

Codes from the Cyclic Group of Order Three

By

M. Asifuzzaman, Kamrul Hasan,
Partha Pratim Dey
Grameenphone Ltd., Dhaka, Bangladesh
BdREN, Dhaka, Bangladesh
North South University, Dhaka, Bangladesh
tamal56@yahoo.com, kamrul@bdren.net.bd,
ppd@northsouth.edu

ABSTRACT

In this paper we use cyclic group Z_3 and its regular representation to produce a couple of linear error-correcting codes. We also discuss their duals.

Keywords

Regular representation, linear code, generator matrix, parity-check matrix

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 $x = (x_1, \dots, x_k)$ where $x_i \in F_p$ for $i = 1, \dots, k$. Let $\{g_1, g_2, g_3\}$ be an enumeration of the elements of the cyclic group Z_3 of order 3 with identity element $g_1 = 0$, $g_2 = 1$, $g_3 = 2$ and let $R(g_i)$ denote the regular representation of g_i in Z_3 using the enumeration $\{g_1, g_2, g_3\}$ to index rows and columns of the representation matrix. Then

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

$$R(g_3) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

For each g_m , $m = 1, 2, 3$ let w_{mi} be the i^{th} row of $R(g_m)$ and let $R^*(g_m)$ be the block matrix given by:

$$R^*(g_m) = \begin{bmatrix} w_{m1} & w_{m2} \\ w_{m1} & w_{m3} \end{bmatrix}.$$

Consider now the following two block matrices:

$$B_{[2,3]}^* = \begin{bmatrix} R^*(g_2) & R^*(g_3) \\ R^*(g_3) & R^*(g_2) \end{bmatrix} \text{ and}$$

$$B_{[3,2]}^* = \begin{bmatrix} R^*(g_3) & R^*(g_2) \\ R^*(g_2) & R^*(g_3) \end{bmatrix}.$$

In $B_{[2,3]}^*$, the first row of blocks is $[R^*(g_2) \ R^*(g_3)]$ and the second row is the cyclic shift of the first, whereas in $B_{[3,2]}^*$, the first row of blocks is $[R^*(g_3) \ R^*(g_2)]$ and the second row is the cyclic shift of the first. We now border each of $B_{[2,3]}^*$ and $B_{[3,2]}^*$ by a row and a column of $[R^*(g_1) \ R^*(g_1)]$ as follows to obtain:

$$M_{[2,3]} = \begin{bmatrix} R^*(g_1) & R^*(g_1) & R^*(g_1) \\ R^*(g_1) & R^*(g_2) & R^*(g_3) \\ R^*(g_1) & R^*(g_3) & R^*(g_2) \end{bmatrix}$$

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

and

$$M_{[3,2]} = \begin{bmatrix} R^*(g_1) & R^*(g_1) & R^*(g_1) \\ R^*(g_1) & R^*(g_3) & R^*(g_2) \\ R^*(g_1) & R^*(g_2) & R^*(g_3) \end{bmatrix}$$

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

Notice that swapping the 3rd row with the 5th and the 4th row with the 6th in $M_{[3,2]}$, we obtain the $M_{[2,3]}$. Hence both $M_{[2,3]}$ and $M_{[3,2]}$ comprise of the same set of rows. We can view each row of $M_{[2,3]}$ or $M_{[3,2]}$ as a row-vector of F_p^9 . Thus the row-vectors of $M_{[2,3]}$ and $M_{[3,2]}$ are identical as set. Hence the linear codes generated i.e. spanned by the row-vectors of $M_{[2,3]}$ or $M_{[3,2]}$ over F_p are identical too. Throughout the rest of the paper we will investigate this linear code over F_p for various p 's and for convenience, denote $M_{[2,3]}$ by M only.

2. M over F_p for

Various p 's

We remove the 3rd, 6th and 9th columns of $M_{[2,3]}$ to obtain the following square matrix:

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

Since $\det Q = 3^3$, the inverse of Q exists in F_p where $p \neq 3$. We use elementary row operations method to evaluate the Q^{-1} . The steps of the deduction are shown in the Appendix, whereas here below we produce the result Q^{-1} only:

$$Q^{-1} = \begin{bmatrix} 0 & \alpha & 0 & \alpha & 0 & \alpha \\ -\alpha & \alpha & -\alpha & \alpha & -\alpha & \alpha \\ 0 & \alpha & \alpha & -\alpha & -\alpha & 0 \\ -\alpha & \alpha & \alpha & 0 & 0 & -\alpha \\ 0 & \alpha & -\alpha & 0 & \alpha & -\alpha \\ -\alpha & \alpha & 0 & -\alpha & \alpha & 0 \end{bmatrix}$$

