On the Hamming Weight Enumerators of Self-Dual Codes over $\mathbb{Z}_k$

Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560, Japan
Email: harada@kszaoh3.kj.yamagata-u.ac.jp
and
Manabu Oura
Graduate School of Mathematics
Kyushu University
Fukuoka 812–81, Japan
Email: ohura@math.kyushu-u.ac.jp

June 5, 2004

Abstract

In this note, we investigate the Hamming weight enumerators of self-dual codes over $\mathbb{F}_q$ and $\mathbb{Z}_k$. Using invariant theory, a basis for the space of invariants to which the Hamming weight enumerators belong for self-dual codes over $\mathbb{F}_q$ and $\mathbb{Z}_k$ is determined.

1 Introduction

Several types of weight enumerators of self-dual codes have been investigated as an application of invariant theory. It is a fundmental and important problem in algebraic coding theory to determine the ring of invariants to which some weight enumerators belong for a class of self-dual codes. MacWilliams [6] showed that the Hamming weight enumerator of the dual code $C^\perp$ is uniquely determined by the Hamming weight enumerator of a code C over a finite field $\mathbb{F}_q$ of q elements where q is a prime power. Recently the MacWilliams identity for codes over the finite ring $\mathbb{Z}_k$ of integers modulo k has been established in [5]. These MacWilliams identities imply that the Hamming weight enumerators of self-dual codes are invariant under the linear transformation derived from the MacWilliams identity. Moreover the Hamming weight enumerators of certain self-dual codes are invariant under a group. For example, the Hamming weight enumerator of binary Type II codes is invariant under a group of order 192 and is a polynomial in the Hamming weight enumerators of the extended Hamming code and the extended Golay code. This is the well-known Gleason's theorem (cf. [8]). As a generalization of Gleason's theorem, a basis for the space of invariants to which a class of weight enumerators belong for formally self-dual codes and self-dual codes over $\mathbb{F}_q$ was given in [7].

In this note, we investigate the Hamming weight enumerators of self-dual codes over $\mathbb{F}_q$ where q is an odd prime power $\equiv 3 \pmod 4$ and over $\mathbb{Z}_k$. In [7] the Hamming weight enumerator of a self-dual code over $\mathbb{F}_q$ was studied for an odd prime power. We emphasize that if $q \equiv 3 \pmod 4$ then the Hamming weight enumerator is also invariant under an additional matrix derived from the restriction on the length. The main results of this note are Theorems 3.5 and 3.6 which summarize the structures of the rings of invariants to which the Hamming weight enumerators belong for self-dual codes over $\mathbb{F}_q$ and $\mathbb{Z}_k$.

2 Preliminaries

2.1 Codes

We give the necessary background from coding theory, define self-dual codes and the Hamming weight enumerators. In particular, recently there has been interest in codes over finite rings as well as finite fields. Thus we first give definitions of codes over finite fields then codes over finite rings, specifically the ring $\mathbb{Z}_k$.

A linear $[n,k]$ code C over $\mathbb{F}_q$ is a k-dimensional vector subspace of $\mathbb{F}_q^n$. The parameter n is called the length of C. The elements of C are called codewords and the Hamming weight $wt(x)$ of a codeword x is the number of its non-zero coordinates. The minimum weight of C is defined by $\min\{wt(x) \mid 0 \neq x \in C\}$. An $[n,k,d]$ code is an $[n,k]$ code with minimum weight d. Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be two elements of $\mathbb{F}_q^n$. We define the inner product of x and y on $\mathbb{F}_q^n$ by $x \cdot y = x_1y_1 + \cdots + x_ny_n$ over $\mathbb{F}_q$. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0 \text{ for all } y \in C\}$. C is *self-dual* if $C = C^\perp$.

A code C of length n over $\mathbb{Z}_k$ is an additive subgroup of $\mathbb{Z}_k^n$. Let $x = (x_1, \ldots, x_n)$ and

$y = (y_1, \ldots, y_n)$ 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 $C^\perp = \{x \in \mathbb{Z}_k^n | \ x \cdot y = 0 \text{ for all } y \in C\}$. The elements of C are called codewords and the Hamming weight $wt(x)$ of a codeword x is the number of its non-zero coordinates. C is *self-dual* if $C = C^\perp$.

