Nihonkai Math. J.
Vol.30(2019), 31–40

NOTE ON E-POLYNOMIALS ASSOCIATED TO $\mathbb{Z}_4$-CODES

NUR HAMID

ABSTRACT. The invariant theory of finite groups can connect the coding theory to the number theory. In this paper, under this conformity, we obtain the minimal generators of the rings of E-polynomials constructed from the groups related to $\mathbb{Z}_4$-codes. In addition, we determine the generators of the invariant rings appearing by E-Polynomials and complete weight enumerators of Type II $\mathbb{Z}_4$-codes.

1. Introduction

Our study is inspired by the idea of Motomura and Oura [6]. In their paper, they introduced the E-polynomials associated to the $\mathbb{Z}_4$-codes. They determined both the ring and the field structures generated by that E-polynomials. E-polynomials associated to the binary codes were investigated in a previously conducted study (see [7]). In the present paper, we deal with $\mathbb{Z}_4$-codes. Then, we define an E-polynomial with respect to the complete weight enumerator of $\mathbb{Z}_4$-codes and show that the ring generated by them is minimally generated by E-polynomials of the following weights:

$$8, 16, 24, 32, 40, 48, 56, 64, 72, 80.$$

It seems that the ring generated by E-polynomials is not sufficient to generate the invariant ring for the finite group G^8 defined in the next section. By combining the E-polynomials and the complete weight enumerators of $\mathbb{Z}_4$-codes, we present the generators of that invariant ring.

We denote by $\mathbb{C}$ the field of complex number as usual. Let A_w be a finite-dimensional vector space over $\mathbb{C}$. We write the dimension formula of A by the formal series

$$\sum_{w=0}^{\infty} (\dim A_w) t^w.$$

2010 *Mathematics Subject Classification.* Primary 11T71; Secondary 11T06.
Key words and phrases. E-polynomial, $\mathbf{Z}_4$-code.

For the dimension formulas and the basic theory of E-polynomials used herein, we refer to references [1] and [6]. For the computations, we use Magma [3] and SageMath [9]. The generator matrices of the groups and the codes used can be found in [5].

2. Preliminaries

We denote a primitive 8-th root of unity by η_8. Following the notation used in [1], let G be a finite matrix group generated by

$$\frac{\eta_8}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

and diag $[1, \eta_8, -1, \eta_8]$. Let G^8 be a matrix group generated by G and diag $[\eta_8, \eta_8, \eta_8, \eta_8]$. The group G is of order 384, whereas G^8 is of order 1536. We denote by $\mathfrak{R}$ and $\mathfrak{R}^8$ the invariant rings of G and G^8, respectively:

$$\mathfrak{R} = \mathbf{C}[t_0, t_1, t_2, t_3]^G,$$

$$\mathfrak{R}^8 = \mathbf{C}[t_0, t_1, t_2, t_3]^{G^8}$$

under an action of such matrices on the polynomial ring of four variables t_0, t_1, t_2, and t_3. The dimension formulas of $\mathfrak{R}$ and $\mathfrak{R}^8$ are given as follows:

$$\sum_w (\dim \mathfrak{R}_w)\, t^w = \frac{1 + t^8 + 2t^{10} + 2t^{12} + 2t^{14} + 2t^{16} + t^{18} + t^{20} + t^{22} + t^{26} + t^{28} + t^{30}}{(1-t^8)^3 (1-t^{12})},$$

$$\sum_w \left(\dim \mathfrak{R}^8_w\right) t^w = \frac{1 + t^8 + 2\,t^{16} + 2\,t^{24} + t^{32} + t^{40}}{(1-t^8)^3 (1-t^{24})}.$$

In the next section, we present a fundamental theory of codes that can help us obtain the generators of ring $\mathfrak{R}^8$.

