Dissertation Abstract

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	: June 21, 2021

Abstract

In this work, 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, the study of codes became inseparable from the study of their weight enumerators. One of our main aims 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.

1 Introduction

F. J. MacWilliams and N. J. A. Sloane [4] 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 [5] 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 [3] 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 [6] 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 [2].

T. Yoshida [7] 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.

Throughout this work, 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 $k \geq 2$.

In this dissertation, 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 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 $\mathfrak{R}$.

T. Yoshida [8] introduced the notion of the average intersection number for two binary codes. T. Yoshida [8] 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.

2 Preliminaries

Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ be the elements of $\mathbb{F}_q^n$, where $q = p^f$ for some prime p. Then the *inner product* of $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q$ is given by $\mathbf{u} \cdot \mathbf{v} := (u_1, v_1) + \cdots + (u_n, v_n)$ where for any $a, b \in \mathbb{F}_q$,

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

Now the *inner product* of $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_k^n$ is given by $\mathbf{u} \cdot \mathbf{v} := u_1v_1 + \cdots + u_nv_n$, where $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$. If $\mathbf{u} \cdot \mathbf{v} = 0$ for $\mathbf{u}, \mathbf{v} \in \mathfrak{R}^n$, we call $\mathbf{u}$ and $\mathbf{v}$ *orthogonal.* An element $\mathbf{u} \in \mathfrak{R}^n$ is called *self-orthogonal* if $\mathbf{u} \cdot \mathbf{u} = 0$.

An $\mathbb{F}_q$-*linear code* of length n is a vector subspace of $\mathbb{F}_q^n$, and a $\mathbb{Z}_k$-*linear code* of length n is an additive group of $\mathbb{Z}_k^n$. Let C be an $\mathfrak{R}$-linear code of length n. The elements of C are called *codewords.* The *dual code* of C is defined as

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

If $C \subseteq C^{\perp}$, then C is called *self-orthogonal*, and if $C = C^{\perp}$, then C is called *self-dual.* Clearly, if C is self-dual, every codeword $\mathbf{u} \in C$ is self-orthogonal.

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 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

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

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 let $A_s^C := |T_s^C|$. 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.

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 $a\in\mathfrak{R}^2$.

We write $\mathcal{S}_n$ for the symmetric group acting on the set $\{1,2,\dots,n\}$, equipped with the composition of permutations. For any $\mathfrak{R}$-linear code C, the code $C^{\sigma}:=\{\mathbf{u}^{\sigma}\mid\mathbf{u}\in C\}$ for some permutation $\sigma\in\mathcal{S}_n$ is called *permutationally equivalent* to C, where $\mathbf{u}^{\sigma}:=(u_{\sigma(1)},\dots,u_{\sigma(n)})$. Then the *average complete joint weight enumerator* of $\mathfrak{R}$-linear codes C and D is defined as

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

3 MacWilliams Identity

The MacWilliams identity for g-fold complete joint weight enumerators of codes over $\mathbb{F}_q$ was established in [6]. Further, in [2], the MacWilliams identity for g-fold joint weight enumerators of codes over $\mathbb{Z}_k$ was given. In this section, we study the MacWilliams type identity for the average complete joint enumerators over $\mathfrak{R}$. At the beginning of this section we recall [2, 3] to take some fixed character over $\mathfrak{R}$.

A *character* χ of $\mathfrak{R}$ is a homomorphism from the additive group $\mathfrak{R}$ 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.

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

Theorem 3.1 ([2, 3])**.** *For a code C over $\mathfrak{R}$ we have*

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

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

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

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

Now we the following MacWilliams type identity for the average of complete joint enumerators of codes over $\mathfrak{R}$.

Theorem 3.2 ([1])**.** *Let C and D be two $\mathfrak{R}$-linear codes of length n. Then we have*

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

4 Generalization of Yoshida's theorem

In this section, we give a generalization of Yoshida's theorem which is presented in the following theorem. 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 4.1 ([1]). *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*

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

Then we have

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

Let $C_1, C_2, \dots, C_g$ be $\mathfrak{R}$-linear codes of length n. Let $(\mathbf{c}_1, \dots, \mathbf{c}_g) \in C_1 \times \cdots \times C_g$,. We denote by $\eta^g(\mathbf{c}_1, \dots, \mathbf{c}_g)$ a vector with non-negative integer components $\eta^g_a(\mathbf{c}_1, \dots, \mathbf{c}_g)$ for $a \in \mathfrak{R}^g$ and defined as:

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

We call $\eta^g(\mathbf{c}_1, \dots, \mathbf{c}_g)$ the *g-fold composition* of $(\mathbf{c}_1, \dots, \mathbf{c}_g) \in C_1 \times \cdots \times C_g$. 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 $T^{C_1,\dots,C_g}_{\eta^g}$ 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:

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

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

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

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

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

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

$$\begin{aligned}[a; j] &:= (a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_g) \in \mathfrak{R}^{g-1},\\ (z; b) &:= (z, b_1, \ldots, b_{g-1}) \in \mathfrak{R}^g \text{ for } z \in \mathfrak{R}.\end{aligned}$$

Now we have a generalization of Theorem 4.1 for the average g-fold complete joint weigh enumerators over $\mathfrak{R}$.

