## Studies on some polynomials related to coding theory

メタデータ	言語: eng
	出版者:
	公開日: 2021-03-17
	キーワード (Ja):
	キーワード (En):
	作成者:
	メールアドレス:
	所属:
URL	http://hdl.handle.net/2297/00061343
	This work is licensed under a Creative Commons

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 International License.



## Dissertation

## 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
Month and Year of Submission	: June, 2020

#### Dedication

To my beloved wife Faizatur Rohmah, my dear daughter, Ushfury Hamidah

Special thanks to my wonderful supervisor, Prof. Manabu Oura.

## Preface

Praise is only to Allah, the most gracious and merciful. With the power given by him, this dissertation is finally can be finished. Our blessings and greetings we convey to the prophet Muhammad.

This dissertation is organized as follows. In chapter 1, we give basic theories related to our research. Chapter 2 shows our investigation of E-polynomial associated to Type II  $\mathbb{Z}_4$ -code. In Chapter 3, we show our results related to Jacobi polynomials. In Chapter 4, we explain our construction of E-polynomial related to classical invariant theory and give the combinatorial properties of the ring arising. Last chapter is the conclusion of this dissertation.

We certainly can not finish this writing without the help of some people. We thank everyone who give the comments and suggestions which develop this writing. Also, we thank specially for my supervisor, Prof. Manabu Oura, who has giving me education very well and humble.

Finally, we hope the readers can enjoy this dissertation. Every questions and critics from the readers are very awaited by us. If there is any question, the reader can send it to my email, hamidelfath@gmail.com.

## List of Tables

4.1	The dimensions of $\mathfrak{R}^8_k$ and $\mathfrak{W}_k$	22
4.2	The number $\kappa$	23
4.3	The number of monomials of $\varphi_k$	23
4.4	The dimensions of $\mathfrak{R}^8_k$ and $\mathfrak{E}^8_k$	24
4.5	The dimensions of $\mathfrak{R}^8_k$ and $\widetilde{\mathfrak{R}}$	24
4.6	The number $\kappa$ of $H_1, H_2 \ldots \ldots$	26
4.7	The dimensions of $\mathfrak{R}(H_1)_k$ and $\mathfrak{E}(H_1)_k$	26
4.8	The dimensions of $\mathfrak{R}(H_2)_k$ and $\mathfrak{E}(H_2)_k$	26

## 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  $\mathbb{Z}_4$ -codes. From the group constructed, we obtain the generators of the ring appearing by the complete weight enumerators of Type II  $\mathbb{Z}_4$ -codes and the E-polynomials. We also show that some invariant rings of some groups can be generated by the E-polynomials.

## Contents

Pr	eface		ii
Al	ostra	$\mathbf{ct}$	$\mathbf{iv}$
1	Intr	oduction	1
<b>2</b>	Bas	ic Theories	3
	2.1	Group	3
	2.2	Ring, Field, and Module	5
	2.3	Codes	7
	2.4	Symmetric Polynomial	10
	2.5	Invariant Theory	10
3	Con	nputations	13
	3.1	Defining the Matrix Group	13
	3.2	Constructing E-polynomials	14
	3.3	Obtaining the generators	15
	3.4	Notes	16
4	E-P	olynomials associated to Type II $\mathbb{Z}_4$ -codes	18
	4.1	Invariant Ring	18
	4.2	E-Polynomials	22
	4.3	Other E-polynomials	25
5	Con	clusions and Discussions	28
	5.1	Conclusions	28
	5.2	Discussion	29
$\mathbf{A}$	Gen	erator Matrices	32

## Chapter 1

## Introduction

Eisenstein polynomial, E-polynomial for short, is combinatorial analogue of Eisenstein series in number theory. E-polynomial was first defined by Oura in [16]. In his paper, Oura gave the notion of E-polynomials related to coding theory. By analogy of E-polynomials with Eisenstein series, he investigated the ring of E-polynomials which is a subring of the ring generated by the weight enumerators of Type II codes.

After the notion given, there are some researches discussing E-polynomials. For example, Miezaki [14] provided analogous properties of Eisenstein polynomials and zeta polynomials.

The investigation of E-polynomials associated to codes then was continued by Motomura and Oura [15]. Following the direction of E-polynomials in [16], they introduced the E-polynomials associated to  $\mathbb{Z}_4$ -codes. As done in [16], the ring generated by Epolynomials was determined.

With the difference in the group used, we continue the study of E-polynomials associated to  $\mathbb{Z}_4$ -codes. While in [16] the weight enumerator exploited is the symmetrized weight enumerator, the weight enumerator taken here is the complete weight enumerator. In this situation, the group mentioned here is of bigger order than in [16].

Besides the bigger order, one needs to consider is the number of variables of the polynomials appearing. Since the complete weight enumerator is a polynomial of four variables, we need to consider the computation to reduce the memory allocation.

In our case, we define an E-polynomial with respect to the complete weight enumerators of  $\mathbb{Z}_4$ -codes. We obtain 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.

Because these polynomials do not generate the invariant ring of a group related to  $\mathbb{Z}_4$ codes, we combine the E-polynomials and the complete weight enumerators of  $\mathbb{Z}_4$ -codes.

Combining the E-polynomials and the complete weight enumerators of  $\mathbb{Z}_4$ -codes, we obtain that the invariant ring mentioned can be generated by the polynomials of weights up to 32. Since by the dimension formula it is enough to compute up to degree 40, we finish the computation up to this degree.

In the end of our results, we show other groups of degrees 24 and 120. The invariant rings of both groups can be generated by the E-polynomials for each group. In this case, the rings of E-polynomials coincide with the invariant ring of the groups.

In this dissertation, the computations are done by Magma [5] and SageMath [20]. Sage-Math is a free open-source Mathematics software which is very useful for the computation.

### Chapter 2

## **Basic** Theories

This chapter contains some definitions and examples. We give basic theories of group, ring, field, and some materials related to coding theory. We refer to [12], [13], and [19] for the details.

#### 2.1 Group

In this section, we give basic theories of a group.

**Definition 2.1.1.** Let G be a non-empty set. Under the operation \*, we call G a group if the following conditions hold.

- 1.  $g_1 * g_2 \in G$  for all  $g_1, g_2 \in G$ . (closed)
- 2.  $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$  for all  $g_1, g_2, g_3 \in G$ . (associative)
- 3. There exists  $1 \in G$  such that 1 \* g = g \* 1 = g for all  $g \in G$ . *(identity)*
- 4. For every  $g \in G$ , there exists  $h \in G$  such that g \* h = h \* g = 1. (inverse)

The element 1 in 3 is called the *identity element*. The element h in 4 is called the *inverse* of g. In general, the inverse of g is denoted by  $g^{-1}$ . The operation \* is called the *law of composition*. If the operation \* is understandable, the notation  $g_1g_2$  is usually used instead of  $g_1 * g_2$  for all  $g_1, g_2 \in G$ . If only conditions 1 and 2 are satisfied, then we call G as a *semigroup*. We call the group G commutative or abelian if G is commutative under \*. By a monoid, we shall mean a set G with operation which is closed and associative, and a unit element.

Let G be a group. The order of G, denoted by |G|, is the number of elements of G. We say G finite if |G| is a finite number. Otherwise, we call G an *infinite group*.

**Example 2.1.1.** The set of integers, denoted by  $\mathbb{Z}$ , is a group under addition,  $\mathbb{Z}$  is not a group under multiplication.

