Higher Weights and Graded Rings for Binary Self-Dual Codes

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510
USA
doughertys1@tiger.uofs.edu

T. Aaron Gulliver
Department of Electrical and Computer Engineering
University of Victoria
P.O. Box 3055, STN CSC
Victoria, BC, Canada V8W 3P6
agullive@ece.uvic.ca

Manabu Oura*
Graduate School of Mathematics
Kyushu University
Fukuoka 812-8581, Japan
ohura@math.kyushu-u.ac.jp

*This work was supported in part by a grant from the Japan Society for the Promotion of Science.

Abstract

The theory of higher weights is applied to binary self-dual codes. Bounds are given for the second minimum higher weight and a Gleason type theorem is derived for the second higher weight enumerator. The second weight enumerator is shown to be unique for the putative $[72, 36, 16]$ Type II code and the first three minimum weights are computed for optimal codes of length less than 32. We also determine the structures of the graded rings associated with the code polynomials of higher weights for small genera, one of which has the property that it is *not* Cohen-Macaulay.

Key Words: Binary Self-Dual Codes, Higher Weights.

1 Introduction

A binary code of length n is a subset of F_2^n and a code is linear if it is a subspace. To this ambient space we attach the standard inner product: $[v, w] = \sum v_i w_i$, and for a code C define $C^\perp = \{v \in \mathbb{F}_2^n \mid [v, w] = 0 \quad \forall w \in C\}$. As usual, if $C \subseteq C^\perp$ we say that C is self-orthogonal, and if $C = C^\perp$ then C is self-dual. For a complete description of the theory of self-dual codes and any undefined terms see [8].

We shall describe the notion of higher weights, introduced by Wei [12], which is a generalization of Hamming weight. We shall follow the notation in [11], see this paper for a complete description of higher weights. Let $D \subseteq \mathbb{F}_2^n$ be a linear subspace, then

(1) $$||D|| = |Supp(D)|,$$

where

(2) $$Supp(D) = \{i \mid \exists v \in D,\ v_i \neq 0\}.$$

For a linear code C define

(3) $$d_r = d_r(C) = min\{||D|| \mid D \subseteq C,\ \dim(D) = r\}.$$

Notice that the minimum Hamming weight of a code C is $d_1(C)$. It also follows that $d_i \leq d_j$ when $i \leq j$ and that $d_k = |supp(C)|$ where k is the dimension of the code. In fact, it can be shown (Proposition 3.1 in [11]), that $d_i < d_j$ when $i < j$. For a self-dual code $d_k = n$ since the all one vector is always present.

The higher weight spectrum is defined as

(4) $$A_i^r = A_i^r(C) = |\{D \subseteq C \mid \dim(D) = r,\ ||D|| = i\}|.$$

This naturally allows us to define the higher weight enumerators

(5) $$W^r(C; y) = W^r(C) = \sum A_i^r y^i.$$

Hence for each $r \leq \dim(C)$ we have a weight enumerator. Note that $W^1(C;y)$ is not the Hamming weight enumerator $H_C(y) = \sum \alpha_i y^i$ where there are α_i vectors of Hamming weight i in C, but rather $W^1(C;y) = H_C(y) - 1$, since the zero vector is not represented.

This weight enumerator can also be written as a homogeneous polynomial:

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

It is immediate that if C is a code with dimension k over $\mathbb{F}_2$ then $W^r(C;1) = \begin{bmatrix} k \\ r \end{bmatrix}$, where $\begin{bmatrix} k \\ r \end{bmatrix} = \frac{(2^k-1)(2^k-2)\ldots(2^k-2^{r-1})}{(2^r-1)(2^r-2)\ldots(2^r-2^{r-1})}$, which is the number of subspaces of dimension r in a k-dimensional space.

Note that simply because two codes have identical Hamming weight enumerators does not imply that the codes have identical $W^r(C;y)$ weight enumerators for all r. We shall drop the y from the notation whenever no confusion will arise.

There exists MacWilliams type identities for the higher weights, see [5], [11]. The MacWilliams relations are given in [11], namely

$$\sum_{r=0}^{s} [s]_r W^r(C^\perp; y) = q^{-sk}(1+(q^s-1)y)^n \sum_{r=0}^{s} W^r(C; \frac{1-y}{1+(q^s-1)y}), \tag{6}$$

where the code has dimension k in $\mathbb{F}_q^n$, and $[s]_r = \prod_{j=0}^{r-1}(q^s - q^j)$. Note that to find $W^s(C^\perp)$ it is necessary to use $W^r(C,y)$ for all r, with $0 \leq r \leq s$. We shall discuss MacWilliams relations in Section 5.

Example 1: Let C be the $[8,4,4]$ Hamming code. Then we have

$$\begin{aligned} W^0(C) &= 1 \qquad W^1(C) = 14y^4 + y^8 \\ W^2(C) &= 28y^6 + 7y^8 \qquad W^3(C) = 8y^7 + 7y^8 \qquad W^4(C) = y^8 \end{aligned}$$

Note that $W^1(C;1) = \begin{bmatrix} 4 \\ 1 \end{bmatrix} = 15$, $W^2(C;1) = \begin{bmatrix} 4 \\ 2 \end{bmatrix} = 35$, and $W^3(C;1) = \begin{bmatrix} 4 \\ 3 \end{bmatrix} = 15$.

2 Binary Self-Dual Codes

We notice that for the binary case any two-dimensional subspace generated by v and w consists of $\{v, w, 0, v+w\}$. This simple fact will be used in proving the next few theorems. We also note the following

$$Supp(\langle v, w \rangle) = |v| + |w| - |v \wedge w|, \tag{7}$$

where $|v \wedge w| = |Supp(v) \cap Supp(w)|$. In addition, $|v + w| = |v| + |w| - 2|v \wedge w|$.

Theorem 2.1 *Let C be a self-orthogonal code with $W^2(C; y) = \sum A_i^2 y^i$. If i is odd then $A_i = 0$.*

Proof. Let a two-dimensional subspace be generated by v and w. Since C is self-orthogonal we have that $|v|$ and $|w|$ are $0 \pmod 2$, and $[v, w] = 0$ implying that $|v \wedge w|$ is $0 \pmod 2$. Hence $Supp(\langle v, w \rangle) = |v| + |w| - |v \wedge w|$ is even. □

This is not true when $r > 2$, see Example 1.

Theorem 2.2 *Let C be a self-orthogonal code. If $d_1 \equiv 0 \pmod 4$ then $d_2 \geq \frac{3}{2}d_1$ and if $d_1 \equiv 2 \pmod 4$ then $d_2 > \frac{3}{2}d_1$.*

Proof. We shall split the proof into two cases.

