DISCRETE MATHEMATICS 9 (1974) 391–400. © North-Holland Publishing Company

WEIGHT ENUMERATORS OF SELF-ORTHOGONAL CODES

C.L. MALLOWS and N.J.A. SLOANE
Bell Laboratories, Murray Hill, N.J. 07974, USA

Received 26 November 1973*

Abstract. Canonical forms are given for (i) the weight enumerator of an $[n, \frac{1}{2}(n-1)]$ self-orthogonal code, and (ii) the split weight enumerator (which classifies the codewords according to the weight of the left- and right-half words) of an $[n, \frac{1}{2}n]$ self-dual code.

1. Results

All codes in this paper are binary. An $[n, k]$ code $\mathcal{C}$ is *self-orthogonal* if $\mathcal{C} \subset \mathcal{C}^\perp$ = dual code, *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. The *weight enumerator* of $\mathcal{C}$ is the homogeneous polynomial of degree n:

$$W_{\mathcal{C}}(x, y) = \sum_{u \in \mathcal{C}} x^{n - wt(u)} y^{wt(u)} = \sum_{i=0}^{n} A_i x^{n-i} y^i ,$$

where A_i is the number of codewords of weight i. See [2, 19, 30] for definitions of coding theory terms, and [1, 3, 6–8, 10–13, 16, 19, 20–22, 26–28] for properties and applications of self-dual codes.

$\mathbf{C}$ denotes the complex numbers, and $\mathbf{C}[\alpha, \beta, ...]$ the ring of polynomials in $\alpha, \beta, ...$ with complex coefficients.

Theorem 1. (A) *For n odd, let $\mathcal{C}$ be an $[n, \frac{1}{2}(n-1)]$ self-orthogonal code. Thus $\mathcal{C}^\perp = \mathcal{C} \cup (1 + \mathcal{C})$. Then*

(i) *$W_{\mathcal{C}}(x, y)$ is an element of the direct sum $x\,\mathbf{C}[f_2, g_8] \oplus \varphi_7 \mathbf{C}[f_2, g_8]$, where $\varphi_7 = x^7 + 7x^3y^4$, $f_2 = x^2 + y^2$, $g_8 = x^8 + 14x^4y^4 + y^8$. In words: $W_{\mathcal{C}}(x, y)$ can be written in a unique way as x times a polynominal in f_2 and g_8, plus φ_7 times another such polynomial.*

(B) *Suppose in addition that all weights in $\mathcal{C}$ are multiples of 4. Then*

* Original version received 14 May 1973.

(ii) *n must be of the form* $8m \pm 1$.

(iii) *If* $n = 8m-1$, *then* $W_{\mathcal{C}}(x, y)$ *is an element of* $\varphi_7\, \mathbf{C}[g_8, h_{24}] \oplus \gamma_{23}\, \mathbf{C}[g_8, h_{24}]$, *where* $\gamma_{23} = x^{23} + 506x^{15}y^8 + 1288x^{11}y^{12} + 253x^7y^{16}$, $h_{24} = x^4y^4(x^4-y^4)^4$.

(iv) *If* $n = 8m+1$, *then* $W_{\mathcal{C}}(x, y)$ *is an element of* $x\,\mathbf{C}[g_8, h_{24}] \oplus \psi_{17}\, \mathbf{C}[g_8, h_{24}]$, *where* $\psi_{17} = x^{17} + 17x^{13}y^4 + 187x^9y^8 + 51x^5y^{12}$.