**Example 2.1.2.** The set of integers modulo n, denoted by  $\mathbb{Z}_n$ , is a group under addition.

**Example 2.1.3** (Cyclic groups). A group G is called *cyclic* if there is an element  $g \in G$  such that every element in G can be written in the form  $g^n$  (if under multiplication) or ng (if under addition) for some integer n. Here, such element g is called a *generator* of G. The group  $\mathbb{Z}$  is one of cyclic groups. Its generator is only 1. We can write  $\mathbb{Z} = \langle 1 \rangle$ .

**Example 2.1.4.** There is a group generated by  $e^{2\pi i/n}$ . It can be written as  $\langle e^{2\pi i/n} \rangle$ . The generator of this group is called the *primitive n*-th root of unitary.

**Example 2.1.5.** If n is a prime number,  $\mathbb{Z}_n - \{0\}$  is a group under multiplication.

**Example 2.1.6.** Let  $GL(n, \mathbb{Z}_k)$  be the set of all invertible  $n \times n$  matrices with entries in  $\mathbb{Z}_k$ . Then  $GL(n, \mathbb{Z}_k)$  is a group under matrix multiplication.

**Example 2.1.7** (*The direct product*). Let  $G_1, G_2$  be groups. The direct product  $G_1 \times G_2$  is defined by the set of all pairs  $(x_1, x_2)$  where  $x_1 \in G_1$  and  $x_2 \in G_2$ . For all  $x_i, y_i \in G_i$ , the law of composition of this set is defined by

$$(x_1, x_2)(y_1, y_2) := (x_1y_1, x_2y_2)$$

The  $G_1 \times G_2$  is a group. The unit element of  $G_1 \times G_2$  is  $(e_1, e_2)$  where  $e_1, e_2$  are the unit elements in  $G_1, G_2$ , respectively. More generally, the direct product  $G_1 \times \cdots \times G_n$  of n groups  $G_1, \ldots, G_n$  is also a group.

We provide more for Example 2.1.7. Let I be an index set. For each  $i \in I$ , let  $G_i$  be a group. By  $G = \prod G_i$ , we mean the direct product of  $G_i$  for all  $i \in I$ . Then G is the set all families  $(x_i)_{i \in I}$  where  $x_i \in G_i$ .

Let  $\{A_i\}_{i\in G}$  be a family of abelian groups. The *direct sum* of  $A_i$ :

$$A = \bigoplus_{i \in I} A_i$$

is the subset of  $\prod A_i$  consisting of all families  $(x_i)_{i \in I}$  with  $x_i \in A_i$  such that  $x_i = 0$  for all but finitely many i.

The next examples are taken from the matrix form.

**Example 2.1.8.** The set of all  $n \times n$  matrices whose determinants are non-zero with entries in  $\mathbb{C}$ , denoted  $GL(n, \mathbb{C})$ , is a group under multiplication. This group is called a *general linear group*. The set of all elements of  $GL(n, \mathbb{C})$  whose determinants are equal to 1, called a *special linear group* and denoted by  $SL(n, \mathbb{C})$ , is a subgroup of  $GL(n, \mathbb{C})$ .

Let H be a subgroup of a group G. A *left coset* of K in G, denoted by  $K \setminus G$ , is a subset of G defined by

$$K \backslash G := \{ak : k \in K\}$$

for some  $a \in G$ . An element of aK is called a *coset representative* of aH. We apply the similar remark to *right coset*, denoted by G/K.

**Proposition 2.1.1.** Let K be a subgroup of a finite group G. Then

$$|K\backslash G| = \frac{|G|}{|K|}.$$

#### 2.2 Ring, Field, and Module

A set R with two binary operations, addition and multiplication, defined on R is called a *(commutative) ring* if the following conditions are satisfied.

- Under addition, R is a (commutative) group.
- Under multiplication, R is closed, has identity, and satisfies the associative law.
- The distribution law holds. That is, a(b+c) = ab + ac for all  $a, b, c \in R$ .

**Example 2.2.1.** Let  $R[x_1, \ldots, x_n]$  be the set of all polynomials in  $x_1, \ldots, x_n$  with coefficients in R. The set  $R[x_1, \ldots, x_n]$  is a ring and called a polynomial ring.

**Example 2.2.2.** The set of all polynomials in  $x_1, \ldots, x_n$  with coefficients in  $\mathbb{C}$  is a ring. This ring is denoted by  $\mathbb{C}[x_1, \ldots, x_n]$ .

We continue by giving the definition of a field. For the shorter word, we can say that a field is a commutative ring such that  $1 \neq 0$  which has a multiplicative inverse and whose non-zero elements form a group under multiplication.

**Definition 2.2.1.** A *field*  $\mathbb{F}$  is a non-empty set with two binary operations + and \* which satisfies the following conditions.

- 1. Under +,  $\mathbb{F}$  is a commutative group.
- 2. Under  $*, \mathbb{F} \{0\}$  is a group.
- 3. a \* (b + c) = a \* b + a \* c for all  $a, b, c \in \mathbb{F}$ .

The finite field of q elements where q is a prime power is denoted by GF(q).

**Example 2.2.3.** The set  $\mathbb{Z}_n$  can be considered as a field if n is a prime number.

**Example 2.2.4.** The set  $\mathbb{F}_4 = \{0, 1, \omega, \omega + 1\}$  is a field where  $\omega^2 = \omega + 1$  and  $\omega(\omega + 1) = 1$ .

Let R, called a *base ring*, be a ring whose elements are called scalars. A non-empty set M is called a module over R (or an R-module) if the following conditions hold.

- 1. Under addition, M is an abelian group.
- 2. For all scalars  $a, b \in R$  and  $u, v \in M$ , the set M fulfills the following conditions.

$$au \in R,$$
  

$$a(u+v) = au + av,$$
  

$$(a+b)u = au + bu,$$
  

$$(ab)u = a(bu),$$
  

$$1 u = u.$$

Let M be an R-module. A subset S of M is called a *submodule* of M if S is an R-module. If S is a group under addition, we call S an additive subgroup of M.

One special type of a module is vector space. If a non-empty set V is a module over a field  $\mathbb{F}$ , then we say V a vector space over  $\mathbb{F}$ . A subset S of V is called a subspace of V if S is also vector space over  $\mathbb{F}$ . We note that the notations on both module and vector space are same. The difference is only on the base ring or field used.

**Definition 2.2.2.** Let S be a non-empty subset of a vector space V over  $\mathbb{F}$ . An expression of the form

 $f_1s_1 + \dots + f_ns_n$ 

where  $s_1, \ldots, s_n \in S$  and  $f_1, \ldots, f_n \in \mathbb{F}$  is called a *linear combination* of vectors in S. If  $f_1 = f_2 = \cdots = 0$ , then we say the linear combination *trivial*. Otherwise, it is called *non-trivial*.

**Definition 2.2.3.** Let S be a subset of a vector space V. The set S is called a *generator* of V if every  $v \in V$  can be expressed as a linear combination of S. In other words, we can say for every  $v \in V$ , we can find  $k_1, \ldots, k_n \in \mathbb{F}$  such that

$$v = k_1 s_1 + \dots + k_n s_n$$

for  $s_1, \ldots, s_n \in S$ . In this case, we say that V can be generated by S and can be denoted by

$$V = \langle S \rangle.$$

**Definition 2.2.4.** Let S be a subset of V. We say that S is *linearly independent* if the trivial linear combination of vectors in S is the only linear combination which is equal to 0.

**Definition 2.2.5.** Let V be a vector space. A basis S of V is a subset of V which is linearly independent and generates V.

Let S be a basis of a vector space V. We call V is of dimension n if S is of cardinality n. The vector space V is a finite dimensional vector space if S is finite.

