Dissertation

The Average of Complete Joint Weight Enumerators of Codes

Graduate School of
Natural Science and Technology
Kanazawa University

Division of Mathematical and Physical Sciences

Student ID No.	: 1824012015
Name	: Himadri Shekhar Chakraborty
Chief advisor	: Professor Manabu Oura
Date of submission	: June 21, 2021

Dedicated to

My Father

Late Sashanka Shekhar Chakraborty

Contents

Acknowledgement v

Abstract vii

Chapter 1. Introduction 1

Chapter 2. Linear Codes 6

2.1. Codes over $\mathbb{F}_q$ 6

2.2. Codes over $\mathbb{Z}_k$ 9

2.3. Weight enumerators 10

2.4. MacWilliams identity 13

Chapter 3. Variants of Weight Enumerators 17

3.1. Joint weight enumerators 18

3.2. Average of joint weight enumerators 20

3.3. Yoshida's theorem 21

Chapter 4. Generalization of Yoshida's Theorem 25

4.1. Basic definitions and properties 25

4.2. Average of complete joint weight enumerators 28

4.3. Average of g-fold complete joint weight enumerators 32

Chapter 5. Average Intersection Number 36

5.1. Properties of average intersection number 36

5.2. Self-dual codes over $\mathbb{F}_q$ 38

Bibliography 44

Acknowledgement

First of all, I would like to express my deep appreciation and gratitude to my supervisor Professor Manabu Oura, Faculty of Mathematics and Physics, Kanazawa University, Japan for his highly valued guidance and constant inspiration throughout the journey of this dissertation. I am sincerely grateful to Professor Tsuyoshi Miezaki, Department of Applied Mathematics, Waseda University, Japan (Ex-Faculty, Faculty of Education, University of the Ryukyus, Japan) for his valuable comments and helpful suggestions during my research work.

I am thankful to my lab members for supporting me at various stages of my research with helpful discussions and to adapt life in Japan easily. I am grateful to Ministry of Education, Culture, Sports, Science and Technology (Monbukagakusho:MEXT) for providing me Japanese Government Scholarship that enabled me to pursue my doctoral program. Thanks to the authority of Shahjalal University of Science and Technology, Sylhet, Bangladesh for permitting me study leave for pursuing my Ph.D. program at Kanazawa University, Japan.

I am immensely grateful to my beloved mother Namita Chakraborty for her blessings and confidence in me, my dearest wife Dulaly Sharma Charza for encouraging me unconditionally, and my loving daughter Deboleena Chakraborty for patiently accept her childhood staying far from me.

Finally, I am thankful to all of my teachers, colleagues, friends and relatives for their support and best wishes which have given me presence of mind leading my research work up to this dissertation.

Abstract

In this thesis, we concentrate on the average of complete joint weight enumerators of linear codes over $\mathbb{F}_q$ and $\mathbb{Z}_k$. From the very beginning in the study of codes became inseparable from the study of their weight enumerators. One of our main results in this work is to give an illustration of the average of complete joint weight enumerators of two linear codes of length n over $\mathbb{F}_q$ and $\mathbb{Z}_k$ in terms of the compositions of n and their distributions in the codes. Next we give a generalization of the illustration for the average of the g-fold complete joint weight enumerators of linear codes over $\mathbb{F}_q$ and $\mathbb{Z}_k$.

Self-dual codes are one of the most remarkable branches in the study of coding theory. The study of the average intersection numbers of a pair of Type I (resp. Type II) codes of length n over $\mathbb{F}_2$, where the average is considered over the all Type I (resp. Type II) codes of length n, inspired us to investigate the analogues for the case of Type III (resp. Type IV) codes of length n over $\mathbb{F}_3$ (resp. $\mathbb{F}_4$). Our another main result is to present an asymptotic bound for the average of intersection numbers of a pair of Type III (resp. Type IV) codes. Finally, we obtain an asymptotic bound for the second moment of the average of intersection numbers of a pair of Type III (resp. Type IV) codes.

CHAPTER 1

Introduction

In 1948, C. Shannon [**20**] introduced a sophisticated branch of mathematics called *coding theory* with an application to the area of *digital communication system*. Among the various types of coding, we are particularly interested in the wing of *error-correcting codes* which have a special role in data transmission through satellite and cellular telephone.

Let $\mathbb{F}_q$ be a finite field, where q is a prime power. An $\mathbb{F}_q$-*code* of length n is a subset of $\mathbb{F}_q^n$. The codes over $\mathbb{F}_2$ are called *binary codes*, while the codes over $\mathbb{F}_3$ and $\mathbb{F}_4$ are known as *ternary codes* and *quaternary codes*, respectively. An $\mathbb{F}_q$-*linear code* is a linear subspace of $\mathbb{F}_q^n$. At the very beginning of the study in coding theory M. J. E. Golay [**7**] and R. W. Hamming [**8**] introduced two different binary linear codes which are known as the *Golay code* and the *Hamming code*, respectively.

In recent years, there has been interest in studying codes over the finite rings $\mathbb{Z}_k$ of integers modulo k $(k \geq 2)$. Like as an $\mathbb{F}_q$-code, the $\mathbb{Z}_k$-*code* of length n is a subset of a $\mathbb{Z}_k^n$. But a $\mathbb{Z}_k$-*linear code* of length n is a submodule of $\mathbb{Z}_k^n$. In 1994, A. R. Hammons et al. [**9**] established the relations between certain well-known families of nonlinear binary codes and $\mathbb{Z}_4$-linear codes.

Throughout our study, we assume that $\mathfrak{R}$ denotes either the finite field $\mathbb{F}_q$ or the finite ring $\mathbb{Z}_k$. The elements of an $\mathfrak{R}$-linear code are known as *codewords* while the number of nonzero coordinates is called the *weight* of a codeword. The *weight enumerator* of an $\mathfrak{R}$-linear code of length n is a homogeneous polynomial of degree n whose each term interprets the number of codewords for a certain weight. Dual of a code plays an important role in the study of coding theory. We can determine the dual of a code with respect to a given inner product on $\mathfrak{R}^n$. F. J. MacWilliams [**11**] showed that without knowing any information about the dual of an $\mathbb{F}_q$-linear code, the weight enumerator of the dual code can be uniquely determined from the weight enumerator of the $\mathbb{F}_q$-linear code. These types of relations are known as *MacWilliams identity*. For binary linear codes, a generalization of the MacWilliams identity for genus g was given by B. Runge [**19**]. Further E. Bannai, S. T. Dougherty, M. Harada and M. Oura [**1**] gave an analogue of the MacWilliams identity for genus g for the codes over $\mathbb{Z}_{2k}$.

F. J. MacWilliams and N. J. A. Sloane [**14**] introduced the notion of the complete weight enumerator of an $\mathbb{F}_q$-linear code and gave a generalization of the MacWilliams identity for the complete weight enumerator. T. Miezaki and M. Oura [**15**] pointed out a relation between the genus g complete weight enumerator and the genus g cycle index of an $\mathbb{F}_q$-linear code. F. J. MacWilliams, C. L. Mallows and N. J. A. Sloane [**12**] introduced the notion of the joint weight enumerator of two $\mathbb{F}_q$-linear codes and also discussed the MacWilliams type identity for the joint weight enumerator. Further, the notion of the g-fold complete joint weight enumerator of g linear codes over $\mathbb{F}_q$ was given by I. Siap and D. K. Ray-Chaudhuri [**21**] while the concept of the g-fold joint weight enumerator and the g-fold multi-weight enumerator of codes over $\mathbb{Z}_k$ was investigated by S. T. Dougherty, M. Harada and M. Oura [**5**].

In 1989, T. Yoshida [**22**] introduced the notion of the average joint weight enumerators of two binary linear codes, and gave a representation of the average joint weight enumerators using the ordinary weight distributions of the codes. In this thesis, we call this representation as *Yoshida's theorem.* This gives rise to a natural question: is there a generalization of the average joint weight enumerators that is analogous to Yoshida's theorem? The first aim of this thesis is to give a candidate that answers this question.

In this thesis, we define the average complete joint weight enumerator of two linear codes over $\mathfrak{R}$, and give a generalization of Yoshida's theorem for it. Moreover, we extend the idea of the average complete joint weight enumerator to the average of the g-fold complete joint weight enumerators of linear codes over $\mathfrak{R}$. We take the average on all permutationally (not monomially) equivalent linear codes over $\mathfrak{R}$.

A *self-dual* code is a code that is equal to its dual. For this type of codes over $\mathbb{F}_q$, it is well-known that the length of the code is twice its dimension. In 1970, A. M. Gleason [**6**] provides the main motivation for studying self-dual codes over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$. These codes have a property that the weight of each codewords of a certain code is divisible by a certain integer greater than 1. A binary self-dual code is called *Type* II if all weights of the codewords are divisible by 4, otherwise called *Type* I. A *Type* III code is a self-dual code over $\mathbb{F}_3$ whose weights of the codewords are divisible by 3. Finally, a self-dual code over $\mathbb{F}_4$ is called *Type* IV if every codeword has even weight.

In 1991, T. Yoshida [**23**], introduced the notion of the average intersection number for two binary codes. T. Yoshida [**23**] also proved that the average of intersection numbers of a pair of Type I (resp. Type II) codes over $\mathbb{F}_2$ and their second moments are asymptotically bounded. Here we have another question: what is the asymptotic bound for the average of intersection numbers and its second moments of a pair of Type III codes over $\mathbb{F}_3$ as well as Type IV codes over $\mathbb{F}_4$? The second aim of this thesis is to answer this question.

In Chapter 2, we give the basic definitions and notations that we use in this thesis. In Section 2.1, we discuss the basic concepts of a linear code over $\mathbb{F}_q$ and its properties. In Section 2.2, we give a brief introduction about $\mathbb{Z}_k$-linear codes. The concept of the weight enumerator of a code is discussed in Section 2.3. The MacWilliams identity plays an important role in the study of weight enumerators of a code. We discuss this identity in Section 2.4.

In Chapter 3, we review various types of weight enumerators, such as joint weight enumerators and its properties specially the MacWilliams type identity in Section 3.1, and average joint weight enumerator in Section 3.2. In Section 3.2, we discuss Yoshida's theorem. This theorem is the main topic of our interest in this thesis.

In Chapter 4, we present a generalization of the concept of the average joint weight enumerator for the binary codes, namely the average of complete joint weight enumerators of two linear codes over $\mathfrak{R}$. In Section 4.1, we give the MacWilliams type identity for the complete joint weight enumerators of codes over $\mathfrak{R}$. The main goal of this chapter is to answer our first question. In Section 4.2, we answer the question and give a generalization of Yoshida's theorem for the average of complete joint weight enumerator of two linear codes over $\mathfrak{R}$. In Section 4.3, we extend the idea of the average complete joint weight enumerator to the average of g-fold complete joint weight enumerators of linear codes over $\mathfrak{R}$ and give a g-fold analogue of Yoshida's theorem.

In Chapter 5, our aim is to find an answer of our second question. In Section 5.1, we define the average intersection number of two codes over $\mathfrak{R}$ and discuss a relation with the average of the complete joint weight enumerator of codes over $\mathfrak{R}$. We also give a formula to evaluate the average intersection numbers. In Section 5.2, we give the asymptotic bounds for the average of intersection numbers of a pair of Type III codes over $\mathbb{F}_3$ (resp. Type IV codes over $\mathbb{F}_4$) and for their second moments which is actually the answer to our second question.

