Note on the Biweight Enumerators of Self-Dual Codes over $\mathbb{Z}_k$

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510
USA

Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560, Japan
and
Manabu Oura
Graduate School of Mathematics
Kyushu University
Fukuoka 812–8581, Japan

June 5, 2004

Abstract

Recently there has been interest in self-dual codes over finite rings. In this note, g-fold joint weight enumerators and g-fold multi-weight enumerators of codes over the ring $\mathbb{Z}_k$ of integers modulo k are introduced as a generalization of the biweight enumerators. We investigate these weight enumerators and the biweight enumerators of self-dual codes over $\mathbb{Z}_k$. The biweight enumerator of a class of binary codes, introduced in this note, is also studied. We derive Gleason-type theorems for the corresponding biweight enumerators with the help of invariant theory.

1 Introduction

The conditions satisfied by the biweight enumerators of binary Type I codes and Type II codes were studied in [7] and [5], respectively. Using invariant theory, a basis for the space of invariants, which the biweight enumerator for such codes belongs, was also given. In this note, g-fold joint weight enumerators and g-fold multi-weight enumerators of codes over the ring $\mathbb{Z}_k$ of integers modulo k are introduced as a generalization of the biweight enumerators. We investigate these weight enumerators and the biweight enumerators of self-dual codes over $\mathbb{Z}_k$. The biweight enumerator of a class of binary codes introduced in this note is also studied. Using invariant theory, we derive Gleason-type theorems for the corresponding biweight enumerators.

We begin with some definitions. A code C of length n over $\mathbb{Z}_k$ is an additive subgroup of $\mathbb{Z}_k^n$. Let $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ be two elements of $\mathbb{Z}_k^n$. We define the inner product of x and y on $\mathbb{Z}_k^n$ by $x \cdot y = x_1 y_1 + \cdots + x_n y_n \pmod{k}$. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{Z}_k^n \mid x \cdot y = 0 \text{ for all } y \in C\}$. The elements of C are called codewords and the Hamming weight of a codeword x is the number of its non-zero coordinates. A matrix whose rows generate the code C is called a generator matrix of C. C is *self-dual* if $C = C^\perp$. A code C is *formally self-dual* if the codes C and $C^\perp$ have identical Hamming weight distributions. Self-dual codes are formally self-dual, but there are formally self-dual codes which are not self-dual. A binary self-dual code is *Type II* if all codewords have weight divisible by four, and *Type I* if there is at least one codeword of weight $\equiv 2 \pmod{4}$. Binary formally self-dual codes are even if all codewords have even weights and odd if there is at least one codeword of odd weight.

If A and B are codes of length n with $v \in A$ and $w \in B$ define:

$$\begin{aligned}
i(v,w) &= \text{the number of } r \text{ with } v_r = 0 \text{ and } w_r = 0,\\
j(v,w) &= \text{the number of } r \text{ with } v_r = 0 \text{ and } w_r \neq 0,\\
k(v,w) &= \text{the number of } r \text{ with } v_r \neq 0 \text{ and } w_r = 0,\\
l(v,w) &= \text{the number of } r \text{ with } v_r \neq 0 \text{ and } w_r \neq 0,
\end{aligned}$$

where $v = (v_1, v_2, \dots, v_n)$ and $w = (w_1, w_2, \dots, w_n)$. The *joint weight enumerator* of the codes A and B is given by:

$$\mathcal{J}_{A,B}(a,b,c,d) = \sum_{v \in A} \sum_{w \in B} a^{i(v,w)} b^{j(v,w)} c^{k(v,w)} d^{l(v,w)}.$$

If $A = B$ then the weight enumerator $\mathcal{J}_{A,A}$ is called the *biweight enumerator* of A.

2 Multi-Weight Enumerators of Self-Dual Codes

In this section, we give a generalization of biweight enumerators of codes over $\mathbb{Z}_k$. We call these weight enumerators g-fold joint weight enumerators. MacWilliams relations for these weight enumerators are given, and we study the conditions satisfied by g-fold joint weight enumerators of self-dual codes over $\mathbb{Z}_k$.