Let A be a ring. We call  $\mathcal{A}$  a graded ring if as an commutative group  $\mathcal{A}$  can be expressed as a direct sum

$$\mathcal{A} = \bigoplus_{r}^{\infty} \mathcal{A}_{r}$$

such that  $\mathcal{A}_p\mathcal{A}_s \subset \mathcal{A}_{p+s}$  for all integers  $p, s \ge 0$ . In particular,  $\mathcal{A}_0$  is a subring. Every set  $\mathcal{A}_r$  is an  $\mathcal{A}_0$ -module. The elements of  $\mathcal{A}_r$  are called the *homogeneous elements* of degree r.

If a (graded) ring  $\mathcal{A}$  can be generated by elements  $f_1, \ldots, f_k$ , then we use the notation  $\mathcal{A} = \mathcal{A}_0[f_1, \ldots, f_k]$ . For example, we denote by  $\mathfrak{W}$  the ring of the weight enumerators of self-dual binary codes. The details of self-dual codes will be discussed later. With  $\mathfrak{W}_0 = \mathbb{C}$ , the ring  $\mathfrak{W}$  is generated by the polynomials

$$W_{e_8} = x^8 + 14x^4y^4 + y^8, \quad W_{g_{24}} = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}, \quad (2.1)$$

and can be written as

$$\mathfrak{W} = \mathbb{C}[W_{e_8}, W_{g_{24}}].$$

#### 2.3 Codes

Let  $\mathbb{F}$  be a field. An [n, k] (linear) code C of length n over  $\mathbb{F}$  is a k-dimensional subspace of  $\mathbb{F}^n$ .

$$\sqrt{1}$$
  $\underbrace{44\cdots 4}_{n \text{ times}}$ 

Here  $\mathbb{F}^n$  means the space of all *n*-tuples of elements of  $\mathbb{F}$ . The element *c* of *C* is called a *codeword*. If we use a ring *R* instead of the field  $\mathbb{F}$ , then a code *C* means the additive subgroup of *R*.

**Example 2.3.1.** The set of all vectors  $c = (c_1, ..., c_n)$  for  $c_1, ..., c_n \in \mathbb{Z}_2$  is a linear code. In general, the code over  $\mathbb{Z}_2$  is called a *binary code*.

We define some notations and terms for a code over  $\mathbb{F}$ . For a code over  $\mathbb{R}$ , the notations and terms are similar.

Let C be a code over  $\mathbb{F}$ . Because C is a subspace of  $\mathbb{F}^n$ , we can find the basis of C. A  $k \times n$  matrix G whose rows are the basis vectors of C is called a *generator matrix*. All the codewords in C can be obtained by the linear combination of row vectors of G.

For example, take the binary generator matrix  $G_1$ :

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Then, we can obtain a linear code by  $G_1$  containing the following codewords.

$$\begin{split} G_1 &= \{(0,0,0,0,0), (1,0,0,1,1), (0,1,0,0,1), (1,1,0,1,0), \\ &\quad (0,0,1,1,1), (1,0,1,0,0), (0,1,1,1,0), (1,1,1,0,1)\}. \end{split}$$

**Example 2.3.2** (Hamming code). The generator matrix of [7,4]-Hamming code is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

**Example 2.3.3.** The extended Hamming code  $e_8$  is the code with the generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Let u, v be codewords of a code C over  $\mathbb{F}$ . The inner product  $u \cdot v$  is defined by

$$u \cdot v := u_1 v_1 + \dots + u_n v_n \in \mathbb{F}.$$

We say that u and v are orthogonal to each other if  $u \cdot v = 0$ . By the orthogonality, we can define a new code called a dual code.

For a code C, the dual of C, denoted by  $C^{\perp}$ , is a code containing vectors  $v \in \mathbb{F}^n$  which are orthogonal to all  $u \in C$ . It is straightforward to show that  $C^{\perp}$  is a code. In other words, we can say that

$$C^{\perp} := \{ v \in \mathbb{F}^n : u \cdot v = 0, \forall u \in C \}.$$

If  $C^{\perp} = C$ , then we say C self-dual.

For a codeword  $c \in C$ , the (Hamming) weight wt(c) is defined as the number of nonzero  $c_i$ . A code C is called *doubly even* if wt(c) is divisible by 4 for all  $c \in C$ .

The weight enumerator  $W_C$  of C is defined by

$$W_C(x,y) := \sum_{c \in C} x^{n-wt(c)} y^{wt(c)}.$$

For example, the weight enumerator of the extended Hamming code is

$$W_{e_8} = x^8 + 14x^4y^4 + y^8$$

The easiest example of a Type II code is the code  $d_n^+$  whose generator matrix is

$\begin{pmatrix} 1 \end{pmatrix}$	1	1	1	0	0		0	0	0	0	
0	0	1	1	1	1		0	0	0	0	
:	÷	·				·					
0	0	0	0	0	0		1	1	1	1	
$\setminus 1$	0	1	0	1	0		1	0	1	0 /	1

For example,  $d_8^+$  has generator matrix

 $\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$ 

The weight enumerator of  $d_8^+$  is

$$W_{d_8^+} = x^8 + 14x^4y^4 + y^8.$$

**Theorem 2.3.1** (MacWilliams identity for binary linear codes, [13]). Let C be an [n, k] binary linear code. Then

$$W_{C^{\perp}}(x,y) = \frac{1}{|C|} W_C(x+y,x-y).$$

Now we discuss a code over  $\mathbb{F}_3 = \{0, 1, 2\}$ . We call a code  $C \subset \mathbb{F}_3^n$  by a *ternary code*. For example, we take the generator matrix

$$\begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

for a code C. Then we have that C contains 9 elements

(0, 0, 0, 0), (1, 0, 2, 2), (2, 0, 1, 1), (0, 1, 2, 1), (1, 1, 1, 0),(2, 1, 0, 2), (0, 2, 1, 2), (1, 2, 0, 1), (2, 2, 2, 0).

If we move to  $\mathbb{Z}_4$ -code C, there are several weight enumerators associated. They are complete and symmetrized weight enumerators. Here are their definitions.

**Definition 2.3.1.** The complete weight enumerator of a code C is

$$CW_C(t_0, t_1, t_2, t_3) := \sum_{c \in C} t_0^{n_0(c)} t_1^{n_1(c)} t_2^{n_2(c)} t_3^{n_3(c)}$$

where

$$n_i(c) = |\{c_i | c_i = i \pmod{4}\}|$$

**Definition 2.3.2.** The symmetrized weight enumerator of a code C is

$$SW_C(t_0, t_1, t_2) := CW_C(t_0, t_1, t_2, t_1)$$

where  $SW_C$  is the complete weight enumerator of C.

