On the cycle index and the weight enumerator *

Manabu Oura †and Tsuyoshi Miezaki ‡

Abstract

In this paper, we introduce the concept of the complete cycle index and discuss a relation with the complete weight enumerator in coding theory. This work was motivated by Cameron's lecture note "Polynomial aspects of codes, matroids and permutation groups."

Key Words and Phrases. Cycle index, Complete weight enumerator.

2010 *Mathematics Subject Classification.* Primary 11T71; Secondary 20B05, 11H71.

1 Introduction

In [2, 3], a relationship between the cycle index and the weight enumerator was given. To state our results, we review this relationship.

Let G be a permutation group on a set Ω, where $|\Omega| = n$. For each element $h \in G$, we can decompose the permutation h into a product of disjoint cycles; let $c_i(h)$ be the number of i-cycles occurring in this decomposition. Let $\mathbb{N}$ be the set of natural numbers. Now the cycle index of G is the polynomial $Z(G; s_i : i \in \mathbb{N})$ in indeterminates $\{s_i\}_{i\in\mathbb{N}}$ given by

$$Z(G; s_i : i \in \mathbb{N}) = \sum_{h\in G} \prod_{i\in\mathbb{N}} s_i^{c_i(h)}.$$

*This work was supported by JSPS KAKENHI (25400014, 15K04775).

†Graduate School of Natural Science and Technology, Kanazawa University, Ishikawa 920–1192, Japan oura@se.kanazawa-u.ac.jp telephone: +81-76-264-5635, Fax: +81-76-264-6065

‡Faculty of Education, Ryukyu University, Okinawa 903–0213, Japan miezaki@edu.u-ryukyu.ac.jp telephone: +81-98-897-8883, Fax: +81-98-897-8883 (Corresponding author)

Let $\mathbb{F}_q$ be the finite field of order q. Let C be a linear $[n,k]$ code over $\mathbb{F}_q$, namely a k-dimensional subspace of $\mathbb{F}_q^n$. The weight enumerator $w_C(x,y)$ of the code C is the homogeneous polynomial

$$w_C(x,y) = \sum_{\mathbf{c}\in C} x^{n-\mathrm{wt}(\mathbf{c})} y^{\mathrm{wt}(\mathbf{c})} = \sum_{i=0}^{n} A_i x^{n-i} y^i,$$

where $A_i = \sharp\{i \mid \mathbf{c} = (c_1,\dots,c_n) \in C, c_i \neq 0\}$.

We construct from C a permutation group $G(C)$ whose cycle index is essentially the weight enumerator of C. The group we construct is the additive group of C. We let it act on the set $\{1,\dots,n\} \times \mathbb{F}_q$ in the following way: the codeword $(a_1,\dots,a_n)$ acts as the permutation

$$(i,x) \mapsto (i; x + a_i)$$

of the set $\{1,\dots,n\} \times \mathbb{F}_q$. Then we have the following result.

Theorem 1.1 ([3, Proposition 7.2])**.** *We have*

$$w_C(x,y) = Z(G(C); s_1 \leftarrow x^{1/q}, s_p \leftarrow y^{p/q}),$$

where q is a power of the prime number p.

A generalization of the weight enumerator is known as the complete weight enumerator of genus g:

$$w_C^{(g)}(x_{\mathbf{a}} : \mathbf{a} \in \mathbb{F}_q^g) = \sum_{\mathbf{v_1},\dots,\mathbf{v_g}\in C} \prod_{\mathbf{a}\in\mathbb{F}_q^g} x_{\mathbf{a}}^{n_{\mathbf{a}}(\mathbf{v_1},\dots,\mathbf{v_g})},$$

where $n_{\mathbf{a}}(\mathbf{v_1},\dots,\mathbf{v_g})$ denotes the number of i such that $\mathbf{a} = (v_{1i},\dots,v_{gi})$. This gives rise to a natural question: is there a generalization of the cycle index that relates the complete weight enumerator $w_C^{(g)}(x_{\mathbf{a}} : \mathbf{a} \in \mathbb{F}_q^g)$? The aim of the present paper is to provide a candidate generalization that answers this. We now present the concept of the complete cycle index.

