Error Correcting [5,2] Codes over GF (5)

Hasina Akter*, Partha Pratim Dey, M. Asifuzzaman

North South University, Bashundhara, Dhaka-1229, Bangladesh
**Email: hasina.akter@northsouth.edu*

Abstract

All the error correcting linear [5, 2]-codes over GF (4) were classified in this study. The [5, 2]-codes over GF (5), instead of GF (4), have been classified. At the end, the weight distribution of the developed codes has been computed.

Keywords: Linear Codes, Generator matrix, Equivalent code, Error correction

1. Introduction

Let $GF(q^n)$ denote the vector space of all n-tuples over the finite field $GF(q)$, of order q. A q-ary linear code C is a linear subspace of $GF(q^n)$. If C has rank k, then C is called an $[n, k]$ –code. Every member $c \in C$ is called a codeword. A generator matrix for an $[n, k]$ –code C is any $k \times n$ matrix G whose rows form a basis for C. The weight, $wt(c)$, of a codeword c is the number of its elements that are non-zero, and the distance between two codewords is the number of elements in which they differ. The minimum distance of a code C is the smallest distance between distinct codewords in C. For linear codes, the minimum distance is also called the minimum weight of the code. If the minimum weight d of an $[n, k]$-code is known, then we refer to the code as an $[n,k,d]$-code. Two linear codes are equivalent if one can be obtained from the other by a series of operations of the following two types:

- An arbitrary permutation of the coordinate positions, and
- In any coordinate position, multiplication by any non-zero scalar.

Two k by n matrices G_1 and G_2 produces equivalent codes if G_2 can be derived from G_1 by a series of operations of the following types:

- permutations of rows or columns or both;
- multiplications of a row or column or both by a non-zero scalar;
- addition of a scalar multiple of one row to another.

For an understanding of coding theory at basic level please see [1], [2] or [3].

Let G given below be a generator matrix of a [5, 2]-code C, where $a_{ij}, b_{ij} \in GF(5)$ and $i = 1, 1 \le j \le 3$.

$$G = \begin{bmatrix} 1 & 0 & a_{11} & a_{12} & a_{13} \\ 0 & 1 & b_{11} & b_{12} & b_{13} \end{bmatrix}.$$

To be error-correcting code, at least two of $\{a_{11}, a_{12}, a_{13}\}$ have to be non-zero. Hence through column permutation,

We can ensure that $a_{11}, a_{12} \neq 0$. Hence, we obtain $\begin{bmatrix} 1 & 0 & 1 & 1 & a_{13} \\ 0 & 1 & a_{11}^{-1}b_{11} & a_{12}^{-1}b_{12} & b_{13} \end{bmatrix}$

Set $p = a_{11}^{-1}b_{11}$ and $q = a_{12}^{-1}b_{12}$ in matrix above to get $\begin{bmatrix} 1 & 0 & 1 & 1 & a_{13} \\ 0 & 1 & p & q & b_{13} \end{bmatrix}$

iLab-Australia © 2018
http://ilab-australia.org/

For the code to be error-correcting, two of $\{p, q, b_{13}\}$ must be non-zero. Without loss, let $p \neq 0$. Then, let us multiply the second row of the above matrix by p^{-1} to get $\begin{bmatrix} 1 & 0 & 1 & 1 & a_{13} \\ 0 & p^{-1} & 1 & p^{-1}q & p^{-1}b_{13} \end{bmatrix}$ and then multiply its second column by p which yields $\begin{bmatrix} 1 & 0 & 1 & 1 & a_{13} \\ 0 & 1 & 1 & p^{-1}q & p^{-1}b_{13} \end{bmatrix}$

We now set $p^{-1}q = m, a_{13} = x$ and $p^{-1}b_{13} = y$ and obtain $\begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 0 & 1 & 1 & m & y \end{bmatrix}$