We give an example of  $\mathbb{Z}_4$ -codes and its complete and symmetrized weight enumerators. The generator matrix used here is

$\begin{pmatrix} 1 \end{pmatrix}$	1	1	0	1	0	0	2	١
1	1	0	1	2	1	2	2	
1	0	1	1	2	0	1	0	
0	1	1	1	0	0	2	1 )	/

The code with that generator is called the *octacode*  $O_8$ . The complete and the symmetrized weight enumerators of  $O_8$  are the following.

$$CW_{O_8} = t_0^8 + 8t_0^3 t_1^4 t_2 + 8t_0 t_1^4 t_2^3 + 14t_0^4 t_2^4 + t_2^8 + 24t_0^3 t_1^3 t_2 t_3$$
$$+ 24t_0 t_1^3 t_2^3 t_3 + 4t_1^6 t_3^2 + 48t_0^3 t_1^2 t_2 t_3^2 + 48t_0 t_1^2 t_2^3 t_3^3$$
$$+ 24t_0^3 t_1 t_2 t_3^3 + 24t_0 t_1 t_2^3 t_3^3 + 8t_1^4 t_3^4 + 8t_0^3 t_2 t_3^4 + 8t_0 t_2^3 t_3^4$$
$$+ 4t_1^2 t_3^6,$$
$$SW_{O_8} = t_2^8 + 16t_0^8 + 112t_2^3 t_0^4 t_1 + 112t_2 t_0^4 t_1^3 + 14t_2^4 t_1^4 + t_1^8.$$

#### 2.4 Symmetric Polynomial

Let  $f \in \mathbb{C}[x_1, \ldots, x_n]$  be a polynomial in variables  $x_1, \ldots, x_n$ . We say that the polynomial f is symmetric if

$$f(x_{i_1},\ldots,x_{i_n})=f(x_1,\ldots,x_n)$$

for every permutation  $x_{i_1}, \ldots, x_{i_n}$  of the variables  $x_1, \ldots, x_n$ . For example, the polynomials x + y + z,  $x^2 + y^2 + z^2$ , and xyz are symmetric. It is clear that the interchanging of x, y, z positions does not bring up a new polynomial.

Let  $\sigma_1, \ldots, \sigma_n \in \mathbb{F}[x_1, \ldots, x_n]$  defined by the following formulas.

$$\sigma_1 = x_1 + \dots + x_n,$$
  

$$\vdots$$
  

$$\sigma_r = \sum_{i_1 < i_2 < \dots < i_r} x_{i_1} x_{i_2} \cdots x_{i_r},$$
  

$$\vdots$$
  

$$\sigma_n = x_1 x_2 \cdots x_n.$$

We call the functions  $\sigma_1, \ldots, \sigma_n$  the elementary symmetric functions.

In fact, every symmetric polynomial can be expressed in elementary symmetric functions. This is known as the fundamental theorem of symmetric polynomials. For example, the function  $f = x^2 + 2xy + y^2$  can be expressed as

$$f = \sigma_1^2 - 2\sigma_2.$$

**Theorem 2.4.1** (The Fundamental Theorem of Symmetric Polynomials, [6]). Every symmetric polynomial in  $\mathbb{F}[x_1, \ldots, x_n]$  can be written uniquely as a polynomial in the elementary symmetric functions  $\sigma_1, \ldots, \sigma_n$ .

#### 2.5 Invariant Theory

We give the definitions of invariant related to binary codes. The definition of invariant in general is not so different from the following. We refer to [13] for the details.

For a self-dual binary code C, the MacWilliams identity is given by

$$W(x,y) = W\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right).$$
(2.2)

The equation (2.2) tells us that W(x, y) is unchanged or *invariant* under the linear transformation T where T replaces x by  $\frac{x+y}{\sqrt{2}}$ 

and 
$$y$$
 by

$$\frac{x-y}{\sqrt{2}}$$

All codeword in C are of weights of a multiple 4. Here is also the known equation.

$$W(x,y) = W(x,iy).$$
(2.3)

This equation also tells us that W(x, y) is invariant under the transformation U where U does not move x but replaces y by iy.

From the previous chapter, we remember that the weight enumerator of a binary code C can be expressed  $W_{e_8}$  and  $W_{g_{24}}$  where

$$W_{e_8} = x^8 + 14x^4y^4 + y^8, \quad W_{g_{24}} = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}.$$
(2.4)

**Theorem 2.5.1.** Any polynomial satisfying Equations (2.2) and (2.3) is a polynomial in  $W_{e_8}$  and  $W_{g_{24}}$ .

Since W(x, y) is invariant under T and U, W(x, y) must be invariant under any combination  $T^2$ , TU, UTU, ... of these transformation.

From the reference, there is information to know how many linearly independent homogeneous invariant of each degree d. Say that there are  $a_d$  linearly independent homogeneous invariants of degree d. It is comfortable to express the numbers  $a_0, a_1, a_2, \ldots$ , by a generating function

$$\mathcal{I}(t) = a_0 + a_1 t + a_2 t^2 + \cdots$$

In reverse, we can obtain the numbers  $a_0, a_1, a_2, \ldots$  if  $\mathcal{I}(t)$  is known.

**Theorem 2.5.2** ([13]). For any finite group G of a complex  $m \times m$  matrices,  $\mathcal{I}(t)$  is given by

$$\mathcal{I}(t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - tg)}$$

where |G| is the order of G, det means the determinant, and I is the unit matrix.

We call  $\mathcal{I}(t)$  the Molien series of G. We give the examples by the famous matrix group G generated by

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1\\ 1 & -1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0\\ 0 & i \end{pmatrix}.$$

This group is of order 192. The weight enumerators of self-dual binary codes are left invariant by G. The formula of its Molien series is

$$\mathcal{I}(t) = \frac{1}{(1 - t^8)(1 - t^{24})}.$$
(2.5)

The formula appearing from the Molien series gives us a useful information. For example, from equation (2.5), we get such information. The ring of the weight enumerators of self-dual binary codes can be generated by two polynomials. These polynomial are of degrees 8 and 24. This fact has a connection to our previous example which is shown in (2.1).

**Definition 2.5.1.** Let G be a matrix group of size  $m \times m$ . Any *invariant* of G is a polynomial f in variables  $t_1, \ldots, t_m$  which is unchanged by every linear transformation in G.

One of our main problem is to find the generators for the invariant ring related to codes. Related to this, we give the following definition.

**Definition 2.5.2.** Polynomials  $f_1, \ldots, f_r$  in variables  $t_1, \ldots, t_m$  are called *algebraically dependent* if there is a polynomial p in r variables with complex coefficients, not all zero, such that

$$p(f_1,\ldots,f_r)=0$$

Otherwise  $f_1, \ldots, f_r$  are called *algebraically independent*.

The following theorem taken from [13, p. 610].

**Theorem 2.5.3.** There always exist m algebraically independent invariants of G.

One of criterion we can use for algebraic independence is Jacobian criterion. Let  $f_1, \ldots, f_m$  be the polynomials in variables  $t_1, \ldots, t_m$ . We denote by  $J(f_1, \ldots, f_m)$  the determinant of the  $m \times m$  matrix whose (i, j)-entry is

$$\frac{\partial f_i}{\partial t_j}.$$

We have the following proposition and refer the proof to [11].

**Proposition 2.5.1.** The polynomials  $f_1, \ldots, f_m$  in variables  $t_1, \ldots, t_m$  are algebraically independent if and only if  $J(f_1, \ldots, f_n) \neq 0$ .

**Example 2.5.1.** The polynomials  $W_{e_8}$  and  $W_{g_{24}}$  are algebraically independent. We can check by direct calculation. If we take  $W_{d_{16}} = t_0^{16} + 28t_0^{12}t_1^4 + 198t_0^8t_1^8 + 28t_0^4t_1^{12} + t_1^{16}$ , then  $W_{e_8}$  and  $W_{d_{16}}$  are algebraically dependent. Let  $p(X, Y) = -X^2 + Y$ . Then we have  $p(W_{e_8}, W_{d_{16}}) = 0$ .

We close this chapter by discussing about an E-polynomial. The definition of this polynomial will be given in Chapter 4. Here, we only give a note that in some cases, the invariant ring related to codes can be generated by the set of E-polynomials. For example, in [16], it was shown that the ring  $\mathfrak{W}$  of the weight enumerators of binary codes in genus 1 can be generated by the E-polynomials of weights 8 and 24.