CHAPTER 2

Linear Codes

In this chapter, we give the basic definitions and notations that we use in the entire thesis. In Section 2.1, we discuss the basic concepts of a linear code over $\mathbb{F}_q$ and its properties. In Section 2.2, we give a brief introduction about $\mathbb{Z}_k$-linear codes. The concept of weight enumerator of a code is discussed in Section 2.3. The MacWilliams identity plays an important role in the study of weight enumerator of a code. We discuss this identity in Section 2.4. We refer the readers to [**1, 10, 14, 16**] for more details about these concepts.

2.1. Codes over $\mathbb{F}_q$

Let $\mathbb{F}_q$ be a finite field of order q, where q is a prime power. We denote by $\mathbb{F}_q^n$ the n-dimensional vector space over $\mathbb{F}_q$. The elements of $\mathbb{F}_q^n$ is usually written in the form $\mathbf{u} = (u_1, u_2, \ldots, u_n)$. A *code* C of length n is a nonempty subset of $\mathbb{F}_q^n$. The elements of C are called *codewords*, and n is the (*word*) *length* of C.

Definition 2.1.1 An $\mathbb{F}_q$-*linear code* is a linear subspace of $\mathbb{F}_q^n$.

If C is an $\mathbb{F}_q$-linear code with dimension k, then C is called an $[n,k]$ *linear code*. An $[n,k]$ linear code C has q^k codewords. A *generator matrix* G for an $[n,k]$ linear code C is any $k \times n$ matrix whose rows form a basis of C. A *parity check matrix* H for the $[n,k]$ code C is an $(n-k) \times n$ matrix over $\mathbb{F}_q$ with *rank* $n-k$ such that for any $\mathbf{u} \in \mathbb{F}_q^n$, $\mathbf{u} \in C$ if and only if $H\mathbf{u}^T = \mathbf{0}$. The generator matrix of an $[n,k]$ linear code is said to be in the *standard form* if it is of the form $[I_k \mid A]$, where I_k is the $k \times k$ identity matrix, and A is a $k \times (n-k)$ matrix. In the following theorem A^T denotes the transpose of A.

Theorem 2.1.1 ([**10**]). *If $G = [I_k \mid A]$ is a generator matrix for the $[n,k]$ linear code C in standard form, then $H = [-A^T \mid I_{n-k}]$ is a parity check matrix for C.*

Example 2.1.1 We denote by $\mathcal{H}_7$ the $[7,4]$ *Hamming code*. The generator matrix $G = [I_4 \mid A]$ of $\mathcal{H}_7$ in standard form is

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right].$$

Then by Theorem 2.1.1, we have a parity check matrix $H = [A^T \mid I_3]$ for $\mathcal{H}_7$ is

$$H = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right].$$

In order to define an *inner product* of the elements $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$ in $\mathbb{F}_q^n$, we let $q = p^f$ for some prime number p. The *inner product* of $\mathbf{u}$ and $\mathbf{v}$ is denoted by $\mathbf{u} \cdot \mathbf{v}$ and is defined as

$$\mathbf{u} \cdot \mathbf{v} := \sum_{i=1}^{n} (u_i, v_i),$$

where for any $a, b \in \mathbb{F}_q$,

$$(a, b) := \begin{cases} ab^{\sqrt{q}} & \text{if } f \text{ is even;} \\ \\ ab & \text{otherwise.} \end{cases}$$

If $\mathbf{u} \cdot \mathbf{v} = 0$, we call $\mathbf{u}$ and $\mathbf{v}$ *orthogonal*. An element $\mathbf{u} \in \mathbb{F}_q^n$ is called *self-orthogonal* if $\mathbf{u} \cdot \mathbf{u} = 0$.

Definition 2.1.2 Let C be an $\mathbb{F}_q$-linear code of length n. Then the *dual code* of C is given by

$$C^{\perp} := \{\mathbf{u} \in \mathbb{F}_q^n \mid \mathbf{u} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{v} \in C\}.$$

It is easy to show that $C^{\perp}$ is the same as the set of all parity checks on C. If C has generator matrix G and parity check matrix H, then the generator and parity check matrices of $C^{\perp}$ are H and G, respectively. This implies that if C is an $[n, k]$ linear code then $C^{\perp}$ is an $[n, n-k]$ linear code.

Definition 2.1.3 An $\mathbb{F}_q$-linear code is said to be *self-orthogonal* if $C \subseteq C^{\perp}$, and *self-dual* if $C = C^{\perp}$.

Remark 2.1.1 The length n of a self-dual code is even and the dimension is $n/2$.

Example 2.1.2 Let $\mathbb{F}_3 = \{0, 1, 2\}$. Let C be a $[4, 2]$ code over $\mathbb{F}_3$ with generator matrix:

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}.$$

It is easy to check that $C = C^{\perp}$. Therefore, C is a self-dual code. The elements of C are listed as follows:

$$\begin{array}{lll} (0,0,0,0), & (0,1,1,2), & (0,2,2,1), \\ (1,0,1,1), & (1,1,2,0), & (1,2,0,2), \\ (2,0,2,2), & (2,1,0,1), & (2,2,1,0). \end{array}$$

2.2. Codes over $\mathbb{Z}_k$

Let $\mathbb{Z}_k$ be the ring of integers modulo k for $k \geq 2$. A $\mathbb{Z}_k$-*linear code* of length n is an additive subgroup of $\mathbb{Z}_k^n$. Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ be the elements of $\mathbb{Z}_k^n$. We define the *inner product* of $\mathbf{u}$ and $\mathbf{v}$ on $\mathbb{Z}_k^n$ as follows:

$$\mathbf{u} \cdot \mathbf{v} := u_1 v_1 + u_2 v_2 + \cdots + u_n v_n.$$

Let C be a $\mathbb{Z}_k$-linear code of length n. Like as the codes over $\mathbb{F}_q$ we call the elements of C *codewords*. The matrix whose rows generate the code C is called a *generator matrix* of C. The *dual code* $C^{\perp}$ of C is defined as

$$C^{\perp} := \{\mathbf{u} \in \mathbb{Z}_k^n \mid \mathbf{u} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{v} \in C\}.$$

We call C *self-orthogonal* if $C \subseteq C^{\perp}$, and *self-dual* if $C = C^{\perp}$.

2.3. Weight enumerators

We assume that $\mathfrak{R}$ denotes either the finite field $\mathbb{F}_q$ of order q, where q is a prime power or the ring $\mathbb{Z}_k$ of integers modulo k for some integer $k \geq 2$.

Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ be the elements of $\mathfrak{R}^n$. The (*Hamming*) *distance* $\operatorname{dist}(\mathbf{u}, \mathbf{v})$ between two elements $\mathbf{u}, \mathbf{v} \in \mathfrak{R}^n$ is defined by

$$\operatorname{dist}(\mathbf{u}, \mathbf{v}) := \#\{i \mid u_i \neq v_i\}.$$

It is immediate from the definition that the distance function $\operatorname{dist}(\mathbf{u}, \mathbf{v})$ is a *metric* on $\mathfrak{R}^n$. That is, the distance function satisfies the following properties:

(i) (*non-negativity*) $\operatorname{dist}(\mathbf{u}, \mathbf{v}) \geq 0$ for all $\mathbf{u}, \mathbf{v} \in \mathfrak{R}^n$.

(ii) $\operatorname{dist}(\mathbf{u}, \mathbf{v}) = 0$ if and only if $\mathbf{u} = \mathbf{v}$.

(iii) (*symmetry*) $\operatorname{dist}(\mathbf{u}, \mathbf{v}) = \operatorname{dist}(\mathbf{v}, \mathbf{u})$ for all $\mathbf{u}, \mathbf{v} \in \mathfrak{R}^n$.

(iv) (*triangle inequality*) $\operatorname{dist}(\mathbf{u}, \mathbf{w}) \leq \operatorname{dist}(\mathbf{u}, \mathbf{v}) + \operatorname{dist}(\mathbf{v}, \mathbf{w})$ for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathfrak{R}^n$.

We denote by $\operatorname{supp}(\mathbf{u})$ of an element $\mathbf{u} \in \mathfrak{R}^n$ the *support* of $\mathbf{u}$ and defined as

$$\operatorname{supp}(\mathbf{u}) := \{i \mid u_i \neq 0\}.$$

The (*Hamming*) *weight* of an element $\mathbf{u} \in \mathfrak{R}^n$ is denoted by $\operatorname{wt}(\mathbf{u})$ and defined as $\operatorname{wt}(\mathbf{u}) := |\operatorname{supp}(\mathbf{u})|$. The *minimum distance* of an $\mathfrak{R}$-linear code C is the minimum of the (Hamming) distance $\operatorname{dist}(\mathbf{u}, \mathbf{v})$ for $\mathbf{u}, \mathbf{v} \in C$ and $\mathbf{u} \neq \mathbf{v}$. The following theorem gives a well-known relation between the distance function and the weight function.

Theorem 2.3.1 ([**1, 10**]). *If* $\mathbf{u}, \mathbf{v} \in \mathfrak{R}^n$, *then* $\mathrm{dist}(\mathbf{u}, \mathbf{v}) = \mathrm{wt}(\mathbf{u} - \mathbf{v}) = \mathrm{wt}(\mathbf{w})$ *for some* $\mathbf{w} \in \mathfrak{R}^n$. *If* C *is an* $\mathfrak{R}$*-linear code, the minimum distance* d *is the same as the minimum weight of the nonzero codewords of* C.

Let C be an $\mathfrak{R}$-linear code of length n. Then for $0 \leq i \leq n$, we call

$$\mathcal{A}_i^C := \#\{\mathbf{u} \in C \mid \mathrm{wt}(\mathbf{u}) = i\}$$

the *weight distribution* of C. We can easily verity the following facts about the weight distribution of an $\mathfrak{R}$-linear code with the minimum distance d.

(i) $\mathcal{A}_0^C = 1$.

(ii) $\mathcal{A}_1^C = \mathcal{A}_2^C = \cdots = \mathcal{A}_{d-1}^C = 0$.

(iii) $\mathcal{A}_0^C + \mathcal{A}_1^C + \cdots + \mathcal{A}_n^C = |C|$.

Example 2.3.1 Let C be the code over $\mathbb{F}_3$ of Example 2.1.2. The weight distribution of C is as follows:

$$\mathcal{A}_0 = 1, \quad \mathcal{A}_1 = A_2 = 0, \quad \mathcal{A}_3 = 8, \quad \mathcal{A}_4 = 0.$$

The *weight enumerator* of an $\mathfrak{R}$-linear code of length n is a homogeneous polynomial of degree n which presents the weight distribution of C and defined as

$$w_C(x, y) := \sum_{\mathbf{u} \in C} x^{n-\mathrm{wt}(\mathbf{u})} y^{\mathrm{wt}(\mathbf{u})} = \sum_{i=0}^{n} \mathcal{A}_i^C x^{n-i} y^i,$$

where x and y are indeterminates. Let the elements of $\mathfrak{R}$ be $0 = \omega_0, \omega_1, \ldots, \omega_{|\mathfrak{R}|-1}$ in some fixed order. Then the *composition* of an element $\mathbf{u} \in \mathfrak{R}^n$ is defined as

$$\mathrm{comp}(\mathbf{u}) := s(\mathbf{u}) := (s_a(\mathbf{u}) : a \in \mathfrak{R}),$$

where $s_a(\mathbf{u})$ denotes the number of coordinates of $\mathbf{u}$ that are equal to $a \in \mathfrak{R}$. Obviously,

$$\sum_{a\in\mathfrak{R}} s_a(\mathbf{u}) = n.$$

In general, a *composition* s of n is a vector $s = (s_a : a \in \mathfrak{R})$ with non-negative integer components such that

$$\sum_{a\in\mathfrak{R}} s_a = n.$$

Let C be an $\mathfrak{R}$-linear code of length n. We denote by T_s^C the set of codewords of C with composition s, that is,

$$T_s^C := \{\mathbf{u} \in C \mid s_a = s_a(\mathbf{u}) \text{ for all } a \in \mathfrak{R}\},$$

and by $A_s^C := |T_s^C|$. Then the *complete weight enumerator* of C is defined as:

$$\mathcal{C}_C(x_a : a \in \mathfrak{R}) := \sum_{\mathbf{u}\in C} \prod_{a\in\mathfrak{R}} x_a^{s_a(\mathbf{u})} = \sum_s A_s^C \prod_{a\in\mathfrak{R}} x_a^{s_a},$$

where x_a for $a \in \mathfrak{R}$ are indeterminates and the sum extends over all compositions s of n.

