Studies on some polynomials related to coding theory

Dissertation Abstract

Studies on some polynomials related to coding theory

符号理論に関連した多項式に関する研究

Graduate School of
Natural Science and Technology
Kanazawa University

Division of Mathematical and Physical Sciences

Student ID No. : 1724012005
Name : Nur Hamid
Chief Advisor : Prof. Manabu Oura

Abstract

Number theory can be connected to coding theory via E-polynomials. By this fact, we continue the investigation of E-polynomials associated to Type II $\mathbb{Z}_4$-codes. In other side, from the invariant theory, we can construct a group related to Type II Z_4-codes. From the group constructed, we obtain the generators of the ring appearing by the complete weight enumerators of Type II Z_4-codes and the E-polynomials. We also show that some invariant rings of some groups can be generated by the E-polynomials.

1 Introduction

The notion of E-polynomials was introduced in [7]. After the introduction, the study of E-polynomials then was continued in [6]. In [6], the generators of the rings generated by the E-polynomials were obtained.

We deal with the codes over $\mathbb{Z}_4$, denoted by $\mathbb{Z}_4$-codes. By some identity in Type II $\mathbb{Z}_4$-codes, we can construct a group G^8 of order 1536 generated by three matrices. Then, we construct E-polynomials for the group G^8 show that the ring generated by them is minimally generated by E-polynomials of the following weights:

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

The investigation is then continued by obtaining the invariant ring related to the matrix group G^8. We remember that the group G^8 is related to the complete weight enumerators of $\mathbb{Z}_4$-codes. The generators of the ring of E-polynomials do not seem to be enough to generate the invariant ring for the finite group G^8 defined in the next section. Because of this condition, we obtain the generators of that invariant ring by using the E-polynomials and the complete weight enumerators of $\mathbb{Z}_4$-codes. For the dimension formulas and the basic theory of E-polynomials used herein, we refer to [1, 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 start by giving three matrices as follows.

$$M_1 = \frac{\eta_8}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}, M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \eta_8 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & \eta_8 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} \eta_8 & 0 & 0 & 0 \\ 0 & \eta_8 & 0 & 0 \\ 0 & 0 & \eta_8 & 0 \\ 0 & 0 & 0 & \eta_8 \end{pmatrix}.$$

Let G, G^8 be the matrix groups defined by the following.

$$G := \langle M_1, M_2 \rangle,$$

$$G^8 := \langle M_1, M_2, M_3 \rangle$$

The group G is of order 384, while G^8 is of order 1536. It is known that the complete weight enumerators of $\mathbb{Z}_4$-codes is left invariant by the matrix group G^8.

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:

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

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

The dimension formula of an invariant ring give us the information related to its generators. This formula can be found by the Molien series.

3 Codes

A code C over $\mathbb{Z}_4$ of length n, called a $\mathbb{Z}_4$-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

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

where $a = (a_1, a_2, ..., a_n)$ and $b = (b_1, b_2, ..., b_n)$. 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.

In this dissertation, we deal with the complete weight enumerator. 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 [2]. From the dimension formula of $\mathfrak{R}^8$, we have the following proposition.

Proposition 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.

Let $p_{8a}, p_{8b}, o_8, k_8, p_{16a}, p_{16b}, q_{24a}, q_{24b}, g_{24}, q_{32}$ be the complete weight enumerators of some codes. The numbers written as subscript denote the degree of each weight enumerators. 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]. The reader interested in these generators can see [5]. The Klemm code has the generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ & 2 & 0 & \cdots & 0 & 2 \\ & & 2 & \cdots & 0 & 2 \\ & & & \ddots & \vdots & \vdots \\ & & & & 2 & 2 \end{pmatrix}.$$

The numbers written as subscript indicate the weight of each complete weight enumerator.

The explicit forms of the complete weight enumerators used are the following.

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

In this dissertation, we omit writing some polynomials because the are too large.

Let W be a set of the the complete weight enumerators aforementioned. We denote by $\mathfrak{W}$ the ring generated by the complete weight enumerators. By generating a ring generated by W, we have the following result.

