

# VAYASAN NURUL JADID PAITON LEMBAGA PENERBITAN, PENELITIAN, & PENGABDIAN KEPADA MASYARAKAT UNIVERSITAS NURUL JADID

© 0888-3077-077
e: lp3m@unuja.ac.id

PP. Nurul Jadid

Karanganyar Paiton

Probolinggo 67291

PROBOLINGGO JAWA TIMUR

w: https://lp3m.unuja.ac.id

#### **SURAT KETERANGAN**

Nomor: NJ-To6/0352/A.03/LP3M/02.2021

Lembaga Penerbitan, Penelitian, dan Pengabdian Masyarakat (LP3M) Universitas Nurul Jadid Probolinggo menerangkan bahwa artikel/karya tulis dengan identitas berikut ini:

Judul

: Note on E-polynomials Associated to Z\_4-codes

Penulis

: NUR HAMID, M.Si, Ph.D..

**Identitas** 

: Nihonkai Mathematical Journal, Vol. XXX, No.2, November 2020,

E-ISSN: 1341-9951, Niigata University

No. Pemeriksaan

:012086

Telah selesai dilakukan *similarity check* dengan menggunakan perangkat lunak **Turnitin** pada 17 Januari 2021 dengan hasil sebagai berikut: Tingkat kesamaan diseluruh artikel (*Similarity Index*) adalah 16 % dengan publikasi yang telah diterbitkan oleh penulis pada Nihonkai Mathematical Journal (https://projecteuclid.org/all/euclid.nihmj)

Demikian Surat Keterangan ini dibuat untuk digunakan sebagaimana mestinya.

Probolinggo, 02 Februari 2021

Kepala LP3M,

ACHMAD FAWAID, M.A., M.A.

NIDN. 2123098702

# NOTE ON E-POLYNOMIALS ASSOCIATED TO Z4-CODES

**Submission date:** 17-Jan-2021 05:07PM (UTC-0800)

**Submission ID:** 1489193525

File name: artikel2\_Note\_ok.pdf (522.9K)

Word count: 3033

Character count: 13694

## NOTE ON E-POLYNOMIALS ASSOCIATED TO Z<sub>4</sub>-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 Z4- codes. In addition, we determine the generators of the invariant rings appearing by E-Polynomials and complete weight enumerators of Type II Z4-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 Z-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 Z-codes. Then, we define an E-polynomial with respect to the complete weight enumerator of Z-codes and show that the ring generated by them is minimally generated by E-polynomials of the following weights:

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  $Z_4$ -codes, we present the generators of that invariant ring.

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

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

<sup>2010</sup> Mathematics Subject Classification. Primary 11T71; Secondary 11T06. Key words and phrases. E-polynomial, Z4-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  $\eta_8$ . Following the notation used in [1], let G be a finite matrix group generated by

and diag [1,  $\eta_s$ , -1,  $\eta_s$ ]. Let  $G^s$  be a matrix group generated by G and diag [ $\eta_s$ ,  $\eta_s$ ,  $\eta_s$ ,  $\eta_s$ ].

The group G is of order 384, whereas  $G^8$  is of order 1536. We denote by R and  $R^8$  the invariant rings of G and  $G^8$ , respectively:

$$R = C[t_0, t_1, t_2, t_3]^G,$$

$$R^8 = C[t_{10}, t_{10}, t_{10}, t_1, t_1]^G$$

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 R and R<sup>8</sup> are given as follows:

$$(\dim \mathbf{R}_{w}) \ \mathbf{t}^{w} = \underbrace{\frac{1 + t^{8} + 2t^{10} + 2t^{12} + 2t^{14} + 2t^{16} + t^{18} + t^{20} + t^{22} + t^{26} + t^{28} + t^{30}}_{w},$$

$$(\mathbf{1 - t^{8}})^{3} \ (\mathbf{1 - t^{12}}),$$

$$(\mathbf{1 - t^{8}})^{3} \ (\mathbf{1 - t^{12}})$$

$$(\mathbf{1 - t^{8}})^{3} \ (\mathbf{1 - t^{24}}).$$

In the next section, we present a fundamental theory of codes that can help us obtain the generators of ring R<sup>8</sup>.