The *left* and *right weight* of a vector $v = (v_1, \ldots, v_m, v_{m+1}, \ldots, v_{2m})$ are respectively

$$w_L = wt(v_1, \ldots, v_m), \qquad w_R = wt(v_{m+1}, \ldots, v_{2m}).$$

The *split weight enumerator* of a $[2m, k]$ code $\mathcal{C}$ is

$$\mathcal{W}_{\mathcal{C}}(x, y, X, Y) = \sum_{v \in \mathcal{C}} x^{m-w_L(v)} y^{w_L(v)} X^{m-w_R(v)} Y^{w_R(v)}.$$

Theorem 2. *Let* $\mathcal{C}$ *be a* $[2m, m]$ *self-dual code satisfying*:

(B1) $\mathcal{C}$ *contains the vectors* $0^m1^m = 0 \ldots 01 \ldots 1$ *and* $\mathbf{1}$;

(B2) *the number of codewords with* $(w_L, w_R) = (j, k)$ *is equal to the number with* $(w_L, w_R) = (k, j)$. *Then*

(i) $\mathcal{W}_{\mathcal{C}}(x, y, X, Y)$ *is an element of* $\mathbf{C}[\rho_4, \eta_8, \theta_{16}]$, *where*

$$\begin{aligned} \rho_4 &= (x^2+y^2)(X^2+Y^2), \\ \eta_8 &= x^4X^4 + x^4Y^4 + y^4X^4 + y^4Y^4 + 12x^2y^2X^2Y^2, \\ \theta_{16} &= (x^2X^2 - y^2Y^2)^2(x^2Y^2 - y^2X^2)^2. \end{aligned}$$

(ii) *Furthermore, if all weights in* $\mathcal{C}$ *are multiples of* 4, *then* $\mathcal{W}_{\mathcal{C}}(x, y, X, Y)$ *is an element of* $\mathbf{C}[\eta_8, \theta_{16}, \gamma_{24}]$, *where*

$$\gamma_{24} = x^2y^2X^2Y^2(x^4-y^4)^2(X^4-Y^4)^2.$$

A code satisfying (B1), (B2) is "balanced" about its midpoint, and the division into two halves is a natural one.

In principle, Theorem 2 could be generalized to consider codewords divided into any number of parts. We shall give one example, applicable to codes which, like the Golay code, can be divided into three parts with complete symmetry between the parts.

For a vector $v = (v_1, \ldots, v_{3m})$, let $w_1 = wt(v_1, \ldots, v_m)$, $w_2 =$

$wt(v_{m+1}, \ldots, v_{2m})$, $w_3 = wt(v_{2m+1}, \ldots, v_{3m})$. The *3-split weight enumerator* of a $[3m, k]$ code $\mathcal{C}$ is

$$\sum_{v \in \mathcal{C}} y_1^{w_1(v)} y_2^{w_2(v)} y_3^{w_3(v)} .$$

Theorem 3. *For m divisible by 8, let $\mathcal{C}$ be a $[3m, \frac{3}{2}m]$ self-dual code in which all weights are divisible by 4, which contains $1^m 0^{2m}$, $0^m 1^m 0^m$, and $0^{2m} 1^m$, and in which the number of codewords with $(w_1, w_2, w_3) = (j, k, l)$ is equal to the number with $(w_1, w_2, w_3) =$ any permutation of j, k, l. Then the 3-split enumerator of $\mathcal{C}$ is an element of*

$$\bigoplus_{i=0}^{3} \gamma_i \, \mathbf{C}[p^2, q^2, rs, r^6 + s^6] ,$$

where

$$\begin{aligned}
A &= (y_1^4 + 1)(y_2^4 + 1)(y_3^4 + 1),\\
B &= y_1^2(y_2^4 + 1)(y_3^4 + 1) + y_2^2(y_1^4 + 1)(y_3^4 + 1) + y_3^2(y_1^4 + 1)(y_2^4 + 1),\\
C &= y_1^2 y_2^2(y_3^4 + 1) + y_1^2 y_3^2(y_2^4 + 1) + y_2^2 y_3^2(y_1^4 + 1),\\
D &= y_1^2 y_2^2 y_3^2,\\
p &= B - 12D,\ q = A - 12C,\\
r, s &= (B + 36D) \pm \tfrac{1}{3}\sqrt{3}\,i(A + 4C),\\
\gamma_0 &= 1,\ \gamma_1 = p(r^3 + s^3),\ \gamma_2 = iq(r^3 - s^3),\ \gamma_3 = \gamma_1\gamma_2 .
\end{aligned}$$