Remark 2.3.1 Let C be an $\mathfrak{R}$-linear code of length n. Then for any $\mathbf{u} \in C$, $\mathrm{wt}(\mathbf{u}) = \sum_{a\in\mathfrak{R},a\neq 0} s_a(\mathbf{u})$. Therefore,

$$\mathcal{C}_C(x_0 \leftarrow x, x_a \leftarrow y \text{ for all } 0 \neq a \in \mathfrak{R}) = w_C(x, y).$$

Example 2.3.2 Let C be the code over $\mathbb{F}_3$ of Example 2.1.2. Let the composition $s = (s_0, s_1, s_2)$. Then we have the following list of non-zero A_s^C:

$$A^C_{(4,0,0)} = 1, \quad A^C_{(1,3,0)} = 1, \quad A^C_{(1,0,3)} = 1, \quad A^C_{(1,2,1)} = 3, \quad A^C_{(1,1,2)} = 3.$$

Therefore, the complete weight enumerator and weight enumerator of C is as follows:

$$\mathcal{C}_C(x_0, x_1, x_2) = x_0^4 x_1^0 x_2^0 + x_0^1 x_1^3 x_2^0 + x_0^1 x_1^0 x_2^3 + 3x_0^1 x_1^2 x_2^1 + 3x_0^1 x_1^1 x_2^2,$$

$$w_C(x, y) = \mathcal{C}_C(x, y, y) = x^4 + 8xy^3.$$

2.4. MacWilliams identity

At the beginning of this section we recall [**5, 12**] to take some fixed characters over $\mathfrak{R}$.

A *character* χ of $\mathfrak{R}$ is a homomorphism from the additive group of $\mathfrak{R}$ to the multiplicative group of non-zero complex numbers.

Let $\mathfrak{R} = \mathbb{F}_q$, where $q = p^f$ for some prime number p. Again let $F(x)$ be a primitive irreducible polynomial of degree f over $\mathbb{F}_p$ and let λ be a root of $F(x)$. Then any element $\alpha \in \mathbb{F}_q$ has a unique representation as:

$$\alpha = \alpha_0 + \alpha_1\lambda + \alpha_2\lambda^2 + \cdots + \alpha_{f-1}\lambda^{f-1}, \tag{1}$$

where $\alpha_i \in \mathbb{F}_p$, and $\chi(\alpha) := \zeta_p^{\alpha_0}$, where ζ_p is the primitive p-th root $e^{2\pi i/p}$ of unity, and α_0 is given by (1).

Again if $\mathfrak{R} = \mathbb{Z}_k$, then for $\alpha \in \mathbb{Z}_k$ we defined χ as $\chi(\alpha) := \zeta_k^{\alpha}$, where ζ_k is the primitive k-th root $e^{2\pi i/k}$ of unity.

Example 2.4.1 Let $\mathfrak{R} = \mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$. Therefore $q = 4 = 2^2$. So, we have $p = f = 2$ and $\zeta_p = \zeta_2 = e^{2\pi i/2}$. Then any element $a \in \mathbb{F}_4$ can be uniquely written for $a_0, a_1 \in \mathbb{F}_2$ as:

$$a = a_0 + a_1\omega.$$

Now the characters of each element of $\mathbb{F}_4$ are as follows:

$$\chi(0) = \zeta_2^0 = 1, \quad \chi(1) = \zeta_2^1 = -1, \quad \chi(\omega) = \zeta_2^0 = 1, \quad \chi(\omega+1) = \zeta_2^1 = -1.$$

Lemma 2.4.1. $\sum_{a \in \mathfrak{R}} \chi(a) = 0.$

Proof. Firstly, let $\mathfrak{R} = \mathbb{F}_q$, where $q = p^f$ for some prime number p. Then we have

$$\begin{aligned}
\sum_{a \in \mathbb{F}_q} \chi(a) &= \sum_{a \in \mathbb{F}_q} \zeta_p^{a_0}, \quad \text{where } a_0 \text{ is given by (1)} \\
&= \prod_{i=0}^{f-1} \left(\sum_{a_0=0}^{p-1} \zeta_p^{a_0} \right) \\
&= f \sum_{k=0}^{p-1} \zeta_p^k \\
&= f \frac{1-\zeta_p^p}{1-\zeta_p} \\
&= 0 \quad \text{since } \zeta_p^p = 1.
\end{aligned}$$

Now if $\mathfrak{R} = \mathbb{Z}_k$, then $\sum_{a \in \mathbb{Z}_k} \chi(a) = \sum_{a \in \mathbb{Z}_k} \zeta_k^a = \sum_{a=0}^{k-1} \zeta_k^a = \dfrac{1-\zeta_k^k}{1-\zeta_k} = 0.$ $\square$

Lemma 2.4.2. *Let C be an $\mathfrak{R}$-linear code of length n. For $\mathbf{v} \in \mathfrak{R}^n$, let*

$$\delta_{C^\perp}(\mathbf{v}) := \begin{cases} 1 & \textit{if} \quad \mathbf{v} \in C^\perp, \\ 0 & \textit{otherwise.} \end{cases}$$

Then we have the following identity

$$\delta_{C^\perp}(\mathbf{v}) = \frac{1}{|C|} \sum_{\mathbf{u} \in C} \chi(\mathbf{u} \cdot \mathbf{v}).$$

Proof. Let $\mathbf{v} \in C^{\perp}$. Then $\mathbf{u} \cdot \mathbf{v} = 0$ for all $\mathbf{u} \in C$. This implies $\sum_{\mathbf{u} \in C} \chi(\mathbf{u} \cdot \mathbf{v}) = |C|$. If $\mathbf{v} \notin C^{\perp}$, then $\chi(\mathbf{u}.\mathbf{v})$ takes each value in $\mathfrak{R}$ equally often, so $\sum_{\mathbf{u} \in C} \chi(\mathbf{u} \cdot \mathbf{v}) = 0$. This completes the proof. $\square$

Now we have the MacWilliams identity for the complete weight enumerator of a code C over $\mathfrak{R}$ as follows.

Theorem 2.4.3 ([**5, 12**]). *For a linear code C over $\mathfrak{R}$ we have*

$$\mathcal{C}_{C^{\perp}}(x_a \text{ with } a \in \mathfrak{R}) = \frac{1}{|C|} T_{\mathfrak{R}} \cdot \mathcal{C}_C(x_a), \tag{2}$$

where $T_{\mathfrak{R}} = (\chi(\alpha\beta))_{\alpha,\beta \in \mathfrak{R}}$.

Proof. Let C be an $\mathfrak{R}$-linear code of length n. Then

$$\begin{aligned}
|C|\mathcal{C}_{C^{\perp}}(x_a : a \in \mathfrak{R}) &= |C| \sum_{\mathbf{u}' \in C^{\perp}} \prod_{a \in \mathfrak{R}} x_a^{s_a(\mathbf{u}')} \\
&= |C| \sum_{\mathbf{v} \in \mathfrak{R}^n} \delta_{C^{\perp}}(\mathbf{v}) \prod_{a \in \mathfrak{R}} x_a^{s_a(\mathbf{v})} \\
&= \sum_{\mathbf{v} \in \mathfrak{R}^n} \sum_{\mathbf{u} \in C} \chi(\mathbf{u} \cdot \mathbf{v}) \prod_{a \in \mathfrak{R}} x_a^{s_a(\mathbf{v})} \\
&= \sum_{\mathbf{u} \in C} \sum_{\mathbf{v} \in \mathfrak{R}^n} \chi(\mathbf{u} \cdot \mathbf{v}) \prod_{a \in \mathfrak{R}} x_a^{s_a(\mathbf{v})} \\
&= \sum_{\mathbf{u} \in C} \sum_{\mathbf{v} \in \mathfrak{R}^n} \chi(u_1 v_1 + \cdots + u_n v_n) \prod_{i=1}^{n} x_{v_i} \\
&= \sum_{\mathbf{u} \in C} \prod_{i=1}^{n} \sum_{v_i \in \mathfrak{R}} \chi(u_i v_i) x_{v_i} \\
&= \sum_{\mathbf{u} \in C} \prod_{\alpha \in \mathfrak{R}} \left(\sum_{\beta \in \mathfrak{R}} \chi(\alpha\beta) x_\beta \right)^{s_\alpha(\mathbf{u})}
\end{aligned}$$

$$= \mathcal{C}_C \left(\sum_{\beta \in \mathfrak{R}} \chi(\alpha\beta) x_\beta \text{ with } \alpha \in \mathfrak{R} \right)$$

$$= T_{\mathfrak{R}} \cdot \mathcal{C}_C(x_a).$$

Hence the proof is completed. □

With the help of Remark 2.3.1, if we replace x_0 by x and x_a by y for all $a \in \mathfrak{R}$ and $a \neq 0$ in (2), then we have the MacWilliams identity presenting the weight enumerator of $C^\perp$.

Theorem 2.4.4 ([**14, 16**]). *If C be an $\mathfrak{R}$-linear code of length n with its $C^\perp$, then*

$$w_{C^\perp}(x, y) = \frac{1}{|C|} w_C(x + (|\mathfrak{R}| - 1)y, x - y).$$

CHAPTER 3

Variants of Weight Enumerators

The notion of the joint weight enumerator of two $\mathbb{F}_q$-linear codes was introduced in [**12**]. Further, the notion of the g-fold complete joint weight enumerator of g linear codes over $\mathbb{F}_q$ was given in [**21**]. The concept of the g-fold joint weight enumerator and the g-fold multi-weight enumerator of codes over $\mathbb{Z}_k$ was investigated in [**5**]. Furthermore, the average of joint weight enumerators of two binary codes was investigated in [**22**] using the ordinary weight distributions of the codes. In this chapter, we give a brief discussion about the above mentioned concepts for the codes over $\mathfrak{R}$ and some of its properties. We thoroughly review [**22**] and its the main result which we call Yoshida's theorem along with the proof.