Theorem 4.2 ([1])**.** *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 compositions of n. Let η^g be the g-fold composition of n such that for $j = 1, 2, \ldots, g$,*

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

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

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

5 The Average of Intersection Numbers

The notion of the average intersection number was introduced in [7] for binary linear codes. We take the same notion for $\mathfrak{R}$-linear codes C and D of length n and define the *average intersection number* as follows:

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

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*

$$\Delta(C, D) = \sum_{r} \frac{A_r^C A_r^D}{\binom{n}{r_0, \ldots, r_{|R|-1}}}.$$

Let $C \subseteq \mathbb{F}_q^n$ for $q = 2, 3, 4$ be a code. Now for $m = 1, 2$ 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 [8].

Theorem 5.1 ([8])**.** *Let C be a binary self-dual code of length n. Then*

(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 ([8])**.** *Let C be a binary self-dual code of length n. Then*

(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*.*

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 as follows.

Theorem 5.3 ([1])**.** *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) $\Delta_{\mathrm{III}}^2(C) = \dfrac{40(3^{n/2})^2}{(3^{n/2} + 3)(3^{n/2} + 9)} \approx 40.$

Theorem 5.4 ([1])**.** *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) $\Delta_{\mathrm{IV}}^2(C) = \dfrac{27(2^{2(n/2)})^2}{(2^{2(n/2)} + 2)(2^{2(n/2)} + 8)} \approx 27.$

References

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

[2] 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** (2001), 437-445.

[3] 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** (1972), 794-805.

[4] F. J. MacWilliams, and N. J. A. Sloane, *The theory of error-correcting codes*, Elsevier/North Holland, New York, first edition, 1977.

[5] T. Miezaki, and M. Oura, On the cycle index and the weight enumerator, *Des. Codes Cryptogr.* **87** (2019), no. 6, 1237–1242.

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

[7] T. Yoshida, The average of joint weight enumerators, *Hokkaido Mathematical Journal* **18** (1989), 217-222.

[8] T. Yoshida, The average intersection number of a pair of self-dual codes, *Hokkaido Mathematical Journal* **20** (1991), 539-548.

令和３年７月２６日

学位論文審査報告書（甲）

１．学位論文題目（外国語の場合は和訳を付けること。）

The average of complete joint weight enumerators of codes

（符号の完全重さ分布多項式の平均）

２．論文提出者　(1) 所　　属　数物科学　　　　専攻

(2) 氏　　名　Himadri Shekhar Chakraborty

３．審査結果の要旨（600～650字）

Himadri Shekhar Chakraborty 氏の学位論文について、各審査委員による個別の事前検討ののち、令和 3 年 7 月 21 日に公聴会を開催し、その後の審査会で審議を行い、以下のように判定した。

吉田知行[1989, 1991]は、2元体上の符号のペアーに対して重さ分布多項式の平均、交叉数の平均の概念を導入し、その詳しい研究を行った。本論文では、これらの結果が拡張、補完される。まず、有限体もしくは有理整数環の剰余環上の符号 C1,…,Cg の種数 g の完全重さ分布多項式を定義する。次にこれら完全重さ分布多項式の平均を考えるとき、これが、C1の完全重さ分布多項式の情報と C2,…,Cg の完全重さ分布多項式の情報で書き下せることを明示的に示した。符号の長さの非負整数の分割を精密に捉え一つの公式へと導いており、計算上も有用公式である。さらに、Type III と Type IV の符号に対して、交叉数の平均の値を明示的に与えた。吉田の結果と合わせると、Type I から Type IV までの交叉数の平均のリストが完成されたことになる。それらの漸近的な値が符号の何を表しているのか、更なる研究課題も示唆しており、興味深い結果となっている。

以上のような成果をもつ本学位論文は、関連する分野の更なる発展が期待されるものであり、博士（理学）の学位に十分に値するものであると判断した。

４．審査結果　(1) 判　　定（いずれかに○印）[✓ 合　格]・　不合格

(2) 授与学位　博　士（　理学　）