Definition. Let $A_1, A_2, \ldots, A_g$ be codes of length n over $\mathbb{Z}_k$. The *g-fold joint weight enumerator* of $A_1, A_2, \ldots, A_g$ is defined as follows:

$$\mathcal{J}_{A_1,\ldots,A_g}(x_a \text{ with } a \in \mathbb{F}_2^g) := \sum_{c_1 \in A_1,\ldots,c_g \in A_g} \prod_{a \in \mathbb{F}_2^g} x_a{}^{n_a(c_1,\ldots,c_g)},$$

where $c_j = (c_{j1}, \ldots, c_{jn})$, $n_a(c_1, \ldots, c_g) = |\{i | a = (\overline{c_{1i}}, \ldots, \overline{c_{gi}})\}|$, and $\overline{c_{ji}} = 1$ if $c_{ji} \neq 0$ and $\overline{c_{ji}} = 0$ if $c_{ji} = 0$. Here (x_a with $a \in \mathbb{F}_2^g$) is a 2^g-tuple of variables with $\mathbb{F}_2^g$, that is $(x_{0,\ldots,0,0}, x_{0,\ldots,0,1}, x_{0,\ldots,1,0}, \ldots, x_{1,\ldots,1,1})$.

Remark. Sometimes we denote $\mathcal{J}_{A_1,\ldots,A_g}(x_a \text{ with } a \in \mathbb{F}_2^g)$ by $\mathcal{J}_{A_1,\ldots,A_g}(x_{0,\ldots,0}, \ldots, x_{1,\ldots,1})$ or $\mathcal{J}_{A_1,\ldots,A_g}(x_a)$.

We now give the MacWilliams relations for g-fold joint weight enumerators, beginning with some notations. Let $\tilde{A}_i$ be either A_i or $A_i^\perp$. Then

$$\delta(A_i, \tilde{A}_i) = \begin{cases} 0 & \text{if } \tilde{A}_i = A_i, \\ 1 & \text{if } \tilde{A}_i = A_i^\perp. \end{cases}$$

Let

$$H = \begin{pmatrix} 1 & k-1 \\ 1 & -1 \end{pmatrix}.$$

Theorem 1 *The MacWilliams relations for the g-fold joint weight enumerator of codes $A_1, \ldots, A_g$ over $\mathbb{Z}_k$ is given by*

$$\mathcal{J}_{\tilde{A}_1,\ldots,\tilde{A}_g}(x_a) = \frac{1}{|A_1|^{\delta(A_1,\tilde{A}_1)} \cdots |A_g|^{\delta(A_g,\tilde{A}_g)}} H^{\delta(A_1,\tilde{A}_1)} \otimes \cdots \otimes H^{\delta(A_g,\tilde{A}_g)} \mathcal{J}_{A_1,\ldots,A_g}(x_a)$$

Proof. It is sufficient to show

$$|A_l| \mathcal{J}_{A_1,\ldots,A_{l-1},A_l^\perp,A_{l+1},\ldots,A_g}(x_a) = (I \otimes \cdots \otimes I \otimes \underset{l\text{-th}}{H} \otimes I \otimes \cdots \otimes I) \mathcal{J}_{A_1,\ldots,A_l,\ldots,A_g}(x_a),$$

i.e., $\tilde{A}_l$ is $A_l^\perp$ and for $l \neq i$ we have $\tilde{A}_i = A_i$ where I is the identity matrix. Let η_k be the k-th primitive root of the unity and let

$$\delta_{A^\perp}(v) = \begin{cases} 1 & \text{if } v \in A^\perp, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\text{(LHS)} \quad = \quad |A_l| \, \mathcal{J}_{A_1,\ldots,A_{l-1},A_l^\perp,A_{l+1},\ldots,A_g} \, (x_a)$$