3.1. Joint weight enumerators

Let $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$ be any two elements of $\mathfrak{R}^n$. Then we define

$$\begin{aligned} i(\mathbf{u},\mathbf{v}) &:= \#\{t \mid u_t = 0, v_t = 0\}, \\ j(\mathbf{u},\mathbf{v}) &:= \#\{t \mid u_t = 0, v_t \neq 0\}, \\ k(\mathbf{u},\mathbf{v}) &:= \#\{t \mid u_t \neq 0, v_t = 0\}, \\ \ell(\mathbf{u},\mathbf{v}) &:= \#\{t \mid u_t \neq 0, v_t \neq 0\}. \end{aligned}$$

Clearly

$$\begin{aligned} i(\mathbf{u},\mathbf{v}) + j(\mathbf{u},\mathbf{v}) + k(\mathbf{u},\mathbf{v}) + \ell(\mathbf{u},\mathbf{v}) &= n, \\ j(\mathbf{u},\mathbf{v}) + \ell(\mathbf{u},\mathbf{v}) &= \mathrm{wt}(\mathbf{v}), \\ k(\mathbf{u},\mathbf{v}) + \ell(\mathbf{u},\mathbf{v}) &= \mathrm{wt}(\mathbf{u}). \end{aligned}$$

Let C and D be two $\mathfrak{R}$-linear codes of length n. The *joint (Hamming) weight enumerator* of C and D is defined as:

$$\begin{aligned} J_{C,D}(x,y,z,w) &:= \sum_{\mathbf{u}\in C}\sum_{\mathbf{v}\in D} x^{i(\mathbf{u},\mathbf{v})} y^{j(\mathbf{u},\mathbf{v})} z^{k(\mathbf{u},\mathbf{v})} w^{\ell(\mathbf{u},\mathbf{v})} \\ &= \sum_{i,j,k,\ell} A^{C,D}_{i,j,k,\ell} x^i y^j z^k w^\ell, \end{aligned}$$

where x, y, z, w are indeterminates and $A^{C,D}_{i,j,k,\ell}$ is the number of the pair of $\mathbf{u} \in C$ and $\mathbf{v} \in D$ such that

$$i(\mathbf{u},\mathbf{v}) = i, \quad j(\mathbf{u},\mathbf{v}) = j, \quad k(\mathbf{u},\mathbf{v}) = k, \quad \ell(\mathbf{u},\mathbf{v}) = \ell.$$

For any two $\mathfrak{R}$-linear codes C and D, it is immediate from the above definition that

$$J_{C,D}(1,1,1,1) = |C||D|,$$

$$J_{D,C}(x,y,z,w) = J_{C,D}(x,z,y,w).$$

Remark 3.1.1 Let C and D be two $\mathfrak{R}$-linear codes of length n. Then

(1) $w_C(x,y) = \frac{1}{|D|} J_{C,D}(x,x,y,y)$,

(2) $w_D(x,y) = \frac{1}{|C|} J_{C,D}(x,y,x,y)$,

(3) If $D = \{(0,0,\ldots,0)\}$, then $w_C(x,y) = J_{C,D}(x,1,y,1)$.

(4) If $C = \{(0,0,\ldots,0)\}$, then $w_D(x,y) = J_{C,D}(x,y,1,1)$.

In [**12**], MacWilliams et al. present the MacWilliams type identity for the joint weight enumerator over $\mathbb{F}_q$ while in [**5**], Dougherty et al. give a generalization of the theorem over $\mathbb{Z}_k$. Hence we have the MacWilliams type identity for the joint weight enumerator over $\mathfrak{R}$. We will give a proof of the above theorem in a more general setting in Theorem 4.1.1.

Theorem 3.1.1 ([**12, 5**]). *Let C and D be two $\mathfrak{R}$-linear codes of length n. Then we have the following relations:*

$$J_{C^\perp,D}(x,y,z,w) = \frac{1}{|C|} J_{C,D}(x+\gamma z, y+\gamma w, x-z, y-w),$$

$$J_{C,D^\perp}(x,y,z,w) = \frac{1}{|D|} J_{C,D}(x+\gamma y, x-y, z+\gamma w, z-w),$$

$$J_{C^\perp,D^\perp}(x,y,z,w) = \frac{1}{|C||D|} J_{C,D}(x+\gamma(y+z)+\gamma^2 w, x-y+ \gamma(z-w), x-z+\gamma(y-w), x-y-z+w).$$

where $\gamma = |\mathfrak{R}| - 1$.

3.2. Average of joint weight enumerators

The concept of the average joint weight enumerators for codes over $\mathbb{F}_2$ was introduced in [**22**]. In this section, we discuss the same notion for the codes over $\mathfrak{R}$. We write $\mathcal{S}_n$ for the symmetric group acting on the set

$$[n] := \{1, 2, \ldots, n\},$$

equipped with the composition of permutations. For any $\mathfrak{R}$-linear code C, the code $C^\sigma := \{u^\sigma \mid u \in C\}$ for permutation $\sigma \in \mathcal{S}_n$ is called *permutationally equivalent* to C, where $u^\sigma := (u_{\sigma(1)}, \ldots, u_{\sigma(n)})$. Then the *average joint weight enumerator* of $\mathfrak{R}$-linear codes C and D is defined as

$$J_{C,D}^{av}(x, y, z, w) := \frac{1}{n!} \sum_{\sigma \in \mathcal{S}_n} J_{C^\sigma, D}(x, y, z, w).$$

Obviously, if C' is permutationally equivalent to C and D' is permutationally equivalent to D, then

$$J_{C',D'}^{av}(x, y, z, w) = J_{C,D}^{av}(x, y, z, w).$$

The following theorem gives the MacWilliams type identity for the average joint weight enumerators over $\mathfrak{R}$.

Theorem 3.2.1. *Let C and D be two $\mathfrak{R}$-linear codes of length n. Then we have the following relations:*

$$J_{C^\perp,D}^{av}(x, y, z, w) = \frac{1}{|C|} J_{C,D}^{av}(x + \gamma z, y + \gamma w, x - z, y - w),$$

where $\gamma = |\mathfrak{R}| - 1$.

Proof. From the definition of the average joint weight enumerator we can write:

$$\begin{aligned}
&J^{av}_{C^\perp,D}(x,y,z,w)\\
&\qquad = \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n} J_{(C^\perp)^\sigma,D}(x,y,z,w)\\
&\qquad = \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n} J_{(C^\sigma)^\perp,D}(x,y,z,w)\\
&\qquad = \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n} \frac{1}{|C^\sigma|} J_{C^\sigma,D}(x+\gamma z, y+\gamma w, x-z, y-w)\\
&\qquad = \frac{1}{|C|} J^{av}_{C,D}(x+\gamma z, y+\gamma w, x-z, y-w).
\end{aligned}$$

This completes the proof. $\square$

Corollary 3.2.2. *For two* $\mathfrak{R}$*-linear codes* C *and* D*, we have*

$$J^{av}_{C,D^\perp}(x,y,z,w) = \frac{1}{|D|} J^{av}_{C,D}(x+\gamma y, x-y, z+\gamma w, z-w)$$

Corollary 3.2.3. *For two* $\mathfrak{R}$*-linear codes* C *and* D*, we have*

$$\begin{aligned}
J^{av}_{C^\perp,D^\perp}(x,y,z,w) = \frac{1}{|C||D|} J^{av}_{C,D}(&x+\gamma(y+z)+\gamma^2 w,\\
&x-y+\gamma(z-w), x-z+\gamma(y-w), x-y-z+w).
\end{aligned}$$

3.3. Yoshida's theorem

In [**22**], Yoshida represented the average of joint weight enumerators of two binary linear codes of length n in terms of the ordinary weight distributions of the codes. That is, if C and D are two binary linear codes of length n, the average joint weight enumerator of C and D can be represented by using the weight distribution of C and D which we have in the the following theorem.

Theorem 3.3.1 ([**22**]). *Let C and D be two binary linear codes of length n. Then*

$$J^{av}_{C,D}(x,y,z,w) = \sum_{i,j} \mathcal{A}^C_i \mathcal{A}^D_j x^{n-i-j} y^j z^i F_{n,i,j}(xw/yz)$$

where

$$F_{n,i,j}(a) := \sum_t \frac{\binom{j}{t}\binom{n-j}{i-t}}{\binom{n}{i}} a^t.$$

Proof. Let C and D be two linear binary codes of length n. Then the joint weight enumerator of C and D is

$$J_{C,D}(x,y,z,w) = \sum_{i,j,k,l} A^{C,D}_{i,j,k,\ell} x^i y^j z^k w^\ell. \tag{3}$$

where $i+j+k+\ell = n$. Now define

$$B^{C,D}_{i,j,t} := \#\{(\mathbf{u},\mathbf{v}) \in C \times D \mid \mathrm{wt}(\mathbf{u}) = i, \mathrm{wt}(\mathbf{v}) = j, \ell(\mathbf{u},\mathbf{v}) = t\}.$$

Therefore

$$A^{C,D}_{i,j,k,\ell} = B^{C,D}_{k+\ell,j+\ell,\ell} \text{ for } i+j+k+\ell = n.$$

Thus we can write from (3)

$$J_{C,D}(x,y,z,w) = \sum_{i,j,t} B^{C,D}_{i,j,t} x^{n-i-j+t} y^{i-t} z^{j-t} w^t. \tag{4}$$

Then we have

$$\sum_{\sigma\in\mathcal{S}_n} B_{i,j,t}^{C^\sigma,D} = \#\{(\mathbf{u},\mathbf{v},\sigma)\in C_i\times D_j\times\mathcal{S}_n \mid \ell(\mathbf{u}^\sigma,\mathbf{v})=t\}$$

$$= \sum_{\mathbf{u}\in C_i}\sum_{\mathbf{v}\in D_j} \#\{\sigma\in\mathcal{S}_n \mid \ell(\mathbf{u}^\sigma,\mathbf{v})=t\},$$

where C_i denotes the set of codewords $\mathbf{u}\in C$ such that $\mathrm{wt}(\mathbf{u})=i$. Let $\mathbf{u}\in C_i$ and $\mathbf{v}\in D_j$. Again let $X:=\mathrm{supp}(\mathbf{u})$, $Y:=\mathrm{supp}(\mathbf{v})$. It is well-known that the order of a subgroup of $\mathcal{S}_n$ which stabilizes a subset X with $|X|=r$ is $r!(n-r)!$. Therefore

$$\sum_{\sigma\in\mathcal{S}_n} B_{i,j,t}^{C^\sigma,D} = \sum_{\mathbf{u}\in C_i}\sum_{\mathbf{v}\in D_j} \#\{\sigma\in\mathcal{S}_n \mid |X^\sigma\cap Y|=t\}$$

$$= A_i^C A_j^D r!(n-r)!\#\{X'\subseteq[n] \mid |X'|=i, |X'\cap Y|=t\}$$

$$= A_i^C A_j^D r!(n-r)!\binom{j}{t}\binom{n-j}{i-t}$$

$$= A_i^C A_j^D n!\frac{\binom{j}{t}\binom{n-j}{i-t}}{\binom{n}{i}}$$

Now by (4) we have

$$J_{C,D}^{av}(x,y,z,w) = \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n} J_{C^\sigma,D}(x,y,z,w)$$

$$= \frac{1}{n!}\sum_{i,j,t}\sum_{\sigma\in\mathcal{S}_n} B_{i,j,t}^{C^\sigma,D} x^{n-i-j+t}y^{i-t}z^{j-t}w^t$$

Hence we have

$$
\begin{aligned}
J^{av}_{C,D}(x,y,z,w) &= \sum_{i,j,t} A_i^C A_j^D \frac{\binom{j}{t}\binom{n-j}{i-t}}{\binom{n}{i}} x^{n-i-j+t} y^{i-t} z^{j-t} w^t \\
&= \sum_{i,j,t} A_i^C A_j^D \frac{\binom{j}{t}\binom{n-j}{i-t}}{\binom{n}{i}} x^{n-i-j+t} y^{i-t} z^{j-t} w^t
\end{aligned}
$$

Hence the proof. $\square$

CHAPTER 4

Generalization of Yoshida's Theorem

In this chapter, we give the notion of the average of complete joint weight enumerators of two linear codes over $\mathfrak{R}$. The main focus of this chapter is to give a generalization of Yoshida's theorem for the average of complete joint weight enumerator of two linear codes over $\mathfrak{R}$. Moreover, we extend the idea of the average complete joint weight enumerator to the average of g-fold complete joint weight enumerators of linear codes over $\mathfrak{R}$.