Case 1: $|v \wedge w| \leq \frac{1}{2}d_1$

Then we have

$$|v| + |w| - |v \wedge w| \geq d_1 + d_1 - \frac{1}{2}d_1 \geq \frac{3}{2}d_1.$$

Case 2: $|v \wedge w| > \frac{1}{2}d_1$

Assume for some v, w we have $|Supp(\langle v, w \rangle)| < \frac{3}{2}d_1$. Then since $v + w$ is a vector in C we have

$$|v| + |w| - 2|v \wedge w| \geq d_1, \tag{8}$$

and since the support is less than $|Supp(\langle v, w \rangle)| < \frac{3}{2}d_1$, then

$$|v| + |w| - |v \wedge w| < \frac{3}{2}d_1. \tag{9}$$

Inequality (8) gives $|v| + |w| \geq d_1 + 2|v \wedge w|$, and placing into (9) gives

$$d_1 + |v \wedge w| \leq d_1 + 2|v \wedge w| - |v \wedge w| \leq |v| + |w| - |v \wedge w| < \frac{3}{2}d_1,$$

so that $d_1 + |v \wedge w| < \frac{3}{2}d_1$ and finally $|v \wedge w| < \frac{1}{2}d_1$. This contradicts our assumption that $|v \wedge w| > \frac{1}{2}d_1$.

If $d_1 \equiv 2 \pmod 4$ then $\frac{3}{2}d_1 \equiv 1 \pmod 2$ and then by Theorem 2.1 the coefficient of $y^{\frac{3}{2}d_1}$ is 0. □

Proposition 2.3 *Let C be a code, if $A_{d_1} > 1$, where A_{d_1} is the number of minimum weight vectors, then $d_2 \leq 2d_1$. If $A_{d_1} = 1$ then $d_2 \leq d_1 + d_1'$ where d_1' is the second smallest non-zero Hamming weight in C.*

Proof. If there are at least two vectors with minimum weight in C, then the two-dimensional subcode generated by these two vectors has support less than or equal to $2d_1$. The second statement follows similarly by taking the unique minimum weight vector with a vector of the second smallest weight. □

Tables 3 and 4 give d_2 and d_3 for all binary self-dual codes with $n \leq 12$, and all optimal self-dual codes with $n \leq 32$. Note that the code $e_8 i_2$ has $d_1 = 2$ and $d_2 = 6$ which is higher than the bound $d_2 \leq 2d_1$ guarantees, so a self-dual code exists which exceeds the bound. Constructions for these binary self-dual codes can be found in [[8], Chapter 4] and the references therein.

3 Shadows

We shall apply higher weights to the shadow codes. Let C be a Type I self-dual code, with C_0 the subcode of doubly-even vectors, and set $C_2 = C - C_0$. Define the shadow to be $S := C_0^\perp - C$, and denote by C_1 and C_3 the cosets of C_0 that comprise S. Hence, $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$ with $C = C_0 \cup C_2$ and $S = C_1 \cup C_3$. See [1] for a complete description.

Define $\Sigma^r(C; y)$ as follows

$$\Sigma^r(C; y) := W^r(C_0^\perp; y) - W^r(C; y). \tag{10}$$

Notice that $\Sigma^r(C; y)$ counts subcodes of dimension r of $C_0^\perp$ that are not subcodes of C. As such this polynomial must have coefficients that are non-negative integers.

Recall that $S = C + s$ where s is some vector in $C_0^\perp$ not in C. Then $\Sigma^r(C; y)$ counts the number of subcodes of the form

$$\langle v_1 + \alpha_1 s, v_s + \alpha_2 s, \ldots, v_k + \alpha_k s \rangle, \tag{11}$$

where $v_i \in C$, $\alpha_i \in \mathbb{F}_2$ and at least one α_i is not 0.

For a code C to exist $W^r(C; y)$ and $\Sigma^r(C; y)$ must have non-negative integral coefficients for all r with $0 \leq r \leq \frac{n}{2}$. In particular, note that if C is a self-dual code with shadow S, then $\Sigma^1(C; y) = H_S(y)$. Hence, the weight enumerator $\Sigma^r(C; y)$ is a generalization of the weight enumerator of the shadow.

Example 2: Consider the self-dual code i_2^3. (See [2] or [8] and the references therein for any undefined notation.) This code has $W^2(C; y) = 3y^4 + 4y^6$, $W^2(C_0; y) = y^6$, and $W^2(C_0^\perp; y) = 15y^4 + 12y^5 + 8y^6$, so $\Sigma^2(C; y) = 12y^4 + 12y^5 + 4y^6$.

3.1 Cosets

In general, let E be a coset of C in C', i.e., $E = C + t$ for some vector t. Then we can define

$$W^r(E, C; y) = \sum A_i^r y^i, \tag{12}$$

where A_i^r is the number of subcodes D of the form

$$D = \langle v_1 + \alpha_1 t, v_2 + \alpha_2 + t, \ldots, v_k + \alpha_k + t \rangle, \tag{13}$$

with $D \subseteq E$, $\dim(D) = r$, and $||D|| = i$, where at least one $\alpha_i \neq 0$, $E = (C + t)$ and the v_i are in C. Namely it counts the higher weights of the subcodes of C' that are contained in E but not contained in C. Hence

$$\Sigma^r(C; y) = W^r(S, C; y) \quad \text{and} \quad W^r(C; y) = W^r(C_0; y) + W^r(C_2, C_0; y).$$

Theorem 3.1 *Let C be an $[n, k, d]$ code with E a coset of C, then*

$$W^r(E, C, 1) = \frac{2^{k+1} - 2^{k-r+1}}{2^{k-r+1} - 1} \begin{bmatrix} k \\ r \end{bmatrix}. \tag{14}$$

Proof. We have that

$$\begin{aligned} W^r(E, C, 1) = & \begin{bmatrix} k+1 \\ r \end{bmatrix} - \begin{bmatrix} k \\ r \end{bmatrix} \\ = & \frac{\prod_{i=0}^{r-1}(2^{k+1} - 2^i) - \prod_{i=0}^{r-1}(2^k - 2^i)}{\prod_{i=0}^{r-1}(2^r - 2^i)}. \end{aligned}$$

The numerator becomes

$$\begin{aligned} & (2^{k+1} - 1)\prod_{i=1}^{r-1}(2^{k+1} - 2^i) - \prod_{i=0}^{r-1}(2^k - 2^i) \\ = & (2^{k+1} - 1)\prod_{i=1}^{r-1} 2(2^k - 2^{i-1}) - (2^k - 2^{r-1})\prod_{i=0}^{r-2}(2^k - 2^i) \\ = & (2^{k+1} - 1)2^{r-1}\prod_{i=0}^{r-2}(2^k - 2^i) - (2^k - 2^{r-1})\prod_{i=0}^{r-2}(2^k - 2^i) \\ = & ((2^{k+1} - 1)2^{r-1} - 2^k + 2^{r-1})\prod_{i=0}^{r-2}(2^k - 2^i) = (2^{k+r} - 2^k)\prod_{i=0}^{r-2}(2^k - 2^i). \end{aligned}$$

Then the quotient becomes

$$\frac{2^k(2^r - 1)\prod_{i=0}^{r-2}(2^k - 2^i)}{(2^{r-1})\prod_{i=0}^{r-2}(2^r - 2^i)} = \frac{2^k(2^r - 1)}{2^k - 2^{r-1}} \begin{bmatrix} k \\ r \end{bmatrix} = \frac{2^{k+1} - 2^{k-r+1}}{2^{k-r+1} - 1} \begin{bmatrix} k \\ r \end{bmatrix}. \tag{15}$$

□

Note that for $r = 1$ this becomes

$$\frac{2^k}{2^k - 1} \begin{bmatrix} k \\ r \end{bmatrix} = \frac{2^k(2^k - 1)}{2^k - 1} = 2^k = \begin{bmatrix} k \\ r \end{bmatrix} + 1,$$

as expected.

