IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 11, Issue 4 Ver. IV (Jul - Aug. 2015), PP 55-60
www.iosrjournals.org

A Note on [5,3] Error Correcting Codes over GF(7)

Partha Pratim Dey [*], A. K. M. Toyarak Rian [**]
[*] *Department of Mathematics & Physics*
[**] *Department of Electrical & Computer Engineering*
North South University, Bangladesh

Abstract: *In this paper we investigate the existence, equivalence and some other features of* $[5,3]$ *error correcting codes over* $GF(7)$.
Key-Words: *Linear code, generator matrix, equivalent code.*

I. Introduction

Let F be the $GF(q)$, the Galois field with q elements. An $[n,k]$ linear code over $GF(q)$ is a $k-$dimensional subspace of F^n, the space of all $n-$tuples with components from F. Since a linear code is a vector sub-space it can be given by a basis. The matrix whose rows are the basis vectors is called a generator matrix. For an acquaintance with coding theory at a basic level the reader may please consult $[1,2,3]$.

A very important concept in coding is the weight of a vector v. By definition, this is the number of non-zero components v has and is denoted by $wt(v)$. The minimum weight of a code, denoted by d, is the weight of a non-zero vector of smallest weight in the code. A

well-known theorem says that if d is the minimum weight of a code C, then C can correct $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ or fewer errors, and conversely. An $[n,k]$ linear code with minimum weight d is often called an $[n,k,d]$ code.

Two linear codes over $GF(q)$ are called equivalent if one can be obtained from the other by a combination of operations of the following types.
(a) permutation of the positions of the code;
(b) multiplication of the symbols appearing in a fixed position by a non-zero scalar.
It is well known [2] that two $k \times n$ matrices generate equivalent linear $[n,k]$ codes over $GF(q)$ if one matrix can be obtained from the other by a sequence of operations of the following types.
(1) permutation of the rows;
(2) multiplication of a row by a non-zero scalar;
(3) addition of a scalar multiple of one row to another;
(4) permutation of the columns;
(5) multiplication of any column by a non-zero scalar.
It is also worth knowing [2] that if G is a generator matrix of an $[n,k]$ code, then by performing operations of types (1), (2), (3), (4) and (5), G can be transformed to standard form
$[I_k \mid A]$,
where I_k is the $k \times k$ identity matrix, A is the $k \times (n-k)$ matrix

II. Existence of a [5, 3] Error Correcting Linear Code over $GF(q)$ if $q \geq 4$

We begin with an existence theorem.

Theorem (2.1). Let $GF(q)$ be a field of order q where $q \geq 4$. Then there do always exist an one error correcting $[5,3]$ code over $GF(q)$.
Proof. Let

$$M = \begin{bmatrix} 1 & 0 & 0 & a_{11} & a_{12} \\ 0 & 1 & 0 & a_{21} & a_{13} \\ 0 & 0 & 1 & a_{31} & a_{14} \end{bmatrix}$$

be a generator matrix of a $[5,3]$ code over $GF(q)$, $q \geq 4$ where $a_{ij} \in GF(q)$ for each i and j, $1 \leq i \leq 3, 1 \leq j \leq 2$ and $a_{ij} \neq 0$.

One then obtains the following equivalence diagram where r_i and c_i denote the i^{th} row and i^{th} column respectively.

$$M = \begin{bmatrix} 1 & 0 & 0 & a_{11} & a_{12} \\ 0 & 1 & 0 & a_{21} & a_{13} \\ 0 & 0 & 1 & a_{31} & a_{14} \end{bmatrix} \xrightarrow{a_{11}^{-1}r_1, a_{21}^{-1}r_2, a_{31}^{-1}r_3} \begin{bmatrix} a_{11}^{-1} & 0 & 0 & 1 & a_{11}^{-1}a_{12} \\ 0 & a_{21}^{-1} & 0 & 1 & a_{21}^{-1}a_{13} \\ 0 & 0 & a_{31}^{-1} & 1 & a_{31}^{-1}a_{14} \end{bmatrix} \xrightarrow{a_{11}c_1, a_{21}c_2, a_{31}c_3}$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & a_{11}^{-1}a_{12} \\ 0 & 1 & 0 & 1 & a_{21}^{-1}a_{13} \\ 0 & 0 & 1 & 1 & a_{31}^{-1}a_{14} \end{bmatrix} \xrightarrow{a=a_{11}^{-1}a_{12}, b=a_{21}^{-1}a_{13}, c=a_{31}^{-1}a_{14}} \begin{bmatrix} 1 & 0 & 0 & 1 & a \\ 0 & 1 & 0 & 1 & b \\ 0 & 0 & 1 & 1 & c \end{bmatrix} \xrightarrow{a^{-1}c_5} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & a^{-1}b \\ 0 & 0 & 1 & 1 & a^{-1}c \end{bmatrix}$$

$$\xrightarrow{x=a^{-1}b, y=a^{-1}c} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & x \\ 0 & 0 & 1 & 1 & y \end{bmatrix} = G.$$