## Chapter 3

## Computations

In this chapter, we explain the details of computation. The main parts of this computation are defining the group used, constructing E-polynomials, and obtaining the generator.

#### 3.1 Defining the Matrix Group

In Chapter 4, we obtain that the groups defined is of order 384 and 1536. Here we show how we generate the group of order 384, the steps for constructing another group is not much different from these steps.

Algorithm 1: Constructing the group	
<b>Result:</b> The order of $G$	
set $CF. < z >=$ CyclotomicField(8);	
set $s^2 = z^7 + z$ ; //defining the square root of 2;	
set $I = z^2$ ; //defining the imaginary number;	
set $M_1 = Matrix(CF, [[1,1,1,1], [1,I,-1,-I], [1,-1,1,-1], [1,-I,-1,I]]);$	
set $M_2 = \text{diagonal\_matrix}(\text{CF}, [1, z, -1, z);$	
obtain $G$ =MatrixGroup $(M_1, M_2);$	
print the order of $G$ ;	

To construct another group, we only need to define the generators. Then we can use the generators to obtain the groups.

In Algorithm 1, the command CyclotomicField(8) is needed to get the 8-th primitive root of 1. Some cases may be different. In case we need

$$\frac{1}{2}(i\sqrt{3}-1),$$

we can use CyclotomicField(8). In another case, we need to compute  $\sqrt{5}$ . In this situation, we can determine CyclotomicField(5) and compute  $\sqrt{5}$  by

$$\frac{2\eta_5^2 + \eta_5 + 2}{\eta_5}$$

where  $\eta_5$  denotes the 5-th primitive root of unity.

#### 3.2 Constructing E-polynomials

The definition of an E-polynomial will be given in the next chapter. However, we give the details how we compute it.

From the previous section, we have the order of the group G as an output. Although we do not write explicitly in the algorithm, we can hold the group G and its elements.

The detail of steps as follows. We set n the row size of the elements of G. Define a set T of variables  $t_0, t_1, \ldots, t_{n-1}$ . For each element  $g \in G$ , we take only the first row  $g_0$  of g. After multiplying  $g_0$  (as a row vector) by T (as a column vector), for each multiplication  $g_0T$ , say gt, then we compute gt to the power of k where k is the weight of E-polynomial. The details of algorithm are below. We obtain the E-polynomials up to weights  $\kappa$ .

<b>Algorithm 2:</b> Computing up to $\kappa$						
Result: E-polynomials						
set $k, G, n;$						
set $\kappa$ ;						
set $T = \{t_i\}$ for $i = 0,, n - 1;$						
set m, the minimum weight such that $\varphi_m \neq 0$ ;						
for $k = m$ to $\kappa$ do						
go to Algorithm 3 construct $(k, G, T)$ ;						
$\mathbf{end}$						
save poly.						
<b>Algorithm 3:</b> Constructing E-polynomials $construct(k, G, T)$						

**Result:** E-polynomial of weight k set poly = 0; for  $g \in G$  do | set  $g_0 = g[0,:]$ ; calculate  $gt = g_0 * T$ ; calculate  $poly = poly + gt^k$ ; end save poly.

print "order of G";

**Example 3.2.1.** The following is an example of constructing group of order 384 and 1536 in SageMath.

```
CF.<z>=CyclotomicField(8);
s2=z**7+z; #square root of 2.
I =z*s2-1;
T=z/2*Matrix(CF,[[1,1,1,1],[1,I,-1,-I],[1,-1,1,-1],[1,-I,-I,I]]);
D=diagonal_matrix(CF,[1,z,-1,z]);
#generating the matrix group G
G=MatrixGroup(T,D);
```

```
print G.order();
Dz=diagonal_matrix(CF,[z,z,z,z]);
```

#generating the matrix group G8
G8=MatrixGroup(T,D,Dz)
print "order of G8";
print G.order();

#### 3.3 Obtaining the generators

After we construct the E-polynomials up to weight  $\kappa$ , we continue to find the polynomials which are the generators of the ring of the E-polynomials. We understand here that the weight of an E-polynomial shows the degree of the polynomial.

Assume we have the set of E-polynomials

$$E = \{\varphi_1, \varphi_2, \dots, \varphi_\kappa\}.$$

Remember that  $\varphi_k$  may be 0 for some k. We set  $\Omega = \{1, 2, ..., \kappa\}$ . For each degree d, we find all  $S \subseteq \Omega$  such that

$$\sum_{s \in S} s = d$$

and  $d \notin S$ .

Let  $S_1, \ldots, S_j$  be the subsets of  $\Omega$  such that the summation of their elements are equal to d. By the elements of  $S_i$ , we obtain the combination

$$p_i = \prod_{s \in S_i} \varphi_s.$$

From  $p_1, p_2, \ldots, p_j$ , we can ensure if  $\varphi_d$  is a basis element or not. If not, we remove  $\varphi_d$  from the set E and d from  $\Omega$ . The steps can be seen in Algorithm 4. The steps to obtain the generators of other invariant rings are not so different.

Algorithm 4: Find the generators

```
Result: The basis P, the set E of generators
set d;
set E, the set of E-polynomials ;
set P = \{\};
set \Omega;
for S \in \{S \subset \Omega | \sum_{s \in S} s = d\} do
    set p = 1;
    for s in S do
         calculate p = p * \varphi_s;
    end
    if p \neq < P > then
        set P = P \cup p;
    end
end
if \varphi_d \notin P > then
    set P = P \cup \varphi_d;
else
 | \quad \text{set } E = E - \varphi_d
\mathbf{end}
```

#### 3.4 Notes

In our computation, we more often use SageMath than Magma. We use Magma when we compute the complete weight enumerators of  $\mathbb{Z}_4$ -codes. SageMath does not provide a command for the code over a ring yet.

Again we say that we only use Magma to compute the complete weight enumerators of  $\mathbb{Z}_4$ -codes. The polynomials obtained from Magma are then moved to SageMath. We combine these polynomials with the E-polynomials obtained in SageMath. We give an example how do we compute  $\mathbb{Z}_4$ -codes.

**Example 3.4.1.** The following is to compute the code over  $\mathbb{Z}_4$  with the generator matrix

(1)	1	1	1	1	1	1	-1
1	1	1	0	0	0	2	1
2	2	0	0	0	0	0	0
2	0	2	0	0	0	0	0
0	0	0	2	2	0	0	0
0	0	0	2	0	2	0	0 /

and show its complete weight enumerator.

```
R := IntegerRing(4);
C0 := LinearCode<R,8 |</pre>
```

[1,1,1,1,1,1,1,-1],[1,1,1,0,0,0,2,1], [2,2,0,0,0,0,0,0],[2,0,2,0,0,0,0,0], [0,0,0,2,2,0,0,0],[0,0,0,2,0,2,0,0]>; CW<t0,t1,t2,t3>:=CompleteWeightEnumerator(CO);

print CW;

#### Chapter 4

# E-Polynomials associated to Type II $\mathbb{Z}_4$ -codes

In this chapter, we construct E-polynomials associated to Type II  $\mathbb{Z}_4$ -codes. We give the minimal generators of the ring generated by the E-polynomials and show the generators of the invariant ring of the complete weight enumerators of Type II codes. Every code defined here is Type II code. In this chapter, we give the details related to [8].

This chapter is the continuation of [15]. In [15], the ring associated to the group defined was generated by the E-polynomials and the symmetrized weight enumerators. Then, in this chapter, with the same motivation, we combine the E-polynomials and the complete weight enumerators of  $\mathbb{Z}_4$ -codes.