2. Exploration of Equivalence Case by Case

CASE A: $(m = 0)$

Then

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

We produce a transformation diagram which shows that each generator matrix of CASE A can be transformed into a matrix of CASE B where $m = 1$.

$$\begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 0 & 1 & 1 & 0 & y \end{bmatrix} \xrightarrow{r_2 = r_2 - r_1} \begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 4 & 1 & 0 & 4 & y - x \end{bmatrix} \xrightarrow{r_2 = 4r_2} \begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 1 & 4 & 0 & 1 & 4(y - x) \end{bmatrix}$$

$$\xrightarrow{c_2 = 4c_2} \begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 1 & 1 & 0 & 1 & 4(y - x) \end{bmatrix} \xrightarrow{swap(c_1, c_3)} \begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 0 & 1 & 1 & 1 & 4(y - x) \end{bmatrix},$$

This is a matrix of the following case i.e. CASE B when $m = 1$.

CASE B: $(m = 1)$

For $(m = 1)$, $G = \begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 0 & 1 & 1 & 1 & y \end{bmatrix}$.

Therefore, $G \sim \begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 4 & 1 & 0 & 0 & y - x \end{bmatrix}$. Let $x = u$ and $y - x = v$. Then $G \sim \begin{bmatrix} 1 & 0 & 1 & 1 & u \\ 4 & 1 & 0 & 0 & v \end{bmatrix}$.

Subcase1: Let $u = v = 0$. Then the code generated by G has no error correction power.

Subcase2: Let $u \neq 0, v = 0$. Again the code generated by G has no error correction power.

Subcase3: Let $u = 0, v \neq 0$ which implies that

$$G \sim \begin{bmatrix} 1 & 0 & 1 & 1 & u \\ 4 & 1 & 0 & 0 & v \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 4 & 1 & 0 & 0 & v \end{bmatrix} \xrightarrow{v^{-1}c_5} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 4 & 1 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{r_2 = r_1 + r_2} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix} = M_1$$

Subcase4: Let $u \neq 0$ and $v \neq 0$.

Then $G \sim \begin{bmatrix} 1 & 0 & 1 & 1 & u \\ 4 & 1 & 0 & 0 & v \end{bmatrix} \xrightarrow{u^{-1}c_5} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 4 & 1 & 0 & 0 & u^{-1}v \end{bmatrix} \xrightarrow{r_2 = r_1 + r_2} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 + u^{-1}v \end{bmatrix}$

$$\xrightarrow{r = 1 + u^{-1}v} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & r \end{bmatrix}.$$

Since $r \in GF(5)$, we obtain the following five generator matrices here:

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

We now notice that the code generated by G_2 does not correct any error as $4r_1 + r_2 = (4,1,0,0,0)$ has weight 2. We now show that M_1 in Subcase3 is equivalent to G_1.

$$M_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{swap(r_1, r_2)} \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} \xrightarrow{swap(c_1, c_2)} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} = G_1$$

Next we produce below a set of transformation diagrams that will establish equivalence among codes generated G_3, G_4 and G_5.

$$G_3 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 2 \end{bmatrix} \xrightarrow{3c_5} \begin{bmatrix} 1 & 0 & 1 & 1 & 3 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{swap(r_1, r_2)} \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 3 \end{bmatrix} \xrightarrow{swap(c_1, c_2)} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 3 \end{bmatrix} = G_4$$

$$G_5 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 4 \end{bmatrix} \xrightarrow{r_2 = 3r_2} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 3 & 3 & 3 & 2 \end{bmatrix} \xrightarrow{2c_2} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 3 & 3 & 2 \end{bmatrix} \xrightarrow{r_2 = 3r_1 + r_2} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 3 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$\xrightarrow{swap(c_1, c_5)} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 3 \end{bmatrix} = G_4$$

Our next goal is to show that the codes generated by G_1 and G_3 are not equivalent. Towards that, we investigate the weight distribution of codes. Our investigation shows that code generated by G_1 has 8 codewords of weight 3 whereas code generated by G_3 has 4 codewords of weight 3. Hence, the codes are not equivalent.