4 Biweight Enumerators and Higher Weights

The MacWilliams relations (6) do not allow for a straightforward application of invariant theory, since $W^r(C^\perp; y)$ is not obtained by a group action on $W^r(C; y)$, but rather involves $W^0(C; y), W^1(C; y), \ldots, W^r(C; y)$. We shall use the biweight enumerator to produce a Gleason type theorem for the second higher weight. We begin with some definitions.

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

$$\begin{aligned} i(v,w) &= \text{the number of } r \text{ with } v_r = 0 \text{ and } w_r = 0, \\ j(v,w) &= \text{the number of } r \text{ with } v_r = 0 \text{ and } w_r = 1, \\ k(v,w) &= \text{the number of } r \text{ with } v_r = 1 \text{ and } w_r = 0, \\ l(v,w) &= \text{the number of } r \text{ with } v_r = 1 \text{ and } w_r = 1. \end{aligned}$$

The *joint weight enumerator* of the codes A and B is given by

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

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

Theorem 4.1 *Let C be a binary code then*

$$\begin{aligned} W^2(C; y) &= \tfrac{1}{6}(J_{C,C}(1,y,y,y) - J_{C,C}(1,0,0,y) \\ &\quad - J_{C,C}(1,0,y,0) - J_{C,C}(1,y,0,0) + 2). \end{aligned} \tag{16}$$

Proof. Let v, w be any two linearly independent vectors then

$$|Supp < v, w > | = j(v,w) + k(v,w) + l(v,w).$$

The biweight enumerator counts all pairs v, w, including $\{v, v\}$, $\{0, v\}$ and $\{v, 0\}$, none of which generate a two-dimensional subcode. We have that $J_{C,C}(1,0,0,y)$ counts pairs of the form $\{v, v\}$, $J_{C,C}(1,0,y,0)$ counts pairs of the form $\{v, 0\}$, and $J_{C,C}(1,y,0,0)$ counts pairs of the form $\{0, v\}$. The 2 at the end of the sum accounts for the number of times $\{0, 0\}$ is counted.

Each space $\{0, v, w, v + w\}$ is counted $P(3,2) = 6$ times in the biweight enumerator, accounting for the $\frac{1}{6}$. □

Note that

$$\tfrac{1}{6}(J_{C,C}(1,1,1,1) - J_{C,C}(1,0,0,1) - J_{C,C}(1,0,1,0) - J_{C,C}(1,1,0,0) + 2) =$$

$$\tfrac{1}{6}(2^{2k} - 3(2^k) + 2) = \begin{bmatrix} k \\ 2 \end{bmatrix}.$$

This relationship is useful to produce Gleason type theorems for the second higher weight enumerator. In Section 5 another relationship between the generalized joint weight enumerator and the higher weights is introduced.

Example 3: The biweight enumerator of the $[8,4,4]$ extended Hamming code is

$$J_{C,C}(a,b,c,d) = d^8 + 14\,c^4d^4 + c^8 + 14\,d^4b^4 + 14\,c^4b^4 + b^8 + 168\,c^2d^2a^2b^2 + 14\,d^4a^4 + 14\,c^4a^4 + 14\,a^4b^4 + a^8.$$

It is a simple calculation to see that

$$\tfrac{1}{6}(J_{C,C}(1,y,y,y) - J_{C,C}(1,0,0,y) - J_{C,C}(1,0,y,0) - J_{C,C}(1,y,0,0) + 2) = 7y^8 + 28y^6 = W^2(C;y).$$

In [6] and [4] Gleason theorems for Type I and Type II codes were given. We state the result in the next lemma, the result in Theorem 4.1 in [4], and the polynomials can be found there.

Lemma 4.2 *Let S be a self-dual linear code. If S is Type I its biweight enumerator is an element of*

$$R_1 = \mathbb{C}[A,C,B^2,D^2] \oplus BD\mathbb{C}[A,C,B^2,D^2]. \tag{17}$$

If S is Type II its biweight enumerator is an element of

$$R_2 = \mathbb{C}[P_8,P_{12}^2,P_{24},P_{20}^2] \oplus P_{12}P_{20}\mathbb{C}[P_8,P_{12}^2,P_{24},P_{20}^2]. \tag{18}$$

Theorem 4.3 *Let C be a self-dual code. Then $W^2(C,y)$ is of the form*

$$\frac{1}{6}(J(1,y,y,y) + J(1,0,0,y) + J(1,0,y,0) + J(1,y,0,0) + 2), \tag{19}$$

where J is an element of R_1 if the code is Type I and J is an element of R_2 if the code is Type II.

Using this theorem, it is easy to compute the possible $W^2(C,y)$ where C is a Type II code of length 72 with minimum weight 16. In fact there is a unique weight enumerator, given that $J(1,0,0,y)$ must be the unique Hamming weight enumerator for such a code. This weight enumerator is given in Table 1. There is also a unique $W^2(C,y)$ for a Type II code of length 48 with minimum weight 12, and this is given in Table 2. Note that $d_2 = \frac{3}{2}d_1$ for these codes.

The results in Table 3 were generated from the codes of the binary self-dual codes via a C program which enumerates all subcodes. The accuracy of the program was confirmed by hand solutions and the method given in Section 5.

Table 1: The Second Higher Weight Enumerator for a Type II $[72, 36, 16]$ Code

coefficient of y^i	weight i
96191865	24
4309395552	26
119312891460	28
2379079500864	30
37327599503964	32
466987648992480	34
4687779244903412	36
37810235197002240	38
244777798274765679	40
1269000323938260672	42
5251816390965277320	44
17262594429823645056	46
44763003632389491540	48
90768836016453484224	50
142313871132195291144	52
170060449665123790080	54
152060783100409784007	56
99349931253373567200	58
45970401654169517364	60
14440224673488398400	62
2900924791551272475	64
340809968304405600	66
20197782231604740	68
451381581930240	70
1617151596337	72

5 Joint Weight Enumerators and the MacWilliams Relations

We generalize the joint weight enumerator:

$$J_C^g(x_a, a \in \mathbb{F}_2^g) := \sum_{v_1,\ldots,v_g \in C} \prod_{a \in \mathbb{F}_2^g} x_a^{n_a(v_1,\ldots,v_g)},$$

where $n_a(v_1, \ldots, v_g)$ denotes the number of i such that $a = (v_{1_i}, \ldots, v_{g_i})$.

We shall now produce a fundamental relationship between the joint weight enumerator and the higher weight enumerator.