#### 4.1 Invariant Ring

We denote by  $\mathbb{C}$  the field of complex numbers 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

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

Let C be a Type II code. We denote a primitive 8-th root of unity by  $\eta_8$ . The MacWilliams identity for  $\mathbb{Z}_4$ -code in term of complete weight enumerator of C is known [4]. The identity is the following.

$$CW_C(t_0, t_1, t_2, t_3) = \frac{1}{|C|} CW_C(t_0 + t_1 + t_2 + t_3, t_0 + it_1 - t_2 - it_3, t_0 - t_1 + t_2 - t_3, t_0 - it_1 - it_2 + t_3).$$
(4.1)

Moreover, since C is doubly even, we have the relation

$$CW_C(t_0, \eta_8 t_1, -t_2, \eta_8 t_3) = CW_C(t_0, t_1, t_2, t_3).$$
(4.2)

By Equations (4.1) and (4.2), we construct three matrices as follows.

$$M_{1} = \frac{\eta_{8}}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix},$$
$$M_{2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \eta_{8} & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & \eta_{8} \end{pmatrix},$$

and  $M_3 = \text{diag} [\eta_8, \eta_8, \eta_8, \eta_8]$ . Let G be the group generated by  $M_1, M_2$  and  $G^8$  generated by  $M_1, M_2, M_3$ . The groups G,  $G^8$  are of order 384, 1536, respectively.

We denote by  $\mathfrak{R}, \mathfrak{R}^8$  the invariant rings of  $G, G^8$ :

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

under an action of such matrices on the polynomial ring of four variables  $t_0$ ,  $t_1$ ,  $t_2$ , and  $t_3$ . The dimension formula of  $\mathfrak{R}$  and  $\mathfrak{R}^8$  is given as follows [1]:

$$\sum_{w} (\dim \Re_{w}) t^{w} = \frac{1 + t^{8} + 2t^{10} + 2t^{12} + 2t^{14} + 2t^{16} + t^{18} + t^{20} + t^{22} + t^{26} + t^{28} + t^{30}}{(1 - t^{8})^{3} (1 - t^{12})},$$
$$\sum_{w} (\dim \Re_{w}^{8}) t^{w} = \frac{1 + t^{8} + 2t^{16} + 2t^{24} + t^{32} + t^{40}}{(1 - t^{8})^{3} (1 - t^{24})}.$$

We continue the discussion only on  $G^8$ . Later we will mention again the group G in the discussion about E-polynomials.

By the dimension formula of  $\mathfrak{R}^8$ , we have an information about its generators. In general, the invariant ring  $\mathfrak{R}^8$  can be generated by the set of the complete weight enumerators of Type II codes consisting at most:

- 1. 4 codes of length 8,
- 2. 2 codes of length 16,
- 3. 3 codes of length 24,
- 4. 1 code of length 32, and
- 5. 1 code of length 40.

Although later we do not give which polynomials are algebraically independence, from the dimension formula, we know that the generators of  $\Re^8$  contain 3 polynomials of degree 8 and 1 polynomial of degree 24 which are algebraically independent.

Let  $W = \{p_{8a}, p_{8b}, o_8, k_8, p_{16a}, p_{16b}, q_{24a}, q_{24b}, g_{24}, q_{32}\}$  be the set of the complete weight enumerators of some codes with the following details. The weight enumerators  $o_8$ ,  $k_8$ , and  $g_{24}$  are the complete weight enumerators of octacode, Klemm code, and Golay code, respectively. The generator matrices of the complete weight enumerators which are denoted by p are taken from [18]. The reader interested in these generators can see [9].

The Klemm code has the generator matrix

The generator matrix of  $q_{24a}$  is given by

( 1	0	1	0	1	1	1	0	0	1	1	0	0	0	2	1	0	0	1	0	1	1	0	1
0	1	0	0	1	1	0	2	0	1	1	0	0	0	2	3	0	0	1	1	0	0	0	0
0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	2	0	0	2	0
0	0	0	1	1	1	0	1	0	0	0	0	0	0	0	2	0	0	0	2	0	0	2	0
0	0	0	0	2	0	0	2	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	2
0	0	0	0	0	2	0	2	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	2
0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	2	0	0	0	2	0	0	2	0
0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	2	0	0	0	2	0	0	0	2
0	0	0	0	0	0	0	0	0	2	0	0	0	0	2	0	0	0	0	2	0	0	0	2
0	0	0	0	0	0	0	0	0	0	2	0	0	0	2	0	0	0	0	2	0	0	0	2
0	0	0	0	0	0	0	0	0	0	0	1	1	1	2	1	0	0	0	1	1	1	2	1
0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2	0	0	0	2	0	0	0	2
0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	2	0	0	0	2	0	0	0	2
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	3	1	1	3	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	2	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	0	2	2
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	<b>2</b>	0	$_{2}$ /

The generator matrix of  $q_{24b}$  is given by

 

 0
 1
 1
 0
 0
 0
 2
 0
 1
 0
 0
 0

 0
 0
 2
 0
 0
 2
 0
 1
 0
 0
 0

 0
 0
 2
 0
 0
 2
 0
 0
 0
 0
 0
 0

 0
 0
 0
 1
 1
 1
 2
 1
 0
 0
 0
 0
 0

 0
 0
 0
 1
 1
 1
 2
 1
 0
 0
 0
 0
 0

 0
 0
 0
 2
 0
 0
 2
 0
 0
 0
 0
 0
 0

  $\mathbf{2}$  $\mathbf{2}$ 0 0 0 0 0 2 0 2 0 0 0 0 0 0 0 0 0 0 0  $\mathbf{2}$  $0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$  $\mathbf{2}$ 0 0 0 0 0 0 0 0 0  $\mathbf{2}$ 0 0 0 0 0 0  $0 \ 2$  $1 \ 1 \ 1 \ 0 \ 1 \ 0$ 0 0 0 0 0 0 0 0 0 0 0 0  $0 \ 2 \ 0 \ 0$  $\mathbf{2}$ 0 0 

 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0 0 0 0 0  $1 \ 2$  $2 \ 0 \ 0 \ 0 \ 0 \ 2 \ 0$  $2 \ 0 \ 0 \ 2 \ 2 \ 2$  $\mathbf{2}$  $\mathbf{2}$ 

The numbers written as subscript indicate the weight of each complete weight enumerator. The details of other complete weight enumerators can be seen in Appendix A.

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

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

In this dissertation, some polynomials are not written because they are too large.

Let  $\mathfrak W$  be a ring generated by the set W of complete weight enumerators:

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

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

**Theorem 4.1.1.** The ring  $\mathfrak{W}$  coincides with  $\mathfrak{R}^8$ . In other words,

$$\mathfrak{W}_d = \mathfrak{R}_d^8$$

for any positive integer d.

*Proof.* By the information taken from the dimension formula of  $\mathfrak{R}^8$ , we generate  $\mathfrak{W}$  by utilizing some complete weight enumerators of non-equivalent codes. The computation shows that the dimension of  $\mathfrak{W}_d$  is equal to the dimension of  $\mathfrak{R}^8_d$  for any positive integer d. The dimension of each  $\mathfrak{W}_k$  is shown in Table 4.1.

Table 4.1: The dimensions of  $\mathfrak{R}^8_k$  and  $\mathfrak{W}_k$ 

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

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

#### 4.2 E-Polynomials

In this section, we define an E-polynomial for a  $4 \times 4$  matrix group. Let **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

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

where

and  $\sigma_0$  is the first row of  $\sigma$ . The definition of E-polynomial for the group  $G^8$  is similar. For simplicity, we write  $\varphi_k$  instead of  $\varphi_k^G$ .