Corollary. *The 3-split weight enumerator is a polynomial in p, q, r, s (but not necessarily in a unique way).*

Remark. Gleason [10] has characterized the weight enumerators of $[n, \frac{1}{2}n]$ self-dual codes – see [3, 19] for proofs and generalizations. Theorems 1–3 are of a similar type. However, the proofs differ in several interesting ways from those given in [19], namely in the use of a group whose order becomes arbitrarily large, and (in Theorem 1) in the introduction of new indeterminates and the use of relative rather than absolute invariants.

2. Examples

Examples of Theorem 1. The code 0: $W = x$. The [7, 3, 4] Hamming code: $W = \varphi_7$. (Aside: the [15, 7, 6] Nordstrom–Robinson *nonlinear* code

[25], to which Theorem 1 does not apply, nevertheless has $W = \frac{1}{4}\{-7x(f_2^7 - f_2^3 g_8) + \varphi_7(7f_2^4 - 3g_8)\}$.) The [17, 8, 4] code $\bar{T}_{17}^{(3)}$ of [26]: $W = \psi_{17}$. The [23, 11, 8] Golay code: $W = \gamma_{23}$. The [31, 15, 8] quadratic residue or QR code: $W = -14\varphi_7 h_{24} + \gamma_{23} g_8$. The [47, 23, 12] QR code: $W = \frac{1}{4}\{-253\varphi_7 g_8^2 h_{24} + \gamma_{23}(7g_8^3 - 41h_{24})\}$. See [26] for other examples.

It is not presently known if a projective plane of order 10 exists. If it does exist, then from [21] the rows of its incidence matrix generate a [111, 55, 12] code with

$$W = \tfrac{1}{4}\{\varphi_7(-253g_8^{10}h_{24} + 24123g_8^7 h_{24}^2 - 430551g_8^4 h_{24}^3 + c_1 g_8 h_{24}^4) + \gamma_{23}(7g_8^{11} - 825g_8^8 h_{24} + 22077g_8^5 h_{24}^2 + c_2 g_8^2 h_{24}^3)\},$$

where c_1, c_2 are constants, at present unknown.

Examples of Theorem 2. If $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ let $u \mid v = (u_1, \ldots, u_n, v_1, \ldots, v_n)$. For $j = 1, 2$, let $\mathcal{C}_j$ be a code of length n with weight enumerator $W_j(x, y)$ and split weight enumerator $\mathcal{W}_j(x, y, X, Y)$. The code $\mathcal{C}_1 \mid \mathcal{C}_2 = \{u \mid v : u \in \mathcal{C}_1, v \in \mathcal{C}_2\}$ has ordinary and split weight enumerators $W_1(x, y)\, W_2(x, y)$ and $W_1(x, y)\, W_2(X, Y)$. The equivalent code $\mathcal{C}_1 \| \mathcal{C}_2 = \{u' | v' | u'' | v'' : u = u' \mid u'' \in \mathcal{C}_1, v = v' \mid v'' \in \mathcal{C}_2\}$, where u and v are broken in half, has ordinary and split weight enumerators $W_1(x, y)\, W_2(x, y)$ and $\mathcal{W}_1(x, y, X, Y)\, \mathcal{W}_2(x, y, X, Y)$. Also let $\mathcal{C}_1 * \mathcal{C}_2 = \{u \mid (u + v) : u \in \mathcal{C}_1, v \in \mathcal{C}_2\}$ (c.f. [29]).