For $r \leq g$, put

$$\mathfrak{A}^r_{\mathbf{e}}(C) = \sharp\{(v_1, \ldots, v_g) \in C^g : \dim\langle v_1, \ldots, v_g\rangle = r,\ n_a(v_1, \ldots, v_g) = e_a,\ \forall a \in \mathbb{F}_2^g\},$$

where $\mathbf{e} = (e_a : a \in \mathbb{F}_2^g)$. Fixing e_0, we have

$$\begin{aligned}\sum{}' \mathfrak{A}^r_{\mathbf{e}}(C) &= \sharp\{(v_1, \ldots, v_g) \in C^g : \dim\langle v_1, \ldots, v_g\rangle = r,\ \|\langle v_1, \ldots, v_g\rangle\| = n - e_0\} \\ &= f(g, r) A^r_{n-e_0}(C),\end{aligned}$$

Table 2: The Second Higher Weight Enumerator for a Type II $[48, 24, 12]$ Code

coefficient of y^i	weight i
2663584	18
64211400	20
1030807008	22
10803665340	24
82241961120	26
453764840760	28
1782244008160	30
4947166777905	32
9527550547680	34
12381654787320	36
10464210515616	38
5432928694380	40
1589848008672	42
227081475720	44
11795491488	46
99273682	48

where $\sum'$ denotes the summation over e_a such that

$$\sum_{e_a (a \neq 0)} = n - e_0, \ 0 \leq e_a \leq n - e_0 (\forall a, \ a \neq 0).$$

$f(g, r)$ is the number of ordered g-elements which span the r-dimensional subspace of the fixed r-dimensional subspace in a g-dimensional space, that is

$$f(g, r) = \sharp\{(v_1, \ldots, v_g) \in D^g : \dim\langle v_1, \ldots, v_g \rangle = r\},$$

where D is a fixed r-dimensional subspace in $\mathbb{F}_2^g$. Note that $f(g, r)$ is independent of the choice of the r-dimensional subspace D. Put

$$[g]_r = \begin{cases} 1 & \text{if } r = 0, \\ (2^g - 1)(2^g - 2) \cdots (2^g - 2^{r-1}) & \text{otherwise.} \end{cases}$$

The number $[g]_r$ is known as the number of ordered linear independent r-elements in the g-dimensional $\mathbb{F}_2$-space. We observe that $f(g, r) = [g]_r$ by induction on g and r, that is

(i) we prove $f(g, 0) = [g]_0$, for all g with $0 \leq g \leq k$,

(ii) assuming $f(g-1, r) = [g-1]_r$ and $f(g-1, r-1) = [g-1]_{r-1}$, we prove $f(g, r) = [g]_r$.

(i) is obvious. Before proving (ii), we claim the following recurrence

$$f(g, r) = 2^r f(g-1, r) + (2^r - 1)2^{r-1} f(g-1, r-1),$$

for $r < g$. Indeed, for a fixed r-dimensional subspace D, we have

$$\begin{aligned}
f(g,r) &= \sharp\{(v_1,\dots,v_g)\in D^g \mid \dim\langle v_1,\dots,v_g\rangle = r\} \\
&= \sharp\{(v_1,\dots,v_g)\in D^g \mid \dim\langle v_1,\dots,v_g\rangle = r, \dim\langle v_1,\dots,v_{g-1}\rangle = r\} \\
&\quad +\sharp\{(v_1,\dots,v_g)\in D^g \mid \dim\langle v_1,\dots,v_g\rangle = r, \dim\langle v_1,\dots,v_{g-1}\rangle = r-1\} \\
&= 2^r\cdot f(g-1,r) + \frac{(2^r-1)(2^{r-1}-1)\cdots(2^2-1)}{(2^{r-1}-1)(2^{r-2}-1)\cdots(2-1)}\cdot(2^r-2^{r-1})\cdot f(g-1,r-1) \\
&= 2^r f(g-1,r) + (2^r-1)2^{r-1} f(g-1,r-1).
\end{aligned}$$

Then we can prove the latter part of the induction, that is

$$\begin{aligned}
f(g,r) &= 2^r f(g-1,r) + (2^r-1)2^{r-1} f(g-1,r-1) \\
&= 2^r [g-1]_r + (2^r-1)2^{r-1}[g-1]_{r-1} \\
&= 2^r(2^{g-1}-1)\cdots(2^{g-1}-2^{r-2})(2^{g-1}-2^{r-1}) \\
&\quad +(2^r-1)2^{r-1}(2^{g-1}-1)\cdots(2^{g-1}-2^{r-3})(2^{g-1}-2^{r-2}) \\
&= (2^g-2)\cdots(2^g-2^{r-1})(2^g-2^r) + (2^r-1)(2^g-2)\cdots(2^g-2^{r-2})(2^g-2^{r-1}) \\
&= (2^g-2)\cdots(2^g-2)\left\{(2^g-2^r)+(2^r-1)\right\} \\
&= (2^g-2)\cdots(2^g-2)\cdot(2^g-1) \\
&= [g]_r.
\end{aligned}$$

Thus the induction is complete.

Therefore we have

$$\sum{}' \mathfrak{A}^r_{\mathbf{e}}(C) = [g]_r A^r_{n-e_0}(C).$$

Finally we give a relation between J^g_C and W^r_C's.

Theorem 5.1 *For C a code over $\mathbb{F}_2$, we get*

$$J^g_C(x_0 = x,\ x_a = y(a\neq 0)) = \sum_{r=0}^{g} [g]_r W^r_C(x,y).$$

Proof. We have

$$\begin{aligned}
J^g_C(x_a, a\in\mathbb{F}_2^g) &:= \sum_{r=0}^{g} \sum_{\substack{v_1,\dots,v_g\in C \\ \dim\langle v_1,\dots,v_g\rangle = r}} \prod_{a\in\mathbb{F}_2^g} x_a^{n_a(v_1,\dots,v_g)} \\
&= \sum_{r=0}^{g}\sum_{e_0=0}^{n}\left(\sum{}' \mathfrak{A}^r_{\mathbf{e}}(C)\prod_{a\neq 0} x_a^{e_a}\right) x_0^{e_0}.
\end{aligned}$$

Putting $x_0 = x,\ x_a = y\ (a \neq 0)$, we have

$$\begin{aligned} J_C^g(x_0 = x,\ x_a = y(a \neq 0)) &= \sum_{r=0}^{g} \sum_{e_0=0}^{n} \left({\sum}' \mathfrak{A}_{\mathbf{e}}^r(C) y^{n-e_0} \right) x^{e_0} \\ &= \sum_{r=0}^{g} \sum_{e_0=0}^{n} [g]_r A_{n-e_0}^r(C) y^{n-e_0} x^{e_0} \end{aligned}$$

Then we put $e_0 \mapsto n - i\ (0 \leq i \leq n)$ and we have

$$\begin{aligned} J_C^g(x_0 = x,\ x_a = y(a \neq 0)) &= \sum_{r=0}^{g} \sum_{i=0}^{n} [g]_r A_i^r(C) x^{n-i} y^i \\ &= \sum_{r=0}^{g} [g]_r W_C^r(x, y). \end{aligned}$$

This completes the proof of Theorem 5.1. □

Example 4: We give examples for the binary case. In the following list, we omit C, x, y. W^0 is always x^n, where n denotes the length of the code C.

$$\begin{aligned} J^1 &= W^0 + W^1, \\ J^2 &= W^0 + 3W^1 + 6W^2, \\ J^3 &= W^0 + 7W^1 + 42W^2 + 168W^3, \\ J^4 &= W^0 + 15W^1 + 210W^2 + 2520W^3 + 20160W^4. \end{aligned}$$

The joint weight enumerator $J_C^g(x_a)$ has the MacWilliams identity (see [8]), that is

$$J_{C^\perp}^g(x_a) = \frac{1}{|C|^g} J_C^g \left(\sum_{b \in \mathbb{F}_2^g} (-1)^{[a,b]} x_b \right).$$

This leads to the MacWilliams identity for W_C^r (see Theorem 1 in [5]):

Corollary 5.2 (MacWilliams Relations) *Let C be a code over $\mathbb{F}_2$. Then we get*

$$\sum_{r=0}^{g} [g]_r W_{C^\perp}^r(x, y) = \frac{1}{|C|^g} \sum_{r=0}^{g} [g]_r W_C^r(x + (2^g - 1)y, x - y).$$

Corollary 5.3 *Let C, D be codes over $\mathbb{F}_2$. Then we get*

$$\sum_{r=0}^{g} [g]_r W_{C \oplus D}^r(x, y) = \sum_{0 \leq r,\ r' \leq g} [g]_r [g]_{r'} W^r(C; x, y) W_D^{r'}(x, y).$$

Proof. This follows from the identity $J_{C \oplus D}^g = J_C^g J_D^g$. □

5.1 A Gleason-type Theorem

In this subsection, we shall use the previous results to produce a Gleason-type theorem for binary self-dual codes.

