Observe that a monomial matrix over $\mathbb{B}$ is just a permutation matrix. On the other hand, if $\mathbf{M}$ is a monomial matrix of order n over a field F with d_i, $1 \le i \le n$, being the non-zero entry in the ith row of $\mathbf{M}$, then $\mathbf{M} = \mathbf{DP}$, where

$$\mathbf{D} = \operatorname{diag}(d_1, d_2, \ldots, d_n)$$

and $\mathbf{P}$ is the permutation matrix obtained from $\mathbf{M}$ by replacing every non-zero entry of $\mathbf{M}$ by 1. Alternatively, we can also write $\mathbf{M} = \mathbf{PD}'$ with

$$\mathbf{D}' = \operatorname{diag}(d'_1, d'_2, \ldots, d'_n)$$

where, for $1 \le i \le n$, d'_i denotes the non-zero entry of $\mathbf{M}$ in the ith column.

Every monomial matrix of order n over a field F is invertible and the set of all monomial matrices of order n forms a group under multiplication. This group is called the **monomial group** of degree n.

Definition 10.3
The **automorphism group** $\operatorname{Aut}(\mathscr{C})$ of a linear code $\mathscr{C}$ over $\mathrm{GF}(q)$, q a prime, is the set of all monomial matrices $\mathbf{M}$ over $\mathrm{GF}(q)$ such that $c\mathbf{M} \in \mathscr{C}\ \forall c \in \mathscr{C}$.

The product of two elements in $\operatorname{Aut}(\mathscr{C})$ is again in $\operatorname{Aut}(\mathscr{C})$ and the monomial group over $\mathrm{GF}(q)$ being finite, $\operatorname{Aut}(\mathscr{C})$ is indeed a group.

Theorem 10.1
If $\mathscr{C}$ is a linear $[n, 1, -]$ code over $F = \mathrm{GF}(q)$, q a prime, then order of $\operatorname{Aut}(\mathscr{C})$ is $(q-1)^{n-m+1}(m!)$ where m is the number of non-zero components in a basis vector of $\mathscr{C}$. ($m!$ denotes the product of $1, 2, \ldots, m$.)

Proof
Let

$$\mathbf{x} = (x_1 \quad x_2 \quad \cdots \quad x_n)$$

be a basis vector of $\mathscr{C}$. If

$$\mathbf{y} = (y_1 \quad y_2 \quad \cdots \quad y_n)$$

is another element of $\mathscr{C}$ which also generates $\mathscr{C}$, then $\mathbf{y}$ is a multiple of $\mathbf{x}$. Therefore

$$y_i = 0 \quad \text{iff} \quad x_i = 0$$

i.e. the positions of non-zero components in any vector forming a basis of $\mathscr{C}$ remain unchanged. Let $\mathbf{M} = \mathbf{PD}$ where $\mathbf{P}$ is a permutation matrix of order n and $\mathbf{D}$ is the diagonal matrix

$$\operatorname{diag}(d_1, d_2, \ldots, d_n)$$

with $d_i \ne 0$, $1 \le i \le n$. Let σ be the permutation of the set $\{1, 2, \ldots, n\}$ corresponding to the permutation matrix $\mathbf{P}$. Then

$$\mathbf{xPD} = (d_1 x_{\sigma(1)} \quad \cdots \quad d_n x_{\sigma(n)})$$

Therefore, $\mathbf{xPD} = ax$ for some $a \neq 0$ in F iff

$$d_i x_{\sigma(i)} = a x_i \forall i, \quad 1 \le i \le n$$

This, in particular, shows that

$$x_{\sigma(i)} \neq 0 \quad \text{iff} \quad x_i \neq 0$$

i.e. σ is effectively a permutation of the non-zero component positions in $\mathbf{x}$. Thus $\mathbf{xPD} \in \mathscr{C}$ iff:

(i) σ is effectively a permutation of the non-zero component positions in x and
(ii) $d_i x_{\sigma(i)} = a x_i$ for some $a \neq 0$ in F.

