# A COUPLE OF ERROR-CORRECTING CODES

**Tanveer Talukder***

**Zubair Ahmed***

**Partha Pratim Dey***

---

**Abstract:-**

In this paper we use Klein group and its regular representation to produce an alternative construction of $3-$error correcting $[16,5]$ BCH code. We also compute the weight distribution of its dual code.

***Key-Words*:-** Regular representation, linear code, generator matrix, parity-check matrix.

* Department of Electrical Engineering and Computer Science, North South University, Bangladesh.

## 1 Introduction

Throughout this paper $F_p$, for some prime $p$, will denote the Galois field $GF(p)$ and $F_p^k$ will be the vector space comprising of vectors $x=(x_1,\ldots,x_k)$ where $x_i \in F_p$ for $i=1,\ldots,k$. Let $\{g_1,\ldots,g_4\}$ be an enumeration of the elements of the Klein four group $Z_2\times Z_2$ of order 4 with identity element $g_1=(0,0)$, $g_2=(1,0)$, $g_3=(0,1)$ and $g_4=(1,1)$ and let $R(g_i)$ denote the regular representation of $g_i$ in $Z_2\times Z_2$ using this enumeration to index rows and columns of the representation matrix. Then

$$R(g_1)=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}, R(g_2)=\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}, R(g_3)=\begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix} \text{ and } R(g_4)=\begin{bmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{bmatrix}$$

and the following:

$$R(Z_2\times Z_2)=\begin{bmatrix}R(g_1)&R(g_1)&R(g_1)&R(g_1)\\R(g_1)&R(g_2)&R(g_3)&R(g_4)\\R(g_1)&R(g_4)&R(g_2)&R(g_3)\\R(g_1)&R(g_3)&R(g_4)&R(g_2)\end{bmatrix}$$

is a normalized square matrix in $F_2$ of order 16 afforded by the enumeration $\{g_1,\ldots,g_4\}$ of $Z_2\times Z_2$. Each of the 16 rows of $R(Z_2\times Z_2)$ can be viewed as a row –vector in $F_2^{16}$. We partition these 16 row-vectors in 4 families $F_1,F_2,F_3$ and $F_4$ where $F_1$ comprises of rows 1 through 4, $F_2$ comprises of rows 5 through 8, $F_3$ comprises of rows 9 through 12 and $F_4$ comprises of the remaining four rows of $R(Z_2\times Z_2)$. For each $m$, we denote the 4 vectors of $F_m$ by $w_{m1},\ldots,w_{m4}$ and let $B_m$ be the block matrix given by

$$B_m=\begin{bmatrix}w_{m1}-w_{m2}\\w_{m1}-w_{m3}\\w_{m1}-w_{m4}\end{bmatrix}.$$

We then gaussjord the following $12\times16$ matrix

$$\begin{bmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \end{bmatrix} = \begin{bmatrix} 1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0 \\ 1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1 \\ 1&1&0&0&1&1&0&0&0&0&1&1&0&0&1&1 \\ 1&0&1&0&0&1&0&1&1&0&1&0&0&1&0&1 \\ 1&0&0&1&0&1&1&0&0&1&1&0&1&0&0&1 \\ 1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1 \\ 1&0&1&0&0&1&0&1&0&1&0&1&1&0&1&0 \\ 1&0&0&1&1&0&0&1&0&1&1&0&0&1&1&0 \\ 1&1&0&0&0&0&1&1&0&0&1&1&1&1&0&0 \\ 1&0&1&0&1&0&1&0&0&1&0&1&0&1&0&1 \\ 1&0&0&1&0&1&1&0&1&0&0&1&0&1&1&0 \end{bmatrix}$$

to obtain

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

which after appropriate permutation of columns becomes

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

Notice that each row of $G$ above is a vector of $F_2^{16}$ and the subspace spanned by its $5$ rows over $F_2$ is a linear code and $G$ is its generator matrix. We will denote this code by $C(G)$ and explore it throughout the rest of the paper. We will also explore the dual code $C(G)^{\perp}$. For an understanding of the linear code at a basic level one may please consult [1] and [2].

## 2 Weight Distribution of $C(G)$

We begin with a theorem.

Theorem (2.1) $C(G)$ is a $[16,5,8]$ linear code with $1$ code-word of weight $0$, $1$ code-word of weight $16$ and $30$ code-words of weight $8$.