Let C be a self-dual Type I code and $W^r(C;x,y)$ its symmetric higher weight enumerator. Consider the polynomial $J^t(x,y)$, the genus t joint weight enumerator. The polynomial $J^t(x,y)$ is held invariant by the action of the MacWilliams relations given by the matrix

$$M_t = \frac{1}{\sqrt{2^t}} \begin{pmatrix} 1 & 2^t - 1 \\ 1 & -1 \end{pmatrix}.$$

It is also held invariant by the matrix

$$-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

because the length of the code must be even.

These two matrices generate the following group: $G_t = \{I, M_t, -M_t, -I\}$. For all t the Molien series is given by

$$\frac{1}{(\lambda^2-1)^2} = 1 + 2\lambda^2 + 3\lambda^4 + 4\lambda^6 + \dots$$

It is easy to find the invariants, giving the following theorem.

Theorem 5.4 *Let C be a Type I binary code, then*

$$J^t(x,y) = \sum_{r \le t} [t]_r W^r(C;x,y) \in \mathbb{C}[x^2 + (2^t-1)y^2, x^2 + (2^t-1)xy]. \tag{20}$$

Note that the only assumption is that the code is formally self-dual with respect to the genus t weight enumerator and that the length of the code is even. Thus any code equivalent to its dual has a weight enumerator of the form given in the previous theorem.

If the code is Type II then the length must be a multiple of 8 and we have that J^t is also held invariant by the matrix ωI, where $\omega^8 = 1$.

Let $G_{II,t} = \langle G_t, \omega I \rangle$. Then $G_{II,t}$ has order 16 and the Molien series is simply a subseries of the Molien series given above where the only terms with non-zero coefficients are those with exponents congruent to $0 \pmod 8$. Moreover, the weight enumerator of a Type II code is an element of the ring given in Theorem 5.4 with the restriction that the length of the code is $0 \pmod 8$.

Using the Gleason theorem given above together with the equation in Theorem 5.1, it is a simple calculation to determine all of the higher weight enumerators for the $[24, 12, 8]$ Type II Golay code, which are given in Tables 5, 6 and 7. It is then easy to compute the genus 12 weight enumerator, and this is given in Table 8.

6 Graded Rings

We consider the graded ring

$$\mathfrak{W}^{(g)} = \mathbb{C}[W^r(C;x,y) : 0 \le r \le g],$$

with C a Type II code, and denote the vector space of $\mathfrak{W}^{(g)}$ of degree ℓ by $\mathfrak{W}^{(g)}_\ell$

$$\mathfrak{W}^{(g)} = \oplus_{\ell \ge 0, \ell \equiv 0 \pmod 8} \mathfrak{W}^{(g)}_\ell.$$

We put

$$\begin{aligned} I_0 &= W^0_{e_8} = x^8, \\ I_1 &= W^1_{e_8} = 14x^4y^4 + y^8, \\ I_2 &= W^1_{g_{24}} = 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}, \end{aligned}$$

where e_8 and g_{24} denote the [8,4,4] extended Hamming code and the [24,12,8] extended Golay code, respectively.

6.1 The graded ring for $g = 0$ and 1

Theorem 6.1 (i) $\mathfrak{W}^{(0)} = \mathbb{C}[I_0]$.
(ii) *I_0 and I_1 are algebraically independent and* $\mathfrak{W}^{(1)} = \mathbb{C}[I_0, I_1] \oplus \mathbb{C}[I_0, I_1]I_2$.

Proof. (i) is obvious and we prove (ii). First we show that I_0 and I_1 are algebraically independent. Otherwise we have

$$\sum_{8i+8j=\ell} \alpha_{ij} I_0^i I_1^j = 0, \tag{21}$$

for some α_{ij}'s and some positive integer ℓ. Dividing both sides by some appropriate power of I_0, we can assume that $\alpha_{0,\ell/8} \ne 0$. Considering the coefficient of y^ℓ, we have $\alpha_{0,\ell/8} = 0$, which contradicts the assumption $\alpha_{0,\ell/8} \ne 0$. Therefore I_0 and I_1 are algebraically independent.

For any Type II code C, there exists some polynomial $P(X,Y)$ such that

$$J^1_C = P(J^1_{e_8}, J^1_{g_{24}}).$$

By Theorem 5.1, we have

$$\begin{aligned} J^1_C &= P(I_0 + I_1, I_0^3 + I_2) \\ &= \widetilde{P}(I_0, I_1, I_2), \end{aligned}$$

for some polynomial $\widetilde{P}(X,Y,Z)$. Again using Theorem 5.1, we have

$$W^1_C = \widetilde{P}(I_0, I_1, I_2) - W^0_C \in \mathbb{C}[I_0, I_1, I_2],$$

therefore we have

$$\mathfrak{W}^1 = \mathbb{C}[I_0, I_1, I_2].$$

Because of the relation

$$\begin{aligned} I_2^2 &= -115273125 I_0^4 I_1^2 - 29552562 I_0^3 I_1^3 - 834555 I_0^2 I_1^4 - 1518 I_0 I_1^5 - I_1^6 \\ &\quad + (29767500 I_0^3 + 718878 I_0^2 I_1 + 3282 I_0 I_1^2 + 2 I_1^3) I_2, \end{aligned}$$

we have

$$\mathfrak{W}^1 = \mathbb{C}[I_0, I_1] + \mathbb{C}[I_0, I_1] I_2.$$

We assume

$$\sum_{8i+8j=\ell} \alpha_{ij} I_0^i I_1^j + \left(\sum_{8i+8j=\ell-24} \beta_{ij} I_0^i I_1^j \right) I_2 = 0. \tag{22}$$

Dividing both sides by some power of I_0, we may assume that at least one of $\alpha_{0,\ell/8}$ and $\beta_{0,(\ell-24)/8}$ is not zero, but this is impossible because the coefficient of y^ℓ must satisfy

$$\alpha_{0,\ell/8} + \beta_{0,(\ell-24)/8} = 0.$$

Therefore we have

$$\mathfrak{W}^{(1)} = \mathbb{C}[I_0, I_1] \oplus \mathbb{C}[I_0, I_1] I_2,$$

which completes the proof of (ii). □

Corollary 6.2 *We obtain*

$$\begin{aligned} \sum_{\ell \geq 0} \dim \mathfrak{W}_\ell^{(0)} t^\ell &= \frac{1}{1-t^8}, \\ \sum_{\ell \geq 0} \dim \mathfrak{W}_\ell^{(1)} t^\ell &= \frac{1+t^{24}}{(1-t^8)^2}. \end{aligned}$$

We shall recall some definitions. Let R be a graded $\mathbb{C}$-algebra of dimension n, where n is the maximal number of elements of R which are algebraically independent over $\mathbb{C}$. A set $\{\theta_1, \ldots, \theta_n\}$ of homogeneous elements of positive degree in R is said to be a homogeneous system of parameters if R is finitely generated as a module over $\mathbb{C}[\theta_1, \ldots, \theta_n]$. If R is a finitely generated free module over $\mathbb{C}[\theta_1, \ldots, \theta_n]$, then R is said to be Cohen-Macaulay. We are now able to state the next corollary.