Definition 1.1. Let G be a permutation group on a set Ω, where $|\Omega| = n$. For each element $h \in G$, we can decompose the permutation h into a product of disjoint cycles; let $c(h,i)$ be the number of i-cycles occurring by the action of h. Now the complete cycle index of G is the polynomial $Z(G; s(h,i) : h \in G, i \in \mathbb{N})$ in indeterminates $\{s(h,i) \mid h \in G, i \in \mathbb{N}\}$ given by

$$Z(G; s(h,i) : h \in G, i \in \mathbb{N}) = \sum_{h\in G} \prod_{i\in\mathbb{N}} s(h,i)^{c(h,i)}.$$

Remark 1.1. Note that if we let $s_i = s(h, i)$, then we obtain the cycle index:

$$Z(G; s_i : h \in G, i \in \mathbb{N}\}) = \sum_{h \in G} \prod_{i \in \mathbb{N}} s_i^{n(h,i)}.$$

The main result of this paper, Theorem 2.1, uses the concept of the complete cycle index. We also give a generalization of Theorem 1.1.

This paper is organized as follows. In Section 2, we give the concept of the higher cycle index and the complete cycle index and also give the main result of this paper and its proof. In Section 3, we give a $\mathbb{Z}_k$-code analog of the main result.

2 Higher cycle index and complete cycle index

2.1 Definitions and examples

In this section, we give the concept of the higher cycle index and the complete cycle index, and provide some examples.

Definition 2.1. Let C be a linear $[n, k]$ code over $\mathbb{F}_q$. We construct from $C^g := \underbrace{C \times \cdots \times C}_{g}$ a permutation group $G(C^g)$. The group we construct is the additive group of C^g. We denote an element of C^g by

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \dots & \vdots \\ a_{g1} & \dots & a_{gn} \end{pmatrix},$$

where $(a_{i1}, \dots, a_{in}) \in C$. We let it act on the set $\{1, \dots, n\} \times \mathbb{F}_q^g$ in the following way:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \dots & \vdots \\ a_{g1} & \dots & a_{gn} \end{pmatrix}$$

acts as the permutation

$$\left(i, \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_g \end{pmatrix} \right) \mapsto \left(i, \begin{pmatrix} x_1 + a_{1i} \\ x_2 + a_{2i} \\ \vdots \\ x_g + a_{gi} \end{pmatrix} \right)$$

of the set $\{1, \ldots, n\} \times \mathbb{F}_q^g$. We call the cycle index

$$Z(G(C^g), s_i : i \in \mathbb{N})$$

the higher cycle index of genus g for code C. We call the complete cycle index

$$Z(G(C^g), s(h, i) : h \in C^g, i \in \mathbb{N})$$

the complete cycle index of genus g for code C.

Remark 2.1. Note that let $s_i = s(h, i)$. Then we obtain the higher cycle index:

$$Z(G(C^g); s_i : h \in G(C^g)) = \sum_{g \in G(C^g)} \prod_{i \in \mathbb{N}} s_i^{n(h,i)}.$$

We now give some examples.

Example 2.1. Let $C = \mathbb{F}_2^2$. Then the higher cycle index, the complete cycle index, and the complete weight enumerator of genus 2 are as follows:

- $Z(G(C^2); s_1, s_2) = s_1^8 + 6s_1^4 s_2^2 + 9s_2^4$,
- $Z(G(C^2); s(h,i) : h \in C^2)$

$$= s(\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, 1)^4 s(\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, 1)^4 + s(\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, 1)^4 s(\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, 2)^2$$
$$+ s(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, 1)^4 + s(\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, 2)^2$$
$$+ s(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, 1)^4 s(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, 2)^2 + s(\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, 1)^4 s(\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, 2)^2$$
$$+ s(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, 2)^2 + s(\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, 2)^2$$
$$+ s(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, 1)^4 + s(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, 2)^2$$
$$+ s(\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, 1)^4 + s(\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, 2)^2$$
$$+ s(\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, 2)^2 + s(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, 2)^2$$
$$+ s(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, 2)^2 + s(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, 2)^2 s(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, 2)^2,$$

- $w_C^{(2)}(x_{00}, \ldots, x_{11}) = \sum x_{ij}^2 + 2 \sum x_{ij} x_{ki}$.

2.2 Main results

In this section, we present the main result of this paper. The following theorem is a generalization of Theorem 1.1.