Theorem 1. *The invariant ring $\mathfrak{R}^8$ can be generated by W.*

Proof. It follows from Proposition 1. The comparison of the rings is shown in Table 1. □

Table 1: The dimensions of $\mathfrak{R}_k^8$ and $\mathfrak{W}_k$

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

4 E-Polynomials

In this section, we define an E-polynomial for a 4×4 matrix group. Let $\mathbf{t}$ be a vector containing 4 variables: t_0, t_1, t_2, and t_3. We understand that the vector here means a column vector. An E-polynomial of weight k for a matrix group 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. The definition of E-polynomial for the group G^8 is similar. For simplicity, we write φ_k instead of φ_k^G.

We denote by $\mathfrak{E}^8$ the ring generated by φ_ks for the group G^8. Denote by κ the cardinality of $K\backslash G$. The numbers κ for G and G^8 can be seen in Table 4.

Table 2: The number κ

Group	Order	K	κ
G	384	8	48
G^8	1536	16	96

Theorem 2. *The ring* $\mathfrak{E}$ *(resp.* $\mathfrak{E}^8$*) can be generated by the polynomials* φ_k *where*

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

$$(\textit{resp. } k \equiv 0 \mod 8, \quad 8 \leq k \leq 96).$$

Proof. Let σ_i be the representative of $K\backslash G^8$ $(1 \leq i \leq \kappa)$. We define

$$x_i = \sigma_{i0}\mathbf{t},$$

where σ_{i0} is the first row of σ_i. For every φ_i, we express φ_i in $\mathbb{C}[x_1, \ldots, x_\kappa]$ and apply the fundamental theorem of symmetric polynomials. Therefore, every φ_i can be written uniquely in $\epsilon_i, \ldots, \epsilon_\kappa \in \mathbb{C}[x_1, \ldots, x_\kappa]$ where

$$\epsilon_r = \sum_{i_1 < i_2 < \cdots < i_r} x_{i_1} x_{i_2} \cdots x_{i_r}, \quad (1 \leq r \leq \kappa).$$

□

We do not write all E-polynomials for this case. In 3, we show the number of monomials of φ_k for G^8.

Table 3: The number of monomials of φ_k

k	$l(\varphi_k)$	k	$l(\varphi_k)$
8	24	56	4082
16	127	64	6009
24	374	72	8464
32	829	80	11511
40	1556	88	15214
48	1619	96	19637

From Theorem 2, we can understand that $\mathfrak{E}^8$ is finitely generated. Under this situation, the interesting point can be disscussed is the minimal generators of $\mathfrak{E}^8$ can be obtained. In the next theorem, we show the minimal generators of $\mathfrak{E}$ and $\mathfrak{E}^8$.

Theorem 3. *The rings* $\mathfrak{E}$*,* $\mathfrak{E}^8$ *are minimally generated by the E-polynomials of weights*

$$\begin{aligned} \mathfrak{E} &: 8, 12, 16, 20, 24, 28, 32, 40, 48, \\ \mathfrak{E}^8 &: 8, 16, 24, 32, 40, 48, 56, 64, 72, 80. \end{aligned}$$

Proof. We do the proof the computation. The dimensions of $\mathfrak{E}^8$ are shown in Table 4. □

Table 4: 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

From Table 4, it seems that the generators of the ring $\mathfrak{E}^8$ is not sufficient to generate $\mathfrak{R}^8$. We can combine $\mathfrak{R}^8$ and $\mathfrak{W}$ to generate the ring $\mathfrak{R}^8$. The combination give us the following theorem.

Theorem 4. *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. This is by the computation. The result is shown in Table 5. □

Table 5: The dimensions of $\mathfrak{R}_k^8$ and $\widetilde{\mathfrak{R}}$

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

5 Other E-polynomials

We refer to [4] for the groups constructed in this section. We define two groups H_1 and H_2.

Let $C \subset \mathbb{F}_3^n$ be a self-dual code. The (Hamming) weight enumerator $W_C(x, y)$ of C is invariant under the transformation of (x, y) by the matrix S_1

$$S_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}.$$

Using the fact that C is self dual, the weight of of every $c \in C$ is multiple of 3. Here, $W_C(x, y)$ is also invariant under transformation of (x, y) by the matrix S_2

$$S_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{3}} \end{pmatrix}.$$

Table 6: The number κ of H_1, H_2

Group	Order	K	κ
H_1	24	3	8
H_2	120	10	12

We define three other matrices T_1, T_2, T_3 by

$$T_1 := \begin{pmatrix} 1 & 2 & 2 \\ 1 & \eta_5+\eta_5^4 & \eta_5^2+\eta_5^3 \\ 1 & \eta_5^2+\eta_5^3 & \eta_5+\eta_5^4 \end{pmatrix}, T_2 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & \eta_5^2 & 0 \\ 0 & 0 & \eta_5^3 \end{pmatrix}, T_3 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

where η_5 denotes the 5-th root of unity. We can write

$$\eta_5 = \frac{1}{4}(\sqrt{5} + i\sqrt{2\sqrt{5}+10} - 1).$$

These matrices are related to the symmetric Hilbert modular form.