4.1. Basic definitions and properties

Let C and D be two $\mathfrak{R}$-linear codes of length n. We denote by $\eta(\mathbf{u}, \mathbf{v})$ the *bi-composition* of the pair $(\mathbf{u}, \mathbf{v})$ for $\mathbf{u}, \mathbf{v} \in \mathfrak{R}^n$ which is a vector with non-negative integer components $\eta_{\alpha\beta}(\mathbf{u}, \mathbf{v})$ defined as

$$\eta_{\alpha\beta}(\mathbf{u}, \mathbf{v}) := \#\{i \mid (u_i, v_i) = (\alpha, \beta)\},$$

where $(\alpha, \beta) \in \mathfrak{R}^2$. Clearly

$$\sum_{\alpha,\beta\in\mathfrak{R}} \eta_{\alpha\beta}(\mathbf{u}, \mathbf{v}) = n.$$

In general, a bi-composition η of n is a vector with non-negative integer components $\eta_{\alpha\beta}$ such that

$$\sum_{\alpha,\beta\in\mathfrak{R}} \eta_{\alpha\beta} = n.$$

The *complete joint weight enumerator* of C and D is defined as

$$\begin{aligned}\mathcal{CJ}_{C,D}(x_a \text{ with } a \in \mathfrak{R}^2) &:= \sum_{\mathbf{u}\in C,\mathbf{v}\in D} \prod_{a\in\mathfrak{R}^2} x_a^{\eta_a(\mathbf{u},\mathbf{v})} \\ &= \sum_{\eta} A_\eta^{C,D} \prod_{a\in\mathfrak{R}^2} x_a^{\eta_a},\end{aligned}$$

where $a := a_1a_2 := (a_1, a_2) \in \mathfrak{R}^2$ and x_a for $a \in \mathfrak{R}^2$ are the indeterminates and $A_\eta^{C,D}$ is the number of pair $(\mathbf{u}, \mathbf{v}) \in C \times D$ such that $\eta_a(\mathbf{u}, \mathbf{v}) = \eta_a$ for all $a \in \mathfrak{R}^2$.

Remark 4.1.1 For $a = a_1a_2 \in \mathfrak{R}^2$, let

$$y_a = \begin{cases} x & \text{if } a_1 = a_2 = 0, \\ y & \text{if } a_1 = 0, a_2 \neq 0, \\ z & \text{if } a_1 \neq 0, a_2 = 0, \\ w & \text{if } a_1 \neq 0, a_2 \neq 0. \end{cases}$$

For two $\mathfrak{R}$-linear codes C and D, we have the following relation between complete joint weight enumerators and joint weight enumerators.

$$\mathcal{CJ}_{C,D}(x_a \leftarrow y_a : a \in \mathfrak{R}^2) = J_{C,D}(x, y, z, w).$$

For a code C over $\mathfrak{R}$ let $\tilde{C}$ denote either C or $C^{\perp}$. Then we define

$$\delta(C,\tilde{C}) := \begin{cases} 0 & \text{if} \quad \tilde{C} = C, \\ 1 & \text{if} \quad \tilde{C} = C^{\perp}. \end{cases}$$

Before giving the MacWilliams type identity for the complete joint weight enumerator of codes, we recall the character χ of $\mathfrak{R}$ and the definition of the matrix $T_{\mathfrak{R}}$ from Chapter 2.

Theorem 4.1.1 ([**3**]). *Let C and D be two $\mathfrak{R}$-linear codes of length n. Then we have the MacWilliams type relation as follows:*

$$\mathcal{CJ}_{\tilde{C},\tilde{D}}(x_a \textit{ with } a \in \mathfrak{R}^2) = \frac{1}{|C|^{\delta(C,\tilde{C})}|D|^{\delta(D,\tilde{D})}} T_{\mathfrak{R}}^{\delta(C,\tilde{C})} \otimes T_{\mathfrak{R}}^{\delta(D,\tilde{D})}$$

$$\mathcal{CJ}_{C,D}(x_a \textit{ with } a \in \mathfrak{R}^2).$$

Proof. It is sufficient to show

$$|D|\mathcal{CJ}_{C,D^{\perp}}(x_a \text{with } a \in \mathfrak{R}^2) = (I \otimes T_R)\mathcal{CJ}_{C,D}(x_a \text{with } a \in \mathfrak{R}^2),$$

where $\tilde{C} = C$, $\tilde{D} = D^{\perp}$, and I is the identity matrix. Now by Lemma 2.4.2, we can write

$$\begin{aligned} &|D|\mathcal{CJ}_{C,D^{\perp}}(x_a \text{ with } a \in \mathfrak{R}^2) \\ &\quad = |D| \sum_{\mathbf{c}\in C} \sum_{\mathbf{d}'\in D^{\perp}} \prod_{a\in\mathfrak{R}^2} x_a^{\eta_a(\mathbf{c},\mathbf{d}')} \\ &\quad = |D| \sum_{\mathbf{c}\in C} \sum_{\mathbf{v}\in\mathfrak{R}^n} \delta_{D^{\perp}}(\mathbf{v}) \prod_{a\in\mathfrak{R}^2} x_a^{\eta_a(\mathbf{c},\mathbf{v})} \\ &\quad = \sum_{\mathbf{c}\in C} \sum_{\mathbf{v}\in\mathfrak{R}^n} \sum_{\mathbf{d}\in D} \chi(\mathbf{d}\cdot\mathbf{v}) \prod_{a\in\mathfrak{R}^2} x_a^{\eta_a(\mathbf{c},\mathbf{v})} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\mathbf{c}\in C} \sum_{\mathbf{d}\in D} \sum_{\mathbf{v}\in \mathfrak{R}^n} \chi(\mathbf{d}\cdot\mathbf{v}) \prod_{a\in\mathfrak{R}^2} x_a^{\eta_a(\mathbf{c},\mathbf{v})} \\
&= \sum_{\mathbf{c}\in C,\mathbf{d}\in D} \sum_{\mathbf{v}\in \mathfrak{R}^n} \chi(d_1v_1+\cdots+d_nv_n) \prod_{i=1}^{n} x_{c_iv_i} \\
&= \sum_{\mathbf{c}\in C,\mathbf{d}\in D} \prod_{i=1}^{n} \sum_{v_i\in\mathfrak{R}} \chi(d_iv_i) x_{c_iv_i} \\
&= \sum_{\mathbf{c}\in C,\mathbf{d}\in D} \prod_{(\alpha,\beta)\in\mathfrak{R}^2} \left(\sum_{v\in\mathfrak{R}} \chi(\beta v) x_{\alpha v} \right)^{\eta_{\alpha\beta}(\mathbf{c},\mathbf{d})} \\
&= \mathcal{CJ}_{C,D}\left(\sum_{v\in\mathfrak{R}} \chi(\beta v) x_{\alpha v} \text{ with } (\alpha,\beta)\in\mathfrak{R}^2 \right) \\
&= (I\otimes T_{\mathfrak{R}})\mathcal{CJ}_{C,D}(x_a \text{with } a\in\mathfrak{R}^2).
\end{aligned}
$$

Hence, the proof is completed. □

4.2. Average of complete joint weight enumerators

We recall from Chapter 3 the symmetric group $\mathcal{S}_n$ acting on $[n]$, equipped with the composition of permutations. We also recall that for any $\mathfrak{R}$-linear code C, the code C^σ denotes the permutationally equivalent code of C for permutation $\sigma \in \mathcal{S}_n$. Then the *average complete joint weight enumerator* of $\mathfrak{R}$-linear codes C and D is defined as

$$
\mathcal{CJ}^{av}_{C,D}(x_a \text{ with } a\in\mathfrak{R}^2) := \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n} \mathcal{CJ}_{C^\sigma,D}(x_a \text{ with } a\in\mathfrak{R}^2).
$$

Remark 4.2.1 Let C and D be two $\mathfrak{R}$-linear codes. Then if C' is permutationally equivalent to C and D' is permutationally equivalent to D, then we have

$$
\mathcal{CJ}^{av}_{C',D'}(x_a \text{ with } a\in\mathfrak{R}^2) = \mathcal{CJ}^{av}_{C,D}(x_a \text{ with } a\in\mathfrak{R}^2).
$$

Now from Theorem 4.1.1, we have the generalized MacWilliams identity for the average complete joint weight enumerator of $\mathfrak{R}$-linear codes C and D as follows:

$$\mathcal{CJ}^{av}_{\tilde{C},\tilde{D}}(x_a \text{ with } a \in \mathfrak{R}^2) = \frac{1}{|C|^{\delta(C,\tilde{C})}|D|^{\delta(D,\tilde{D})}} T_{\mathfrak{R}}^{\delta(C,\tilde{C})} \otimes T_{\mathfrak{R}}^{\delta(D,\tilde{D})}$$
$$\mathcal{CJ}^{av}_{C,D}(x_a \text{ with } a \in \mathfrak{R}^2).$$

Now we presents a generalization of Yoshida's theorem (Theorem 3.3.1) as follows. Before stating the theorem we put

$$\binom{a}{b_1, b_2, \ldots, b_m} := \frac{a!}{b_1! b_2! \ldots b_m!}.$$

Theorem 4.2.1 ([**3**])**.** *Let C and D be two $\mathfrak{R}$-linear codes of length n, and r and s be the compositions of n. Again let η be the bi-composition of n such that*

$$r = \left(\sum_{\beta \in \mathfrak{R}} \eta_{\omega_0 \beta}, \ldots, \sum_{\beta \in \mathfrak{R}} \eta_{\omega_{|\mathfrak{R}|-1} \beta} \right),$$
$$s = \left(\sum_{\alpha \in \mathfrak{R}} \eta_{\alpha \omega_0}, \ldots, \sum_{\alpha \in \mathfrak{R}} \eta_{\alpha \omega_{|\mathfrak{R}|-1}} \right).$$

Then we have

$$\mathcal{CJ}^{av}_{C,D}(x_a \ \textit{with}\ a \in \mathfrak{R}^2)$$
$$= \sum_{r,s,\eta} A_r^C A_s^D \frac{\prod_{b \in \mathfrak{R}} \binom{s_b}{\eta_{\omega_0 b}, \ldots, \eta_{\omega_{|\mathfrak{R}|-1} b}}}{\binom{n}{r_{\omega_0}, \ldots, r_{\omega_{|\mathfrak{R}|-1}}}} \prod_{a \in \mathfrak{R}^2} x_a^{\eta_a},$$