Theorem 2.1. *Let C be a code over $\mathbb{F}_q$ of length n, where q is a prime power of p. Let $w_C^{(g)}(x_{\mathbf{a}} : \mathbf{a} \in \mathbb{F}_q^g)$ be the complete weight enumerator of genus g and $Z(G(C^g); s(h,i) : h \in C^g, i \in \mathbb{N})$ be the complete cycle index of genus g.*

Let T be a map defined as follows: for each $h = (\mathbf{a_1}, \ldots, \mathbf{a_n}) \in C^g$ and $i \in \{1, \ldots, n\}$, if $\mathbf{a_i} = \mathbf{0}$, then

$$s(h, 1) \mapsto x_{\mathbf{a_i}}^{1/q^g},$$

if $\mathbf{a_i} \neq \mathbf{0}$, then

$$s(h, p) \mapsto x_{\mathbf{a_i}}^{p/q^g}.$$

Then we have

$$w_C^{(g)}(x_a : a \in \mathbb{F}_q^g) = T(Z(G(C^g); s(h,i) : h \in C^g, i \in \mathbb{N})).$$

Proof. Let $h = (\mathbf{a_1}, \ldots, \mathbf{a_n}) \in C^g$ and

$$\mathrm{wt}^{(g)}(h) = \sharp\{i \mid \mathbf{a_i} \neq \mathbf{0}\}.$$

If $\mathbf{a_i} = 0$, then the q^g points of the form $(i, \mathbf{x}) \in \{1, \ldots, n\} \times \mathbb{F}_q^g$ are all fixed by this element; if $\mathbf{a_i} \neq 0$, they are permuted in q/p cycles of length p. Thus, $h = (\mathbf{a_1}, \ldots, \mathbf{a_n}) \in C^g$ contributes

$$s(h,1)^{q^g(n-\mathrm{wt}^{(g)}(h))} s(h,p)^{q^g/p\,\mathrm{wt}^{(g)}(h)}$$

to the sum in the formula for the complete cycle index, and

$$x_{\mathbf{a_1}} x_{\mathbf{a_2}} \cdots x_{\mathbf{a_n}}$$

to the sum in the formula for the complete weight enumerator. The result follows. □

To explain a relation between a higher cycle index and a higher weight enumerator, we review the concept behind it.

Definition 2.2. Let C be a code over $\mathbb{F}_q$ of length n. We have

$$\|D\| = |\mathrm{supp}(D)|,$$

where $|\mathrm{supp}(D)| = \{i \mid \exists v \in D, v_i \neq 0\}$. In addition,

$$\begin{cases} d_r = d_r(C) = \min\{\|D\| \mid D \leq C, \dim(D) = r\}, \\ A_i^r = A_i^r(C) = |\{D \leq C \mid \dim(D) = r, \|D\| = i\}|. \end{cases}$$

Then the higher-weight enumerator is defined as follows:

$$\begin{aligned} w_C^r(x,y) :&= \sum_{D \leq C, \dim(D) = r} x^{n-\|D\|} y^{\|D\|} \\ &= \sum_{i=0}^{n} A_i^r(C) x^{n-i} y^i. \end{aligned}$$

Theorem 2.2 ([4, 5])**.** *Let C be a code over $\mathbb{F}_q$ of length n. Then*

$$w_C^{(g)}(x_{\mathbf{0}} = x, x_{\mathbf{a}} = y\ (\mathbf{a} \neq 0)) = \sum_{r=0}^{g} [g]_r w_C^r(x, y),$$

where

$$[g]_r = \begin{cases} 1 & \text{if } r = 0 \\ (q^g - 1)(q^g - q) \cdots (q^g - q^{r-1}) & \text{otherwise.} \end{cases}$$

The following theorem gives a relation between the higher cycle index and the higher weight enumerator.

Theorem 2.3. *Let C be a code over $\mathbb{F}_q$ of length n, where q is a prime power of p. Then we have*

$$Z(G(C^g); s_i : i \in \mathbb{N}) = \sum_{r=0}^{g} [g]_r w_C^r(s_1^{q^g}, s_p^{q^g/p}).$$

Proof. We claim that

$$Z(G(C^g); s_i : i \in \mathbb{N}) = w_C^{(g)}(x_{\mathbf{0}} = s_1^{q^g}, x_{\mathbf{a}} = s_p^{q^g/p}\ (\mathbf{a} \neq \mathbf{0})).$$

Let $h = (\mathbf{a_1}, \dots, \mathbf{a_n}) \in C^g$ and

$$\mathrm{wt}^{(g)}(h) = \sharp\{i \mid \mathbf{a_i} \neq \mathbf{0}\}.$$

If $\mathbf{a_i} = 0$, then the q^g points of the form $(i, \mathbf{x}) \in \{1, \dots, n\} \times \mathbb{F}_q^g$ are all fixed by this element; if $\mathbf{a_i} \neq 0$, they are permuted in q/p cycles of length p. Thus, $h = (\mathbf{a_1}, \dots, \mathbf{a_n}) \in C^g$ contributes

$$s_1^{q^g(n - \mathrm{wt}^{(g)}(h))} s_p^{q^g/p\,\mathrm{wt}^{(g)}(h)}$$

to the sum in the formula for the complete cycle index, and

$$x_{\mathbf{a_1}} x_{\mathbf{a_2}} \cdots x_{\mathbf{a_n}}$$

to the sum in the formula for the complete weight enumerator.

