

MACWILLIAMS IDENTITIES OF LINEAR CODES OVER THE RING

$$\frac{\mathbb{Z}_4[u]}{\langle u^2 - 1 \rangle}$$

Mehmet ÖZEN and Fatma Zehra UZEKMEK

Department of Mathematics, Sakarya University, Turkey

ozen@sakarya.edu.tr, zehra.uzekmek@hotmail.com

Abstract: Linear codes are considered over the ring $\frac{\mathbb{Z}_4[u]}{\langle u^2 - 1 \rangle}$. The Lee weight enumerators, the complete weight enumerators and the symmetrized weight enumerators for the linear codes over the ring $R = \frac{\mathbb{Z}_4[u]}{\langle u^2 - 1 \rangle}$ are defined and Gray map Φ from $R \rightarrow \mathbb{Z}_4$ is constructed. Then, MacWilliams identities for these weight enumerators are proved.

Keywords: Weight enumerator, MacWilliams identities

Introduction and Motivation

Attracted the attention of many coding theory researchers in the last two decades are codes over rings. So, codes over the ring have been a common research topic in coding theory. The interest in codes over rings started with the seminal work in 1994 (Hammons, Kumar, Calderbank, Sloane and Sole) and expanded in many directions. Because decoding algorithm is more quickly, linear codes are more useful than other codes, especially. So, linear codes are an important and intensely studied class of codes. Another research topic in coding theory is MacWilliams identity which relates the weight enumerator of linear code to the weight enumerator of its dual code. Yildiz and Karadeniz analysed for MacWilliams identity, projections and formally self dual codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ in the linear codes. Consequently, they found optimal code. Using Gray map, R. Bandi and M. Baintwal determined MacWilliams identity for Lee and Gray enumerator over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $v^2 = v$. There is a connection between \mathbb{Z}_4 and $F_2 + uF_2$ which has generated a lot of among coding researchers starting with Dougherty, Gaborit, Harada and Sole's work in 1999. Considered by this similiarity (and difference) between two

rings and Yildiz and Karadeniz's works at references, we study codes over the ring $\frac{\mathbb{Z}_4[u]}{\langle u^2 - 1 \rangle}$. In 2006, Yu and Zhu investigated MacWilliams identity over the ring $F_2 + uF_2$. In Yildiz and Karadeniz's article (2010), the researchers discussed the linear codes over $F_2 + uF_2 + vF_2 + uvF_2$, as well as MacWilliams identity for the complete and Lee weight enumerator over the ring. In 2015, J. Gao studied linear codes over the ring $F_p + uF_p + u^2F_p$, where p is an odd prime and also defined Gray map and MacWilliams identity of linear codes.

In this article, mainly focused on $\mathbb{Z}_4 + \mathbb{Z}_4$, where $u^2 = 1$. In Section II, we are considered linear codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 = \{b + (a-b)u \mid a, b \in \mathbb{Z}_4\}$, where $u^2 = 1$, we define linear Gray maps from $\mathbb{Z}_4 + u\mathbb{Z}_4$ to \mathbb{Z}_4^{2n} and we give definitions of Lee distance and dual code of linear code. In Section III, we have studied complete, symmetrized and Lee weight enumerators and proved MacWilliams identity for all the weight enumerators involved.

Lee Weight and Gray Map of Linear Codes Over the Ring $\frac{\mathbb{Z}_4[u]}{\langle u^2-1 \rangle}$

Definition 1 A linear code C of length n over $R = \frac{\mathbb{Z}_4[u]}{\langle u^2-1 \rangle}$ is an R -submodule of R^n . Elements of C are called codewords.

Definition 2 For any $z = b + (a-b)u \in R$ and $a, b \in \mathbb{Z}_4$, we define the Gray map $\phi: R \rightarrow \mathbb{Z}_4^2$ by $\phi(z) = (b, a+b)$.

Definition 3 The Lee weight $w_L(z)$ of $z \in \mathbb{Z}_4$ is $\min\{x, 4-x\}$. The Lee weight of a vector in $v \in \mathbb{Z}_4^n$ is then defined as the rational sum of the Lee weight of its coordinates. So, we can define the Lee weights of an element of $z = b + (a-b)u \in R$ as $w_L(z) = w_L(b + (a-b)u) = w_L((b, a+b))$. For any $z_1, z_2 \in R^n$, the Lee distance is given by $d_L(z_1, z_2) = w_L(z_1 - z_2)$.