Proof. Let $w_i$ denote the $i^{th}$ row of $G$ and $wt(w_i)$ denote the weight of $w_i$. Also let $w_i * w_j$ denote the number of $1$'s $w_i$ and $w_j$ have in common. Since

$$G \cdot G^{tr} = \begin{bmatrix} 8 & 4 & 4 & 4 & 4 \\ 4 & 8 & 4 & 4 & 4 \\ 4 & 4 & 8 & 4 & 4 \\ 4 & 4 & 4 & 8 & 4 \\ 4 & 4 & 4 & 4 & 8 \end{bmatrix},$$

it is obvious that $wt(w_i) = 8$ for $\forall\ i$ and $w_i * w_j = 4$ for $i \neq j$. As $wt(w_i + w_j) = wt(w_i) + wt(w_j) - 2(w_i * w_j)$, we have $wt(w_i + w_j) = 8$ for $i \neq j$.
Thus each row-vector of $G$ and each linear combination of two distinct row-vectors of $G$ has weight $8$. Notice that $\sum_{i=1}^{5} w_i = 1_{16}$ where $1_{16}$ is an all-one row-vector with 16 coordinates. Hence a linear combination of $4$ row-vectors of $G$ like $\sum_{m \in \{1,2,3,4,5\} \setminus \{i\}} w_m$ is in fact the vector $1_{16} + w_i$, which clearly has weight $8$. Similarly a linear combination of 3 row-vectors like $\sum_{m \in \{1,2,3,4,5\} \setminus \{i,j\}} w_m$ is $1_{16} + (w_i + w_j)$, a vector of weight $8$. ■

Corollary (2.2) $C(G)$ can correct $3$ errors.
Proof. Since $3$ is the largest integer less than half of minimum weight $8$ of the code, $C(G)$ can correct $3$ errors. ■

Next we show that this code $C(G)$ is in fact the [16,5,8] extended BCH code.
Let $f(x) = x^{15} - 1$ and we choose the primitive polynomial $p(x) = x^4 + x^3 + 1$ in $F_2[x]$. Then $F_2[x]/(p(x))$ is a finite field of order 16 and $a, a^2, \ldots, a^{15}$ (where $a = x$) constitute all the non-zero elements in $F_2[x]/(p(x))$. Let $C$ be the code that results from considering the first six powers of $a$. To determine the generator polynomial $g(x)$ for $C$, we must find the minimum polynomials $m_1(x), m_2(x), \cdots, m_6(x)$ for $a, a^2, \ldots, a^6$ respectively. Notice that $m_1(x) = m_2(x) = m_4(x) = x^4 + x^3 + 1$. To get the others, we factor $x^{15} - 1$ to obtain $x^{15} - 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$. Obviously then $m_3(x) = m_6(x) = x^4 + x^3 + x^2 + x + 1$ and $m_5(x) = x^2 + x + 1$. Thus $g(x) = (x^2+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1) = 1 + x^2 + x^5 + x^6 + x^8 + x^9 + x^{10}$ and generator matrix $J$ of $C$ is given by:

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

Then $J^{ext} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$

We gaussjord $J^{ext}$ to get

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

which after appropriate permutation of columns becomes $G$. Thus we have the following theorem.

Theorem (2.3) $C(G)$ is the triple error-correcting extended $[16,5,8]$ BCH code generated by $g(x) = 1 + x^2 + x^5 + x^6 + x^8 + x^9 + x^{10}$.

## 3 Weight Distribution of the Dual Code $C(G)^{\perp}$

Since $G = [I_5 : M]$ where

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix},$$

we have for the parity check matrix of $C(G)$

$H = [M^{tr} : I_{11}]$.

Notice that each row of $H$ above is a vector of $F_2^{16}$ and the subspace spanned by its $11$ rows over $F_2$ is a linear code $C(H)$ and $H$ is its generator matrix. As $GH^{tr} = 0$, $C(H) = C(G)^{\perp}$. We will find weight distribution of $C(H)$ from the weight distribution of $C(G)$.

Theorem (3.1) $C(H)$ is a $[16,11,4]$ linear code.

Proof. Since each row-vector of $H$ has even weight $(4 \text{ or } 6)$, weight of each code-word of $C(H)$ is even. Assume now that $c \in C(H)$ and $wt(c) = 2$. Then $c$ has to be a linear combination of $2$ row-vectors of $H$. Moreover the first $5$ coordinates of the row-vectors must coincide. Since there are no two row-vectors with identical first five coordinates, a code-word of weight $2$ does not exist in $C(H)$. Hence the minimum distance of $C(H)$ is $4$ ■

Corollary (3.2) There is no code-word of weight $14$ in $C(H)$.