The number of permutations σ which are effectively permutations of the non-zero component positions in x is $m!$ and the number of choices for a is $q-1$. Also, every diagonal entry d_i corresponding to $x_i = 0$ has $q-1$ choices. Hence, the total number of choices for $\mathbf{D}$ is $(q-1)^{n-m+1}$ and, therefore, the number of choices for $\mathbf{PD}$ in $\mathrm{Aut}(\mathscr{C})$ is $(q-1)^{n-m+1}(m!)$, i.e.

$$\text{order of } \mathrm{Aut}(\mathscr{C}) = (q-1)^{n-m+1}(m!)$$

Remark 10.3

Every monomial matrix over $\mathbb{B}$ being a permutation matrix and every permutation matrix may be regarded as a permutation of the set $\{1, 2, \ldots, n\}$, $\mathrm{Aut}(\mathscr{C})$ for a binary linear code as defined earlier is identical with $\mathrm{Aut}(\mathscr{C})$ as defined above. We could, as such, have avoided giving separate definitions for $\mathrm{Aut}(\mathscr{C})$ for binary and non-binary codes but the procedure adopted is more instructive, especially for binary codes.

Examples 10.4

Case (i)

For the $[3, 1, 2]$ ternary linear code

$$\mathscr{C} = \{000, 110, 220\}$$

we have

$$\mathrm{Aut}(\mathscr{C}) = \left\{ \mathbf{I}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & d \end{pmatrix}, 2\mathbf{I}, \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & d \end{pmatrix}; \text{where } d = 1, 2 \right\}$$

Case (ii)

The automorphism group of the $[3, 1, 2]$ ternary code

$$\mathscr{C} = \{000, 101, 202\}$$

is

$$\left\{ \mathbf{I}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & d & 0 \\ 1 & 0 & 0 \end{pmatrix}, 2\mathbf{I}, \begin{pmatrix} 0 & 0 & 2 \\ 0 & d & 0 \\ 2 & 0 & 0 \end{pmatrix}; \text{where } d = 1, 2 \right\}$$

Case (iii)

Next, consider the [3, 1, 3] ternary code

$$\mathscr{C} = \{000, 111, 222\}$$

The basis word 111 is left invariant by every element of S_3 and so the order of Aut($\mathscr{C}$) is $(2 \times 3!) = 12$. Also

$$\mathrm{Aut}(\mathscr{C}) = \left\{ \mathbf{I}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \right.$$

$$\left. 2\mathbf{I}, \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 2 \\ 0 & 2 & 0 \\ 2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 2 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} \right\}$$

Case (iv)

Consider the [3, 1, 3] code over GF(5) generated by $(1 \quad 2 \quad 3)$. Let $\mathbf{P}$ be a permutation matrix of order 3 with σ as its corresponding permutation and

$$\mathbf{D} = \mathrm{diag}(d_1, d_2, d_3), \quad d_1 d_2 d_3 \neq 0$$

Then

$$(1 \quad 2 \quad 3)\mathbf{PD} = a(1 \quad 2 \quad 3)$$

for some $a \neq 0$ in GF(5) iff

$$(d_1\sigma(1), d_2\sigma(2), d_3\sigma(3)) = a(1 \quad 2 \quad 3)$$

i.e. iff

$$\begin{aligned} d_1 &= a\sigma(1)^{-1} \\ d_2 &= a2\sigma(2)^{-1} \\ d_3 &= a3\sigma(3)^{-1} \end{aligned}$$

Therefore

$$(1 \quad 2 \quad 3)\mathbf{PD} = a(\sigma(1)^{-1} \quad 2\sigma(2)^{-1} \quad 3\sigma(3)^{-1})$$

Giving all possible values to σ we find

$$\mathrm{Aut}(\mathscr{C}) = \left\{ a\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, a\begin{pmatrix} 0 & 2 & 0 \\ 3 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, a\begin{pmatrix} 0 & 0 & 3 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \end{pmatrix}, \right.$$

$$\left. a\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 4 \\ 0 & 4 & 0 \end{pmatrix}, a\begin{pmatrix} 0 & 0 & 3 \\ 3 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix}, a\begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 4 \\ 2 & 0 & 0 \end{pmatrix} \right\}$$

where a runs over all the non-zero elements of GF(5).