Since $q \geq 4$, exist nonzero $x, y \in GF(q)$ such that $1, x$ and y are all distinct. Then no two columns of the parity check matrix

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

are dependent and exist 3 columns of H

$$\begin{bmatrix} -1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{and} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

which are dependent. Hence by a well known theorem [2] the minimum weight of the code generated by G or M is 3. ■

Thus there exists an one error correcting $[5,3]$ linear code over $GF(7)$.

III. Equivalence of One Error Correcting $[5,3]$ Linear Codes over $GF(7)$

Let

$$M = \begin{bmatrix} 1 & 0 & 0 & a_{11} & a_{12} \\ 0 & 1 & 0 & a_{21} & a_{13} \\ 0 & 0 & 1 & a_{31} & a_{14} \end{bmatrix}$$

be the generator matrix of a $[5,3]$ linear code over $GF(7)$. If the code is to be error correcting, the minimum weight d should be at least 3. Hence $a_{ij} \neq 0$ for each i and j, $1 \leq i \leq 3, 1 \leq j \leq 2$. Then as in Theorem (2.1) above, M can be shown to be equivalent to

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & x \\ 0 & 0 & 1 & 1 & y \end{bmatrix}$$

Notice that x in G above can't be 1, as in that case the first two rows of G if subtracted will produce a codeword of weight 2 and the code generated by G will not be error-correcting. On the other hand x and y can't be same, as then the last two rows of G if subtracted will give a codeword of weight 2 . Moreover the diagram below

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & x \\ 0 & 0 & 1 & 1 & y \end{bmatrix} \xrightarrow{swap(r_{21}, r_3)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & y \\ 0 & 1 & 0 & 1 & x \end{bmatrix} \xrightarrow{swap(c_2, c_3)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & y \\ 0 & 0 & 1 & 1 & x \end{bmatrix} = B$$

Shows that the codes generated by

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & x \\ 0 & 0 & 1 & 1 & y \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & y \\ 0 & 0 & 1 & 1 & x \end{bmatrix}$$

are equivalent. Thus from among the 36 possible choices for $\begin{pmatrix} x \\ y \end{pmatrix}$ below:

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \begin{pmatrix} 1 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ 6 \end{pmatrix}; \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \begin{pmatrix} 2 \\ 6 \end{pmatrix}; \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \end{pmatrix};$$

$$\begin{pmatrix} 4 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 4 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \end{pmatrix}, \begin{pmatrix} 4 \\ 6 \end{pmatrix}; \begin{pmatrix} 5 \\ 1 \end{pmatrix}, \begin{pmatrix} 5 \\ 2 \end{pmatrix}, \begin{pmatrix} 5 \\ 3 \end{pmatrix}, \begin{pmatrix} 5 \\ 4 \end{pmatrix}, \begin{pmatrix} 5 \\ 5 \end{pmatrix}, \begin{pmatrix} 5 \\ 6 \end{pmatrix}; \begin{pmatrix} 6 \\ 1 \end{pmatrix}, \begin{pmatrix} 6 \\ 2 \end{pmatrix}, \begin{pmatrix} 6 \\ 3 \end{pmatrix}, \begin{pmatrix} 6 \\ 4 \end{pmatrix}, \begin{pmatrix} 6 \\ 5 \end{pmatrix}, \begin{pmatrix} 6 \\ 6 \end{pmatrix}$$

for $\begin{pmatrix} x \\ y \end{pmatrix}$ in G , we have only ten choices, namely,

$\begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \begin{pmatrix} 2 \\ 6 \end{pmatrix}; \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \end{pmatrix}, \begin{pmatrix} 4 \\ 6 \end{pmatrix}$ and $\begin{pmatrix} 5 \\ 6 \end{pmatrix}$ which could yield ten generator matrices

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix}, G_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 4 \end{bmatrix}, G_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 5 \end{bmatrix}, G_4 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix}, G_5 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 1 & 4 \end{bmatrix},$$

$$G_6 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 1 & 5 \end{bmatrix},$$

$$G_7 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix}, G_8 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 4 \\ 0 & 0 & 1 & 1 & 5 \end{bmatrix}, G_9 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 4 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix}$$

and

$$G_{10} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 5 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix}$$

producing ten in-equivalent codes.