#### 3. Codes

A code C over  $Z_4$  of length n, called  $Z_4$ -code, is an additive subgroup of  $Z_4^n$ . The inner product of two elements a, b  $\in$  C on  $Z_4^n$  is given by

$$(a, b) = a_1b_1 + a_2b_2 + ... + a_nb_n \mod 4$$
  
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  $C^{\perp} = \{y \in Z_{\underline{A}}^n | (x, y) \equiv 0 \mod 4, \ \forall x \in C\}.$ 

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  $Z_i$ -code can only exist when its length is multiple of 8. There are several types of weight enumerators associated with a  $Z_i$ -code. In this paper, we deal with complete weight enumerators.

The complete weight enumerator (CW) of a Z-code C is defined by

$$CW_C(t_0, t_1, t_2, t_3) = \sum_{\substack{0 \ c \in C}} t^{n_0(c)} t^{n_1(c)} t^{n_2(c)} t^{n_4(c)}$$

where  $n_i(c)$  denotes the number of c components which are equivalent to i modulo **4.** For every Type II  $Z_i$ -code,  $CW_C$  ( $t_i$ ,  $t_i$ ,  $t_i$ ,  $t_i$ ) is  $G^s$ -invariant (see [2]). From the dimension formula of  $R^s$ , we have the following proposition.

**Proposition 3.1.** The invariant ring  $R^8$  can be generated by the set of complete weight enumerators of Type II Z<sub>4</sub>-codes consisting of at most

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

2

3

We denote by  $p_{8a}$ ,  $p_{8b}$ ,  $o_{8}$ ,  $k_{8}$ ,  $p_{16a}$ ,  $p_{16b}$ ,  $q_{24a}$ ,  $q_{24a}$ ,  $q_{24}$ ,  $q_{24}$ ,  $q_{32}$  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:

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

Let W be a ring generated by the complete weight enumerators aforementioned:

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

By obtaining the dimension of W, we have the following result.

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

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

TABLE 1. The dimensions of  $\mathbf{R}_k^s$  and  $\mathbf{W}_k$ 

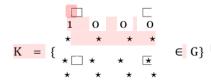
It is noteworthy that we do not need to use the code of length 40. On the next section, we shall give the generators of R<sup>8</sup> by the weight enumerators of Type II Z<sub>4</sub>-codes and E-polynomials.

#### 4. E-Polynomials

Let  $\mathbf{t}$  be a column vector that comprises the following:  $\mathbf{t}_0$ ,  $\mathbf{t}_1$ ,  $\mathbf{t}_2$ , and  $\mathbf{t}_3$ . An E-polynomial of weight  $\mathbf{k}$  for G is defined by

$$\varphi^{G} = \varphi^{G}(\mathbf{t}) = \frac{1}{|G|} \sum_{\sigma \in G} (\mathbf{t})^{k} = \frac{|K|}{|G|} \sum_{K \setminus G \ni \sigma} (\sigma \cdot \mathbf{t})^{k}$$

where



and  $\sigma_0$  is the first row of  $\sigma$ . 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  $\phi_k$  without specifying the group. We denote by E and  $E^8$  the rings generated by  $\phi_k$ 's for the groups G and  $G^8$ , respectively.

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

**Theorem 4.1.** (1) The ring E is generated by  $\varphi_k$  where

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

(2) The ring  $E^8$  is generated by  $\phi_k$  where

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

*Proof.* (1) For each representative  $\sigma_i$  of K\G (1 \leq i \leq \kappa), let  $x_i = \sigma_i^* t$ , where  $\sigma_i^*$  is the first row of  $\sigma_i$ . Then, every  $\varphi_i$  can be expressed in C[x<sub>1</sub>, . . . , x<sub>\kappa</sub>]. By the fundamental theorem of symmetric polynomials, every  $\varphi_i$  can be written uniquely in  $\varepsilon_{ij}$ ...,  $\varepsilon_{\kappa} \in C[x_{ij}, \dots, x_{\kappa}]$  where

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

We mention that  $\varphi_{4}=0$ . This completes the proof.