Corollary 6.3 *The graded rings $\mathfrak{W}^{(g)}$ for $g = 0,\ 1$ are Cohen-Macaulay.*

Remark. The decomposition given in the above theorem is not unique. In fact, we have

$$\begin{aligned}
\mathfrak{W}^{(0)} &= \mathbb{C}[I_0^2]\,(1 \oplus I_0)\,, \\
\sum_{\ell \geq 0} \dim \mathfrak{W}_\ell^{(0)} t^\ell &= \frac{1+t^8}{1-t^{16}}, \\
\mathfrak{W}^{(1)} &= \mathbb{C}[I_0, I_2]\left(1 \oplus I_1 \oplus I_1^2 \oplus I_1^3 \oplus I_1^4 \oplus I_1^5\right), \\
\sum_{\ell \geq 0} \dim \mathfrak{W}_\ell^{(1)} t^\ell &= \frac{1+t^8+t^{16}+t^{24}+t^{32}+t^{40}}{(1-t^8)(1-t^{24})}.
\end{aligned}$$

The details are omitted.

6.2 The graded ring for $g = 2$

The homogeneous polynomials $I_0,\ I_1$ and I_2 are the same as the previous section. Moreover we put

$$\begin{aligned}
I_3 = W_{e_8}^2 &= 28x^2y^6 + 7y^8, \\
I_4 = W_{g_{24}}^2 &= 35420x^{12}y^{12} + 170016x^{10}y^{14} + 648945x^8y^{16} + \\
&\quad 1020096x^6y^{18} + 743820x^4y^{20} + 170016x^2y^{22} + 5842y^{24},
\end{aligned}$$

and $I_5 = W_{d_{24}^+}^2,\ I_6 = W_{d_{32}^+}^2,\ I_7 = W_{d_{40}^+}^2$, where d_n^+ denotes the code of length n whose generator matrix is given by

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

Lemma 6.4 (i) *For $\ell = 8,\ 16$, the homogeneous polynomials*

$$I_0^i I_1^j I_3^k \ (0 \leq i, j, k \leq \ell/8, 8i + 8j + 8k = \ell),$$

are linearly independent over $\mathbb{C}$.

(ii) *For $\ell \geq 24$, the homogeneous polynomials*

$$\begin{aligned}
&I_0^i I_1^j I_3^k \ (0 \leq i, j \leq \ell/8, 0 \leq k \leq 3,\ 8i + 8j + 8k = \ell), \\
&I_0^{(\ell-24)/8} I_2,\ I_0^{(\ell-24)/8} I_4
\end{aligned}$$

are linearly independent over $\mathbb{C}$.

Proof. We can show the case $\ell = 8, 16$ by direct computation. We assume $\ell \geq 24$ and put

$$\sum_{\substack{0 \leq i,j \leq \ell/8, 0 \leq k \leq 3 \\ 8i+8j+8k=\ell}} \alpha_{i,j,k} I_0^i I_1^j I_3^k + \beta I_0^{(\ell-24)/8} I_2 + \gamma I_0^{(\ell-24)/8} I_4 = 0.$$

First Step: for $\ell \geq 24$, we have

$$\alpha_{\ell/8,0,0} = \alpha_{\ell/8-1,1,0} = \alpha_{\ell/8-1,0,1} = \alpha_{\ell/8-2,1,1} = 0.$$

Second Step: for $\ell \geq 32$, we have

$$\alpha_{i,\ell/8-i,0} = \alpha_{i,\ell/8-i-1,1} = \alpha_{i,\ell/8-i-2,2} = \alpha_{i,\ell/8-i-3,3} = 0 \quad \text{forall } i \ (0 \leq i \leq \frac{\ell}{8} - 4).$$

Third Step: for $\ell \geq 24$, we have

$$\alpha_{\ell/8-2,2,0} = \alpha_{\ell/8-2,0,2} = \alpha_{\ell/8-3,3,0} = \alpha_{\ell/8-3,2,1} = \alpha_{\ell/8-3,1,2} = \alpha_{\ell/8-3,0,3} = \beta = \gamma = 0.$$

Proof of the First Step: looking at the coefficients of the monomials x^ℓ, $x^{\ell-4}y^4$, $x^{\ell-6}y^6$, $x^{\ell-10}y^{10}$, we have

$$\alpha_{\ell/8,0,0} = 14\alpha_{\ell/8-1,1,0} = 28\alpha_{\ell/8-1,0,1} = 14 \cdot 28\alpha_{\ell/8-2,1,1} = 0.$$

Proof of the Second Step: by induction on i. For $i = 0$, looking at the coefficients of the monomials y^ℓ, $x^2y^{\ell-2}$, $x^4y^{\ell-4}$, $x^6y^{\ell-6}$, the matrix of the coefficients of $\alpha_{0,\ell/8,0}, \alpha_{0,\ell/8-1,1}, \alpha_{0,\ell/8-2,2}, \alpha_{0,\ell/8-3,3}$ is given by

$$\begin{pmatrix} 1 & 7 & 7^2 & 7^3 \\ 0 & 28 & 2 \cdot 28 \cdot 7 & 3 \cdot 28 \cdot 7^2 \\ (\ell/8) \cdot 14 & (\ell/8-1) \cdot 14 \cdot 7 & (\ell/8-2) \cdot 14 \cdot 7^2 + 28^2 & (\ell/8-3) \cdot 14 \cdot 7^3 + 3 \cdot 28^2 \cdot 7 \\ 0 & (\ell/8-1) \cdot 14 \cdot 28 & (\ell/8-2) \cdot 14 \cdot 2 \cdot 28 \cdot 7 & (\ell/8-3) \cdot 14 \cdot 3 \cdot 28 \cdot 7^2 + 28^3 \end{pmatrix} \begin{pmatrix} \alpha_{0,\ell/8,0} \\ \alpha_{i,\ell/8-1,1} \\ \alpha_{0,\ell/8-2,2} \\ \alpha_{i,\ell/8-3,3} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

The determinant of this matrix is 481890304 and this matrix has an inverse. Therefore we have

$$\alpha_{0,\ell/8,0} = \alpha_{0,\ell/8-1,1} = \alpha_{0,\ell/8-2,2} = \alpha_{0,\ell/8-3,3} = 0.$$