The minimum Lee Distance of C is defined by $d_L(C) = \min_{\substack{c_1, c_2 \in C \\ c_1 \neq c_2}} d_L(c_1, c_2)$ and the minimum Lee weight of C

is defined by $w_L(C) = \min_{\substack{c_1, c_2 \in C \\ c_1 \neq c_2}} w_L(c_1, c_2)$. So, if C is a linear code, then the minimum Lee weight is equal to minimum Lee distance.

Theorem 4 The map ϕ is a distance preserving linear isometry from R^n to \mathbb{Z}_4^{2n} with Lee weight.

Corollary 5 If C is linear code over R of length n , then $\phi(C)$ linear code over \mathbb{Z}_4 of length $2n$.

Definition 6 For $x = (x_1, x_2, \dots, x_{n-1})$, $y = (y_1, y_2, \dots, y_{n-1}) \in R^n$, the Euclidean inner product on R^n by defining

$$\langle (x_0, x_1, \dots, x_{n-1}), (y_0, y_1, \dots, y_{n-1}) \rangle = x_0 y_0 + x_1 y_1 + \dots + x_{n-1} y_{n-1}$$

where the operations are performed in $\mathbb{Z}_4 + u\mathbb{Z}_4$.

Definition 7 Let C be a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length n . Then, the dual code of C is defined as follow:

$$C^\perp = \{x \in R^n : \langle x, y \rangle = 0, \forall y \in C\}$$

Weight Enumerators and MacWilliams Identities

3.1 The Complete Weight Enumerators and MacWilliams Identities

$\mathbb{Z}_4 + u\mathbb{Z}_4 = \{s_1, s_2, \dots, s_{16}\}$ be given as

$$\mathbb{Z}_4 + u\mathbb{Z}_4 = \{0, u, 2u, 3u, 1, 1+u, 1+2u, 1+3u, 2, 2+u, 2+2u, 2+3u, 3, 3+u, 3+2u, 3+3u\}.$$

Definition 8 Let $n_{s_i}(\bar{c})$ be the number of $s_i(\bar{c})$ in the vector \bar{c} . The complete weight enumerator of a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ is defined as

$$cwe_C(x_1, x_2, \dots, x_{16}) = \sum_{c \in C} \left(x_1^{n_{s_1}(c)} x_2^{n_{s_2}(c)} \dots x_{16}^{n_{s_{16}}(c)} \right).$$

Because $\mathbb{Z}_4 + u\mathbb{Z}_4$ is a Frobenius ring, the MacWilliams identities for the complete weight enumerator is preserved. Now we define the character on $\mathbb{Z}_4 + u\mathbb{Z}_4$ to find the exact identities.

Definition 9 Define $\chi: \mathbb{Z}_4 + u\mathbb{Z}_4 \rightarrow \mathbb{C}^\times$ by $\chi(b + (a-b)u) = i^{a+b}$. Let the 16×16 matrix is T , by giving $T(i, j) = \chi(s_i \cdot s_j)$. Then, T is defined as follows:

$$T = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & i & -i & i & -i & -1 & 1 & -1 & 1 & -i & i & -i & i \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -i & i & -i & i & -1 & 1 & -1 & 1 & i & -i & i & -i \\ 1 & i & -1 & -i & -1 & -i & 1 & i & 1 & i & -1 & -i & -1 & -i & 1 & i \\ 1 & -i & -1 & i & -i & -1 & i & 1 & -1 & i & 1 & -i & i & 1 & -i & -1 \\ 1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & -i & -1 & i & i & 1 & -i & -1 & -1 & i & 1 & -i & -i & -1 & i & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & i & i & i & i & -1 & -1 & -1 & -1 & -i & -i & -i & -i \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -i & -i & -i & -i & -1 & -1 & -1 & -1 & i & i & i & i \\ 1 & -i & -1 & i & -1 & i & 1 & -i & 1 & -i & -1 & i & -1 & i & 1 & -i \\ 1 & i & -1 & -i & -i & 1 & i & -1 & -1 & -i & 1 & i & i & -1 & -i & 1 \\ 1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & i & -1 & -i & i & -1 & -i & 1 & -1 & -i & 1 & i & -i & 1 & i & -1 \end{bmatrix}$$

Theorem 10 Let C is a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length n and C^\perp is a dual code of C .

$$cwe_{C^\perp}(x_1, x_2, \dots, x_{16}) = \frac{1}{|C|} cwe_C(T \cdot (x_1, x_2, \dots, x_{16})^t)$$

where T is the $|R| \times |R|$ matrix and $T(i, j) = \chi(s_i \cdot s_j)$.