Proof. Let C and D be two $\mathfrak{R}$-linear codes of length n. Then the complete joint weight enumerator of C and D is

$$\mathcal{CJ}_{C,D}(x_a \text{ with } a \in \mathfrak{R}^2) := \sum_{\eta} A_{\eta}^{C,D} \prod_{a\in\mathfrak{R}^2} x_a^{\eta_a}, \tag{5}$$

where $\sum_{a\in\mathfrak{R}^2} \eta_a = n$. Now let us define

$$B_{r,s,\eta}^{C,D} := \#\{(\mathbf{u},\mathbf{v}) \in C \times D \mid \mathrm{comp}(\mathbf{u}) = r, \mathrm{comp}(\mathbf{v}) = s, \eta(\mathbf{u},\mathbf{v}) = \eta\}.$$

Therefore, $A_{\eta}^{C,D} = B_{r,s,\eta}^{C,D}$, where

$$r = (r_{\omega_0}, \ldots, r_{\omega_{|\mathfrak{R}|-1}}) = \left(\sum_{\beta\in\mathfrak{R}} \eta_{\omega_0\beta}, \ldots, \sum_{\beta\in\mathfrak{R}} \eta_{\omega_{|\mathfrak{R}|-1}\beta}\right),$$

$$s = (s_{\omega_0}, \ldots, s_{\omega_{|\mathfrak{R}|-1}}) = \left(\sum_{\alpha\in\mathfrak{R}} \eta_{\alpha\omega_0}, \ldots, \sum_{\alpha\in\mathfrak{R}} \eta_{\alpha\omega_{|\mathfrak{R}|-1}}\right).$$

Hence, we can write from (5)

$$\mathcal{CJ}_{C,D}(x_a \text{ with } a \in \mathfrak{R}^2) := \sum_{r,s,\eta} B_{r,s,\eta}^{C,D} \prod_{a\in\mathfrak{R}^2} x_a^{\eta_a}. \tag{6}$$

Now

$$\sum_{\sigma\in\mathcal{S}_n} B_{r,s,\eta}^{C^\sigma,D} = \#\{(\mathbf{u},\mathbf{v},\sigma) \in T_r^C \times T_s^D \times \mathcal{S}_n \mid \eta(\mathbf{u}^\sigma,\mathbf{v}) = \eta\}$$

$$= \sum_{\mathbf{u}\in T_r^C} \sum_{\mathbf{v}\in T_s^D} \#\{\sigma \in \mathcal{S}_n \mid \eta(\mathbf{u}^\sigma,\mathbf{v}) = \eta\}.$$

It is well known that the order of a subgroup of $\mathcal{S}_n$ which stabilizes $\mathbf{u} \in T_r^C$ is $\prod_{b\in\mathfrak{R}} r_b!$. Therefore,

$$
\begin{aligned}
\sum_{\sigma\in\mathcal{S}_n} B^{C^\sigma,D}_{r,s,\eta} &= \sum_{\mathbf{u}\in T^C_r}\sum_{\mathbf{v}\in T^D_s}\prod_{i=0}^{|R|-1} r_{\omega_i}! \\
&\qquad \#\{\mathbf{u}'\in\mathfrak{R}^n \mid \mathrm{comp}(\mathbf{u}')=r, \eta(\mathbf{u}',\mathbf{v})=\eta\} \\
&= \sum_{\mathbf{u}\in T^C_r}\sum_{\mathbf{v}\in T^D_s}\prod_{i=0}^{|\mathfrak{R}|-1} r_{\omega_i}! \prod_{i=0}^{|\mathfrak{R}|-1}\frac{s_{\omega_i}!}{\prod_{j=0}^{|\mathfrak{R}|-1}\eta_{\omega_j\omega_i}!} \\
&= A^C_r A^D_s \prod_{i=0}^{|\mathfrak{R}|-1} r_{\omega_i}! \prod_{i=0}^{|\mathfrak{R}|-1}\frac{s_{\omega_i}!}{\prod_{j=0}^{|\mathfrak{R}|-1}\eta_{\omega_j\omega_i}!} \\
&= A^C_r A^D_s n! \frac{\prod_{i=0}^{|\mathfrak{R}|-1}\frac{s_{\omega_i}!}{\prod_{j=0}^{|\mathfrak{R}|-1}\eta_{\omega_j\omega_i}!}}{\frac{n!}{\prod_{i=0}^{|\mathfrak{R}|-1} r_{\omega_i}!}} \\
&= A^C_r A^D_s n! \frac{\prod_{i=0}^{|R|-1}\binom{s_{\omega_i}}{\eta_{\omega_0\omega_i},\dots,\eta_{\omega_{|\mathfrak{R}|-1}\omega_i}}}{\binom{n}{r_{\omega_0},\dots,r_{\omega_{|\mathfrak{R}|-1}}}}.
\end{aligned}
$$

Now we have

$$
\begin{aligned}
&\mathcal{CJ}^{av}_{C,D}(x_a \text{ with } a\in\mathfrak{R}^2) \\
&\quad = \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n}\mathcal{CJ}_{C^\sigma,D}(x_a \text{ with } a\in\mathfrak{R}^2) \\
&\quad = \frac{1}{n!}\sum_{r,s,\eta}\sum_{\sigma\in\mathcal{S}_n} B^{C^\sigma,D}_{r,s,\eta}\prod_{a\in\mathfrak{R}^2} x_a^{\eta_a} \\
&\quad = \sum_{r,s,\eta} A^C_r A^D_s \frac{\prod_{b\in\mathfrak{R}}\binom{s_b}{\eta_{\omega_0 b},\dots,\eta_{\omega_{|\mathfrak{R}|-1}b}}}{\binom{n}{r_{\omega_0},\dots,r_{\omega_{|\mathfrak{R}|-1}}}}\prod_{a\in\mathfrak{R}^2} x_a^{\eta_a}.
\end{aligned}
$$

This completes the proof. □

4.3. Average of g-fold complete joint weight enumerators

In this section, we give a generalization of Theorem 4.2.1 for the average g-fold complete joint weight enumerators of codes over $\mathfrak{R}$.

Let $C_1, C_2, \ldots, C_g$ be $\mathfrak{R}$-linear codes of length n. For any g-tuple

$$(\mathbf{c}_1, \ldots, \mathbf{c}_g) \in C_1 \times \cdots \times C_g,$$

we denote by $\eta^g(\mathbf{c}_1, \ldots, \mathbf{c}_g)$ a vector with non-negative integer components

$$\eta^g_a(\mathbf{c}_1, \ldots, \mathbf{c}_g) \text{ for } a \in \mathfrak{R}^g$$

and defined as:

$$\eta^g_a(\mathbf{c}_1, \ldots, \mathbf{c}_g) := \#\{i \mid (\mathbf{c}_{1i}, \ldots, \mathbf{c}_{gi}) = a\}.$$

We call $\eta^g(\mathbf{c}_1, \ldots, \mathbf{c}_g)$ the *g-fold composition* of $(\mathbf{c}_1, \ldots, \mathbf{c}_g) \in C_1 \times \cdots \times C_g$. We denote by η^g a g-fold composition of n, a vector with non-negative integer components η^g_a for $a \in \mathfrak{R}^g$ such that

$$\sum_{a \in \mathfrak{R}^g} \eta^g_a = n.$$

We also denote by $T^{C_1,\ldots,C_g}_{\eta^g}$ the set of codewords of $C_1 \times \ldots \times C_g$ with g-fold composition η^g. The *g-fold complete joint weight enumerator* is defined as follows:

$$\begin{aligned}\mathcal{CJ}_{C_1,\ldots,C_g}(x_a \text{ with } a \in \mathfrak{R}^g) &:= \sum_{\mathbf{c}_1 \in C_1, \ldots, \mathbf{c}_g \in C_g} \prod_{a \in \mathfrak{R}^g} x_a^{\eta^g_a(c_1,\ldots,c_g)} \\ &= \sum_{\eta^g} A^{C_1,\ldots,C_g}_{\eta^g} \prod_{a \in \mathfrak{R}^g} x_a^{\eta^g_a},\end{aligned}$$

where x_a for $a \in \mathfrak{R}^g$ are the indeterminates and $A_{\eta^g}^{C_1,\ldots,C_g}$ is the number of g-tuples $(\mathbf{c}_1, \ldots, \mathbf{c}_g) \in C_1 \times \cdots \times C_g$ such that

$$\eta^g(c_1, \ldots, c_g) = \eta^g.$$

The *average g-fold complete joint weight enumerators* are defined as:

$$\mathcal{CJ}^{av}_{C_1,C_2,\ldots,C_g}(x_a : a \in \mathfrak{R}^g) := \frac{1}{n!} \sum_{\sigma \in \mathcal{S}_n} \mathcal{CJ}_{C_1^\sigma,C_2,\ldots,C_g}(x_a : a \in \mathfrak{R}^g).$$

Let $a = (a_1, \ldots, a_g) \in \mathfrak{R}^g$ and $b = (b_1, \ldots, b_{g-1}) \in \mathfrak{R}^{g-1}$. Then we denote

$$[a; j] := (a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_g) \in \mathfrak{R}^{g-1},$$

$$(z; b) := (z, b_1, \ldots, b_{g-1}) \in \mathfrak{R}^g \text{ for } z \in \mathfrak{R}.$$

Now we have the following generalization of Theorem 4.2.1.

Theorem 4.3.1 ([**3**]). *Let $C_1, C_2, \ldots, C_g$ be the $\mathfrak{R}$-linear codes of length n and $s_1, s_2, \ldots, s_g$ be the composition of n. Let η^g be the g-fold composition of n such that for $j = 1, 2, \ldots, g$,*

$$s_j = \left(\sum_{a \in \mathfrak{R}^g} \eta^g_a \text{ with } a_j = \omega_i \text{ for } i = 0, 1, \ldots, |\mathfrak{R}| - 1 \right).$$

Again let η^{g-1} be the $(g-1)$-fold composition of n such that the non-negative integer components η^{g-1}_b for $b \in \mathfrak{R}^{g-1}$ is equal to the sum of η^g_a over all $a \in \mathfrak{R}^g$ with $[a; 1] = b$, that is,

$$\eta^{g-1}_b = \sum_{a \in \mathfrak{R}^g} \eta^g_{a|_{[a;1]=b}}.$$

Then we have

$$\mathcal{CJ}^{av}_{C_1,\dots,C_g}(x_a \text{ } \textit{with} \text{ } a \in \mathfrak{R}^g)$$
$$= \sum_{s_1,\eta^{g-1},\eta^g} A^{C_1}_{s_1} A^{C_2,\dots,C_g}_{\eta^{g-1}} \frac{\prod_{b\in\mathfrak{R}^{g-1}} \binom{\eta^{g-1}_b}{\eta^g_{(\omega_0;b)},\dots,\eta^g_{(\omega_{|\mathfrak{R}|-1};b)}}}{\binom{n}{s_{1\omega_0},\dots,s_{1\omega_{|\mathfrak{R}|-1}}}} \prod_{a\in\mathfrak{R}^g} x_a^{\eta^g_a}.$$

Proof. Let $C_1,\dots,C_g$ be $\mathfrak{R}$-linear codes of length n. Then by the definition of g-fold complete joint weight enumerator of the codes $C_1,\dots,C_g$ we have,

$$\mathcal{CJ}_{C_1,\dots,C_g}(x_a \text{ with } a \in \mathfrak{R}^g) := \sum_{\eta^g} A^{C_1,\dots,C_g}_{\eta^g} \prod_{a\in\mathfrak{R}^g} x_a^{\eta^g_a}, \tag{7}$$

where

$$\sum_{a\in\mathfrak{R}^g} \eta^g_a = n.$$

Now let us define

$$B^{C_1,\dots,C_g}_{s_1,\eta^{g-1},\eta^g} := \#\{(\mathbf{c}_1,\dots,\mathbf{c}_g)\in C_1\times\cdots\times C_g \mid \mathrm{comp}(\mathbf{c}_1)=s_1,$$
$$\eta^{g-1}(\mathbf{c}_2,\dots,\mathbf{c}_g)=\eta^{g-1}, \eta^g(\mathbf{c}_1,\dots,\mathbf{c}_g)=\eta^g\}.$$