The MacWilliams identity for split weight enumerators is (c.f. [17,18])

$$\text{(1)} \qquad \mathcal{W}_{\mathcal{C}^\perp}(x, y, X, Y) = \frac{1}{|\mathcal{C}|}\, \mathcal{W}_{\mathcal{C}}(x+y, x-y, X+Y, X-Y).$$

We use a detached-coefficient notation for $\mathcal{W}$, and instead of the terms

$$\alpha(x^a y^b X^c Y^d + x^a y^b X^d Y^c + x^b y^a X^c Y^d + x^b y^a X^d Y^c)$$

we write a row of a table:

$c/0$	x	y	X	Y	#
α	a	b	c	d	4

giving respectively the coefficient, the exponents, and the number of

Table 1
Split weight enumerators

Code	$\mathcal{W}$	$c/0$	x	y	X	Y	#
$\mathcal{H}_8$	η_8	1	4	0	4	0	4
		12	2	2	2	2	1
	θ_{16}	1	8	0	4	4	4
		−2	6	2	6	2	4
		4	4	4	4	4	1
	γ_{24}	1	10	2	10	2	4
		−2	10	2	6	6	4
		4	6	6	6	6	1
$\mathcal{G}_{24}$		1	12	0	12	0	4
		132	10	2	6	6	4
		495	8	4	8	4	4
		1584	6	6	6	6	1
$\mathcal{Q}_{48}$		1	24	0	24	0	4
		276	22	2	14	10	8
		3864	20	4	16	8	8
		13524	20	4	12	12	4
		9016	18	6	18	6	4
		125580	18	6	14	10	8
		256335	16	8	16	8	4
		950544	16	8	12	12	4
		1835400	14	10	14	10	4
		3480176	12	12	12	12	1

terms of this type. The sum of the products of the first and last columns is the total number of codewords.

A QR of length $8l = q + 1$, where q is a prime, with generator matrix in the canonical form of [15, Figs. 1, 7], satisfies the hypotheses of Theorem 2(ii). Table 1 gives 3 such examples, the [8, 4, 4] Hamming code $\mathcal{H}_8$, the [24, 12, 8] Golay code $\mathcal{G}_{24}$ for which $\mathcal{W} = \eta_8^3 - 3\eta_8\theta_{16} - 42\gamma_{24}$, and the [48, 24, 12] code $\mathcal{Q}_{48}$. Also if $\delta_2 = \{00, 11\}$, $\delta_2 \mid \delta_2$ has $\mathcal{W} = \rho_4$. $\mathcal{H}_8 \mid \mathcal{H}_8$ has $\mathcal{W} = \eta_8^2 + 12\theta_{16}$. Let $\mathcal{R}(r, m)$ denote an rth order Reed–Muller (RM) code of length 2^m. Then RM codes can be constructed recursively from $\mathcal{R}(r+1, m) * \mathcal{R}(r, m) = \mathcal{R}(r+1, m+1)$ (see [29]). The first order RM code of length n obtained in this way has

$$\mathcal{W} = (x^{n/2} + y^{n/2})(X^{n/2} + Y^{n/2}) + (2n-4)(xyXY)^{n/4}.$$

We have also found $\mathcal{W}$ for $\mathcal{R}(2, m)$.

Examples of Theorem 3. The 3-split enumerator of $\mathcal{H}_8 | \mathcal{H}_8 | \mathcal{H}_8$ is $12p^2 + q^2$; of $\{u' | v' | u'' ; w' | v'' | w'' :$ where $u = u' | u''$, $v = v' | v''$, $w = w' ; w'' \in \mathcal{H}_8\}$ is $\frac{3}{2}rs - \frac{1}{4}p^2 - \frac{1}{4}q^2$; of the [24, 12, 8] Golay code in a form satisfying Theorem 3 is $\frac{7}{6}rs - \frac{19}{6}p^2 + \frac{1}{6}q^2 = (1 + y_1^8)(1 + y_2^8)(1 + y_3^8) + 28[y_1^4 y_2^4 + \ldots] + 224[y_1^2 y_2^2 y_3^4 + \ldots] + 1232(y_1 y_2 y_3)^4$.