The Hamming weight enumerator of a code C of length n over $\mathbb{F}_q$ (or $\mathbb{Z}_k$) is the polynomial

$$W_C(x, y) = \sum_{c \in C} x^{n - wt(c)} y^{wt(c)}.$$

The MacWilliams identity for a code over $\mathbb{F}_q$ gives the Hamming weight enumerator of $C^\perp$ in terms of that of C.

Theorem 2.1 (MacWilliams [6]) *Let C be a linear code over $\mathbb{F}_q$. Then*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y).$$

Recently the MacWilliams identity for codes over $\mathbb{Z}_k$ has been established.

Theorem 2.2 (Klemm [5]) *Let C be a code over $\mathbb{Z}_k$ then*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (k-1)y, x - y).$$

We now describe restrictions on the lengths of self-dual codes.

Lemma 2.3 (Pless [9]) *Suppose that $q \equiv 1 \pmod 4$, a self-dual code over $\mathbb{F}_q$ of length n exists if and only if n is even. Suppose that $q \equiv 3 \pmod 4$, a self-dual code over $\mathbb{F}_q$ of length n exists if and only if n is divisible by four.*

Lemma 2.4 (Dougherty et al. [3]) *Suppose that k is a square then there are self-dual codes over $\mathbb{Z}_k$ for all lengths.*

2.2 Invariants

The conditions satisfied by the Hamming enumerators of self-dual codes over $\mathbb{F}_q$ were investigated in [7]. The Hamming enumerators of self-dual codes belong to the ring of polynomials fixed by the group of substitutions and it is possible to find explicit generator polynomials for this ring by the Molien series. For any finite group G of complex $m \times m$ 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. For a general reference of invariant theory, see e.g. [10] and [8, Chap. 19].

Using invariant theory, a basis for the space of invariants to which the Hamming weight enumerators belong for self-dual codes over $\mathbb{F}_q$ was given in [7].

Proposition 2.5 (MacWilliams, Mallows and Sloane [7]) *Let $G_1(q)$ be the group generated by*

$$M_1(q) = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}.$$

Then $\mathbb{C}[x,y]^{G_1(q)} = \mathbb{C}[\phi_{1,1}, \phi_{1,2}]$, where

$$\begin{aligned} \phi_{1,1} &= x + (\sqrt{q}-1)y, \\ \phi_{1,2} &= y(x-y). \end{aligned}$$

Remark. $\mathbb{C}[x,y]^G = \{f \in \mathbb{C}[x,y] \mid f = f \circ A \text{ for any } A \in G\}$ is called the invariant ring for G.

Proposition 2.6 (MacWilliams, Mallows and Sloane [7]) *Let $G_2(q)$ be the group generated by*

$$M_1(q) = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix} \text{ and } M_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then $\mathbb{C}[x,y]^{G_1(2)} = \mathbb{C}[\phi_{2,1}, \phi_{2,2}]$, where

$$\begin{aligned} \phi_{2,1} &= x^2 + (q-1)xy, \\ \phi_{2,2} &= x^2 + (q-1)y^2. \end{aligned}$$

The above proposition means that the Hamming weight enumerator of a self-dual code over $\mathbb{F}_q$ is an element of $\mathbb{C}[\phi_{2,1}, \phi_{2,2}]$.

By Lemma 2.3, if $q \equiv 3 \pmod 4$ then the Hamming weight enumerator over $\mathbb{F}_q$ is also invariant by

$$M_3 = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix},$$

where $i^2 = -1$.

It is the aim of this note to determine the structure of the invariant ring of the group generated by $M_1(q)$ and M_3 and give a basis for the space of invariants to which the Hamming weight enumerators belong for self-dual codes over $\mathbb{F}_q$ where $q \equiv 3 \pmod 4$ and the finite ring $\mathbb{Z}_k$.