Next we will show that contrary to our expectation the codes generated by $G_1, G_2, \ldots, G_{10}$ are all equivalent.

The diagram below shows a few cases of equivalence:

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix} \xrightarrow{5c_5} \begin{bmatrix} 1 & 0 & 0 & 1 & 5 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{swap(r_1,r_3)} \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 3 \\ 1 & 0 & 0 & 1 & 5 \end{bmatrix}$$

$$\xrightarrow{swap(c_1,c_3)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 1 & 5 \end{bmatrix} = G_6$$

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix} \xrightarrow{4c_5} \begin{bmatrix} 1 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 5 \end{bmatrix} \xrightarrow{swap(r_1,r_3)} \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 4 \\ 0 & 0 & 1 & 1 & 5 \end{bmatrix} \xrightarrow{swap(c_1,c_2)}$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 4 \\ 0 & 0 & 1 & 1 & 5 \end{bmatrix} = G_8 .$$

$$G_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 5 \end{bmatrix} \xrightarrow{4c_5} \begin{bmatrix} 1 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix} \xrightarrow{swap(r_1,r_2)} \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 4 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix} \xrightarrow{swap(c_1,c_2)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 4 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix}$$

$$= G_9$$

$$G_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 5 \end{bmatrix} \xrightarrow{3c_5} \begin{bmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 1 & 6 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{swap(r_1,r_3)} \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 6 \\ 1 & 0 & 0 & 1 & 3 \end{bmatrix} \xrightarrow{swap(r_2,r_3)}$$

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 1 & 6 \end{bmatrix} \xrightarrow{swap(c_2,c_3)} \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 3 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix} \xrightarrow{swap(c_1,c_2)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix} = G_7 .$$

$$G_4 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix} \xrightarrow{4c_5} \begin{bmatrix} 1 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix} \xrightarrow{swap(r_1,r_2)} \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 4 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix} \xrightarrow{swap(r_2,r_3)}$$

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 3 \\ 1 & 0 & 0 & 1 & 4 \end{bmatrix} \xrightarrow{swap(c_1,c_2)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 3 \\ 0 & 1 & 0 & 1 & 4 \end{bmatrix} \xrightarrow{swap(c_2,c_3)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 1 & 4 \end{bmatrix} = G_5 .$$

$$G_4 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix} \xrightarrow{6c_5} \begin{bmatrix} 1 & 0 & 0 & 1 & 6 \\ 0 & 0 & 1 & 1 & 5 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} \xrightarrow{swap(r_1,r_3)} \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 5 \\ 1 & 0 & 0 & 1 & 6 \end{bmatrix} \xrightarrow{swap(c_1,c_2)}$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 5 \\ 0 & 1 & 0 & 1 & 6 \end{bmatrix} \xrightarrow{swap(c_2,c_3)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 5 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix} = G_{10}$$

Now we will show that G_1, G_2, G_3 and G_4 are equivalent.

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix} \xrightarrow{r_2 = r_2 + 5r_1, r_3 = r_3 + 4r_1} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 5 & 1 & 0 & 6 & 0 \\ 4 & 0 & 1 & 5 & 0 \end{bmatrix} \xrightarrow{swap(c_1, c_5)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 6 & 5 \\ 0 & 0 & 1 & 5 & 4 \end{bmatrix}$$

$$\xrightarrow{r_2 = 6r_2, r_3 = 3r_3} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 6 & 0 & 1 & 2 \\ 0 & 0 & 3 & 1 & 5 \end{bmatrix} \xrightarrow{c_2 = 6c_2, c_3 = 5c_3} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 5 \end{bmatrix} = G_3.$$

$$G_4 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix} \xrightarrow{swap(c_5, c_6)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 6 & 1 \end{bmatrix} \xrightarrow{r_2 = 4r_2, r_3 = 6r_3} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 4 & 0 & 1 & 4 \\ 0 & 0 & 6 & 1 & 6 \end{bmatrix} \xrightarrow{r_1 = r_1 + r_3, r_2 = r_2 + 4r_3}$$

$$\begin{bmatrix} 1 & 0 & 6 & 2 & 0 \\ 0 & 4 & 3 & 5 & 0 \\ 0 & 0 & 6 & 1 & 6 \end{bmatrix} \xrightarrow{swap(c_3, c_6)} \begin{bmatrix} 1 & 0 & 0 & 2 & 6 \\ 0 & 4 & 0 & 5 & 3 \\ 0 & 0 & 6 & 1 & 6 \end{bmatrix} \xrightarrow{r_1 = 4r_1, r_2 = 3r_2} \begin{bmatrix} 4 & 0 & 0 & 1 & 3 \\ 0 & 5 & 0 & 1 & 2 \\ 0 & 0 & 6 & 1 & 6 \end{bmatrix} \xrightarrow{2c_1, 3c_2, 6c_3, 5c_5}$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 1 & 2 \end{bmatrix} \xrightarrow{swap(r_2, r_3)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 3 \end{bmatrix} \xrightarrow{swap(c_2, c_3)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix} = G_1$$