$$
\begin{aligned}
&= |A_l| \sum_{c_1\in A_1,\dots,c_{l-1}\in A_{l-1},c_{l+1}\in A_{l+1},\dots,c_g\in A_g} \sum_{d_l\in A_l^\perp} \prod_{a\in\mathbb{F}_2^g} x_a^{n_a(c_1,\dots,d_l,\dots,c_g)} \\
&= |A_l| \sum_{c_1,\dots,c_{l-1},c_{l+1},\dots,c_g} \sum_{v\in\mathbb{Z}_k^n} \delta_{A_l^\perp}(v) \prod_{a\in\mathbb{F}_2^g} x_a^{n_a(c_1,\dots,c_{l-1},v,c_{l+1},\dots,c_g)} \\
&= \sum_{c_1,\dots,c_{l-1},c_{l+1},\dots,c_g} \sum_{v\in\mathbb{Z}_k^n} \sum_{c_l\in A_l} \eta_k^{v\cdot c_l} \prod_{a\in\mathbb{F}_2^g} x_a^{n_a(c_1,\dots,c_{l-1},v,c_{l+1},\dots,c_g)} \\
&= \sum_{c_1,\dots,c_l,\dots,c_g} \sum_{v\in\mathbb{Z}_k^n} \eta_k^{v\cdot c_l} \prod_{a\in\mathbb{F}_2^g} x_a^{n_a(c_1,\dots,c_{l-1},v,c_{l+1},\dots,c_g)} \\
&= \sum_{c_1,\dots,c_l,\dots,c_g} \sum_{(v_1,\dots,v_n)\in\mathbb{Z}_k^n} \eta_k^{v_1c_{l1}+\cdots+v_nc_{ln}} \prod_{1\le i\le n} x_{\overline{c_{1,i}}\cdots\overline{c_{l-1,i}}\,\overline{v_i}\,\overline{c_{l+1,i}}\cdots\overline{c_{g,i}}} \\
&= \sum_{c_1,\dots,c_l,\dots,c_g} \prod_{1\le i\le n} \left(\sum_{v_i\in\mathbb{Z}_k} \eta_k^{v_ic_{li}} x_{\overline{c_{1i}}\cdots\overline{c_{l-1,i}}\,\overline{v_i}\,\overline{c_{l+1,i}}\cdots\overline{c_{gi}}}\right) \\
&= \sum_{c_1,\dots,c_l,\dots,c_g} \prod_{a=(a_1,\dots,a_l,\dots,a_g)\in\mathbb{F}_2^g} \left(\sum_{v\in\mathbb{Z}_k} \eta_k^{a_lv} x_{a_1\dots a_{l-1}\,\overline{v}\,a_{l+1}\dots a_g}\right)^{n_a(c_1,\dots,c_l,\dots,c_g)} \\
&= \mathcal{J}_{A_1,\dots,A_l,\dots,A_g}\left(\sum_{v\in\mathbb{Z}_k} \eta_k^{a_lv} x_{a_1\dots a_{l-1}\,\overline{v}\,a_{l+1}\dots a_g},\ \text{with } (a_1,\dots,a_l,\dots,a_g)\in\mathbb{F}_2^g\right) \\
&= (I\otimes\cdots\otimes I\otimes H\otimes I\otimes\cdots\otimes I)\ \mathcal{J}_{A_1,\dots,A_l,\dots,A_g}(x_a) \\
&= \text{(RHS)},
\end{aligned}
$$

since we have the following identity

$$
\delta_{A^\perp}(v) = \frac{1}{|A|}\sum_{c\in A}\eta_k^{v\cdot c}.
$$

□

Remark. The above theorem, when $g = 1$, is the well-known MacWilliams relations for Hamming weight enumerators, and the case $g = 2$ was shown in [1].

$\mathcal{J}_{C,C,\dots,C}(x_a)$ is the generalization of the biweight enumerator and is called the *g-fold multi-weight enumerator*. Of course, the case $g = 2$ is the biweight enumerator. For binary codes, these weight enumerators are defined in [4] and [8], and called the g-fold weight enumerators and g-th weight polynomials, respectively. The corresponding MacWilliams relations for binary codes were also given in [8].

We investigate the group generated by the 2^g by 2^g matrices which fix the g-fold multi-weight enumerator of a self-dual code C over $\mathbb{Z}_k$. Consider the g-fold multi-weight enumerators $\mathcal{J}_{C,\dots,C}(x_{y_0}, x_{y_1}, \dots, x_{y_{2^g-1}})$ where $y_i \in \mathbb{F}_2^g$, $y_0 = (0,\dots,0)$ and $y_{2^g-1} = (1,\dots,1)$. By Theorem 1, $\mathcal{J}_{C,\dots,C}(x_{y_0}, x_{y_1}, \dots, x_{y_{2^g-1}})$ is invariant under the 2^g matrices $(1/\sqrt{k}H)^{j_1}\otimes\cdots\otimes(1/\sqrt{k}H)^{j_g}$ ($j_i = 0$ or 1) obtained from Theorem 1.