(Here $()^t$ denotes the transpose.)

3.2 The Symmetrized Weight Enumerator and Lee Weight Enumerator

Fistly, we define the Lee weights of the elements of $\mathbb{Z}_4 + u\mathbb{Z}_4$.

Tablo 3.1: $\mathbb{Z}_4 + u\mathbb{Z}_4$ teki elemanların Lee ağırlıkları

d	d nin Lee Ağırlığı	Değişken Karşılıkları
0	0	X_1
u	1	X_2
$2u$	2	X_3
$3u$	1	X_4
1	3	X_5
$1 + u$	2	X_6
$1 + 2u$	1	X_7
$1 + 3u$	2	X_8
2	2	X_9
$2 + u$	3	X_{10}
$2 + 2u$	4	X_{11}
$2 + 3u$	3	X_{12}
3	3	X_{13}
$3 + u$	2	X_{14}
$3 + 2u$	1	X_{15}
$3 + 3u$	2	X_{16}

Now we can define the symmetrized weight enumerator as follow:

Definition 11 Let C be a linear code of length n over $\mathbb{Z}_4 + u\mathbb{Z}_4$. Then, the symmetrized weight enumerator of C as

$$swe_c(X, Y, Z, W, S) = cwe_c(X, Y, Z, Y, W, Z, Y, Z, Z, W, S, W, W, Z, Y, Z).$$

Here X represents the element have weight 0, Y represents the element have weight 1, Z represents the element have weight 2, W represents the element have weight 3, S represents the element have weight 4.

Theorem 12 Let C be a linear code of length n over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and let C^\perp be its dual. Then, we have

$$swe_{c^\perp}(X, Y, Z, W, S) = \frac{1}{|C|} \cdot swe(X + 4Y + 4W + 6Z + S, X - 2Y + 2W - S, X - 2Z + S, X + 2Y - 2W - S, X - 4Y + 6Z - 4W + S)$$

Definition 13 Let C be a linear code of length n over \mathbb{Z}_4 . Then, the Lee weight enumerator of C is defined as follow:

$$Lee_c(Y, X) = \sum_{\bar{c} \in C} Y^{4n-w_L(\bar{c})} X^{w_L(\bar{c})}$$

Definition 14 Let C be a linear code of length n over $\mathbb{Z}_4 + u\mathbb{Z}_4$. Then,

$$Lee_c(Y, X) = swe_c(Y^4, Y^3X, Y^2X^2, YX^3, X^4).$$

Lee weight and n of C is defined as follow:

$$1) w_L(c) = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4$$

$$2) n = \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$$

Here α_i is the number of weight i , where $i = 0, 1, 2, 3, 4$.

Theorem 15 Let C be a linear code of length n over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and let C^\perp be its dual. Then,

$$Lee_{C^\perp}(Y, X) = \frac{1}{|C|} \cdot Lee_C(Y + X, Y - X).$$

Conclusions

In this paper we searched linear codes over the ring $\frac{\mathbb{Z}_4[u]}{\langle u^2 - 1 \rangle}$. Lee weights, Gray maps and all weight enumerators for these codes are defined and MacWilliams identities for the complete, symmetrized and Lee weight enumerators proved.

References

- S.T. Dougherty, P. Gaborit, M. Harada & P. Sole (1999). Type II Codes over $F_2 + uF_2$, IEEE Trans. Inform. Theory, 45, 32-45.
- B. Yildiz & S. Karadeniz (2014). Linear Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$: Macwilliams Identities, Projections and Formally Self-Dual Codes, Finite Fields Appl., 27, 24-40.
- Yu H. & Zhu S. (2006). Identities of linear codes and their Codes over $F_2 + uF_2$, Journal of University of Science and Technology of China, 36 (12): 1285-1288.
- R.K. Bandi & M. Baintwal, Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, IEEE.
- B. Yildiz & S. Karadeniz (2010). Linear Codes over $F_2 + uF_2 + vF_2 + uvF_2$, Des. Codes Crypt., 54: 61-81.
- J. Gao (2015). Some Results on Linear Codes over $F_p + uF_p + u^2F_p$, J. Appl. Math. Comput., 47:473-485.
- A.R. Hammons, P.V/ Kumar, A.R. Calderbank, N.J.A. Sloane & P. Sole (1994). The \mathbb{Z}_4 Linearity of Kerdock, Preparata, Goethals and Related Codes, IEEE Transactions on Information Theory, Vol. 40, No.2, pp. 301-319.