CASE C: $(m = 2)$

Then $G = \begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 0 & 1 & 1 & 2 & y \end{bmatrix}$.

Subcase1: Let $x = 0$ and $y = 0$. $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 0 \end{bmatrix}$.

Then using the technique as in CASE B, we get the following weight distribution for the code generated by G in this case: $A_0 = 1, A_3 = 16, A_4 = 8$.

Subcase2: Let $x \neq 0$ and $y = 0$.

$G = \begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 0 & 1 & 1 & 2 & 0 \end{bmatrix}$, which is equivalent to $\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 0 \end{bmatrix}$.

The following diagram shows that the code generated by matrix above is equivalent to the code generated by G_3 in CASE B.

$$G_3 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 2 \end{bmatrix} \xrightarrow{r_2 = r_2 - r_1} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 4 & 1 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{r_1 = r_1 + r_2} \begin{bmatrix} 0 & 1 & 1 & 1 & 2 \\ 4 & 1 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{c_1 = 4c_1} \begin{bmatrix} 0 & 1 & 1 & 1 & 2 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{swap(r_1, r_2)} \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 2 \end{bmatrix} \xrightarrow{swap(c_2, c_3)} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 2 \end{bmatrix} \xrightarrow{r_2 = 3r_2} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 3 & 3 & 3 & 1 \end{bmatrix} \xrightarrow{c_2 = 2c_2, c_3 = 2c_3, c_4 = 2c_4}$$

$$\begin{bmatrix}1&0&2&0&1\\0&1&1&1&1\end{bmatrix} \xrightarrow{swap(r_1,r_2)} \begin{bmatrix}0&1&1&1&1\\1&0&2&0&1\end{bmatrix} \xrightarrow{swap(c_1,c_2),swap(c_4,c_5)} \begin{bmatrix}1&0&1&1&1\\0&1&2&1&0\end{bmatrix}$$

Subcase3: Let $x = 0$ and $y \neq 0$.

$G = \begin{bmatrix}1&0&1&1&0\\0&1&1&2&y\end{bmatrix}$, which is equivalent to $\begin{bmatrix}1&0&1&1&0\\0&1&1&2&1\end{bmatrix}$.

The following diagram shows that the code generated by matrix above is equivalent to the code generated by G_3 in CASE B.

$$G_3 = \begin{bmatrix}1&0&1&1&1\\0&1&1&1&2\end{bmatrix} \xrightarrow{r_2=r_2-r_1} \begin{bmatrix}1&0&1&1&1\\4&1&0&0&1\end{bmatrix} \xrightarrow{r_1=r_1+r_2} \begin{bmatrix}0&1&1&1&2\\4&1&0&0&1\end{bmatrix} \xrightarrow{c_1=4c_1} \begin{bmatrix}0&1&1&1&2\\1&1&0&0&1\end{bmatrix}$$

$$\xrightarrow{swap(r_1,r_2)} \begin{bmatrix}1&1&0&0&1\\0&1&1&1&2\end{bmatrix} \xrightarrow{swap(c_2,c_3)} \begin{bmatrix}1&0&1&0&1\\0&1&1&1&2\end{bmatrix} \xrightarrow{swap(c_4,c_5)} \begin{bmatrix}1&0&1&1&0\\0&1&1&2&1\end{bmatrix}.$$

Subcase4: Let $x \neq 0$ and $y \neq 0$.

Then $G = \begin{bmatrix}1&0&1&1&x\\0&1&1&2&y\end{bmatrix}$, which is equivalent to $\begin{bmatrix}1&0&1&1&1\\0&1&1&2&x^{-1}y\end{bmatrix}$.

