum_{i=0}^{n-1} \alpha_i X^i + I\right) = \sum_{i=0}^{n-1} \alpha_i a^i = 0$$

then $\alpha_i = 0 \ \forall i$, $0 \leq i \leq n-1$. Thus θ is a monomorphism and, hence, an isomorphism.

Remark 6.3
The map $\theta: F[X]/I \to FA$ being an algebra isomorphism, the ideals of $F[X]/I$ get mapped onto ideals of FA. Thus a cyclic code of length n over F may be regarded as an ideal of the group algebra FA of a cyclic group A of order n over F and conversely.

Generalizing this way of looking at cyclic codes, Berman (1967) has defined and extensively studied Abelian codes of length n as ideals of the group algebra FA where A is an Abelian group of order n. However, we do not pursue the subject matter regarding Abelian codes any further except for the following:

Recall that an Abelian group C is called the direct sum of its subgroups A and B if every element of C can be uniquely written as ab, $a \in A$, $b \in B$.