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 4 \end{bmatrix} \xrightarrow{r_1 = r_1 + 5r_1, r_2 = r_2 + 3r_3} \begin{bmatrix} 1 & 0 & 5 & 6 & 0 \\ 0 & 1 & 3 & 4 & 0 \\ 0 & 0 & 1 & 1 & 4 \end{bmatrix} \xrightarrow{swap(c_3, c_5)} \begin{bmatrix} 1 & 0 & 0 & 6 & 5 \\ 0 & 1 & 0 & 4 & 3 \\ 0 & 0 & 4 & 1 & 1 \end{bmatrix} \xrightarrow{2c_3}$$

$$\begin{bmatrix} 1 & 0 & 0 & 6 & 5 \\ 0 & 1 & 0 & 4 & 3 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{r_1 = 6r_1, r_2 = 2r_2} \begin{bmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 1 & 6 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{swap(r_2, r_3)} \begin{bmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 6 \end{bmatrix} \xrightarrow{swap(r_1, r_2)}$$

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 1 & 6 \end{bmatrix} \xrightarrow{swap(c_2, c_3)} \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix} \xrightarrow{swap(c_1, c_2)} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 6 \end{bmatrix} = G_4.$$

Thus we have obtained the following theorem.

Theorem(3.1) An $1-$error correcting $[5,3]$ code over $GF(7)$ is equivalent to the code with the following generator matrix G_1 where

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix}.$$

IV. Weight Distribution of a [5, 3] Linear Code over GF(7)

We begin with the following theorem [3].

Theorem (4.1) Let C be a $[n,k,d]$ MDS code over $GF(q)$ with $d = n-k+1$. Then $A_0 = 1,\ A_i = 0,\ 1 \le i < d$ and

$$A_i = \binom{n}{i}\sum_{j=0}^{i-d}(-1)^j\binom{i}{j}(q^{i+1-d-j}-1),\ d \le i \le n.$$

Applying this theorem on a [5,3,3] code C we obtain, $A_0 = 1,\ A_1 = A_2 = 0$,

$$A_3 = \binom{5}{3}(-1)^0\binom{3}{0}(7-1) = 60$$

$$A_4 = \binom{5}{4}\sum_{j=0}^{1}(-1)^j\binom{4}{j}(7^{2-j}-1) = 5\left[(-1)^0\binom{4}{0}(48) + (-1)^1\binom{4}{1}(6)\right] = 5(48-24) = 120$$

and

$$A_5 = \binom{5}{5}\sum_{j=0}^{2}(-1)^j\binom{5}{j}(7^{3-j}-1) = (7^3-1) - 5(7^2-1) + 10(7-1) = 162.$$

It is well-known [1] that if C is an MDS code, so is $C^\perp$. Hence the minimum distance of $C^\perp$ is $5-2+1=4$. Then by Theorem (3.1) above, $A_0 = 1,\ A_1 = A_2 = A_3 = 0$,

$$A_4 = \binom{5}{4}(-1)^0\binom{4}{0}(7-1) = 30 \text{ and}$$

$$A_5 = \binom{5}{5}\sum_{j=0}^{1}(-1)^j\binom{5}{j}(7^{2-j}-1) = (7^2-1) - 5(7-1) = 48-30 = 18.$$

Thus we have the following theorem.

Theorem(4.2). A $[5,3,3]$ code C over $GF(7)$ has the following weight distribution.

Weight	Number of Words
0	1
3	60
4	120
5	162

On the other hand, a $[5,2,4]$ code $C^\perp$ has the following weight distribution.

Weight	Number of Words
0	1
4	30
5	18

References

[1]. Pless, V. (2003) Introduction to the Theory of Error Correcting Codes, Wiley Student Edition, John Wiley & Sons (Asia) Pte. Ltd., Singapore.

[2]. Hill, R. (1986) A First Course in Coding Theory, The Oxford University Press, Oxford, UK.

[3]. Huffman,W.C. and Pless,V. (2003) Fundamentals of Error Correcting Codes, Cambridge University Press, New York.