Therefore,

$$A^{C_1,\dots,C_g}_{\eta^g} = B^{C_1,\dots,C_g}_{s_1,\eta^{g-1},\eta^g}.$$

Hence, we can write from (7)

$$\mathcal{CJ}_{C_1,\dots,C_g}(x_a \text{ with } a \in \mathfrak{R}^g) := \sum_{s_1,\eta^{g-1},\eta^g} B^{C_1,\dots,C_g}_{s_1,\eta^{g-1},\eta^g} \prod_{a\in\mathfrak{R}^g} x_a^{\eta^g_a}. \tag{8}$$

Now

$$\sum_{\sigma\in\mathcal{S}_n} B^{C_1^\sigma,C_2,\dots,C_g}_{s_1,\eta^{g-1},\eta^g}$$

$$= \#\{(\mathbf{c}_1,\dots,\mathbf{c}_g,\sigma)\in T^{C_1}_{s_1}\times\dots\times T^{C_g}_{s_g}\times\mathcal{S}_n \mid$$

$$\eta^g(\mathbf{c}_1^\sigma,\mathbf{c}_2,\dots,\mathbf{c}_g)=\eta^g\}$$

$$= \sum_{\mathbf{c}_1\in T^{C_1}_{s_1}} \sum_{(\mathbf{c}_2,\dots,\mathbf{c}_g)\in T^{C_2,\dots,C_g}_{\eta^{g-1}}} \#\{\sigma\in\mathcal{S}_n \mid \eta^g(\mathbf{c}_1^\sigma,\mathbf{c}_2,\dots,\mathbf{c}_g)=\eta^g\}.$$

The order of a subgroup of $\mathcal{S}_n$ stabilizing $\mathbf{c}_1\in T^{C_1}_{s_1}$ is $\prod_{i=0}^{|\mathfrak{R}|-1} s_{1\omega_i}!$. Therefore,

$$\sum_{\sigma\in\mathcal{S}_n} B^{C_1^\sigma,C_2,\dots,C_g}_{s_1,\eta^{g-1},\eta^g}$$

$$= \sum_{\mathbf{c}_1\in T^{C_1}_{s_1}} \sum_{(\mathbf{c}_2,\dots,\mathbf{c}_g)\in T^{C_2,\dots,C_g}_{\eta^{g-1}}} \prod_{i=0}^{|\mathfrak{R}|-1} s_{1\omega_i}!$$

$$\#\{c_1'\in\mathfrak{R}^n \mid \mathrm{comp}(\mathbf{c}_1')=s_1, \eta^g(\mathbf{c}_1',\mathbf{c}_2,\dots,\mathbf{c}_g)=\eta^g\}$$

$$= A^{C_1}_{s_1} A^{C_2,\dots,C_g}_{\eta^{g-1}} \prod_{i=0}^{|\mathfrak{R}|-1} s_{1\omega i}! \prod_{b\in\mathfrak{R}^{g-1}} \frac{(\eta^{g-1}_b)!}{(\eta^g_{(\omega_0;b)})!\cdots(\eta^g_{(\omega_{|\mathfrak{R}|-1};b)})!}.$$

Now it is easy to complete the proof by following similar arguments stated in the proof of Theorem 4.2.1. □

CHAPTER 5

Average Intersection Number

The notion of the average intersection number for a pair binary linear codes was introduced in [**22**]. In this chapter, we adopt the same notion for the $\mathfrak{R}$-linear codes of length n. In [**23**], Yoshida gave the asymptotic bound for the average of intersection numbers of a pair of Type I (resp. Type II) codes over $\mathbb{F}_2$ and also for their second moments. We give the asymptotic bound for the average of intersection numbers of a pair of Type III codes over $\mathbb{F}_3$ (resp. Type IV codes over $\mathbb{F}_4$) and for their second moments.

5.1. Properties of average intersection number

Let C and D be two $\mathfrak{R}$-linear codes of length n. Then the *average intersection number* of C and D are given as follows:

$$\Delta(C, D) := \frac{1}{n!} \sum_{\sigma \in \mathcal{S}_n} |C \cap D^{\sigma}|.$$

Let $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (u_1, \ldots, u_n)$ be two elements of $\mathfrak{R}^n$. Then it is easy to say that for any $a = (a_1, a_2) \in \mathfrak{R}^2$ such that $a_1 \neq a_2$, $\eta_a(\mathbf{u}, \mathbf{v}) = 0$ if and only if $\mathbf{u} = \mathbf{v}$. Thus we have the following remark.

Remark 5.1.1 For $a = (a_1, a_2) \in \mathfrak{R}^2$, we let

$$y_a := \begin{cases} 0 & \text{if } a_1 \neq a_2, \\ 1 & \text{otherwise.} \end{cases}$$

Then $\mathcal{CJ}^{av}_{C,D}(x_a \leftarrow y_a : a \in \mathfrak{R}^2) = \Delta(C, D)$.

Now we have the following result.

Proposition 5.1.1. *Let C, D be two $\mathfrak{R}$-linear code of length n, and r be the composition of n. Then we have*

$$\Delta(C, D) = \sum_r \frac{A_r^C A_r^D}{\binom{n}{r_{\omega_0}, \ldots, r_{\omega_{|R|-1}}}}.$$

Proof. Let T_r^C and T_r^D be the set of all elements of C and D, respectively, with the composition $r = (r_{\omega_0}, \ldots, r_{\omega_{|R|-1}})$ of n. Then we can write

$$\begin{aligned} n!\Delta(C, D) &= \sum_{\sigma \in \mathcal{S}_n} |C \cap D^\sigma| \\ &= \#\{(\mathbf{u}, \mathbf{v}, \sigma) \in C \times D \times \mathcal{S}_n \mid \mathbf{u} = \mathbf{v}^\sigma\} \\ &= \sum_r \sum_{\mathbf{u} \in T_r^C} \sum_{\mathbf{v} \in T_r^D} \#\{\sigma \in \mathcal{S}_n \mid \mathbf{u} = \mathbf{v}^\sigma\} \\ &= \sum_r A_r^C A_r^D \prod_{i=0}^{|\mathfrak{R}|-1} r_i!. \end{aligned}$$

Hence, this completes the proof. □

5.2. Self-dual codes over $\mathbb{F}_q$

We recall the definition of the self-dual codes from Chapter 2. It is well known that the length n of a self-dual code over $\mathbb{F}_q$ is even and the dimension is $n/2$. A self-dual code C over $\mathbb{F}_2$ is called *Type* II if the weight of each codeword of C is a multiple of 4. It is well-known that the length n of a Type II code is a multiple of 8. A self-dual code over $\mathbb{F}_2$ which is not Type II is called *Type* I. A self-dual code C over $\mathbb{F}_3$ is called *Type* III if the weight of each codeword of C is a multiple of 3. The length of a Type III code is a multiple of 4. Finally, a self-dual code C over $\mathbb{F}_4$ having even weight is called *Type* IV.

Let C be an $\mathbb{F}_q$-linear code of length n for $q = 2, 3, 4$. For $m = 1$ and 2, we define

$$\Delta_J^m(C) := \frac{1}{|J_n|} \sum_{D \in J_n} |C \cap D|^m,$$

where J_n denotes the set of self-dual codes of Type J, where J stands for I, II, III or IV. The following results for $J = $ I and II are presented in [**23**].

Theorem 5.2.1 ([**23**]). *Let $C \subseteq \mathbb{F}_q^n$ be a binary self-dual code. Then the following hold:*

(i) $\Delta_{\mathrm{I}}(C) \approx 4$ *if C is of Type* I,

(ii) $\Delta_{\mathrm{II}}(C) \approx 6$ *if C is of Type* II.

Theorem 5.2.2 ([**23**]). *Let $C \subseteq \mathbb{F}_q^n$ be a binary self-dual code. Then we have*

(i) $\Delta_{\mathrm{I}}^2(C) \approx 24$ *if C is of Type* I,

(ii) $\Delta_{\mathrm{II}}^2(C) \approx 60$ *if C is of Type* II.

In this section, we give the analogous results of the above theorems for Type III and Type IV codes over $\mathbb{F}_3$ and $\mathbb{F}_4$, respectively. Before presenting our findings, we adopt the following mass formulas which give the numbers of Type III and Type IV codes over $\mathbb{F}_3$ and $\mathbb{F}_4$, respectively.

Theorem 5.2.3 ([**13, 17**]). *The following hold:*

(i) *The number of Type* III *codes over* $\mathbb{F}_3$ *of length* $n \equiv 0 \pmod 4$ *is*

$$2 \prod_{i=1}^{n/2-1} (3^i + 1).$$

(ii) *The number of Type* IV *codes over* $\mathbb{F}_4$ *of length* $n \equiv 0 \pmod 2$ *is*

$$\prod_{i=0}^{n/2-1} (2^{2i+1} + 1).$$

Let $C' \subseteq \mathbb{F}_3^n$ be a self-orthogonal code of dimension k. We denote by $N_{n,k}^{\mathrm{III}}$ the number of Type III codes over $\mathbb{F}_3$ of length n containing C'. Then from [**2**] we have

$$N_{n,k}^{\mathrm{III}} = 2 \prod_{i=1}^{n/2-k-1} (3^i + 1).$$

For $k = 1$, we get from [**18**] the number of Type III codes over $\mathbb{F}_3$ of length n containing a self-orthogonal vector of $\mathbb{F}_3^n$. The following theorem is a Type III analogue of Theorem 5.2.1 and Theorem 5.2.2.

Theorem 5.2.4 ([**3**]). *Let C be a Type* III *code over* $\mathbb{F}_3$ *of length* $n \equiv 0 \pmod 4$. *Then we have*

(i) $\Delta_{\mathrm{III}}(C) = 4 - \dfrac{4}{3^{n/2-1} + 1} \approx 4,$

(ii) $\Delta_{\mathrm{III}}^2(C) = \dfrac{40(3^{n/2})^2}{(3^{n/2} + 3)(3^{n/2} + 9)} \approx 40.$

Proof. (i) Let $C \in \mathrm{III}_n$. Then

$$\begin{aligned}
\sum_{D\in \mathrm{III}_n} |C \cap D| &= \#\{(\mathbf{u}, D) \in C \times \mathrm{III}_n \mid \mathbf{u} \in D\} \\
&= \sum_{\mathbf{u}\in C} \#\{D \in \mathrm{III}_n \mid \mathbf{u} \in D\} \\
&= \left(\sum_{\mathbf{u}=0} + \sum_{\mathbf{u}\in C\setminus\{0\}}\right) \#\{D \in \mathrm{III}_n \mid \mathbf{u} \in D\} \\
&= |\mathrm{III}_n| + (|C| - 1)N^{\mathrm{III}}_{n,1}.
\end{aligned}$$

Since $|\mathrm{III}_n| = 2\prod_{i=1}^{n/2-1}(3^i + 1)$, therefore we can write

$$\begin{aligned}
\Delta_{\mathrm{III}}(C) &= 1 + (|C| - 1)\frac{N^{\mathrm{III}}_{n,1}}{|\mathrm{III}_n|} \\
&= 1 + \frac{3^{n/2} - 1}{3^{n/2-1} + 1} \\
&= \frac{3^{n/2-1} + 3^{n/2}}{3^{n/2-1} + 1} \\
&= \frac{3^{n/2-1} + 3.3^{n/2-1}}{3^{n/2-1} + 1} \\
&= \frac{4.3^{n/2-1}}{3^{n/2-1} + 1} \\
&= 4 - \frac{4}{3^{n/2-1} + 1}.
\end{aligned}$$

This completes the proof of (i).