Proof. Let $c \in C(H)$ and $wt(c) = 14$. As the sum of row-vectors of $H$ is $1_{16}$, we have $1_{16} \in C(H)$. Hence $c + 1_{16} \in C(H)$ and has weight $2$, a contradiction to the fact that the minimum weight in $C(H)$ is $4$. ■

Thus in $C(H)$ there could be code-words only of weight $0,4,6,8,10,12$ and $16$. Obviously, the zero code-word is the only code-word of weight $0$ and $1_{16}$ is the only code-word of weight $16$. Below we state a theorem [3] due to Mac Williams that will help us to find the weight distribution of the other code-words.

Theorem (3.3) (Mac Williams) Let $C$ be an $[n,k]$ code over $GF(q)$ with $A_i$, the number of vectors of weight $i$ in $C$ and $B_i$, the number of vectors of weight $i$ in $C^{\perp}$. The following relations relate the $\{A_i\}$ and $\{B_i\}$:

$$\sum_{j=0}^{n} \binom{n-j}{\upsilon} A_j = q^{k-\upsilon} \sum_{j=0}^{n} \binom{n-j}{\upsilon-j} B_j, \text{ where } \upsilon = 0,\ldots,n.$$

Let $C = C(H)$. Then $C^{\perp} = C(H)^{\perp} = C(G)$ and $B_8 = 30,\ B_0 = 1$ and $B_{16} = 1$ by Theorem (2.1).

Notice that $\sum_{i=0}^{8} A_{2i} = 2^{11}$. Since $A_0 = A_{16} = 1,\ A_2 = A_{14} = 0,\ A_4 = A_{12},\ A_6 = A_{10}$, we have

$\sum_{i=0}^{8} A_{2i} = 2 + 2A_4 + 2A_6 + A_8$ and $2A_4 + 2A_6 + A_8 = 2^{11} - 2$ i.e. $2A_4 + 2A_6 + A_8 = 2046$. Taking $\upsilon = 12$ in Mac Williams equation, we obtain:

$$\sum_{j=0}^{16} \binom{16-j}{12} A_j = 2^{11-12} \sum_{j=0}^{16} \binom{16-j}{12-j} B_j$$

or $\binom{16}{12} A_0 + \binom{12}{12} A_4 = \frac{1}{2}\left[\binom{16}{12} B_0 + B_8 \binom{8}{4}\right]$

or $2(1820 + A_4) = 1820 + 2100$

$\therefore A_4 = 140$.

We insert $A_4 = 140$ in $2A_4 + 2A_6 + A_8 = 2046$ to get $2A_6 + A_8 = 1766$.

Next we take $\upsilon = 8$ and obtain:

$$\sum_{j=0}^{16} \binom{16-j}{8} A_j = 2^{11-8} \sum_{j=0}^{16} \binom{16-j}{8-j} B_j$$

or $\binom{16}{8} + \binom{12}{8} A_4 + \binom{10}{8} A_6 + \binom{8}{8} A_8 = 2^3 \left[\binom{16}{8} B_0 + B_8 \binom{8}{0}\right]$

or $\binom{16}{8} + \binom{12}{8} A_4 + \binom{10}{8} A_6 + \binom{8}{8} A_8 = 2^3 \left[\binom{16}{8} + 30\binom{8}{0}\right]$

or $12870 + 495A_4 + 45A_6 + A_8 = 8[12870 + 30]$

$\therefore 495A_4 + 45A_6 + A_8 = 90330$.

We now insert $A_4 = 140$ in $495A_4 + 45A_6 + A_8 = 90330$ to get $45A_6 + A_8 = 21030$.

Solving now the system

$$\begin{cases} 2A_6 + A_8 = 1766 \\ 45A_6 + A_8 = 21030 \end{cases}$$

we obtain $A_6 = 448$ and $A_8 = 870$.

Thus we have the following theorem.

Theorem (3.4) The dual code $C(G)^{\perp} = C(H)$ has the following weight distribution.

| Weight | Number of Words |
|---|---|
| 0 | 1 |
| 4 | 140 |
| 6 | 448 |
| 8 | 870 |
| 10 | 448 |
| 12 | 140 |
| 16 | 1 |

**References**

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

[2] Klima, R.E., Sigmon, N. and Stitzinger, E. (2000) Applications of Abstract Algebra with MAPLE, CRC Press, Boca Raton.

[3] MacWilliams, F. J. (1963) A theorem on the distribution of weights in a systematic code, Bell Syst. Tech. Journal, **42** pp 79-94.