Let $s = x^{-1}y$. Since $r \in GF(5) \setminus \{0\}$, we obtain the following five generator matrices here:

$$\overline{G}_1 = \begin{bmatrix}1&0&1&1&1\\0&1&1&2&1\end{bmatrix}, \overline{G}_2 = \begin{bmatrix}1&0&1&1&1\\0&1&1&2&2\end{bmatrix}, \overline{G}_3 = \begin{bmatrix}1&0&1&1&1\\0&1&1&2&3\end{bmatrix}, \overline{G}_4 = \begin{bmatrix}1&0&1&1&1\\0&1&1&2&4\end{bmatrix}.$$

In $\overline{G}_1$, if we swap columns four and five, we obtain the following matrix:

$\begin{bmatrix}1&0&1&1&1\\0&1&1&1&2\end{bmatrix}$ which is a generator matrix, investigated in CASE B when $m = 1$.

The diagram below shows that code generated by $\overline{G}_2$ is equivalent to code generated by G_3.

$$\overline{G}_2 = \begin{bmatrix}1&0&1&1&1\\0&1&1&2&2\end{bmatrix} \xrightarrow{r_2=r_2-2r_1} \begin{bmatrix}1&0&1&1&1\\3&1&4&0&0\end{bmatrix} \xrightarrow{r_2=4r_2} \begin{bmatrix}1&0&1&1&1\\2&4&1&0&0\end{bmatrix} \xrightarrow{c_2=4c_2} \begin{bmatrix}1&0&1&1&1\\2&1&1&0&0\end{bmatrix}$$

$\xrightarrow{swap(c_1,c_4)} \begin{bmatrix}1&0&1&1&1\\0&1&1&2&0\end{bmatrix}$, a matrix which is investigated above in CASE C, Subcase2. Hence code generated by $\overline{G}_2$ is equivalent to code generated by G_3.

Now using the same technique as in CASE B ($(m = 1)$, Subcase4, we can find the weight distribution of the code generated by $\overline{G}_3$, which is as follows: $A_0 = 1, A_4 = 20, A_5 = 4$.

Next we show that the codes generated by $\overline{G}_3$ and $\overline{G}_4$ are equivalent.

$$\overline{G}_3 = \begin{bmatrix}1&0&1&1&1\\0&1&1&2&3\end{bmatrix} \xrightarrow{r_2=2r_2} \begin{bmatrix}1&0&1&1&1\\0&2&2&4&1\end{bmatrix} \xrightarrow{swap(c_4,c_5)} \begin{bmatrix}1&0&1&1&1\\0&2&2&1&4\end{bmatrix} \xrightarrow{swap(c_3,c_4)} \begin{bmatrix}1&0&1&1&1\\0&2&1&2&4\end{bmatrix}$$

$$\xrightarrow{c_2=3c_2} \begin{bmatrix}1&0&1&1&1\\0&1&1&2&4\end{bmatrix} = \overline{G}_4$$

CASE D $(m = 3)$

Then $G = \begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 0 & 1 & 1 & 3 & y \end{bmatrix}$. One can easily check that each matrix of this case transforms into a matrix of CASE C, where $m = 2$. Hence matrices of this case require no further investigation.

CASE E $(m = 4)$

Here $G = \begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 0 & 1 & 1 & 4 & y \end{bmatrix}$. As in CASE D, each matrix of this case transforms into a matrix of CASE C, hence matrices of this case require no further investigation.

From the discussion above, the following theorem is obtained by us.

3. Conclusion

There exist 4 classes of non-equivalent [5, 2]-codes over *GF* (5) generated by the following four matrices:

$$G_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}, G_3 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 2 \end{bmatrix}, G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 0 \end{bmatrix}, \overline{G}_3 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \end{bmatrix}$$

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.
4. A.K.M. Toyarak Rian,P.Dey.(2015) "A Study on Equivalence of 1-Error-Correcting [5,2] Quaternary Codes", Journal of Information & Optimization Sciences, Vol 36, No 5, pp 501-510.