The entry α in Q^{-1} above is the inverse of 3 in F_p . Since $p \neq 3$, the inverse of 3 in F_p exists. Consider now:

$$Q^{-1}M$$

$$= \begin{bmatrix} 0 & \alpha & 0 & \alpha & 0 & \alpha \\ -\alpha & \alpha & -\alpha & \alpha & -\alpha & \alpha \\ 0 & \alpha & \alpha & -\alpha & -\alpha & 0 \\ -\alpha & \alpha & \alpha & 0 & 0 & -\alpha \\ 0 & \alpha & -\alpha & 0 & \alpha & -\alpha \\ -\alpha & \alpha & 0 & -\alpha & \alpha & 0 \end{bmatrix}.$$

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

$$= \begin{bmatrix} 3a & 0 & -3a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3a & -3a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3a & 0 & -3a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3a & -3a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3a & 0 & -3a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3a & -3a \end{bmatrix}$$

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

Thus $(1,0,-1,0,0,0,0,0,0)$ is a code-word of weight 2 of the linear code generated by the row-vectors of M over F_p with $p \neq 3$. Hence these codes do not have error-correction capabilities.

It is thus appropriate that we would like to consider the linear code generated by the row-vectors of M over F_p where $p = 3$.

Towards that goal, we gaussjordan M over F_3 to obtain:

$$\begin{bmatrix} 1 & 0 & 2 & 0 & 2 & 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \end{bmatrix}$$

which after appropriate permutation of columns becomes

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

Notice that each row of G above is a vector of F_3^{16} and the subspace spanned by its 3 rows over F_3 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].

3.Weight

Distribution of $C(G)$

We begin with a theorem.

Theorem (3.1) The code $C(G)$ has the following weight distribution.

Weight	Number of Words
0	1
9	2
6	24

Moreover each code-word of $C(G)$ but for $0_9, 1_9$ and 2_9 contains exactly three zeros, three ones and three twos.

Proof. Given $\alpha \in F_3$, let α_9 denote the row-vector $(\alpha, \dots, \alpha)$ with 9 co-ordinates each of whose co-ordinates is α . Notice that for any $c \in C(G)$,

$$c = wG = (\alpha, \beta, \gamma, 2(\beta + \gamma), 2(\alpha + \gamma), 2(\alpha + \beta), \alpha + \beta + 2\gamma, 2\alpha + \beta + \lambda, \alpha + 2\beta + \gamma)$$

for some $w = (\alpha, \beta, \gamma) \in F_3^3$. Let $\alpha = \beta = \gamma$. Then

$$c = (\alpha, \alpha, \alpha, 2 \cdot 2\alpha, 2 \cdot 2\alpha, 2 \cdot 2\alpha, 4\alpha, 4\alpha, 4\alpha)$$

$$= (\alpha, \dots, \alpha) = \alpha 1_9, \text{ giving 3 code-words: } 0_9, 1_9 \text{ and } 2_9.$$

Assume now that α, β and γ are all distinct. Without loss, let $\alpha = 0$. Then $\beta = 2\gamma, \gamma = 2\beta, \beta + \gamma = 0$ and therefore

$$c = (0, \beta, \gamma, 2 \cdot 0, 2\gamma, 2\beta, 0 + \beta + \gamma + \gamma, 0 + 0,$$

$$0 + \beta + \beta + \gamma) =$$

$$(0, \beta, \gamma, 0, \beta, \gamma, 0, \beta), \text{ Finally, let us suppose that 2 of}$$

α, β and γ are identical. Let without loss, $\alpha = \beta$ and $\gamma \neq \alpha$. Then

$$c = (\alpha, \alpha, \gamma, 2(\alpha + \gamma), 2(\alpha + \gamma), \alpha, 2(\alpha + \gamma), \gamma, \gamma).$$

Suppose $2(\alpha + \gamma) = \alpha$. Then $\alpha = \gamma$, a contradiction.

Hence $2(\alpha + \gamma) \neq \alpha$. Similarly $2(\alpha + \gamma) \neq \gamma$. Hence

$\alpha, \gamma, 2(\alpha + \gamma)$ are distinct elements of F_3 and therefore

$$c = (\alpha, \alpha, \gamma, 2(\alpha + \gamma), 2(\alpha + \gamma), \alpha, 2(\alpha + \gamma), \gamma, \gamma)$$

contains three zeros, three ones and three twos. ■

Corollary (3.2) $C(G)$ can correct 2 errors.

Proof. Since 2 is the largest integer less than half of minimum weight 6 of the code, $C(G)$ can correct 2 errors. ■

Next we show that this code $C(G)$ is in fact an 2 – error-correcting extended [9,3,6] BCH code.