The subgroup K of  $G^8$  is of order 16. We denote by  $\mathfrak{E}^8$  the ring generated by  $\varphi_k$  for the group  $G^8$ .

Denote by  $\kappa$  the cardinality of  $K \setminus G$ . The numbers  $\kappa$  for G and  $G^8$  can be seen in Table 4.2.

Table 4.2: The number $\kappa$									
Group	Order	K	$\kappa$						
G	384	8	48						
$G^8$	1536	16	96						

**Theorem 4.2.1.** The ring  $\mathfrak{E}$  (resp.  $\mathfrak{E}^8$ ) can be generated by the polynomials  $\varphi_k$  where

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

(resp. 
$$k \equiv 0 \mod 8$$
,  $8 \le k \le 96$ ).

*Proof.* Let  $\sigma_i$  be the representative of  $K \setminus G^8$   $(1 \le i \le \kappa)$ . We define

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

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

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

We give the explicit forms of  $\varphi_8$  for the group  $G^8$  as follows.

$$\begin{split} \varphi_8 = &\frac{1}{1536} (148t_0^8 + 4t_1^8 + 1120t_0^3t_1^4t_2 - 336t_0^6t_2^2 + 1120t_0t_1^4t_2^3 + 1400t_0^4t_2^4 - 336t_0^2t_2^6 + 148t_2^8 \\ &+ 32t_1^7t_3 + 4480t_0^3t_1^3t_2t_3 + 4480t_0t_1^3t_2^3t_3 + 112t_1^6t_3^2 + 6720t_0^3t_1^2t_2t_3^2 + 6720t_0t_1^2t_2^3t_3^2 \\ &+ 224t_1^5t_3^3 + 4480t_0^3t_1t_2t_3^3 + 4480t_0t_1t_2^3t_3^3 + 280t_1^4t_3^4 + 1120t_0^3t_2t_3^4 + 1120t_0t_2^3t_3^4 + 224t_1^3t_3^5 \\ &+ 112t_1^2t_3^6 + 32t_1t_3^7 + 4t_3^8), \end{split}$$

It is difficult to write all E-polynomials happening. In Table 4.3, we show the number of monomials of  $\varphi_k$  for  $G^8$ .

1001	0 1.0. II	io mun		lonomi	$\varphi_{l}$
k	$l(\varphi_k)$	k	$l(\varphi_k)$	k	$l(\varphi_k)$
8	24	40	1556	72	8464
16	127	48	2619	80	11511
24	374	56	4082	88	15214
32	829	64	6009	96	19637

Table 4.3: The number of monomials of  $\varphi_k$ 

The information we get from Theorem 4.2.1 is the fact that the rings  $\mathfrak{E}, \mathfrak{E}^8$  are finitely generated. By this condition, the natural question is if we can find the minimal generators of  $\mathfrak{E}$  and  $\mathfrak{E}^8$ . In the next theorem, we determine the generators of  $\mathfrak{E}$  and  $\mathfrak{E}^8$ .

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

Table 4.4: The dimensions of  $\mathfrak{R}^8_k$  and  $\mathfrak{E}^8_k$ 

**Theorem 4.2.2.** The rings  $\mathfrak{E}$ ,  $\mathfrak{E}^8$  are minimally generated by the *E*-polynomials of weights

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

*Proof.* This is done by the computation. After constructing the polynomials, we ensure if the polynomial can be expressed by other polynomials. The dimensions of  $\mathfrak{E}^8$  are demonstrated in Table 4.4.

For example, we show the generator for n = 40. In Table 4.4, the dimension of  $\mathfrak{E}_{40}^8$  is 7. The basis elements of this space is

$$\varphi_8^5, \varphi_8^3\varphi_{16}, \varphi_8^2\varphi_{24}, \varphi_8\varphi_{32}, \varphi_8\varphi_{16}^2, \varphi_{16}\varphi_{24}, \varphi_{40}.$$

From Table 4.4, we can see that 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 4.2.3.** The invariant ring  $\Re^8$  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

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

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

*Proof.* This is by the computation. The result is shown in Table 4.5.

Die 4.5: The dimensions of $\mathcal{A}_k$						
	k	8	16	24	32	40
	$\mathrm{dim}\mathfrak{R}^8_k$	4	11	25	48	83
	$\mathrm{dim}\widetilde{\mathfrak{R}}$	4	11	25	48	83

Table 4.5: The dimensions of  $\mathfrak{R}^8_k$  and  $\widetilde{\mathfrak{R}}$ 

Since the polynomials in  $\Re^G$  are in 4 variables, by Theorem 2.5.3, there are 4 polynomials which are algebraically independents. Using the criterion in Proposition 2.5.1, we can show that the polynomials

$$p_{8a}, o_8, k_8, q_{24a}$$

are algebraically independent.

#### 4.3 Other E-polynomials

The groups defined here is referred to [7]. We define two groups  $H_1$  and  $H_2$  taken from the reference.

Let  $C \subset \mathbb{F}_3^n$  be a self-dual code. There are some facts about C. 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  $S_2$ 

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

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  $\eta_5$  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. We omit the details of the modular form because we only focus on the matrices occur.

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 4.6.

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.

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

Table 4.6: The number  $\kappa$  of  $H_1$ ,  $H_2$ 

	Group	Order	K	$\kappa$	
	$H_1$	24	3	8	
	$H_2$	120	10	12	
		'			
и		1	-		
11	$2 \cdot \frac{1}{(1 - 1)^2}$	$(-t^2)(1-$	$t^{6})(1$	$-t^{10}$	j.

From the dimension formulas above, we have some information about the generators of each ring. The ring  $\Re(H_1)$  can be generated by some polynomials related to the ternary codes of weights 4 and 6, while  $\Re(H_2)$  can be generated by some polynomials of degrees 2,6, and 10 related to the symmetric Hilbert modular form of weight. We use the term degree in  $\Re(H_2)$  because "weight" has a different meaning in modular form.

Following the method described in the previous section, we obtain that the ring generated by  $\varphi_k^{H_1}$  (respectively  $\varphi_k^{H_2}$ ) is minimally generated by the E-polynomials  $\varphi_4$  and  $\varphi_6$ (respectively  $\varphi_2$ ,  $\varphi_6$ , and  $\varphi_{10}$ ). Therefore, in this situation we can write

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

and

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

Since the size of matrices in  $H_1$ ,  $H_2$  are different with the matrices in the previous section, we note that there is a difference between the E-polynomials defined. The difference is only on the number of variables. In the group  $H_1$ , we use two variables  $t_1, t_2$ . We deal with the variables  $t_1, t_2, t_3$  for the group  $H_2$ .

The following tables shows the comparisons between the the invariant rings and the E-polynomials.

Table 4.7: The dimensions of  $\mathfrak{R}(H_1)_k$  and  $\mathfrak{E}(H_1)_k$ 

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

Table 4.8: The dimensions of  $\mathfrak{R}(H_2)_k$  and  $\mathfrak{E}(H_2)_k$ 

l	2	4	6	8	10
$\dim \mathfrak{R}(H_2)_l$	1	1	2	2	3
$\dim \mathfrak{E}(H_2)_l$	1	1	2	2	3

The conclusion we have from Tables 4.7 and 4.8 is the following. We obtain that

$$\dim \mathfrak{E}(H_1)_k = \dim \mathfrak{R}(H_1)_k$$

$$(\dim \mathfrak{E}(H_2)_l = \dim \mathfrak{R}(H_2)_l)$$

for  $k \ge 4$  and  $k \equiv 0 \mod 2$  (respectively  $l \equiv 0 \mod 2$ ).

