ORIGINAL PAPER

SOME RESULTS ON LINEAR CODES OVER THE FINITE RING $Z_4 + uZ_4 + vZ_4$; MacWilliams IDENTITIES, MDS CODES

ABDULLAH DERTLI[1], YASEMIN CENGELLENMIS[2]

Manuscript received: 30.06.2016; Accepted paper: 26.07.2016;
Published online: 30.09.2016.

Abstract. *In this paper, the MacWilliams identities for the linear codes over* $D = Z_4 + uZ_4 + vZ_4, u^2 = u, v^2 = v, uv = vu = 0$ *are studied and some properties of MDS codes over D are discussed.*

Keywords: *linear codes, finite ring, MacWilliams identities, MDS code.*

1. INTRODUCTION

One of the most important subject on coding theory is the MacWilliams identity that describes the correlation between a linear code and its dual code on the weight enumerator. It is used to determine error correcting and error detecting capabilities of code. The MacWilliams identities for the linear code over finite fields were determined in [7]. A number of papers have been published about MacWilliams identities for the linear code over some finite rings for the different type weight enumerators [1, 5, 9, 10].

As the maximum distance seperable (MDS) or optimal codes attains maximum minimum distances, the class of them is an important class of codes. These codes appear in many areas of research. At the beginning, MDS codes over finite fields were studied. But later a number of papers have been published about MDS codes over finite rings [3, 4, 6, 8].

In [2], the finite ring $D = Z_4 + uZ_4 + vZ_4$, where $u^2 = u, v^2 = v, uv = vu = 0$ was introduced, firstly. The linear codes over the ring D were studied. The Gray images of cyclic, constacyclic and quasi-cyclic codes over D were determined. The cyclic DNA codes over D were introduced. A non trivial automorphism was given. The skew cyclic, constacyclic, quasi-cyclic codes were introduced. The Gray images of them were determined. The skew cyclic DNA codes over D were introduced.

In this paper, we consider the MacWilliams identities for the linear codes over D on both Lee weight and Gray weight in section 3. In section 4, we discuss some properties of MDS codes over D.

[1] Ondokuz Mays University, Faculty of Arts and Sciences, Mathematics Department, Samsun, Turkey.
E-mail: abdullah.dertli@gmail.com.
[2] Trakya University, Faculty of Sciences, Mathematics Department, Edirne, Turkey.
E-mail: ycengellenmis@gmail.com.

2. PRELIMINARIES

In [2], the finite ring $D = Z_4 + uZ_4 + vZ_4,\ u^2 = u, v^2 = v, uv = vu = 0$ was introduced. The ring D can be also viewed as the quotient ring $Z_4[u,v]/\langle u^2 - u, v^2 - v, uv = vu\rangle$.

The ring D has the following properties;

* The finite ring D is with 64 elements.

* Any d element of D can be expressed uniquely as $d = a + ub + vc$, where $a, b, c \in Z_4$.

* The units of the ring D are

$$1,3,1+2u,1+2v,2u+3,2v+3,1+2u+2v,3+2u+2v$$

* The ring D has 26 non trivial ideals.

* The ring D is a principal ideal ring and is not a finite chain ring.

In [2], the Gray map is defined as follows

$$\Phi:\ D \to Z_4^3$$

$$a + ub + vc \ \mapsto\ (a, a+b, a+c)$$

This map is extended componentwise to

$$\Phi:\ D^n \to Z_4^{3n}$$

$$(\alpha_1, \dots, \alpha_n) \mapsto (a_1, \dots, a_n, a_1 + b_1, \dots, a_n + b_n, a_1 + c_1, \dots, a_n + c_n)$$

where $\alpha_i = a_i + ub_i + vc_i$ with $i = 1, \dots, n$. The Gray map Φ is a Z_4- module isomorphism.

The Gray weight of any $x \in D$ is defined as $w_G(x) = w_H(a, a+b, a+c)$, where w_H Hamming weight.

The Lee weight of $0,1,2,3 \in Z_4$ are defined by $w_L(0) = 0, w_H(1) = w_H(3) = 1, w_H(2) = 2$.