We assume the validity for less than i. Looking at the coefficients of the monomials $x^{8i}y^{\ell-8i}$, $x^{8i+2}y^{\ell-8i-2}$, $x^{8i+4}y^{\ell-8i-4}$, $x^{8i+6}y^{\ell-8i-6}$, we have

$$\begin{pmatrix} 1 & 7 & 7^2 & 7^3 \\ 0 & 28 & 2 \cdot 28 \cdot 7 & 3 \cdot 28 \cdot 7^2 \\ (\ell/8-i) \cdot 14 & (\ell/8-i-1) \cdot 14 \cdot 7 & (\ell/8-i-2) \cdot 14 \cdot 7^2 + 28^2 & (\ell/8-i-3) \cdot 14 \cdot 7^3 + 3 \cdot 28^2 \cdot 7 \\ 0 & (\ell/8-i-1) \cdot 14 \cdot 28 & (\ell/8-i-2) \cdot 14 \cdot 2 \cdot 28 \cdot 7 & (\ell/8-i-3) \cdot 14 \cdot 3 \cdot 28 \cdot 7^2 + 28^3 \end{pmatrix} \begin{pmatrix} \alpha_{i,\ell/8-i,0} \\ \alpha_{i,\ell/8-i-1,1} \\ \alpha_{i,\ell/8-i-2,2} \\ \alpha_{i,\ell/8-i-3,3} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

whose determinant is also 481890304. So we have

$$\alpha_{i,\ell/8-i,0} = \alpha_{i,\ell/8-i-1,1} = \alpha_{i,\ell/8-i-2,2} = \alpha_{i,\ell/8-i-3,3} = 0.$$

This completes the induction.

Proof of the Third Step: looking at the coefficients of the monomials $x^{\ell-8}y^8,\ x^{\ell-12}y^{12},\ x^{\ell-14}y^{14},\ x^{\ell-16}y^{16},\ x^{\ell-18}y^{18},\ x^{\ell-20}y^{20},\ x^{\ell-22}y^{22},\ x^{\ell-24}y^{24}$, we have

$$\begin{pmatrix} 14^2 & 0 & 0 & 0 & 0 & 0 & 759 & 0 \\ 2\cdot 14 & 28^2 & 14^3 & 0 & 0 & 0 & 2576 & 35420 \\ 0 & 2\cdot 28\cdot 7 & 0 & 14^2\cdot 28 & 0 & 0 & 0 & 170016 \\ 1 & 7^2 & 3\cdot 14^2 & 14^2\cdot 7 & 14\cdot 28^2 & 0 & 759 & 648945 \\ 0 & 0 & 0 & 28^2 & 14\cdot 2\cdot 28\cdot 7 & 28^3 & 0 & 1020096 \\ 0 & 0 & 3\cdot 14 & 2\cdot 14\cdot 7 & 14\cdot 7^2+28^2 & 3\cdot 28^2\cdot 7 & 0 & 743820 \\ 0 & 0 & 0 & 28 & 2\cdot 28\cdot 7 & 3\cdot 28\cdot 7^2 & 0 & 170016 \\ 0 & 0 & 1 & 7 & 7^2 & 7^3 & 1 & 5842 \end{pmatrix} \begin{pmatrix} \alpha_{\ell/8-2,2,0} \\ \alpha_{\ell/8-2,0,2} \\ \alpha_{\ell/8-3,3,0} \\ \alpha_{\ell/8-3,2,1} \\ \alpha_{\ell/8-3,1,2} \\ \alpha_{\ell/8-3,0,3} \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

whose determinant is 30215558351462089516664640, which implies

$$\alpha_{\ell/8-2,2,0} = \alpha_{\ell/8-2,0,2} = \alpha_{\ell/8-3,3,0} = \alpha_{\ell/8-3,2,1} = \alpha_{\ell/8-3,1,2} = \alpha_{\ell/8-3,0,3} = \beta = \gamma = 0.$$

This completes the proof of Lemma 6.4. □

We put

$$V(\ell) = \begin{cases} \bigoplus_{\substack{0\le i,j,k\le \ell/8 \\ 8i+8j+8k=\ell}} \mathbb{C} I_0^i I_1^j I_3^k & \ell = 0,\ 8,\ 16, \\ \left(\bigoplus_{\substack{0\le i,j\le \ell/8, 0\le k\le 3 \\ 8i+8j+8k=\ell}} \mathbb{C} I_0^i I_1^j I_3^k \right) \oplus \mathbb{C} I_0^{(\ell-24)/8} I_2 \oplus \mathbb{C} I_0^{(\ell-24)/8} I_4 & \ell \ge 24, \ell \equiv 0 (\mathrm{mod}\ 8), \end{cases}$$

and put $V = \oplus_{\ell \ge 0} V(\ell)$.

Lemma 6.5 $I_5,\ I_1I_2,\ I_1I_4,\ I_3I_2,\ I_3I_4,\ I_6,\ I_7,\ I_2^2,\ I_2I_4,\ I_4^2 \in V.$

Proof. By direct computation using Magma. The explicit relations can be found at [7]. □

Theorem 6.6 *We get* $\mathfrak{W}^{(2)} = V$.

Proof. By a Theorem of Duke [3], for any Type II code C, we have

$$J_C^2 = P_1(J_{e_8}^2, J_{d_{24}^+}^2, J_{g_{24}}^2 J_{d_{40}^+}^2) + P_2(J_{e_8}^2, J_{d_{24}^+}^2, J_{g_{24}}^2, J_{d_{40}^+}^2) J_{d_{32}^+}^2,$$

for some polynomials $P_1(X,Y,Z,W),\ P_2(X,Y,Z,W)$. By Theorems 1 and 5, we have

$$W_C^2 \in \mathbb{C}[I_0, I_1, I_2, I_3, I_4, I_5, I_6, I_7],$$

or

$$\mathfrak{W}^{(2)} = \mathbb{C}[I_0, I_1, I_2, I_3, I_4, I_5, I_6, I_7].$$

By the explicit relations given in Lemma 6.5, we have

$$\mathfrak{W}^{(2)} = \mathbb{C}[I_0, I_1, I_2, I_3, I_4].$$

In order to prove Theorem 6.6, it is enough to show that the elements $I_0^*I_1^*I_3^*I_2^*I_4^*$ are the elements of V, where $*$ denotes any non-negative integer. By the explicit relations given in Lemma 6.5, we know that $I_0^*I_1^*I_3^*I_2^*I_4^*$ can be written as the sum of the elements

$$I_0^*I_1^*I_3^*,\ I_0^*I_1^*I_3^*I_2,\ I_0^*I_1^*I_3^*I_4.$$

Again from Lemma 6.5 we know that $I_0^*I_1^*I_3^*I_2, I_0^*I_1^*I_3^*I_4$ can be written as the sum of the elements

$$I_0^*I_1^*I_3^*,\ I_0^*I_1^*I_2,\ I_0^*I_1^*I_4.$$

Again from Lemma 6.5 we know that $I_0^*I_1^*I_2, I_0^*I_1^*I_4$ can be written as the sum of the elements

$$I_0^*I_1^*I_3^*,\ I_0^*I_2,\ I_0^*I_4.$$

The elements $I_0^*I_1^*I_3^*$ are contained in V because of the equality

$$\mathbb{C}[I_0, I_1, I_3] = \mathbb{C}[I_0, I_1](1 \oplus I_3 \oplus I_3^2 \oplus I_3^3).$$

Therefore we have shown that any elements of the form $I_0^*I_1^*I_3^*I_2^*I_4^*$ are contained in V, and this completes the proof of Theorem 6.6. □