Let H_1, H_2 be the groups defined as follows.

$$H_1 := \langle S_1, S_2 \rangle,$$

$$H_2 := \langle T_1, T_2, T_3 \rangle.$$

The details of the subgroup K of each group can be seen in Table 6.

Let $\mathfrak{R}(H_1), \mathfrak{R}(H_2)$ be the invariant rings of H_1, H_2, respectively. The dimension formulas of $\mathfrak{R}(H_1), \mathfrak{R}(H_2)$ are the following.

$$H_1 : \quad \frac{1}{(1-t^4)(1-t^6)},$$

$$H_2 : \quad \frac{1}{(1-t^2)(1-t^6)(1-t^{10})}.$$

Following the method described in the previous section, we obtain that the ring generated by $\varphi_k^{H_1}$ (resp. $\varphi_k^{H_2}$) is minimally generated by the E-polynomials φ_4 and φ_6 (resp. φ_2, φ_6, and φ_{10}). From the computation, the rings of $\varphi_k^{H_1}$ (resp. $\varphi_k^{H_2}$) coincide with $\mathfrak{R}(H_1)$ (resp. $\mathfrak{R}(H_2)$). Therefore, in this situation we can write

$$\mathfrak{R}(H_1) = \mathbb{C}[\varphi_4, \varphi_6],$$

and

$$\mathfrak{R}(H_2) = \mathbb{C}[\varphi_2, \varphi_6, \varphi_{10}].$$

References

[1] E. Bannai, S. T. Dougherty, M. Harada, M. Oura *Type II Codes, Even Unimodular Lattices and Invariant Rings*, IEEE Trans. Inform. Theory. **45** (1999), 1194-1205.

[2] A. Bonnecaze, P. Solé, C. Bachoc, B. Mourrain *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 October 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.

令和　2　年　7　月　27　日

学位論文審査報告書（甲）

1．学位論文題目（外国語の場合は和訳を付けること。）

Studies on some polynomials related to coding theory

（符号理論に関連した多項式に関する研究）

2．論文提出者　(1) 所　　属　　数物科学　　専攻

(2) 氏（ふり）　名（がな）　Nur（ヌル）　Hamid（ハミド）

3．審査結果の要旨（600～650字）

Nur Hamid 氏の学位論文について、各審査委員による個別の事前検討の後、令和2年7月21日に公聴会を開催し、その後の審査会で審議を行い、以下のように判定した。

本学位論文は、Type II Z4 符号の完全重み多項式環、及びそれに付随する有限群の不変式環に注目し、環の生成元などを具体的に決定したものである。符号理論は情報・通信の分野にその研究の発端を持ち、数学の分野でも研究が行われるようになった。従来、有限体上で定義されていた符号は、有限環上でも定義され、有限群の不変式環、モジュラー形式との関連などが活発に研究されるに至った。Nur Hamid 氏は、本論文において特に Type II Z4 符号の完全重み多項式に注目し、それまで主に研究されていた対称化された重み多項式に関する結果に新しい知見を加えることに成功した。具体的には、Nur Hamid 氏は、対応するある有限群の E-多項式が生成する環の具体的な生成元を与え、また、そこにいくつかの Type II Z4 符号の完全重み多項式を加えることにより、不変式環全体の生成元を与えることに成功した。これらの結果は、一般に Type II Z2k 符号の完全重み多項式のなす環、それに付随する有限群の不変式環の研究に大きな進歩を与えるものである。

以上のように本学位論文は代数的組合せ論の更なる発展に寄与するものと期待され、博士（理学）の学位に十分値すると判断した。

4．審査結果　(1) 判　　定（いずれかに○印）　（合　格）　・　不合格

(2) 授与学位　　博　士（　理学　）