We close this section by giving the explicit forms of the generators.

$$\begin{split} \varphi_4^{H_1} = & \frac{1}{24} (8t_0^4 + 64t_0t_1^3), \\ \varphi_6^{H_1} = & \frac{6}{24} (32t_0^6 - 640t_0^3t_1^3 - 256t_1^6) \\ \varphi_2^{H_2} = & \frac{1}{120} (40t_0^2 + 160t_1t_2) \\ \varphi_6^{H_2} = & \frac{5}{120} (104t_0^6 + 768t_0t_1^5 + 480t_0^4t_1t_2 + 5760t_0^2t_1^2t_2^2 + 5120t_1^3t_2^3 + 768t_0t_2^5) \\ \varphi_{10}^{H_2} = & \frac{125}{120} (2504t_0^{10} + 32256t_0^5t_1^5 + 4096t_1^{10} + 1440t_0^8t_1t_2 + 430080t_0^3t_1^6t_2 \\ & + 80640t_0^6t_1^2t_2^2 + 737280t_0t_1^7t_2^2 + 1075200t_0^4t_1^3t_2^3 + 3225600t_0^2t_1^4t_2^4 \\ & + 32256t_0^5t_2^5 + 1032192t_1^5t_2^5 + 430080t_0^3t_1t_2^6 + 737280t_0t_1^2t_2^7 + 4096t_2^{10}). \end{split}$$

### Chapter 5

## **Conclusions and Discussions**

In this chapter, we give the conclusions of our dissertations. In the end of this chapter, we close by delivering the discussion that may be able to continue in the future.

#### 5.1 Conclusions

From the previous chapter, we can say that the main part of our dissertation is finding the generator of a ring appearing. We start from the ring generated by the E-polynomials related to the group  $G^8$ . The ring of E-polynomials occurred is minimally generated by E-polynomials of weights

The ring generated by the E-polynomials here is strictly smaller than the ring  $\mathfrak{W}$  of the complete of weight enumerators of Type II  $\mathbb{Z}_4$ -codes. Then we can generate the ring  $\mathfrak{W}$  by combing the E-polynomials and the complete weight enumerators of some  $\mathbb{Z}_4$ -codes. We can write as follows.

$$\Re^8 = \mathbb{C}[\varphi_k, p_8, o_8, k_8, p_{16}, p_{24}, q_{24}, p_{32} \mid k = 8, 16, 24].$$

The dimension formula of  $\Re^8$  is

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

For the groups  $H_1$ ,  $H_2$  with  $|H_1| = 24$ ,  $|H_2| = 120$ , the E-polynomials of each group can generate the ring of each group. We can write

$$\mathfrak{R}(H_1) = \mathbb{C}[\varphi_4, \varphi_6],$$
  
 $\mathfrak{R}(H_2) = \mathbb{C}[\varphi_2, \varphi_6, \varphi_{10}]$ 

The dimension formulas of  $\mathfrak{R}(H_1), \mathfrak{R}(H_2)$  are the following.

$$H_1: \quad \frac{1}{(1-t^4)(1-t^6)},$$
  
$$H_2: \quad \frac{1}{(1-t^2)(1-t^6)(1-t^{10})}.$$

#### 5.2 Discussion

The notion of E-polynomials in the perspective of coding theory make us curious whether we can connect number theory to invariant theory. With the known theory in classical invariant theory and number theory, we propose in the future to construct the analogue theory of Eisenstein series. The reader who is interested in this discussion can see [10].

The discussion about the invariant ring related to  $\mathbb{Z}_4$ -codes also encourages us to continue investigating another ring. It is the ring related to Jacobi polynomials of binary codes. The notion of Jacobi polynomials for codes first introduced by Ozeki [17]. Its main theorem described the transformation formula for the Jacobi polynomials of a code. The Molien series and the structure of the invariant ring of Jacobi polynomials then were determined in [2]. By defining a new map from the space of Jacobi polynomials into the space of Jacobi forms, Bannai and Ozeki [2] also extended Broué-Enguehard correspondence. The Jacobi polynomial notions in the sense of coordinates then were given in [3]. In [3], it was shown that, in some cases, the Jacobi polynomials can be determined uniquely by the polarization operator.

For the closing sentence, I thank to Allah the almighty who created integers. Also, prayers and greeting are delivered to the prophet Muhammad.

## Bibliography

- Bannai, E., Dougherty, S. T., Harada, M., and Oura, M. (1999). Type ii codes, even unimodular lattices and invariant rings. J. Jour., 45:1194–1205.
- [2] Bannai, E. and Ozeki, M. (1996). Construction of Jacobi forms from certain combinatorial polynomials. *Proc. Japan Acad.*
- [3] Bonnecaze, A., Mourrain, B., and Solé, P. (1999). Jacobi polynomials, Type II codes, and designs. *Des. Codes Cryptogr.*
- [4] Bonnecaze, A., Solé, P., Bachoc, C., and Mourrain, B. (1997). Type II codes over Z<sub>4</sub>. *IEEE Trans. Inform. Theory*, 43:969–976.
- [5] Bosma, W., Cannon, J., and Playoust, C. (1997). The magma algebra system i: The user language. J. Symbolic Comput., 24(3-4):235–265.
- [6] Cox, D., Little, J., and O'shea, D. (1996). Ideals, varieties, and algorithms : an introduction to computational algebraic geometry and commutative algebra. Springer, New York.
- [7] Ebeling, W. (2013). Lattices and Codes: A course Partially Based on Lectures by F. Hirzebruch. Springer, New York.
- [8] Hamid, N. (2019). Note on E-polynomials associated to  $\mathbb{Z}_4$ -codes. Nihonkai Math. J.
- [9] Hamid, N. (2019 (accessed May 6, 2020)). The generator matrices. https://sites.google.com/view/hamidelfath/generators.
- [10] Hamid, N., Kosuda, M., and Oura, M. Certain subrings in classical invariant theory. *Preprint.*
- [11] Humphreys, J. E. (1990). *Reflection groups and Coxeter groups*. Cambridge University Press, New York.
- [12] Lang, S. (1993). Algebra, Revised Third Edition. Springer-Verlag.
- [13] MacWilliams, F. J. and Sloane, N. (1981). The theory of error-correcting codes. North-Holland, New York.
- [14] Miezaki, T. (2019). On Eisenstein polynomials and zeta polynomials. J. Pure Appl. Algebra.

- [15] Motomura, T. and Oura, M. (2018). E-polynomials associated to Z<sub>4</sub>-codes. Hokkaido Math. J., 2:339–350.
- [16] Oura, M. (2009). Eisenstein polynomials associated to binary codes i. Int. J. Number Theory, 5(4):635–640.
- [17] Ozeki, M. (1997). On the notion of Jacobi polynomials for codes. Math. Proc. Camb. Phil. Soc.
- [18] Pless, V., Leon, J. S., and Fields, J. (1997). All Z<sub>4</sub> codes of Type II and length 16 are known. Journal of Combinatorial Theory, Series A,, 78:32–50.
- [19] Roman, S. (2008). Advanced Linear Algebra. Springer, New York.
- [20] The Sage Developers (2017). SageMath, the Sage Mathematics Software System (Version 8.1). https://www.sagemath.org.

## Appendix A

## **Generator Matrices**

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