3 Main Results

3.1 Structure of the Invariant Ring

In this subsection, we determine the structure of the invariant ring for the finite group $G_3(k)$ generated by

$$M_1(k) = \frac{1}{\sqrt{k}} \begin{pmatrix} 1 & k-1 \\ 1 & -1 \end{pmatrix} \text{ and } M_3 = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}.$$

Lemma 3.1 *The Molien series of the invariant ring for $G_3(k)$ is given by*

$$\frac{1+\lambda^4}{(1-\lambda^4)^2} = 1 + 3\lambda^4 + 5\lambda^8 + 7\lambda^{12} + \cdots.$$

Proof. $G_3(k)$ has order 8 and $\det(I - \lambda g)$ is given in Table 1 for each element g of $G_3(k)$. The Molien series follows from Table 1.

Table 1: Determinants of $G_3(k)$

element g	I	$M_1(k)$	$M_1(k)M_3$	$M_1(k){M_3}^2$
$\det(I-\lambda g)$	$(\lambda-1)^2$	$-\lambda^2+1$	λ^2+1	$-\lambda^2+1$
element g	$M_1(k){M_3}^3$	M_3	${M_3}^2$	${M_3}^3$
$\det(I-\lambda g)$	λ^2+1	$(i\lambda-1)^2$	$(\lambda+1)^2$	$(i\lambda+1)^2$

□

Lemma 3.2 *The invariant ring $\mathbb{C}[x,y]^{G_3(k)}$ is generated by the polynomials $\phi_{3,1}, \phi_{3,2}$, and $\phi_{3,3}$, where*

$$\begin{aligned}
\phi_{3,1} &= x^4 + 4(k-1)xy^3 + (k^2-4k+3)y^4, \\
\phi_{3,2} &= x^3y + (k-3)xy^3 - (k-2)y^4, \\
\phi_{3,3} &= x^2y^2 - 2xy^3 + y^4.
\end{aligned}$$

Proof. Direct calculation shows that $\phi_{3,1}, \phi_{3,2}$ and $\phi_{3,3}$ are elements of $\mathbb{C}[x,y]^{G_3(k)}$. It is sufficient to show that every element with degree at most 8, which is the order of the group $G_3(k)$, can be obtained from the elements $\phi_{3,1}, \phi_{3,2}, \phi_{3,3}$ (see Theorem 2.1.4 in [10]). We shall show that the vector spaces spanned by $\{\phi_{3,1}, \phi_{3,2}, \phi_{3,3}\}$ and $\{\phi_{3,1}^2, \phi_{3,2}^2, \phi_{3,1}\phi_{3,2}, \phi_{3,1}\phi_{3,3}, \phi_{3,2}\phi_{3,3}\}$ are in dimension 3 and 5, respectively. By the coefficients of x^4, x^3y and x^2y^2, $\phi_{3,1}, \phi_{3,2}, \phi_{3,3}$ are linear independent. Moreover consider the coefficients of $x^8, x^7y, x^6y^2, x^5y^3, x^4y^4$ of polynomials $\phi_{3,1}^2, \phi_{3,2}^2, \phi_{3,1}\phi_{3,2}, \phi_{3,1}\phi_{3,3}$ and $\phi_{3,2}\phi_{3,3}$. Then this shows that the set $\{\phi_{3,1}^2, \phi_{3,2}^2, \phi_{3,1}\phi_{3,2}, \phi_{3,1}\phi_{3,3}, \phi_{3,2}\phi_{3,3}\}$ forms a 5-dimensional vector space. □

Lemma 3.3 *$\phi_{3,1}$ and $\phi_{3,2}$ are algebraically independent.*

Proof. First, we order monomials by the lexicographical order on the sequence of exponents, i.e., $x^{e_1}y^{e_2} > x^{d_1}y^{d_2}$ if and only if $e_1 > d_1$ or $e_1 = d_1$ and $e_2 > d_2$.