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

**Theorem 4.2.** (1) E is minimally generated by the E-polynomials of weights 8, 12, 16, 20, 24, 28, 32, 40, 48.

TABLE 2. The dimensions of  $R_k$  and  $E_k$ 

											48
$\dim R_k$ $\dim E_k$	4	3	16	11	25	27	48	54	83	94	133
$\dim \mathbf{E}_k$	1	1	2	2	4	4	4	7	7	10	18

TABLE 3. The dimensions of  $\mathbb{R}^8$  and

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

(2) E<sup>8</sup> is minimally generated by the E-polynomials of weights

*Proof.* For each k, we construct the rings  $E_k$  and  $E^s$ . Then, we determine whether  $\varphi_k$  is generator or not. The dimensions of each E and  $E^s$  are demonstrated in Tables 2 and 3. This completes the proof of Theorem 4.2.

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

**Theorem 4.3.** The invariant ring  $R^s$  can be generated by  $E^s$  and the complete weight enumerators

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

More specifically, the set

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

generates ring R8.

*Proof.* Denote by  $\widetilde{\mathbf{R}}$  the polynomial generated by  $\mathbf{E}^s$  and the complete weight enu-

merators aforementioned. Then we construct  $R_k$  for  $k \equiv 0 \mod 8$  and  $8 \le k \le 96$ . It follows that each  $\varphi_k$  for  $k \neq 8$ , 16, 24 is linearly dependent. We compute the dimension of each  $\widetilde{R}_k$  and write the results in Table 4. This completes the proof.  $\square$ 

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

#### **Appendices**

#### 5.1. Other E-polynomials

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 Epolynomials  $\varphi_k^G$ s (respectively  $\varphi_k^H$ s) is minimally generated by E-polynomials  $\varphi_k^G$  and

 $\varphi_6$  (respectively  $\varphi_2$ ,  $\varphi_6$ , and  $\varphi_{10}$ ). Thus, we have that

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

and

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

The following tables present the dimensions of E for each group.

TABLE 5. The dimensions of  $R(G)_k$  and  $E(G)_k$ 

$$\begin{array}{c|ccc} k & 4 & 6 \\ \dim R_k & 1 & 1 \\ \dim E_k & 1 & 1 \end{array}$$

TABLE 6. The dimensions of  $R(H)_k$  and  $E(H)_k$ 

From Tables 5 and 6, we can conclude that E(G) (respectively E(H)) satisfies  $\dim E(G)_k = \dim R(G)_k$ 

$$(\dim E(H)_l = \dim R(H)_l)$$

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

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

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

#### 5.2. Generator Matrices

The generator matrix of  $q_{^{24}\alpha}$  and  $q_{^{24}b}$  are given by

	101011100110002100101101	100000100100000201011213
	$\square$ 010011020110002300110000 $\square$	□ 011000020100000201011011 □
	002000000000000200020020	0020002000000000000000202
	000111010000000200020020	0001112100000000000000202
	$^{igsq}$ 0000200200000000000020002 $^{igsq}$	<sup>□</sup> 0000200200000000000000000000000000000
	□ 0000020200000000000020002 □	□ 00000202000000000000000000 □
	000000200000000200020020	000000001110001200011323
	000000001110001200020002	0000000002000000000000000000000000000
$q_{24\alpha}$	. — 000000000200002000020002	000000000020000000000000000
<b>4</b> 24 <i>a</i>	000000000002000200020002	$\square$ 0000000000011101000000002 $_{\square}$
	$q$ $\Box$	000000000000200200000000
	000000000001112100011121	000000000000020200000000
	00000000000020020002	000000000000002000000200
	□ 0000000000000020200020002 □	00000000000000011100012 000000000000000
	$ 00000000000000011131131 \\ \square \ 0000000000000000000200020 \\ \square $	000000000000000000000000000000000000000
	00000000000000000220022	0000000000000000000000000000000000
	$\square$ 000000000000000000000000000000000000	00000000000000000000002002
	000000000000000000000000000000000000000	