3. Codes

A code C over $\mathbb{Z}_4$ of length n, called $\mathbb{Z}_4$-code, is an additive subgroup of $\mathbb{Z}_4^n$. The inner product of two elements $a, b \in C$ on $\mathbb{Z}_4^n$ is given by

$$(a, b) = a_1 b_1 + a_2 b_2 + \dots + a_n b_n \mod 4$$

where $a = (a_1, a_2, \dots, a_n)$ and $b = (b_1, b_2, \dots, b_n)$. The dual of C is code $C^\perp$ satisfying

$$C^\perp = \{y \in \mathbb{Z}_4^n | (x, y) \equiv 0 \mod 4, \forall x \in C\}.$$

We say that C is self-orthogonal if $C \subset C^{\perp}$ and self-dual if $C = C^{\perp}$. A code C is called *Type II* if it is self-dual and satisfies

$$(x, x) \equiv 0 \mod 8$$

for all $x \in C$. Type II $\mathbb{Z}_4$-code can only exist when its length is multiple of 8.

There are several types of weight enumerators associated with a $\mathbb{Z}_4$-code. In this paper, we deal with complete weight enumerators.

The *complete weight enumerator* (CW) of a $\mathbb{Z}_4$-code C is defined by

$$CW_C(t_0, t_1, t_2, t_3) = \sum_{c \in C} t_0^{n_0(c)} t_1^{n_1(c)} t_2^{n_2(c)} t_3^{n_4(c)}$$

where $n_i(c)$ denotes the number of c components which are equivalent to i modulo 4. For every Type II $\mathbb{Z}_4$-code, $CW_C(t_0, t_1, t_2, t_3)$ is G^8-invariant (see [2]). From the dimension formula of $\mathfrak{R}^8$, we have the following proposition.

Proposition 3.1. *The invariant ring $\mathfrak{R}^8$ can be generated by the set of complete weight enumerators of Type II $\mathbb{Z}_4$-codes consisting of at most*

4 codes of length 8,
2 codes of length 16,
3 codes of length 24,
1 code of length 32,
1 code of length 40.

We denote by $p_{8a}, p_{8b}, o_8, k_8, p_{16a}, p_{16b}, q_{24a}, q_{24b}, g_{24}, q_{32}$ the complete weight enumerators of some codes. The numbers written as subscript denote the degree of each polynomial. The codes o_8, k_8, and g_{24} are known as octacode, Klemm code, and Golay code, respectively. The generator matrices of the complete weight enumerators which are denoted by p are taken from [8]. We give the generator matrices of other complete weight enumerators in Appendix 5.2. The following are the explicit forms of some complete weight enumerators:

$$\begin{aligned}
p_{8a} &= t_0^8 + 4t_0^3t_1^4t_2 + 12t_0^6t_2^2 + 4t_0t_1^4t_2^3 + 38t_0^4t_2^4 + 12t_0^2t_2^6 + t_2^8 + 4t_1^7t_3 + 16t_0^3t_1^3t_2t_3 \\
&\quad + 16t_0t_1^3t_2^3t_3 + 24t_0^3t_1^2t_2t_3^2 + 24t_0t_1^2t_2^3t_3^2 + 28t_1^5t_3^3 + 16t_0^3t_1t_2t_3^3 + 16t_0t_1t_2^3t_3^3 \\
&\quad + 4t_0^3t_2t_3^4 + 4t_0t_2^3t_3^4 + 28t_1^3t_3^5 + 4t_1t_3^7, \\
p_{8b} &= t_0^8 + 8t_0^3t_1^4t_2 + 12t_0^6t_2^2 + 8t_0t_1^4t_2^3 + 38t_0^4t_2^4 + 12t_0^2t_2^6 + t_2^8 + 16t_1^6t_3^2 + 48t_0^3t_1^2t_2t_3^2 \\
&\quad + 48t_0t_1^2t_2^3t_3^2 + 32t_1^4t_3^4 + 8t_0^3t_2t_3^4 + 8t_0t_2^3t_3^4 + 16t_1^2t_3^6, \\
k_8 &= t_0^8 + t_1^8 + 28t_0^6t_2^2 + 70t_0^4t_2^4 + 28t_0^2t_2^6 + t_2^8 + 28t_1^6t_3^2 + 70t_1^4t_3^4 + 28t_1^2t_3^6 + t_3^8, \\
o_8 &= t_0^8 + t_1^8 + 14t_0^4t_2^4 + t_2^8 + 56t_0^3t_1^3t_2t_3 + 56t_0t_1^3t_2^3t_3 + 56t_0^3t_1t_2t_3^3 + 56t_0t_1t_2^3t_3^3 \\
&\quad + 14t_1^4t_3^4 + t_3^8, \\
p_{16a} &= t_0^{16} + 30t_0^8t_1^8 + t_1^{16} + 140t_0^{12}t_2^4 + 420t_0^4t_1^8t_2^4 + 448t_0^{10}t_2^6 + 870t_0^8t_2^8 + 30t_1^8t_2^8 \\
&\quad + 448t_0^6t_2^{10} + 140t_0^4t_2^{12} + t_2^{16} + 3360t_0^6t_1^6t_2^2t_3^2 + 6720t_0^4t_1^6t_2^4t_3^2 + 3360t_0^2t_1^6t_2^6t_3^2 \\
&\quad + 420t_0^8t_1^4t_3^4 + 140t_1^{12}t_3^4 + 6720t_0^6t_1^4t_2^2t_3^4 + 19320t_0^4t_1^4t_2^4t_3^4 + 6720t_0^2t_1^4t_2^6t_3^4 \\
&\quad + 420t_1^4t_2^8t_3^4 + 448t_1^{10}t_3^6 + 3360t_0^6t_1^2t_2^2t_3^6 + 6720t_0^4t_1^2t_2^4t_3^6 + 3360t_0^2t_1^2t_2^6t_3^6 \\
&\quad + 30t_0^8t_3^8 + 870t_1^8t_3^8 + 420t_0^4t_2^4t_3^8 + 30t_2^8t_3^8 + 448t_1^6t_3^{10} + 140t_1^4t_3^{12} + t_3^{16}.
\end{aligned}$$

Since other weight enumerators are too large, we do not write them.

Let $\mathfrak{W}$ be a ring generated by the complete weight enumerators aforementioned:

$$\mathfrak{W} = \mathbb{C}[p_{8a}, p_{8b}, o_8, k_8, p_{16a}, p_{16b}, q_{24a}, q_{24b}, g_{24}, q_{32}].$$

By obtaining the dimension of $\mathfrak{W}$, we have the following result.

Theorem 3.1. *The invariant ring $\mathfrak{R}^8$ can be generated by $\mathfrak{W}$.*

Proof. By Proposition 3.1, we generate $\mathfrak{W}$ by utilizing some complete weight enumerators of non-equivalent codes. Then, we compute the dimension of $\mathfrak{W}$. The dimension of each $\mathfrak{W}_k$ is shown in Table 1. This completes the proof of Theorem 3.1. □

TABLE 1. The dimensions of $\mathfrak{R}^8_k$ and $\mathfrak{W}_k$

k	8	16	24	32	40
$\dim\mathfrak{R}^8_k$	4	11	25	48	83
$\dim\mathfrak{W}$	4	11	25	48	83

It is noteworthy that we do not need to use the code of length 40. On the next section, we shall give the generators of $\mathfrak{R}^8$ by the weight enumerators of Type II $\mathbb{Z}_4$-codes and E-polynomials.

4. E-Polynomials

Let $\mathbf{t}$ be a column vector that comprises the following: t_0, t_1, t_2, and t_3. An E-polynomial of weight k for G is defined by

$$\varphi_k^G = \varphi_k^G(\mathbf{t}) = \frac{1}{|G|}\sum_{\sigma\in G}(\sigma_0\mathbf{t})^k = \frac{|K|}{|G|}\sum_{K\backslash G\ni\sigma}(\sigma_0\mathbf{t})^k$$

where

$$K = \{\begin{pmatrix} 1 & 0 & 0 & 0 \\ \star & \star & \star & \star \\ \star & \star & \star & \star \\ \star & \star & \star & \star \end{pmatrix} \in G\}$$

and σ_0 is the first row of σ. We apply the same definition for G^8. The subgroup K of G is of order 8 and K^8 of G^8 is of order 16. For simplicity, we denote by φ_k without specifying the group. We denote by $\mathfrak{E}$ and $\mathfrak{E}^8$ the rings generated by φ_k's for the groups G and G^8, respectively.