Moreover, suppose that the weight of y_i is the same as y_j. Then it follows from the definition of the weight enumerators that

$$\mathcal{J}_{C,\dots,C}(x_{y_0}, x_{y_1}, \dots, x_{y_{2^g-1}}) = \mathcal{J}_{C,\dots,C}(x_{y_0}, \dots, x_{y_{i-1}}, x_{y_j}, x_{y_{i+1}}, \dots, x_{y_{j-1}}, x_{y_i}, x_{y_{j+1}}, \dots, x_{y_{2^g-1}}).$$

There are $\sum_{k=1}^{g-1}\binom{g}{k}$ such permutation matrices derived from interchanging x_{y_i} and x_{y_j} for each i and j. These permutation matrices fix $\mathcal{J}_{C,\dots,C}(x_{y_0}, x_{y_1}, \dots, x_{y_{2^g-1}})$ and we denote the set of such matrices by P_J.

Therefore we have the following:

Theorem 2 *The g-fold multi-weight enumerator of a self-dual code C over $\mathbb{Z}_k$ is invariant under the group generated by the matrices $(1/\sqrt{k}H)^{j_1} \otimes \cdots \otimes (1/\sqrt{k}H)^{j_g}$ and P_J.*

Remark. See Lemma 3 and Proposition 4 for examples to illustrate the above theorem.

3 Biweight Enumerators of Self-Dual Codes over $\mathbb{Z}_k$

In this section, we study some properties of the biweight enumerator of self-dual codes over $\mathbb{Z}_k$. The biweight enumerators of self-dual codes are invariants of a group of substitutions. We investigate this group.

Lemma 3 *Let C be a code over $\mathbb{Z}_k$ then*

$$\mathcal{J}_{C,C}(a, b, c, d) = \mathcal{J}_{C,C}(a, c, b, d).$$

Proof. Follows from Theorem 2. □

By Theorem 2, the biweight enumerators of self-dual codes over $\mathbb{Z}_k$ are held invariant by the following four matrices:

$$Q_0(k) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad Q_1(k) = \frac{1}{k}\begin{pmatrix} 1 & k-1 & k-1 & (k-1)^2 \\ 1 & -1 & k-1 & -(k-1) \\ 1 & k-1 & -1 & -(k-1) \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

$$Q_2(k) = \frac{1}{\sqrt{k}}\begin{pmatrix} 1 & 0 & k-1 & 0 \\ 0 & 1 & 0 & k-1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}, \quad Q_3(k) = \frac{1}{\sqrt{k}}\begin{pmatrix} 1 & k-1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & k-1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Note that $Q_1(k) = Q_2(k)Q_3(k)$.

If C is a self-dual code over $\mathbb{Z}_k$, of length n, then $|C|^2 = k^n$ so either k is a square or n is even. Hence, if k is not a square, the length of a self-dual code must be divisible by 2 and so the biweight enumerator is held invariant by the diagonal matrix $Q_4(k)_{jj} = -1$.

In addition, it was shown in [3] that if there is a prime $p \equiv 3 \pmod 4$ such that p sharply divides k, then the length of a self-dual code over $\mathbb{Z}_k$ must be divisible by four. In this case, the biweight enumerator is also invariant by the diagonal matrix $Q_5(k)_{jj} = i$ where i is the complex number with $i^2 = -1$.

Proposition 4 *If k is a square then the biweight enumerator of a self-dual code over $\mathbb{Z}_k$ is invariant under the group $H_1(k) =< Q_0(k), Q_2(k), Q_3(k) >$, which has order 8. If k is a non-square, then the biweight enumerator of a self-dual code over $\mathbb{Z}_k$ is invariant under the group $H_2(k) =< Q_0(k), Q_2(k), Q_3(k), Q_4(k) >$, which has order 16. If there is a prime $p \equiv 3 \pmod 4$ such that p sharply divides k, then the biweight enumerator of a self-dual code over $\mathbb{Z}_k$ is invariant under the group $H_3(k) =< Q_0(k), Q_2(k), Q_3(k), Q_5(k) >$, which has order 32.*