Let $f(x) = x^8 - 1 \in F_3[x]$ and we choose the primitive polynomial $p(a) = a^2 + a + 2$ in $F_3[a]$. Then $F_3[a]/(p(a))$ is a finite field of order 9 and

$a, a^2, \dots, a^8$ constitute all the non-zero elements in $F_3[a]/(p(a))$. Let C be the code that results from considering the first four powers of a , namely a, a^2, a^3 and a^4 . To determine the generator polynomial $g(x)$ for C , we must find the minimum polynomials $m_1(x), m_2(x), \dots, m_4(x)$ for $a, a^2, \dots, a^4$ respectively. Since

$$x^8 - 1 = (x + 1)(x + 2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)$$

we have $m_1(x) = m_3(x) = x^2 + x + 2$,

$m_2(x) = x^2 + 1$ and $m_4(x) = x + 1$. Thus

$$g(x) = (x^2 + x + 2)(x^2 + 1)(x + 1) = 2 + x^2 + x^3 + 2x^4 + x^5$$

. Hence $C = \langle g(x) \rangle$ and generator matrix J of C is given by:

$$J = \begin{bmatrix} 2 & 0 & 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 & 1 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 & 1 & 2 & 1 \end{bmatrix}$$

$$\text{Then } J^{ext} = \begin{bmatrix} 2 & 0 & 1 & 1 & 2 & 1 & 0 & 0 & 2 \\ 0 & 2 & 0 & 1 & 1 & 2 & 1 & 0 & 2 \\ 0 & 0 & 2 & 0 & 1 & 1 & 2 & 1 & 2 \end{bmatrix}.$$

We gaussjor J^{ext} to get

$$\begin{bmatrix} 1 & 0 & 0 & 2 & 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 0 & 2 & 2 & 1 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 2 & 2 & 1 & 2 & 1 \end{bmatrix}$$

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

Theorem (3.3) $C(G)$ is the double error-correcting extended [9,3,6] BCH code generated by

$$g(x) = 2 + x^2 + x^3 + 2x^4 + x^5.$$

4 Weight Distribution of the Dual Code $C(G)^\perp$

Since $G = [I_3 : M]$ where

$$M = \begin{bmatrix} 0 & 2 & 2 & 1 & 2 & 1 \\ 2 & 0 & 2 & 1 & 1 & 2 \\ 2 & 2 & 0 & 2 & 1 & 1 \end{bmatrix},$$

we have $H = [M^tr : 2I_6]$ for the parity check matrix H of $C(G)$.

Hence

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

Notice that each row of H above is a vector of F_3^9 and the subspace spanned by its 6 rows over F_3 is a linear code $C(H)$ and H is its generator matrix. As $GH^T = 0$, $C(H) = C(G)^\perp$. We will find weight distribution of $C(H)$ from the weight distribution of $C(G)$. 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 (4.1) (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 $\{B_i\}$:

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

Let $C = C(H)$. Then $C^\perp = C(H)^\perp = C(G)$ and $B_0 = 1, B_6 = 24$, and $B_9 = 2$ by Theorem (3.1). Now taking $v = 8$ in Mac Williams equation, we obtain:

$$\sum_{j=0}^9 \binom{9-j}{8} A_j = 3^{6-8} \sum_{j=0}^9 \binom{9-j}{8-j} B_j$$

$$\text{or } \binom{9}{8} A_0 + \binom{8}{8} A_1 = \frac{1}{9} \left[\binom{9}{8} B_0 + B_6 \binom{3}{2} \right]$$

$$\text{or } 9A_0 + A_1 = \frac{1}{9} (9B_0 + 3B_6)$$

$$\text{or } 9 \cdot 1 + A_1 = \frac{1}{9} (9 \cdot 1 + 3 \cdot 24)$$

$$\therefore A_1 = 0$$

Inserting $v = 7$ again in Mac Williams equation,

$$\binom{9}{7} A_0 + \binom{7}{7} A_2 = 3^{6-7} \left[\binom{9}{7} B_0 + B_6 \binom{3}{1} \right]$$

$$\text{or } \binom{9}{7} \cdot 1 + A_2 = \frac{1}{3} \left[\binom{9}{7} \cdot 1 + 24 \cdot \binom{3}{1} \right]$$

$$\therefore A_2 = 0.$$

Similarly inserting $v = 6, 5, 4, 3, 2$ and 1 in the Mac Williams equation, we obtain:

$$A_3 = 24, A_4 = 108, A_5 = 108, A_6 = 192,$$

$$A_7 = 216, A_8 = 54.$$

Thus we have the following theorem.

Theorem (4.2) The dual code $C(G)^\perp = C(H)$ has the following weight distribution.

Weight	Number of Words
0	1
3	24
4	108
5	108
6	192
7	216
8	54
9	26

7. REFERENCES

- [1] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code", *Bell Syst. Tech. Journal*, 42 pp 79-94, 1993.
- [2] R.E., Klima, N. Sigmon and E. Stitzinger, "Applications of Abstract Algebra with MAPLE", ISBN 0-8493-8170-3, CRC Press, Boca Raton, 2000.
- [3] V. Pless, "Introduction to the Theory of Error Correcting Codes", ISBN 9814-12-688-8, Wiley Student Edition, John Wiley & Sons (Asia) Pte. Ltd., Singapore, 2003.