The generator matrix of  $q_{32}$  is given by

	1	
	10101010011000000010001201012123	
	01001000011000000010001201001020	
_	002000020000000000000000000000000000000	
	00011103000000000000000000013101	
	000020020000000000000000000000000000000	_
	000002020000000000000000000000000000000	H
	0000002200000000000000000000000000022	
	000000001110001200000000000002002	
	000000002000020000000000000000000000000	
_	000000000020002000000000000000000000000	Н
_	000000000001112100000000000000000	
	0000000000002002000000000000000000000	
	00000000000002020000000000000000	
	00000000000000001110001200002002	L
_	000000000000000000000000000000000000000	
	00000000000000000020002000000000	
	000000000000000001112100000000	_
	000000000000000000000000000000000000000	_
	000000000000000000000020200000000	
_	]0000000000000000000000001111133	
	000000000000000000000000000002002022	
	000000000000000000000000000000000000000	_
	000000000000000000000000000000000000000	E
	000000000000000000000000000000000000000	

#### 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 Z<sub>4</sub>, 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 Z4-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 Z4 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, Kana: University, Japan, (2) Universitas Nurul Jadid, Paiton, Probolinggo, Indonesia

Email address: hamidelfath@gmail.com

Received 2019.10.1 Revised 2019.10.7

### NOTE ON E-POLYNOMIALS ASSOCIATED TO Z4-CODES

ORIGIN	ALITY REPORT	
	6% 15% 9% 2% ARITY INDEX INTERNET SOURCES PUBLICATIONS STUDENT IS	PAPERS
PRIMAF	RY SOURCES	
1	compgroups.net Internet Source	6%
2	export.arxiv.org Internet Source	2%
3	www.neari.org Internet Source	1%
4	pubs.rsna.org Internet Source	1%
5	"Stochastic Switching Systems", Springer Science and Business Media LLC, 2006 Publication	1%
6	Liu Shuyang, Li Jianping. "A Self-Adaptive Decoding Scheme for BICM-ID Embedded Turbo Codes", Physics Procedia, 2012 Publication	1%
7	Wachspress, Eugene. "The Quadrilateral", Rational Bases and Generalized Barycentrics, 2016. Publication	1%

8	www.hybrid-analysis.com Internet Source	1%
9	E. Haro-Poniatowski, M. Jouanne, J. F. Morhange, M. Kanehisa, R. Serna, C. N. Afonso. "Size effects investigated by Raman spectroscopy in Bi nanocrystals", Physical Review B, 1999  Publication	<1%
10	theses.gla.ac.uk Internet Source	<1%
11	"   "   Control Problem", Control Engineering,  2006  Publication	<1%
12	Joel M. Tendler. "A stiffly stable integration process using cyclic composite methods", ACM Transactions on Mathematical Software, 12/1/1978 Publication	<1%
13	Milici, S "Minimum embedding of P"3-designs into TS(v,@I)", Discrete Mathematics, 20080206	<1%
14	Xiang-Bin Wang, Xiao-Long Hu, Zong-Wen Yu. "Practical Long-Distance Side-Channel-Free Quantum Key Distribution", Physical Review Applied, 2019 Publication	<1%



<1%

16

H. M. Dufour, D. Burette. "Presentation synthetique des methodes semi-iteratives de resolution des systemes lineaires", Bulletin géodésique, 2008

<1%

Publication

Exclude quotes Off

Exclude bibliography Off

Exclude matches

Off