Proof. We consider only the order of each group. It is easy to see that $Q_2(k)^2 = Q_3(k)^2 = I$, $Q_2(k)Q_3(k) = Q_3(k)Q_2(k)$, $Q_0(k)Q_2(k)Q_0(k) = Q_3(k)$, where I is the identity matrix. Thus the group $H_1(k)$ is isomorphic to the dihedral group of order 8 for every k. Since $Q_4(k)$ and $Q_5(k)$ are diagonal matrices, the orders of the groups $H_2(k)$ and $H_3(k)$ are 16 and 32, respectively. $\square$

The biweight enumerator of a self-dual code belongs to the ring of polynomials fixed by the group of substitutions. It is possible to find explicit generator polynomials for this ring. For any finite group G of complex m by m matrices, the Molien series $\Phi_G(\lambda)$ is given by $\Phi_G(\lambda) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{det(I-\lambda g)}$ where $|G|$ is the order of G, *det* stands for determinant, and I is the identity matrix. The number of linearly independent homogeneous invariants of degree d is given by the coefficient of λ^d in the Molien series.

Proposition 5 *For every k, we have*

$$\begin{aligned}
\Phi_{H_1(k)}(\lambda) &= \frac{1+\lambda^3}{(1-\lambda)(1-\lambda^2)^2(1-\lambda^4)} &= 1+\lambda+3\lambda^2+4\lambda^3+8\lambda^4+\cdots, \\
\Phi_{H_2(k)}(\lambda) &= \frac{1+\lambda^4}{(1-\lambda^2)^3(1-\lambda^4)} &= 1+3\lambda^2+8\lambda^4+16\lambda^6+29\lambda^8+\cdots, \\
\Phi_{H_3(k)}(\lambda) &= \frac{1+4\lambda^4+3\lambda^8}{(1-\lambda^4)^4} &= 1+8\lambda^4+29\lambda^8+72\lambda^{12}+145\lambda^{16}+\cdots.
\end{aligned}$$

Proof. By direct calculation, we have

$$\begin{aligned}
\Phi_{H_1(k)}(\lambda) &= \sum_{g\in H_1(k)}\frac{1}{\det(I-\lambda g)} \\
&= \frac{1+\lambda}{(1-\lambda)(1-\lambda^2)^2(1-\lambda^4)}.
\end{aligned}$$

Since $H_2(k) = \{a, -a \mid a \in H_1(k)\}$, we have

$$\begin{aligned}\Phi_{H_2(k)}(\lambda) &= \frac{1}{2}\left\{\Phi_{H_1(k)}(\lambda) + \Phi_{H_1(k)}(-\lambda)\right\} \\ &= \frac{1+\lambda^4}{(1-\lambda^2)^3(1-\lambda^4)}.\end{aligned}$$

Similarly, we have that

$$\Phi_{H_3(k)}(\lambda) = \frac{1+4\lambda^4+3\lambda^8}{(1-\lambda^4)^4}.$$

□

As examples, we determine a basis for the space of invariants, which the biweight enumerator for self-dual codes over $\mathbb{Z}_4$ and $\mathbb{Z}_5$ belongs.

Theorem 6 *The biweight enumerator of a self-dual code over* $\mathbb{Z}_4$ *is an element of the ring*

$$R_4 \oplus e_{4,3}R_4$$

with Molien series

$$\frac{1+\lambda^3}{(1-\lambda)(1-\lambda^2)^2(1-\lambda^4)} = 1 + \lambda + 3\lambda^2 + 4\lambda^3 + 8\lambda^4 + 10\lambda^5 + \cdots,$$