Denote by κ the cardinality of $K\backslash G$. For clarity, we write κ_G instead of κ by including the group objected. It is clear that $\kappa_G = 48$ and $\kappa_{G^8} = 96$.

Theorem 4.1. *(1) The ring $\mathfrak{E}$ is generated by φ_k where*

$$k \equiv 0 \mod 4, \quad 8 \le k \le 48.$$

(2) The ring $\mathfrak{E}^8$ is generated by φ_k where

$$k \equiv 0 \mod 8, \quad 8 \le k \le 96.$$

Proof. (1) For each representative σ_i of $K\backslash G$ $(1 \le i \le \kappa)$, let $x_i = \sigma_i'\mathbf{t}$, where σ_i' is the first row of σ_i. Then, every φ_i can be expressed in $\mathbb{C}[x_1, \ldots, x_\kappa]$. By the fundamental theorem of symmetric polynomials, every φ_i can be written uniquely in $\varepsilon_i, \ldots, \varepsilon_\kappa \in \mathbb{C}[x_1, \ldots, x_\kappa]$ where

$$\varepsilon_r = \sum_{i_1<i_2<\ldots<i_r} x_{i_1}x_{i_2}\ldots x_{i_r}, \quad (1 \le r \le \kappa).$$

We mention that φ_4=0. This completes the proof.

(2) The proof follows similarly that of Theorem 4.1 (1). □

Theorem 4.1 informs us that the rings $\mathfrak{E}$ and $\mathfrak{E}^8$ are finitely generated. Hence, we can find their minimal generators. In the next theorem, we determine the generators of both $\mathfrak{E}$ and $\mathfrak{E}^8$.

Theorem 4.2. *(1) $\mathfrak{E}$ is minimally generated by the E-polynomials of weights*

$$8, 12, 16, 20, 24, 28, 32, 40, 48.$$

TABLE 2. The dimensions of $\mathfrak{R}_k$ and $\mathfrak{E}_k$

k	8	12	16	20	24	28	32	36	40	44	48
$\dim \mathfrak{R}_k$	4	3	16	11	25	27	48	54	83	94	133
$\dim \mathfrak{E}_k$	1	1	2	2	4	4	4	7	7	10	18

TABLE 3. The dimensions of $\mathfrak{R}_k^8$ and $\mathfrak{E}_k^8$

k	8	16	24	32	40	48	56	64	72	80	88	96
$\dim \mathfrak{R}_k^8$	4	11	25	48	83	133	200	287	397	532	695	889
$\dim \mathfrak{E}_k^8$	1	2	3	5	7	11	15	22	30	42	52	61

(2) $\mathfrak{E}^8$ is minimally generated by the E-polynomials of weights

$$8, 16, 24, 32, 40, 48, 56, 64, 72, 80.$$

Proof. For each k, we construct the rings $\mathfrak{E}_k$ and $\mathfrak{E}_k^8$. Then, we determine whether φ_k is generator or not. The dimensions of each $\mathfrak{E}$ and $\mathfrak{E}^8$ are demonstrated in Tables 2 and 3. This completes the proof of Theorem 4.2.

Now, we obtain the relation between $\mathfrak{E}^8$ and $\mathfrak{R}^8$. From Table 3, we observe that the ring $\mathfrak{E}^8$ is not sufficient to generate $\mathfrak{R}^8$. By combining $\mathfrak{R}^8$ and $\mathfrak{W}$, we have the following theorem.