Let $d = a + ub + vc$ be an element of D, then Lee weight of d is defined as $w_L(d) = w_L(a, a+b, a+c)$, where $a, b, c \in Z_4$. The Lee weight of a vector $c = (c_0, \dots, c_{n-1}) \in D^n$ to be the sum of Lee weights its components. For any elements $c_1, c_2 \in D^n$, the Lee distance between c_1 and c_2 is given by $d_L(c_1, c_2) = w_L(c_1 - c_2)$. The minimum Lee distance of C is defined as $d_L(C)$ =min $d_L(c, c')$, where for any $c' \in C$, $c \neq c'$in [2]. In [2], it was shown that the Gray map Φ is distance preserving map from (D^n, Lee distance) to (Z_4^{3n}, Lee distance).

The Lee weights and the Gray weights of the elements of D is given as follows:

a	The Gray image of a	The Lee weight of a	The Gray weight of a
0	(0,0,0)	0	0
1	(1,1,1)	3	3
2	(2,2,2)	6	3
3	(3,3,3)	3	3
u	(0,1,0)	1	1
⋮	⋮	⋮	⋮

3. MACWILLIAMS IDENTITIES

The MacWilliams identity which describes how the weight enumerator of a linear code and weight enumerator of the dual code relate to each other is very important subject in coding theory. It is used to determine error detecting and error correcting capabilities of a code.

In this section, we study MacWilliams identities. Let the elements of D be represented as $D = \{g_1, g_2, \dots, g_{64}\}$.

Definition 3.1 The complete weight enumerator of a linear code C over D is defined as

$$cwe_C(X_1, \dots, X_{64}) = \sum_{\tilde{c} \in C} X_1^{n_{g_1}(\tilde{c})} \dots X_{64}^{n_{g_{64}}(\tilde{c})}$$

where $n_{g_i}(\tilde{c})$ is the number of apperance of g_i in vector $\tilde{c}$.

Definition 3.2 Define the generating character

$$\chi : D \longrightarrow \mathbb{C}^*$$

$$a + ub + vc \longmapsto \chi(a + ub + vc) = i^{a+b+c}$$

By taking $M_{i,j} = \chi(g_i g_j)$, the matrix M is constructed.

Definition 3.3 Let C be a linear code of length n over D and $C^{\perp}$ be its dual. Then

$$clwe_{C^{\perp}}(y_1, \dots, y_{64}) = \frac{1}{|C|} clwe_C(M[y_1 \dots y_{64}]^T)$$

Definition 3.4 Let C be a linear code of length n over D. The symmetrized Lee weight enumerator is defined as

$$slwe_C(x_0, x_1, \dots, x_6) = clwe_C\left(x_0, \underbrace{x_1, \dots, x_1}_{6\ times}, \underbrace{x_2, \dots, x_2}_{15\ times}, \underbrace{x_3, \dots, x_3}_{20\ times}, \underbrace{x_4, \dots, x_4}_{15\ times}, \underbrace{x_5, \dots, x_5}_{6\ times}, x_6\right)$$

where x_0 is the element of Lee weight 0, x_1 is the element of Lee weight 1, x_2 is the element of Lee weight 2, x_3 is the element of Lee weight 3, x_4 is the element of Lee weight 4, x_5 is the element of Lee weight 5, x_6 is the element of Lee weight 6.

Theorem 3.5 Let C be a linear code of length n over D. Then

$$slwe_{C^{\perp}}(x_0, x_1, \dots, x_6) = \frac{1}{|C|} slwe_C(w_1, w_2, \dots, w_7)$$

where

$$w_1 = x_0 + 6x_1 + 15x_2 + 20x_3 + 15x_4 + 6x_5 + x_6$$
$$w_2 = x_0 - 6x_1 + 15x_2 - 20x_3 + 15x_4 - 6x_5 + x_6$$
$$w_3 = x_0 + 4x_1 + 5x_2 - 5x_4 - 4x_5 - x_6$$
$$w_4 = x_0 + 2x_1 - x_2 - 4x_3 - x_4 + 2x_5 + x_6$$
$$w_5 = x_0 - 3x_2 + 3x_4 - x_6$$
$$w_6 = x_0 - 2x_1 - x_2 + 4x_3 - x_4 - 2x_5 + x_6$$
$$w_7 = x_0 - 4x_1 + 5x_2 - 5x_4 + 4x_5 - x_6$$

Theorem 3.6 Let C be a linear code of length n over D. Then

$$Lee_C(x,y) = slwe_C(x^6, x^5y, x^4y^2, x^3y^3, x^2y^4, xy^5, y^6)$$

$$Lee_{C^\perp}(x,y) = \frac{1}{|C|} Lee_C(x+y, x-y)$$

Similarly, the following is obtained for the Gray weight.