where R_4 *is the ring* $\mathbb{C}[e_{4,1}, e_{4,2}, f_{4,2}, e_{4,4}]$ *and*

$$\begin{aligned}
e_{4,1} &= a+b+c+d, \\
e_{4,2} &= a^2+3b^2+3c^2+9d^2, \\
f_{4,2} &= ab+ac-b^2+3bd-c^2+3cd-6d^2, \\
e_{4,4} &= a^4+12/17a^3b+12/17a^3c+36/289a^3d+54/17a^2b^2+108/289a^2bc+324/289a^2bd \\
&\quad +54/17a^2c^2+324/289a^2cd+486/289a^2d^2+108/17ab^3+324/289ab^2c+972/289ab^2d \\
&\quad +324/289abc^2+1944/289abcd+2916/289abd^2+108/17ac^3+972/289ac^2d \\
&\quad +2916/289acd^2+2916/289ad^3+81/17b^4+324/289b^3c+972/289b^3d+486/289b^2c^2 \\
&\quad +2916/289b^2cd+4374/289b^2d^2+324/289bc^3+2916/289bc^2d+8748/289bcd^2 \\
&\quad +8748/289bd^3+81/17c^4+972/289c^3d+4374/289c^2d^2+8748/289cd^3+6561/289d^4, \\
e_{4,3} &= a^3-a^2b-a^2c-a^2d+3ab^2-2abc-2abd+3ac^2-2acd+3ad^2+5b^3 \\
&\quad -b^2c-b^2d-bc^2+6bcd+15bd^2+5c^3-c^2d+15cd^2+21d^3.
\end{aligned}$$

Proof. We sketch the proof. The biweight enumerator of a self-dual code over $\mathbb{Z}_4$ is invariant under the group $H_1(4)$ in Proposition 4, which has order 8. Using Magma we found the generator polynomials of this ring. Indeed, the structure of the direct sum in the ring follows from the Molien series in Proposition 5. □

The coefficient of λ^d in the Molien series gives the number of linearly independent homogeneous invariants of degree d. It was shown, in [2], that there are exactly two inequivalent self-dual codes of length 4. Thus unfortunately the set of biweight enumerators of all self-dual codes over $\mathbb{Z}_4$ can not generate the above ring $R_4 \oplus e_{4,3}R_4$.

Corollary 7 *The biweight enumerator of a self-dual code over $\mathbb{Z}_5$ ($\mathbb{F}_5$) is an element of the ring*

$$R_5 \oplus f_{5,4}R_5$$

with Molien series

$$\frac{1+\lambda^4}{(1-\lambda^2)^3(1-\lambda^4)} = 1 + 3\lambda^2 + 8\lambda^4 + 16\lambda^6 + 29\lambda^8 + 47\lambda^{12} + \cdots,$$

where R_5 is the ring $\mathbb{C}[e_{5,2}, f_{5,2}, g_{5,2}, e_{5,4}]$ and

$$\begin{aligned}
e_{5,2} &= a^2+4b^2+4c^2+16d^2,\\
f_{5,2} &= ab+ac-b^2+4bd-c^2+4cd-8d^2,\\
g_{5,2} &= ad+bc-2bd-2cd+2d^2,\\
e_{5,4} &= a^4+8/13a^3b+8/13a^3c+16/169a^3d+48/13a^2b^2+48/169a^2bc+192/169a^2bd\\
&\quad +48/13a^2c^2+192/169a^2cd+384/169a^2d^2+128/13ab^3+192/169ab^2c+768/169ab^2d\\
&\quad +192/169abc^2+1536/169abcd+3072/169abd^2+128/13ac^3+768/169ac^2d+3072/169acd^2\\
&\quad +4096/169ad^3+128/13b^4+256/169b^3c+1024/169b^3d+384/169b^2c^2+3072/169b^2cd\\
&\quad +6144/169b^2d^2+256/169bc^3+3072/169bc^2d+12288/169bcd^2+16384/169bd^3+128/13c^4\\
&\quad +1024/169c^3d+6144/169c^2d^2+16384/169cd^3+16384/169d^4,\\
f_{5,4} &= a^3b+a^3c+4/13a^3d-1/2a^2b^2+12/13a^2bc+22/13a^2bd-1/2a^2c^2+22/13a^2cd\\
&\quad -8/13a^2d^2+3ab^3+22/13ab^2c+114/13ab^2d+22/13abc^2-32/13abcd+40/13abd^2\\
&\quad +3ac^3+114/13ac^2d+40/13acd^2+192/13ad^3-7/2b^4+38/13b^3c+100/13b^3d\\
&\quad -8/13b^2c^2+40/13b^2cd-232/13b^2d^2+38/13bc^3+40/13bc^2d+576/13bcd^2-64/13bd^3\\
&\quad -7/2c^4+100/13c^3d-232/13c^2d^2-64/13cd^3-896/13d^4.
\end{aligned}$$

Similarly one can easily determine the ring of polynomials fixed by the group for $k = 3$ and $k \geq 6$, so we omit giving explicit generator polynomials to save space.