Assume that we have the finite sum $\sum_{i,j} c_{ij}\phi_{3,1}^i\phi_{3,2}^j$ which is identically zero. The leading term of $\phi_{3,1}^i\,\phi_{3,2}^j$ is $x^{4i+3j}\,y^j$. Since the distinct summands in the equation have distinct leading terms, we have $c_{ij} = 0$ for all i, j. Therefore $\phi_{3,1}$ and $\phi_{3,2}$ are algebraically independent. □

Theorem 3.4 *The invariant ring has the structure*

$$\mathbb{C}[\phi_{3,1}, \phi_{3,2}] \oplus \phi_{3,3}\mathbb{C}[\phi_{3,1}, \phi_{3,2}].$$

Proof. Since $\phi_{3,1}, \phi_{3,2}, \phi_{3,3}$ satisfy the relation $(-2k+3)\phi_{3,3}^2 - \phi_{3,1}\phi_{3,3} - 2\phi_{3,2}\phi_{3,3} + \phi_{3,2}^2 = 0$, we have

$$\mathbb{C}[\phi_{3,1}, \phi_{3,2}, \phi_{3,3}] = \mathbb{C}[\phi_{3,1}, \phi_{3,2}] + \phi_{3,3}\mathbb{C}[\phi_{3,1}, \phi_{3,2}].$$

Assume that there exists some $f\,(\geq 1)$ such that $\mathbb{C}[\phi_{3,1}, \phi_{3,2}]_{4f+4} \cap \phi_{3,3}\mathbb{C}[\phi_{3,1}, \phi_{3,2}]_{4f} \neq \{0\}$ where $\mathbb{C}[\phi_1, \phi_2]_f$ denotes the f-th homogeneous part of $\mathbb{C}[\phi_1, \phi_2]$. The dimension of the vector space spanned by $\{g, \phi_{3,3}h \,|\, g \in \mathbb{C}[\phi_{3,1}, \phi_{3,2}],\ h \in \mathbb{C}[\phi_{3,1}, \phi_{3,2}]_{4f}\}$ is less than $\dim \mathbb{C}[\phi_{3,1}, \phi_{3,2}]_{4f+4} + \dim \mathbb{C}[\phi_{3,1}, \phi_{3,2}]_{4f}$.

On the other hand, by Lemma 3.3, we have $\dim \mathbb{C}[\phi_{3,1}, \phi_{3,2}]_{4f+4} + \dim \mathbb{C}[\phi_{3,1}, \phi_{3,2}]_{4f} = 2f + 3$, which is equal to $\dim \mathbb{C}[\phi_{3,1}, \phi_{3,2}, \phi_{3,3}]_{4f+4}$ by Lemma 3.1. This is a contradiction.

Therefore we have

$$\mathbb{C}[\phi_{3,1}, \phi_{3,2}, \phi_{3,3}] = \mathbb{C}[\phi_{3,1}, \phi_{3,2}] \oplus \phi_{3,3}\mathbb{C}[\phi_{3,1}, \phi_{3,2}],$$

and the theorem follows from Lemma 3.2. □

3.2 Gleason-Type Theorems

Combining Theorem 3.4 with the results in Section 2, we have the following Gleason-type theorems. These theorems summarize the structures of the rings of invariants to which the Hamming weight enumerators belong for self-dual codes over $\mathbb{F}_q$ and $\mathbb{Z}_k$.

Theorem 3.5 *Let C be a self-dual code over $\mathbb{F}_q$.*

(1) If $q \equiv 1 \pmod 4$ then the Hamming weight enumerator of C is an element of the ring $\mathbb{C}[x^2 + (q-1)xy, x^2 + (q-1)y^2]$.

(2) If $q \equiv 3 \pmod 4$ then the Hamming weight enumerator of C is an element of the ring $\mathbb{C}[\phi_{3,1}, \phi_{3,2}] \oplus \phi_{3,3}\mathbb{C}[\phi_{3,1}, \phi_{3,2}]$ where

$$\begin{aligned} \phi_{3,1} &= x^4 + 4(q-1)xy^3 + (q^2 - 4q + 3)y^4, \\ \phi_{3,2} &= x^3y + (q-3)xy^3 - (q-2)y^4, \\ \phi_{3,3} &= x^2y^2 - 2xy^3 + y^4. \end{aligned}$$

Remark. The ring is often smaller than the above ring for small q, e.g. $q = 3$ (cf. [8]).

Theorem 3.6 *Let C be a self-dual code over $\mathbb{Z}_k$.*

(1) If k is a square then the Hamming weight enumerator of C is an element of the ring $\mathbb{C}[x + (\sqrt{k} - 1)y, y(x - y)]$.

(2) Suppose that no self-dual code over $\mathbb{Z}_k$ for all odd lengths. Then the Hamming weight enumerator of C is an element of the ring $\mathbb{C}[x^2+(k-1)xy, x^2+(k-1)y^2]$.