Case (v)

Let $\mathscr{C}$ be the linear code of length 3 over GF(5) generated by 102, 201. The two elements being linearly independent, $\mathscr{C}$ is of dimension 2 and

$$\mathscr{C} = \{000, 102, 204, 301, 403, 201, 402, 103, 304, 303, 004, 200, 401, 400, 101, 302, 003, 002, 203, 404, 100, 104, 300, 001, 202\}$$

Let **M** be a monomial matrix of order 3 with (1, 2) entry or (3, 2) entry non-zero. Then the second column of **M** is

$$\begin{pmatrix} 0 \\ 0 \\ a \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix}$$

where $a \neq 0$. The products

$$(1 \quad 0 \quad 2) \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix} = a$$

$$(2 \quad 0 \quad 1) \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix} = 2a$$

$$(1 \quad 0 \quad 2) \begin{pmatrix} 0 \\ 0 \\ a \end{pmatrix} = 2a$$

$$(2 \quad 0 \quad 1) \begin{pmatrix} 0 \\ 0 \\ a \end{pmatrix} = a$$

show that in $(1 \quad 0 \quad 2)\mathbf{M}$ and $(2 \quad 0 \quad 1)\mathbf{M}$ the middle entries are non-zero. Therefore $\mathbf{M} \notin \mathrm{Aut}(\mathscr{C})$. Hence if $\mathbf{M} \in \mathrm{Aut}(\mathscr{C})$, then

$$\mathbf{M} = \begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ c & 0 & 0 \end{pmatrix}$$

or

$$\mathbf{M} = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$$

where $abc \neq 0$. Observe that

$$(1 \quad 0 \quad 2) \begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ c & 0 & 0 \end{pmatrix} = x(102) + y(201)$$

where $x = c - a$, $y = 3a + 3c$. Thus

$$(1\quad 0\quad 2)\begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ c & 0 & 0 \end{pmatrix} \in \mathscr{C}$$

Similarly, we can show that

$$(2\quad 0\quad 1)\begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ c & 0 & 0 \end{pmatrix} \in \mathscr{C}$$

Hence

$$\begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ c & 0 & 0 \end{pmatrix} \in \mathrm{Aut}(\mathscr{C})$$

Similarly, we can prove that

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \in \mathrm{Aut}(\mathscr{C})$$

We thus have

$$\mathrm{Aut}(\mathscr{C}) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}, \begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ c & 0 & 0 \end{pmatrix} \,\middle|\, a, b, c \in \mathrm{GF}(5),\ abc \neq 0 \right\}$$

Exercise 10.2

1. Find $\mathrm{Aut}(\mathscr{C})$, when $\mathscr{C}$ is the linear code
   (i) of length 3 over GF(5) generated by 120, 210;
   (ii) of length 3 over GF(5) generated by 013, 031;
   (iii) of length 3 over GF(3) generated by 120, 110;
   (iv) of length 3 over GF(3) generated by 102, 101;
   (v) of length 3 over GF(3) generated by 102, 201;
   (vi) of length 3 over GF(5) generated by 112; and
   (vii) of length 3 over GF(3) generated by 110 and 101.
2. Prove that every monomial matrix of order n over GF(q) is invertible.
3. Prove that the set of all monomial matrices of order n over GF(q) forms a group under multiplication.

10.3 AUTOMORPHISM GROUP – ITS RELATION WITH MINIMUM DISTANCE

We prove here only one result of Sloane and Thompson (1983) showing the relevance of the automorphism group of a code in connection with its minimum distance. For this, we need a few observations about permutation groups and these are available with their proofs in W. R. Scott (1964).

Let G be a permutation group defined on a non-empty set M. Mark the deviation from earlier notation: so far we have used $\mathbf{G}$ to denote a generator matrix. An **orbit** of G is a subset S of M such that there exists an element $\mathbf{a} \in M$ for which $S = \mathbf{a}G = \{\sigma(\mathbf{a}) | \sigma \in G\}$. The group G is called **transitive** if it has only one orbit, i.e. if $\forall \mathbf{a}, \mathbf{b} \in M$, there exists $\sigma \in G$ such that $\sigma(\mathbf{a}) = \mathbf{b}$. For $\mathbf{a} \in M$, let

$$G_{\mathbf{a}} = \{\sigma \in G \,|\, \sigma(\mathbf{a}) = \mathbf{a}\}$$

i.e. the subgroup of G fixing the element $\mathbf{a}$ of M.

Proposition 10.3
If S is an orbit of G, and $\mathbf{a} \in S$, then

(i) $\mathrm{O}(G) = \mathrm{O}(G_{\mathbf{a}})\mathrm{O}(S)$;
(ii) if G is transitive, then $\mathrm{O}(G) = \mathrm{O}(G_{\mathbf{a}}) \deg G$.

As an immediate consequence of this we have the following lemma.

Lemma 10.1
If $\mathrm{O}(G)$ is odd while $\mathrm{O}(M)$ is even, then G is **not transitive**.