4 Biweight Enumerators of Binary Codes

In this section, we introduce two classes of binary linear $[2n, n]$ codes with respect to biweight enumerators.

4.1 Bi-Formally Self-Dual Codes

Binary self-dual codes are divided into two classes, namely Type I codes and Type II codes. Biweight enumerators of these two classes were characterized in [7] and [5], respectively.

Binary formally self-dual codes are divided into two classes, namely even formally self-dual codes and odd formally self-dual codes. Recall that a formally self-dual code and its dual code have identical Hamming weight enumerators. We say that C is a *bi-formally self-dual code* if C and $C^\perp$ have identical biweight enumerators. In addition, such a code is an *even* bi-formally self-dual code if all Hamming weights are even, and an *odd* bi-formally self-dual code otherwise. C is called *isodual* if C and $C^\perp$ are equivalent.

Lemma 8 *If C is self-dual or isodual then C is bi-formally.*

Proof. Since $C = C^\perp$ or C and $C^\perp$ are equivalent, C and $C^\perp$ have the identical biweight enumerators. □

Most of the known formally self-dual codes are such codes. An even formally self-dual code of length 10 which is not equivalent to its dual code was given in [6]. We have verified that the code is not a bi-formally self-dual code.

In this subsection, we investigate biweight enumerators of even bi-formally self-dual codes and odd bi-formally self-dual codes.

Theorem 9 *The biweight enumerator of an odd bi-formally self-dual code is invariant under the group $< Q_0(2), Q_1(2), Q_4(2) >$ which has order 8. The biweight enumerator of a binary odd bi-formally self-dual code is an element of the ring*

$$R_2 \oplus i_{2,2} R_2$$

with Molien series

$$\frac{1+\lambda^2}{(1-\lambda^2)^4} = 1 + 5\,\lambda^2 + 14\,\lambda^4 + 30\,\lambda^6 + 55\,\lambda^8 + 91\,\lambda^{10} + \cdots,$$

where R_2 is the ring $\mathbb{C}[e_{2,2}, f_{2,2}, g_{2,2}, h_{2,2}]$ and

$$\begin{aligned}
e_{2,2} &= a^2 + 2bd + 2cd - d^2,\\
f_{2,2} &= ab + ac - bd - cd,\\
g_{2,2} &= b^2 - 2bd + c^2 - 2cd + 2d^2,\\
h_{2,2} &= bc - bd - cd + d^2,\\
i_{2,2} &= ad - bd - cd + d^2.
\end{aligned}$$

Proof. Since $\mathcal{J}_{C,C}(a,b,c,d) = \mathcal{J}_{C^\perp,C^\perp}(a,b,c,d)$ and $\mathcal{J}_{C,C}(a,b,c,d) = \mathcal{J}_{C,C}(a,c,b,d)$, the biweight enumerator of an odd bi-formally self-dual code C is invariant under the matrices $Q_0(2)$ and $Q_1(2)$. Since $|C| = |C^\perp|$, the length must be even. Thus the biweight enumerator is also invariant under $Q_4(2)$. The group is the elementary Abelian group of order 8. Using Magma we obtained its Molien series and determined the ring. □

We investigate the conditions satisfied by the biweight enumerators of even bi-formally self-dual codes. We need additional matrices for such codes.

Let C be an even bi-formally self-dual code of length n then

$$\begin{aligned} n &\equiv 0 \pmod 2 & (1)\\ k(v,w)+l(v,w) &\equiv 0 \pmod 2, & (2)\\ j(v,w)+l(v,w) &\equiv 0 \pmod 2, & (3)\end{aligned}$$

where $v, w \in C$. Since n is even, we have

$$i(v,w) \equiv j(v,w) \equiv k(v,w) \equiv l(v,w) \pmod 2. \quad (4)$$

The corresponding matrices to conditions (1) and (4) are

$$F_1 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad F_2 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$F_3 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad F_4 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Corollary 10 *The biweight enumerator of an even bi-formally self-dual code is invariant under the group* $< Q_0(2), Q_1(2), F_1, F_2, F_3, F_4 >$ *which has order* 128. *The biweight enumerator of an even bi-formally self-dual code is an element of the ring*