Definition 3.7 Let C be a linear code of length n over D. The symmetrized Gray weight enumerator is defined as

$$sgwe_C(s,t,q,p) = cgwe_C\left(s, \underbrace{t,\dots,t}_{9\ times}, \underbrace{q,\dots,q}_{27\ times}, , \underbrace{p,\dots,p}_{27\ times}\right)$$

where s is the element of Gray weight 0, t is the element of Gray weight 1, q is the element of Gray weight 2, p is the element of Gray weight 3.

Theorem 3.8 Let C be a linear code of length n over D. Then

$$G_C(x,y) = sgwe_C(x^3, x^2y, xy^2, y^3)$$

$$G_{C^\perp}(x,y) = \frac{1}{|C|} G_C(x+3y, x-y)$$

4. MDS CODES OVER *D*

Let C be a linear code of length n over D and d_H be the minimum Hamming distance. We have

$$|C| \leq |D|^{n-d_H+1}$$

So $d_H \leq n - \log_{|D|}|C| + 1$. This inequality is called Singleton bound. If C meet the Singleton bound, then C is called MDS code.

Lemma 4.1 Let C be a linear code of length n over Z_4, the C is a MDS code if and only if C is either Z_4^n with parameters $(n, 4^n, 1)$ or $\langle 1 \rangle$ with parameters $(n, 4, n)$ or $\langle 1 \rangle^\perp$ with parameters $(n, 4^{n-1}, 2)$, where 1 denote the all 1 vectors [6].

Let C be a linear code of length n over D. Then

$$C = (1-u-v)C_1 \oplus uC_2 \oplus vC_3$$

where C_i is a linear code of length n over Z_4, for $1 \leq i \leq 3$, [2].

Let d_H be the Hamming distance of C. Then $d_H = \min\{d_{H_i}\}$ for $1 \leq i \leq 3$, where d_{H_i} is Hamming distance of C_i. Thus the Singleton bound can be written as

$$d_H \leq n - \frac{1}{3}\sum_{i=1}^{3} \log_4|C_i| + 1$$

since $d_H \leq n - \log_{|D|}|C| + 1$.

Lemma 4.2 Let C be a MDS codes over D.
If $d_H = 1$, then all of C_i are MDS codes with parameters $(n, 4^n, 1)$.
If $d_H = 2$, then all of C_i are MDS codes with parameters $(n, 4^{n-1}, 2)$.

Proof:
(i) If $d_H = 1$, $\sum_{i=1}^{3} \log_4|C_i| = 3n$, since C is a MDS code over D. But $|C_i| \leq 4^n$, then the identity is true iff $|C_i| = 4^n$. Therefore C is a $(n, 4^{3n}, 1)$ MDS code iff all of C_i are $(n, 4^n, 1)$ MDS codes.
(ii) If $d_H = 2$, then $\sum_{i=1}^{3} \log_4|C_i| = 3(n-1)$. Since $d_H = \min\{d_{H_1}, d_{H_2}, d_{H_3}\}$, then $d_{H_i} \geq 2$, for $1 \leq i \leq 3$. By using Singleton bound of code over Z_4, we get $|C_i| \leq 4^{n-d_{H_i}+1}$. For all i, since $d_{H_i} \geq 2$, we have $4^{n-d_{H_i}+1} \leq 4^{n-1}$. Then we have all of C_i are $(n, 4^{n-1}, 2)$.

Theorem 4.3 If C is a MDS codes over D. Then there is at least one C_i, $1 \leq i \leq 3$, be MDS code.

Proof: Suppose that none of C_i is MDS code, then $d_{H_i} < n - \log_4|C_i| + 1$. Since $d_H = \min\{d_{H_1}, d_{H_2}, d_{H_3}\}$, then $d_H < n - \log_4|C_i| + 1$. But we know that $d_H < n - \frac{1}{3}\sum_{i=1}^{3} \log_4|C_i| + 1$. So this is contradiction.

Theorem 4.4 If C is a MDS codes over D and there exist two MDS code of C_i, $1 \leq i \leq 3$, then the other C_i must be MDS code and all C_i with same parameters.