(ii) Similarly as (i) we can write

$$\begin{aligned}
\sum_{D\in \mathrm{III}_n} |C\cap D|^2 &= \#\{(\mathbf{u},\mathbf{v},D)\ \in C\times C\times \mathrm{III}_n \mid \mathbf{u},\mathbf{v}\in D\} \\
&= \sum_{\mathbf{u},\mathbf{v}\in C} \#\{D\in \mathrm{III}_n \mid \langle \mathbf{u},\mathbf{v}\rangle \subseteq D\} \\
&= \left(\sum_{\mathbf{u},\mathbf{v}=0} + \sum_{\dim\langle \mathbf{u},\mathbf{v}\rangle=1} + \sum_{\dim\langle \mathbf{u},\mathbf{v}\rangle=2}\right) \\
&\qquad\qquad \#\{D\in \mathrm{III}_n \mid \langle \mathbf{u},\mathbf{v}\rangle \subseteq D\} \\
&= |\mathrm{III}_n| + 4(|C|-1)N^{\mathrm{III}}_{n,1} + (|C|-1)(|C|-3)N^{\mathrm{III}}_{n,2}.
\end{aligned}$$

Since $|\mathrm{III}_n| = 2\prod_{i=1}^{n/2-1}(3^i+1)$, therefore we can write

$$\begin{aligned}
\Delta^2_{\mathrm{III}}(C) &= 1 + 4(|C|-1)\frac{N^{\mathrm{III}}_{n,1}}{|\mathrm{III}_n|} + (|C|-1)(|C|-3)\frac{N^{\mathrm{III}}_{n,2}}{|\mathrm{III}_n|} \\
&= 1 + \frac{4(3^{n/2}-1)}{3^{n/2-1}+1} + \frac{(3^{n/2}-1)(3^{n/2}-3)}{(3^{n/2-2}+1)(3^{n/2-1}+1)} \\
&= 1 + \frac{12(3^{n/2}-1)}{3^{n/2}+3} + \frac{27(3^{n/2}-1)(3^{n/2}-3)}{(3^{n/2}+9)(3^{n/2}+3)} \\
&= \frac{40(3^{n/2})^2}{(3^{n/2}+3)(3^{n/2}+9)}.
\end{aligned}$$

This completes the proof of (ii). □

Now if $C' \subseteq \mathbb{F}_4^n$ is a self-orthogonal code having dimension k, then the number of Type IV codes over $\mathbb{F}_4$ of length n containing C', denoted by $N^{\mathrm{IV}}_{n,k}$, is given in [**4**] as follows:

$$N^{\mathrm{IV}}_{n,k} = \prod_{i=0}^{n/2-k-1}(2^{2i+1}+1).$$

In particular, for $k=1$ we get the number from [**13**].

We close this paper with the following Type IV analogue of Theorem 5.2.1 and Theorem 5.2.2.

Theorem 5.2.5 ([**3**]). *Let C be a Type* IV *code over $\mathbb{F}_4$ of length $n \equiv 0 \pmod 2$. Then we have*

(i) $\Delta_{\mathrm{IV}}(C) = 3 - \dfrac{3}{2^{2(n/2)-1}+1} \approx 3,$

(ii) $\Delta^2_{\mathrm{IV}}(C) = \dfrac{27(2^{2(n/2)})^2}{(2^{2(n/2)}+2)(2^{2(n/2)}+8)} \approx 27.$

Proof. (i) Let $C \in \mathrm{IV}_n$. Then

$$\begin{aligned}
\sum_{D \in \mathrm{IV}_n} |C \cap D| &= \#\{(\mathbf{u}, D) \in C \times \mathrm{IV}_n \mid \mathbf{u} \in D\} \\
&= \sum_{\mathbf{u} \in C} \#\{D \in \mathrm{IV}_n \mid \mathbf{u} \in D\} \\
&= \left(\sum_{\mathbf{u}=0} + \sum_{\mathbf{u} \in C \setminus \{0\}} \right) \#\{D \in \mathrm{IV}_n \mid \mathbf{u} \in D\} \\
&= |\mathrm{IV}_n| + (|C| - 1) N^{\mathrm{IV}}_{n,1}.
\end{aligned}$$

Since $|\mathrm{IV}_n| = \prod_{i=0}^{n/2-1} (2^{2i+1}+1)$, therefore,

$$\begin{aligned}
\Delta_{\mathrm{IV}}(C) &= 1 + (|C| - 1) \frac{N^{\mathrm{IV}}_{n,1}}{|\mathrm{IV}_n|} \\
&= 1 + \frac{2^{2(n/2)} - 1}{2^{2(n/2)-1} + 1} \\
&= \frac{2^{2(n/2)-1} + 2^{2(n/2)}}{2^{2(n/2)-1} + 1} \\
&= \frac{3.2^{2(n/2)-1}}{2^{2(n/2)-1} + 1} \\
&= 3 - \frac{3}{2^{2(n/2)-1} + 1}.
\end{aligned}$$

This completes the proof of (i).

(ii) Similarly as (i) we can write

$$\begin{aligned}
\sum_{D\in \mathrm{IV}_n} |C\cap D|^2 &= \#\{(\mathbf{u},\mathbf{v},D)\in C\times C\times \mathrm{IV}_n \mid \mathbf{u},\mathbf{v}\in D\} \\
&= \sum_{\mathbf{u},\mathbf{v}\in C} \#\{D\in \mathrm{IV}_n \mid \langle \mathbf{u},\mathbf{v}\rangle \subseteq D\} \\
&= \left(\sum_{\mathbf{u},\mathbf{v}=0} + \sum_{\dim\langle \mathbf{u},\mathbf{v}\rangle=1} + \sum_{\dim\langle \mathbf{u},\mathbf{v}\rangle=2}\right) \\
&\qquad\qquad \#\{D\in \mathrm{IV}_n \mid \langle \mathbf{u},\mathbf{v}\rangle \subseteq D\} \\
&= |\mathrm{IV}_n| + 5(|C|-1)N_{n,1}^{\mathrm{IV}} + (|C|-1)(|C|-4)N_{n,2}^{\mathrm{IV}}.
\end{aligned}$$

Since $|\mathrm{IV}_n| = \prod_{i=0}^{n/2-1}(2^{2i+1}+1)$, therefore,

$$\begin{aligned}
\Delta_{\mathrm{IV}}^2(C) &= 1 + 5(|C|-1)\frac{N_{n,1}^{\mathrm{IV}}}{|\mathrm{IV}_n|} + (|C|-1)(|C|-4)\frac{N_{n,2}^{\mathrm{IV}}}{|\mathrm{IV}_n|} \\
&= 1 + 5\frac{2^{2(n/2)}-1}{2^{2(n/2)-1}+1} + \frac{(2^{2(n/2)}-1)(2^{2(n/2)}-4)}{(2^{2(n/2)-3}+1)(2^{2(n/2)-1}+1)} \\
&= 1 + 10\frac{2^{2(n/2)}-1}{2^{2(n/2)}+2} + 16\frac{(2^{2(n/2)}-1)(2^{2(n/2)}-4)}{(2^{2(n/2)}+8)(2^{2(n/2)}+2)} \\
&= \frac{27\left(2^{2(n/2)}\right)^2}{(2^{2(n/2)}+8)(2^{2(n/2)}+2)}.
\end{aligned}$$

This completes the proof of (ii). $\square$

Bibliography

[1] E. Bannai, S.T. Dougherty, M. Harada, and M. Oura. Type II codes, even unimodular lattices, and invariant rings. *IEEE Transactions on Information Theory*, 45(4):1194–1205, 1999.

[2] A. Bassa and N. Tutas. Extending self-orthogonal codes. *Turk. J. Math.*, 43:2177–2182, 2019.

[3] H. S. Chakraborty and T. Miezaki. Average of complete joint weight enumerators and self-dual codes. *Des. Codes Cryptogr.*, 89(6):1241–1254, 2021.

[4] J. H. Conway, V. Pless, and N. J. A. Sloane. Self-dual codes over $\mathtt{GF}(3)$ and $\mathtt{GF}(4)$ of length not exceeding 16. *IEEE Trans. Inf. Theory*, 25(3):312–322, 1979.

[5] S. T. Dougherty, M. Harada, and M. Oura. Note on the g-fold joint weight enumerators of self-dual codes over $\mathbb{Z}_k$. *Applicable Algebra in Engineering, Communication and Computing*, 11:437–445, 2001.

[6] A. M. Gleason. Weight polynomials of self-dual codes and the macwilliams identities. *Act. Congr. Int. Math.*, 3:211–215, 1970.

[7] M. J. E. Golay. Notes on digital coding. *Proc. IEEE*, 37:657, 1949.

[8] R. W. Hamming. Error detecting and error correcting codes. *Bell System Tech. J.*, 29:147–160, 1950.

[9] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Slone, and P. Solé. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inform. Theory*, IT-40:301–319, 1994.

[10] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes.* Cambridge university press, first edition, 2003.

[11] F. J. MacWilliams. A theorem on the distribution of weights in a systematic code. *Bell System Tech. J.*, 42:79–94, 1963.

[12] F. J. MacWilliams, C. L. Mallows, and N. J. A. Sloane. Generalizations of Gleason's theorem on weight enumerators of self-dual codes. *IEEE Trans. Information Theory*, IT-18:794–805, 1972.

[13] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, and H. N. Ward. Self-dual codes over $\mathtt{GF}(4)$. *J. Comb. Theory*, 25(A):288–318, 1978.

[14] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier/North Holland, New York, first edition, 1977.

[15] T. Miezaki and M. Oura. On the cycle index and the weight enumerator. *Des. Codes Cryptogr.*, 87(6):1237–1242, 2019.

[16] G. Nebe, E. M. Rains, and N. J. A. Sloane. *Self-Dual Codes and Invariant Theory*. Springer-Verlag, New York, first edition, 2006.

[17] V. Pless. On the uniqueness of the golay codes. *J. Comb. Theory*, 5:215–228, 1968.

[18] V. Pless and J. N. Pierce. Self-dual codes over $\mathtt{GF}(q)$ satisfy a modified Varshamov-Gilbert bound. *Information and Control*, 23:35–40, 1973.

[19] B. Runge. Codes Siegel modular forms. *Discrete Math.*, 148:175–204, 1996.

[20] C. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.

[21] I. Siap and D. K. Ray-Chaudhuri. On r-fold complete weight enumerator of r linear codes. *Contemp. Math.*, 259:501–513, 2000.

[22] T. Yoshida. The average of joint weight enumerators. *Hokkaido Math. J.*, 18:539–548, 1989.

[23] T. Yoshida. The average of intersection number of a pair of self-dual codes. *Hokkaido Math. J.*, 20:539–548, 1991.