$$R_2' \oplus e_{2,6} R_2'$$

with Molien series

$$\frac{1+\lambda^6}{(1-\lambda^2)(1-\lambda^4)^2(1-\lambda^8)} = 1 + \lambda^2 + 3\,\lambda^4 + 4\,\lambda^6 + 8\,\lambda^8 + 10\,\lambda^{10} + \cdots,$$

where R_2' *is the ring* $\mathbb{C}[j_{2,2}, e_{2,4}, f_{2,4}, e_{2,8}]$ *and*

$$\begin{aligned} j_{2,2} &= a^2+b^2+c^2+d^2,\\ e_{2,4} &= a^4+2a^2d^2+8abcd+b^4+2b^2c^2+c^4+d^4,\\ f_{2,4} &= a^2b^2+a^2c^2-2/3a^2d^2-8/3abcd-2/3b^2c^2+b^2d^2+c^2d^2,\\ e_{2,8} &= a^8+28/65a^6b^2+28/65a^6c^2+28/65a^6d^2+336/65a^5bcd+14/13a^4b^4+84/13a^4b^2c^2\\ &\quad +84/13a^4b^2d^2+14/13a^4c^4+84/13a^4c^2d^2+14/13a^4d^4+224/13a^3b^3cd+224/13a^3bc^3d\\ &\quad +224/13a^3bcd^3+28/65a^2b^6+84/13a^2b^4c^2+84/13a^2b^4d^2+84/13a^2b^2c^4\\ &\quad +504/13a^2b^2c^2d^2+84/13a^2b^2d^4+28/65a^2c^6+84/13a^2c^4d^2+84/13a^2c^2d^4\end{aligned}$$

$$
\begin{aligned}
&+28/65a^2d^6+336/65ab^5cd+224/13ab^3c^3d+224/13ab^3cd^3+336/65abc^5d+224/13abc^3d^3\\
&+336/65abcd^5+b^8+28/65b^6c^2+28/65b^6d^2+14/13b^4c^4+84/13b^4c^2d^2+14/13b^4d^4\\
&+28/65b^2c^6+84/13b^2c^4d^2+84/13b^2c^2d^4+28/65b^2d^6+c^8+28/65c^6d^2\\
&+14/13c^4d^4+28/65c^2d^6+d^8,\\
e_{2,6} \;=\;& a^6+15/17a^4b^2+15/17a^4c^2+15/17a^4d^2+120/17a^3bcd+15/17a^2b^4+90/17a^2b^2c^2\\
&+90/17a^2b^2d^2+15/17a^2c^4+90/17a^2c^2d^2+15/17a^2d^4+120/17ab^3cd+120/17abc^3d\\
&+120/17abcd^3+b^6+15/17b^4c^2+15/17b^4d^2+15/17b^2c^4+90/17b^2c^2d^2+15/17b^2d^4\\
&+c^6+15/17c^4d^2+15/17c^2d^4+d^6.
\end{aligned}
$$

Acknowledgments. The authors wish to thank Patrick Solé for interesting discussions and comments.

References

[1] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices and invariant rings, (preprint).

[2] J.H. Conway and N.J.A. Sloane, Self-dual codes over the integers modulo 4, J. Combin. Theory Ser. A **62** (1993), 30–45.

[3] S.T. Dougherty, M. Harada and P. Solé, Self-dual codes over rings and the Chinese remainder theorem, (submitted).

[4] W. Duke, On codes and Siegel modular forms, Inter. Math. Res. Notices (1993), 125–136.

[5] W.C. Huffman, The biweight enumerator of self-orthogonal binary codes, Discrete Math. **26** (1979), 129–143.

[6] G.T. Kennedy and V. Pless, On designs and formally self-dual codes, Des. Codes and Cryptogr. **4** (1994), 43–55.

[7] 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. Inform. Theory **18** (1972), 794–805.

[8] B. Runge, Codes and Siegel modular forms, Discrete Math. **148** (1996), 175–204.