Definition 10.4
Let G be transitive. A proper subset B of M is called a **block** of G if:

(i) $\mathrm{O}(B) > 1$;
(ii) for any $\sigma \in G$, either $B = B\sigma$ or $B \cap B\sigma = \emptyset$.

Definition 10.5
A transitive group without blocks is called **primitive** and a transitive group with blocks is called **imprimitive**.

By a block system of an imprimitive permutation group G, we mean a set S of blocks of G such that:

(i) M is the disjoint union of all the blocks of G in S;
(ii) if $B \in S$ and $\sigma \in G$, then $B\sigma \in S$.

Proposition 10.4
Order of every block of G divides the order of M.

Theorem 10.2
If the permutation group G is transitive and has a non-trivial normal subgroup H which is intransitive, then the set of orbits for H is a block system for G.

Recall that if G is a finite group (not necessarily a permutation group) of order $p^r m$, where p is a prime not dividing m, then any subgroup of G of order p^r is called a **Sylow** p-subgroup of G. Sylow p-subgroups in G always exist. We need the next proposition.

Proposition 10.5
Let p be a prime divisor of the order $O(G)$ of a finite group G. If G contains a cyclic Sylow p-subgroup P of G, then G contains a normal subgroup N with $G/N \cong P$.

Next, we recall the definition of a projective special linear group over GF(p), p a prime.

Let p be an odd prime and $M = \{0, 1, \ldots, p-1, \infty\}$ where ∞ is the symbol introduced to represent any element of the form $a/0$, $a \neq 0$. It is fairly easy to see that if $a, b, c, d \in \mathrm{GF}(p)$, $y, z \in M$ such that

$$ay + b \neq 0 \qquad cy + d \neq 0$$

and

$$\frac{ay+b}{cy+d} = \frac{az+b}{cz+d}$$

then $y = z$. Thus

$$y \to \frac{ay+b}{cy+d}$$

for $ad - bc = 1$, $a, b, c, d \in \mathrm{GF}(p)$ is a one–one map: $M \to M$ and, hence, it is a permutation of M. If σ, σ' are permutations of M given by

$$\sigma(y) = \frac{ay+b}{cy+d}$$

$$\sigma'(y) = \frac{a'y+b'}{c'y+d'}$$

$$ad - bc = a'd' - b'c' = 1$$

then

$$\sigma'\sigma(y) = \frac{(aa' + b'c)y + (a'b + b'd)}{(ac' + cd')y + (bc' + dd')}$$

and

$$(aa' + b'c)(bc' + dd') - (a'b + b'd)(ac' + cd') = (ad - bc)(a'd' - b'c') = 1$$

Therefore a product of two permutations of M of the form described is again a permutation of the same form. Hence, the set of all such permutations of M is a group called the projective special linear group and is denoted by $PSL_2(p)$. We recall the following result of Assmus and Mattson (1969) without proof.

Theorem 10.3

The automorphism groups of the two extended quadratic residue codes each contain a subgroup of which the permutation part is precisely $PSL_2(p)$.

Using this theorem they then deduce the following corollary.

Corollary

The minimum distance in the augmented code $\hat{\mathscr{F}}$ is one less than that in $\mathscr{F}$.

For some other applications of the automorphism group we may refer to Assmus and Mattson (1972). We next recall the following theorem.

Theorem 10.4

If all the characteristic roots of a linear transformation T of a vector space V of dimension n are equal, each equal to a (say), then there exists a basis of V w.r.t. which the matrix of T is the square matrix (Jordan normal form) of order n

$$\begin{pmatrix} a & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & a & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & a & \cdots & 0 & 0 & 0 \\ \vdots & & \ddots & \cdots & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & a \end{pmatrix}$$

We now recall the following theorem.

Theorem 10.5

Suppose $\mathscr{C}$ is a binary self-dual code of length n and is fixed (setwise) by a group of permutations H with $O(H)$ odd. Let

$$(\mathbb{B}^n)_0 = \{v \in \mathbb{B}^n \mid vh = v, \forall h \in H\} \quad \text{and} \quad \mathscr{C}_0 = \mathscr{C} \cap (\mathbb{B}^n)_0.$$

Then

$$\dim(\mathbb{B}^n)_0 = 2 \dim \mathscr{C}_0$$

Proposition 10.6

Let V be a finite dimensional vector space of dimension n over a field F and T a linear transformation of V all the characteristic roots of which are equal to 1. For every k, $1 \leq k \leq n$, V has exactly one T-invariant subspace of dimension k.