The result follows by Theorem 2.2. □

3 $\mathbb{Z}_k$-code analog of the main results

In [1], the authors introduced the concept of the $\mathbb{Z}_k$-codes. In this section, we give a $\mathbb{Z}_k$-code analog of Theorem 2.1.

Let $\mathbb{Z}_k$ be the ring of integers modulo k, where k is a positive integer. In this paper, we always assume that $k \geq 2$ and we take the set $\mathbb{Z}_k$ to be $\{0, 1, \ldots, k-1\}$. A $\mathbb{Z}_k$-code C of length n (or a code C of length n over $\mathbb{Z}_k$) is a $\mathbb{Z}_k$-submodule of $\mathbb{Z}_k^n$.

The complete weight enumerator of genus g:

$$w_C^{(g)}(x_{\mathbf{a}} : \mathbf{a} \in \mathbb{Z}_k^g) = \sum_{\mathbf{v_1},\ldots,\mathbf{v_g} \in C} \prod_{\mathbf{a} \in \mathbb{Z}_k^g} x_{\mathbf{a}}^{n_{\mathbf{a}}(\mathbf{v_1},\ldots,\mathbf{v_g})},$$

where $n_{\mathbf{a}}(\mathbf{v_1}, \ldots, \mathbf{v_g})$ denotes the number of i such that $\mathbf{a} = (v_{1i}, \ldots, v_{gi})$.

The following theorem is a $\mathbb{Z}_k$-code analog of Theorem 2.1.

Theorem 3.1. *Let C be a code over $\mathbb{Z}_k$ of length n. Let $w_C^{(g)}(x_{\mathbf{a}} : \mathbf{a} \in \mathbb{Z}_k^g)$ be the complete weight enumerator of genus g and let $Z(G(C^g); s(h,i) : h \in C^g, i \in \mathbb{N})$ be the complete cycle index of genus g.*

Let T be a map defined as follows: for each $h = (\mathbf{a_1}, \ldots, \mathbf{a_n}) \in C^g$ and $i \in \{1, \ldots, n\}$, if $\mathbf{a_i} = \mathbf{0}$, then

$$s(h, 1) \mapsto x_{\mathbf{a_i}}^{1/k^g},$$

if $\mathbf{a_i} = (a_{i1}, \ldots, a_{ig}) \neq \mathbf{0}$, then

$$s(h, k/\gcd(a_{i1}, \ldots, a_{ig}, k)) \mapsto x_{\mathbf{a_i}}^{(k/\gcd(a_{i1},\ldots,a_{ig},k))/k^g}.$$

Then we have

$$w_C^{(g)}(x_a : a \in \mathbb{Z}_k^g) = T(Z(G(C^g); s(h,i) : h \in C^g, i \in \mathbb{N})).$$

Proof. Let $h = (\mathbf{a_1}, \ldots, \mathbf{a_n}) \in C^g$ and

$$\mathrm{wt}^{(g)}(h) = \sharp\{i \mid \mathbf{a_i} \neq \mathbf{0}\}.$$

If $\mathbf{a_i} = 0$, then the k^g points of the form $(i, \mathbf{x}) \in \{1, \ldots, n\} \times \mathbb{Z}_k^g$ are all fixed by this element; if $\mathbf{a_i} \neq 0$, they are permuted in $(k/\gcd(a_{i1}, \ldots, a_{ig}, k))/k^g$ cycles of length $k/\gcd(a_{i1}, \ldots, a_{ig}, k)$. Then the result follows from the argument of Theorem 2.1. □

References

[1] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices and invariant rings, *IEEE Trans. Inform. Theory* **45** (1999), 257–269.

[2] P. J. Cameron, Cycle index, weight enumerator, and Tutte polynomial, *Electron. J. Combin.* **9** (2002), no. 1, Note 2.

[3] P. J. Cameron, Polynomial aspects of codes, matroids and permutation groups, http://www.maths.qmul.ac.uk/∼pjc/csgnotes/cmpgpoly.pdf.

[4] S.T. Dougherty, T.A. Gulliver, M. Oura, Higher weights and graded rings for binary self-dual codes, *Discrete Appl. Math.* **128** (2003), no. 1, 121–143.

[5] S.T. Dougherty, T.A. Gulliver, M. Oura, Higher weights for ternary and quaternary self-dual codes, *Des. Codes Cryptogr.* **38** (2006), no. 1, 97–112.