Theorem 4.3. *The invariant ring $\mathfrak{R}^8$ can be generated by $\mathfrak{E}^8$ and the complete weight enumerators*

$$p_8, o_8, k_8, p_{16}, p_{24}, q_{24}, p_{32}.$$

More specifically, the set

$$\{\varphi_k, p_8, o_8, k_8, p_{16}, p_{24}, q_{24}, p_{32} \quad | \quad k = 8, 16, 24\}$$

generates ring $\mathfrak{R}^8$.

Proof. Denote by $\widetilde{\mathfrak{R}}$ the polynomial generated by $\mathfrak{E}^8$ and the complete weight enumerators aforementioned. Then we construct $\widetilde{\mathfrak{R}}_k$ for $k \equiv 0 \mod 8$ and $8 \leq k \leq 96$. It follows that each φ_k for $k \neq 8, 16, 24$ is linearly dependent. We compute the dimension of each $\widetilde{\mathfrak{R}}_k$ and write the results in Table 4. This completes the proof. □

TABLE 4. The dimensions of $\mathfrak{R}_k^8$ and $\widetilde{\mathfrak{R}}_k$

k	8	16	24	32	40
$\dim \mathfrak{R}_k^8$	4	11	25	48	83
$\dim \widetilde{\mathfrak{R}}_k$	4	11	25	48	83

Acknowledgements. The author would like to thank Prof. Manabu Oura for his advice and suggestions.

5. Appendices

5.1. Other E-polynomials

Let G and H be the matrix groups described as follows:

$$G = \langle \frac{1}{i\sqrt{3}} \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{3}} \end{pmatrix} \rangle,$$

$$H = \langle \begin{pmatrix} 1 & 2 & 2 \\ 1 & \zeta+\zeta^4 & \zeta^2+\zeta^3 \\ 1 & \zeta^2+\zeta^3 & \zeta+\zeta^4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta^3 \end{pmatrix}, -\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \rangle.$$

The group G is of order 24, whereas H is of order 120. The group G is related to the self-dual ternary codes, whereas H is related to the ring of symmetric Hilbert modular form. The discussion on these group can be found in [4].

By utilizing the same method discussed, we have that the ring generated by E-polynomials φ_k^Gs (respectively φ_k^Hs) is minimally generated by E-polynomials φ_4 and φ_6 (respectively φ_2, φ_6, and φ_{10}). Thus, we have that

$$\mathfrak{E}(G) = \langle \varphi_4, \varphi_6 \rangle$$

and

$$\mathfrak{E}(H) = \langle \varphi_2, \varphi_6, \varphi_{10} \rangle.$$

The following tables present the dimensions of $\mathfrak{E}$ for each group.

TABLE 5. The dimensions of $\mathfrak{R}(G)_k$ and $\mathfrak{E}(G)_k$

k	4	6
$\dim \mathfrak{R}_k$	1	1
$\dim \mathfrak{E}_k$	1	1

TABLE 6. The dimensions of $\mathfrak{R}(H)_k$ and $\mathfrak{E}(H)_k$

k	2	4	6	8	10
$\dim \mathfrak{R}_k^8$	1	1	2	2	3
$\dim \mathfrak{E}_k^8$	1	1	2	2	3

From Tables 5 and 6, we can conclude that $\mathfrak{E}(G)$ (respectively $\mathfrak{E}(H)$) satisfies

$$\dim \mathfrak{E}(G)_k = \dim \mathfrak{R}(G)_k$$

$$(\dim \mathfrak{E}(H)_l = \dim \mathfrak{R}(H)_l)$$

for $k \geq 4$ and $k \equiv 0 \mod 2$ (respectively $l \equiv 0 \mod 2$). The dimension formulas of $\mathfrak{R}(G)$ and $\mathfrak{R}(H)$ can be written as follows.