(3) Suppose that no self-dual code over $\mathbb{Z}_k$ for lengths $n \not\equiv 0 \pmod 4$. Then the Hamming weight enumerator of C is an element of the ring $\mathbb{C}[\phi_{3,1},\phi_{3,2}] \oplus \phi_{3,3}\mathbb{C}[\phi_{3,1},\phi_{3,2}]$ where

$$\begin{aligned}\phi_{3,1} &= x^4+4(k-1)xy^3+(k^2-4k+3)y^4,\\ \phi_{3,2} &= x^3y+(k-3)xy^3-(k-2)y^4,\\ \phi_{3,3} &= x^2y^2-2xy^3+y^4.\end{aligned}$$

Remark. The rings of invariants to which the Hamming weight enumerators belong for self-dual codes over $\mathbb{Z}_k$ were determined in [2] and [4] for only $k = 4, 6$ and 12.

3.3 Applications

Recently Type II codes over $\mathbb{Z}_{2k}$ have been introduced in [1]. Similarly to binary Type II codes, it was shown in [1] that there is a Type II code over $\mathbb{Z}_{2k}$ of length n if and only if $n \equiv 0 \pmod 8$. Thus the Hamming weight enumerator of a Type II code is also invariant under the matrix

$$M_4 = \begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix},$$

where w is an 8-th root of unity. The group $G_4(2k)$ generated by the matrices $M_1(2k)$ and M_4 has order 16 for every k.

Theorem 3.7 *The Hamming weight enumerator of a Type II code over $\mathbb{Z}_{2k}$ is an element of the ring*

$$\mathbb{C}[\psi_{4,1},\psi_{4,2}] \oplus \psi_{4,3}\mathbb{C}[\psi_{4,1},\psi_{4,2}] \oplus \psi_{4,4}\mathbb{C}[\psi_{4,1},\psi_{4,2}] \oplus \psi_{4,5}\mathbb{C}[\psi_{4,1},\psi_{4,2}],$$

where

$$\begin{aligned}\psi_{4,1} &= x^8+56(2k-1)x^3y^5+28(2k-1)(2k-5)x^2y^6\\ &\quad +8(2k-1)(4k^2-12k+15)xy^7+(2k-1)(8k^3-28k^2+42k-35)y^8,\\ \psi_{4,2} &= x^7y+7(6k-5)x^3y^5+14(2k^2-9k+6)x^2y^6\\ &\quad +2(4k^3-28k^2+63k-35))xy^7-2(4k^3-14k^2+21k-10)y^8,\\ \psi_{4,3} &= x^6y^2+4(3k-5)x^3y^5+(2k-3)(2k-15)x^2y^6\\ &\quad -4(k-3)(2k-3)xy^7+2(2k^2-6k+5)y^8,\\ \psi_{4,4} &= (x-y)^3y^3\{x^2+3xy+2(k-2)y^2\},\\ \psi_{4,5} &= (x-y)^4y^4.\end{aligned}$$

The invariant ring has the Molien series

$$\frac{1+3\lambda^8}{(1-\lambda^8)^2} = 1+5\lambda^8+9\lambda^{16}+13\lambda^{24}+\cdots.$$

Proof. Similar to that of Theorem 3.4. □

Acknowledgments. The authors would like to thank Steven T. Dougherty and the referees for their useful comments on the manuscript.

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, T.A. Gulliver and M. Harada, Type II self-dual codes over finite rings and even unimodular lattices, *J. Alg. Combin.*, (to appear).

[4] T.A. Gulliver and M. Harada, Double circulant self-dual codes over $\mathbb{Z}_{2k}$, *IEEE Trans. Inform. Theory*, (to appear).

[5] M. Klemm, Ueber die Identität von MacWilliams für die Gewichtsfunktion von Codes, *Arch. Math.* **49** (1987) 400–406.

[6] F.J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell Syst. Tech. J.* **42** (1963) 79–84.

[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] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam 1977.

[9] V. Pless, On the uniqueness of the Golay codes, *J. Combin. Theory* **5** (1968) 215–228.

[10] B. Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, New York 1993.