Proof: Let C_1 and C_2 be MDS codes, without loss of generality. So $d_{H_i} = n - \log_4|C_i| + 1$ for $1 \leq i \leq 2$. Since C is a MDS code over D, then $d_H = n - \frac{1}{3}\sum_{i=1}^{3} \log_4|C_i| + 1$. So $3dH = 3n - \sum_{i=1}^{3} \log 4Ci + 3$. Since $dH1 + dH2 = 2n - \log 4C1 + \log 4C2 + 2$, we have

$$3d_H - \sum_{i=1}^{2} d_{H_i} = n - \log_4|C_3| + 1 \geq d_{H_3}$$

So $3d_H \geq \sum_{i=1}^{3} d_{H_i}$. Since $d_H = \min\{d_{H_1}, d_{H_2}, d_{H_3}\}$, then $d_H = d_{H_1} = d_{H_2} = d_{H_3}$.

Theorem 4.5 If C is a MDS codes over D and C_1 is a MDS code with parameters $(n, 4, n)$. Then C_2, C_3 are also MDS codes with parameters $(n, 4, n)$.

Proof: Since C is a MDS codes over D and C_1 is a MDS code with parameters $(n, 4, n)$, then $d_H \geq 3$ and we have

$$3d_H = 3n - (\log_4 4 + \log_4|C_2| + \log_4|C_3|) + 3$$

So $\log_4|C_2||C_3| = 3n - 3d_H + 2$.

Let C_2 and C_3 be not MDS codes. So, $|C_i| < 4^{n-d_{H_i}+1}$ for $i = 2,3$. For $d_{H_2} \geq d_H$, $d_{H_3} \geq d_H$, we have $|C_i| \leq 4^{n-d_H+1}$ for $i = 2,3$. By using this, we have $|C_2||C_3| < 4^{2n-2d_H+2}$. Therefore $\log_4|C_2||C_3| < 2n - 2d_H + 2$. From $3n - 3d_H + 2 < 2n - 2d_H + 2$, we have $d_H \geq n$. So $d_H = n$.

From $\log_4|C_2||C_3| = 3n - 3d_H + 2$, we have $\log_4|C_2||C_3| = 2$. Since $|C_i| \leq 4^{n-d_H+1} = 4$ for $i = 2,3$, the equality is true if and only if $|C_i| = 4$ for $i = 2,3$. Then C_i has the same parameters for $i = 2,3$.

Corollary 4.6 C is a MDS codes over D if and only if all of C_i for $i = 1,2,3$ are MDS codes over Z_4 with same parameters.

5. CONCLUSION

In this paper, the MacWilliams identities for the linear codes over $D = Z_4 + uZ_4 + vZ_4$, $u^2 = u, v^2 = v, uv = vu = 0$ were obtained and some properties of MDS codes over D were determined.

REFERENCES

[1] Bandi, R.K., Bhaintwal, M., Codes over $Z_4 + vZ_4$, *Proceedings of Advances in Computing, Communications and Informatics* (ICACCI, 2014), 422, 2014.
[2] Dertli A., Cengellenmis Y., On the codes over the ring $Z_4 + uZ_4 + vZ_4$ cyclic, constacyclic, quasi-cyclic codes, their skew codes, cyclic DNA and skew cyclic DNA codes, *Journal of Science*, to be submitted.
[3] Dougherty, S. T., Shiromoto, K., *IEEE Trans. Inform. Theory*, **46**, 265, 2000.
[4] Dougherty, S.T., Shiromoto, K., *IEEE Trans. Inform. Theory*, **47**, 400, 2001.
[5] Gao J., Gao Y., Some Results on Linear Codes over $Z_4 + vZ_4$, arXiv:1402.6771v1, 2014.
[6] Li, P., Guo, X., Zhu, S., Some results of linear codes over the ring $Z_4 + uZ_4 + vZ_4 + uvZ_4$, arXiv:1601.04453v1, 2016.
[7] MacWilliams, F.J., Sloane, N.J.A., *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, Netherlands, 1977.
[8] Shiromoto, K., *Journal of Algebraic Combinatorics*, **12**, 95, 2000.
[9] Wood, J., *Amer. J. Math.*, **121**, 555, 1993.
[10] Yildiz, B., Karadeniz, S., *Finite fields and their applications*, **27**, 24, 2014.