Corollary 6.7 *We get*

$$\dim \mathfrak{W}_\ell^{(2)} = \begin{cases} 1 & \ell = 0, \\ 3\ell/8 & \ell = 8,\ 16, \\ \ell/2 & \ell \geq 24. \end{cases}$$

Corollary 6.8 *The graded ring $\mathfrak{W}^{(2)}$ is not Cohen-Macaulay.*

Proof. Assume that $\mathfrak{W}^{(2)}$ is Cohen-Macaulay. From Theorem 6.6, $\mathfrak{W}^{(2)}$ is a finitely generated $\mathbb{C}[I_0, I_1]$-module, for example, take $1, I_3, I_3^2, I_3^3, I_2, I_4$ as a set of generators. This implies that a set $\{I_0, I_1\}$ is a homogeneous system of parameters (See [10]). Theorem 2.3.1 in [10] says that the ring $\mathfrak{W}^{(2)}$ must be a finitely generated *free* $\mathbb{C}[I_0, I_1]$-module. Then the dimension formula of $\mathfrak{W}^{(2)}$ must be in the form

$$\frac{f(t)}{(1-t^8)^2}, \quad f(t) \in \mathbb{Z}_{\geq 0}[t],$$

but this is impossible since Theorem 6.6 (and Corollary 6.7) gives the equality

$$\frac{f(t)}{(1-t^8)^2} = \frac{1+t^8+t^{16}+t^{24}}{(1-t^8)^2} + \frac{t^{24}}{1-t^8} + \frac{t^{24}}{1-t^8},$$

that is

$$f(t) = 1 + t^8 + t^{16} + 3t^{24} - 2t^{32}.$$

This completes the proof of Corollary 6.8.

Acknowledgment. The third author wishes to thank Professor K. Yokoyama for interesting discussions on the paper.

References

[1] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory*, vol. 36, pp. 1319–1333, 1990.

[2] S.T Dougherty, Masaaki Harada and Aaron Gulliver, Extremal Binary Self-Dual Codes, *IEEE Trans. Inform. Theory*, vol. 43, No. 6, pp. 2036 – 2046, 1997.

[3] W. Duke, On codes and Siegel modular forms, *Int. Math. Res. Notices*, no. 5 pp. 125–136. 1993.

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

[5] T. Kløve, Support weight distributions of linear codes, *Discrete Math*, vol. 106/107, pp. 311–316, 1992.

[6] 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*, vol. 18, pp. 794–805, 1972.

[7] Oura, Manabu, Explicit Relations, http://web.sapmed.ac.jp/math.

[8] E. Rains and N.J.A. Sloane, Self-Dual Codes in *Handbook of Coding Theory*, V. Pless and W.C. Huffman, Eds, Amsterdam, The Netherlands: Elsevier Science, 1998.

[9] B. Runge, Codes and Siegel modular forms, *Discrete Math.*, vol. 148, 175–204, 1996.

[10] B. Sturmfels, *Algorithms in invariant theory*, Texts and Monographs in Symbolic Computation, Springer-Verlag Wien New York, 1993.

[11] M.A. Tsfasman and S.G. Vladut, Geometric approach to higher weights, *IEEE Trans. Inform. Theory* vol. 41, pp. 1564–1588, 1995.

[12] V.K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory*, vol. 37, pp. 1412-1418, 1991.

Table 3: Binary Self-Dual Codes with $n \leq 26$

n	Code	d_I	d_{II}	d_2	d_3
2	i_2	2			
4	i_2^2	2		4	
6	i_2^3	2		4	6
8	i_2^4	2		4	6
8	e_8		4	6	7
10	i_2^5	2		4	6
10	$e_8 i_2$	2		6	7
12	i_2^6	2		4	6
12	$i_2^2 e_8$	2		4	7
12	d_{12}^+	4		6	8
14	e_7^{2+}	4		6	7
16	d_8^{2+}	4		6	8
16	d_{16}^+		4	6	8
16	e_8^2		4	6	7
18	d_6^{3+}	4		6	9
18	$(d_{10} e_7 f_1)^+$	4		6	7
20	d_{20}^+	4		6	8
20	$(d_{12} e_8)^+$	4		6	7
20	$(d_{12} d_8)^+$	4		6	8
20	$(d_8^2 d_4)^+$	4		6	8
20	$(e_7^2 d_6)^+$	4		6	7
20	$(d_6^3 f_2)^+$	4		6	9
20	d_4^{5+}	4		6	10
22	g_{22}	6		10	12
24	g_{24}		8	12	14
24	h_{24}^+	6		10	12
26	f_{13}^2	6		10	12

Table 4: Binary Self-Dual Codes with $28 \le n \le 32$

n	Code	d_I	d_{II}	d_2	d_3
28	$A28$	6		10	13
28	$B28$	6		10	12
28	$C28$	6		10	12
30	$A30$	6		10	12
30	$B30$	6		10	12
30	$C30$	6		10	13
30	$D30$	6		10	12
30	$E30$	6		10	12
30	$F30$	6		10	12
30	$G30$	6		10	12
30	$H30$	6		10	13
30	$I30$	6		10	12
30	$J30$	6		10	12
30	$K30$	6		10	12
32	$C81$ (q_{32})		8	12	14
32	$C82$ (r_{32})		8	12	14
32	$C83$ (g_{16}^{2+})		8	12	14
32	$C84$ (f_4^{8+})		8	12	14
32	$C85$ (f_2^{16+})		8	12	14
32	$g_{16}^{2+} - I$	8		12	14
32	$f_4^{8+} - I$	8		12	14
32	$r_{32} - I$	8		12	14

Table 5: Higher Weight Enumerators for the $[24, 12, 8]$ Golay Code

W^1	W^2	W^3	W^4	weight i
759				8
2576	35420			12
	170016	91080		14
		566720	12144	15
759	648945	1939245	648945	16
		6800640	5100480	17
	1020096	19126800	32728080	18
		41483904	160665120	19
	743820	73744440	613842768	20
		97475840	1766466240	21
	170016	93721320	3627594960	22
		56785344	4739378160	23
1	5842	16610462	2964543186	24

Table 6: Higher Weight Enumerators for the $[24, 12, 8]$ Golay Code

W^5	W^6	W^7	W^8	weight i
759				16
340032				17
6078072	134596			18
69706560	4590432	42504		19
580710900	89736570	2497110	10626	20
3545513664	1187440320	77498960	991760	21
15228970680	10684676772	1504064760	45054240	22
41367370176	59857703136	17539208808	1129817040	23
53630338872	158850111409	95305717573	12735106417	24

Table 7: Higher Weight Enumerators for the $[24, 12, 8]$ Golay Code

W^9	W^{10}	W^{11}	W^{12}	weight i
2024				21
276276	276			22
16194024	48576	24		23
391873471	2745303	4071	1	24

Table 8: The Genus 12 Weight Enumerator for a the $[24, 12, 8]$ Golay Code

coefficient of y^i	weight i
1	0
3108105	8
593824369320	12
6251128987783680	14
344460661176183552O	15
1050587410792264700355	16
390501288700263630489600	17
63284842299967754432174208O	18
818341578256851211988997411840	19
837777240517422043317084461495640	20
653466247556108310233433567871027200	21
364901493237608612477185876631883214080	22
129936662157218014626595565640177642647040	23
22170442980575323746852678066521975856155955	24