$$G: \quad \frac{1}{(1-t^4)(1-t^6)},$$

$$H: \quad \frac{1}{(1-t^2)(1-t^6)(1-t^{10})}.$$

5.2. Generator Matrices

The generator matrix of q_{24a} and q_{24b} are given by

$$q_{24a}: \begin{pmatrix} 101011100110002100101101 \\ 010011020110002300110000 \\ 002000000000000200020020 \\ 000111010000000200020020 \\ 000020020000000000020002 \\ 000002020000000000020002 \\ 000000200000000200020020 \\ 000000001110001200020002 \\ 000000000200002000020002 \\ 000000000020002000020002 \\ 000000000001112100011121 \\ 000000000000200200020002 \\ 000000000000020200020002 \\ 000000000000000011131131 \\ 000000000000000002000020 \\ 000000000000000000220022 \\ 000000000000000000002002 \\ 000000000000000000000202 \end{pmatrix}, q_{24b}: \begin{pmatrix} 100000100100000201011213 \\ 011000020100000201011011 \\ 002000200000000000000202 \\ 000111210000000000000202 \\ 000020020000000000000000 \\ 000002020000000000000000 \\ 000000001110001200011323 \\ 000000000200000000000002 \\ 000000000020000000000200 \\ 000000000001110100000002 \\ 000000000000200200000000 \\ 000000000000020200000000 \\ 000000000000002000000200 \\ 000000000000000011100012 \\ 000000000000000002000020 \\ 000000000000000000200222 \\ 000000000000000000020002 \\ 000000000000000000002002 \end{pmatrix}$$

The generator matrix of q_{32} is given by

$$\begin{pmatrix}
10101010011000000010001201012123 \\
01001000011000000010001201001020 \\
00200002000000000000000000000022 \\
00011103000000000000000000013101 \\
00002002000000000000000000002002 \\
00000202000000000000000000000000 \\
00000022000000000000000000000022 \\
00000000111000120000000000002002 \\
00000000020000200000000000002002 \\
00000000002000200000000000002002 \\
00000000000111210000000000000000 \\
00000000000020020000000000000000 \\
00000000000002020000000000000000 \\
00000000000000001110001200002002 \\
00000000000000000200002000002002 \\
00000000000000000020002000000000 \\
00000000000000000001112100000000 \\
00000000000000000000200200000000 \\
00000000000000000000020200000000 \\
00000000000000000000000011111133 \\
00000000000000000000000002002022 \\
00000000000000000000000000200020 \\
00000000000000000000000000020002 \\
00000000000000000000000000000202
\end{pmatrix}$$

References

[1] E. Bannai, et.al., *Type II Codes, Even Unimodular Lattices and Invariant Rings*, IEEE Trans. Inform. Theory. **45** (1999), 1194-1205.

[2] A. Bonnecaze, Et.al., *Type II Codes over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory. **43** (1997), 969-976.

[3] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput., **24**, no. 3-4 (1997), 235–265.

[4] W. Ebeling, *Lattices and Codes: A course Partially Based on Lectures by F. Hirzebruch*, 1994, Vieweg, Germany.

[5] N. Hamid. *The generator matrices*, https://sites.google.com/view/hamidelfath/generators, last accessed: 7 Ocotber 2019.

[6] T. Motomura and M. Oura, *E-Polynomials Associated to $\mathbb{Z}_4$-codes*, Hokkaido Math. J. **2** (2018), 339-350.

[7] M. Oura, *Eisenstein Polynomials Associated to Binary Codes*, Int. J. Number Theory. **5** (2009), 635-640.

[8] V. Pless, et.al., *All $\mathbb{Z}_4$ Codes of Type II and Length 16 are Known*, J. Combin. Theory Ser A. **78**, 32-50, 1997.

[9] The Sage Developers, Sagemath, the Sage Mathematics Software System (Version 8.1), http://www.sagemath.org, 2017.

(Nur Hamid) (1) Graduate School of Natural Science and Technology, Kanazawa University, Japan, (2) Universitas Nurul Jadid, Paiton, Probolinggo, Indonesia

Email address: `hamidelfath@gmail.com`

Received 2019.10.1
Revised 2019.10.7