3. The proofs

Proof of Theorem 1. For an $n \times n$ matrix $A = (a_{ij})$ and a polynomial $f(x) = f(x_1, \ldots, x_n)$, the result of transforming the variables of f by A is denoted $A \circ f(x) = f(\Sigma a_{1i} x_i, \ldots, \Sigma a_{ni} x_i)$. Note that $B \circ (A \circ f(x)) = (AB) \circ f(x)$.

Let $\mathcal{C}$ be a code of length $4m - 1$ satisfying the hypotheses (A) and (B) of Theorem 1, with weight enumerator $W(x) = W(x, y)$. Let

$$M = 2^{-1/2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad J = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \qquad R = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = M J^2 M.$$

By the MacWilliams identity [18; 30, p. 120],

$$M \circ W(x) = 2^{-1/2}(W(x) + R \circ W(x)).$$

Also $J \circ W(x) = W(x)$. Let $\mathfrak{M}$ be the set of all polynomials satisfying these two equations. It is easily verified that $\mathfrak{M}$ contains $\mathfrak{N} = \varphi_7\, \mathbf{C}[g_8, h_{24}] \oplus \gamma_{23}\, \mathbf{C}[g_8, h_{24}]$. To show $\mathfrak{M} = \mathfrak{N}$, let $a_d (b_d)$ be the number of linearly independent polynomials of degree d in $\mathfrak{M}$ ($\mathfrak{N}$). Clearly

$$\sum_0^\infty b_d \lambda^d = (\lambda^7 + \lambda^{23})/(1 - \lambda^8)(1 - \lambda^{24}).$$

We show $\mathfrak{M} = \mathfrak{N}$ by showing $a_d = b_d$ for all d.

Let $\mathfrak{G}$ be a group of $n \times n$ complex matrices and let $\chi : \mathfrak{G} \to \mathbf{C}$ be a 1-dimensional representation of $\mathfrak{G}$. Then $f(x)$ is called a *relative invariant* of $\mathfrak{G}$ with respect to χ if $A \circ f(x) = \chi(A) f(x)$ for all $A \in \mathfrak{G}$. If χ is identically 1, $f(x)$ is called an *(absolute) invariant* of $\mathfrak{G}$. The number n_d of linearly independent relative invariants of degree d is given by the Molien series [24; 5, p. 301; 23, p. 259; 19, Theorem 427]

$$(2)\qquad \sum_{0}^{\infty} n_d \lambda^d = \frac{1}{|\mathfrak{G}|} \sum_{A \in \mathfrak{G}} \frac{\bar{\chi}(A)}{|I - \lambda A|} .$$

The key device is to consider not $W(x, y)$ but $f(u, v, x, y) = uW(x, y) + vW(y, x)$. Then $f(u, v, x, y)$ is invariant under

$$M^+ = \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix} \text{ and } J^+ = \begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix} \quad \text{acting on} \begin{bmatrix} u \\ v \\ x \\ y \end{bmatrix} .$$

Let ω be a primitive complex pth root of unity, where p is a prime greater than deg W = length of $\mathcal{C}$. Then $f(u, v, x, y)$ is a relative invariant under $P = \operatorname{diag}(\omega, \omega, 1, 1)$ with respect to $\chi(P) = \omega$.

Now M, J generate a group $\mathfrak{G}_{192}$ of order 192, consisting of the matrices

$$(3)\qquad r^\nu \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}, \quad r^\nu \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix}, \quad r^\nu\, 2^{-1/2} \begin{pmatrix} 1 & \beta \\ \alpha & -\alpha\beta \end{pmatrix},$$

where $r = 2^{-1/2}(1+i)$, $0 \le \nu \le 7$, $\alpha, \beta \in \{1, i, -1, -i\}$ (see [19]). So M^+, J^+, P generate a group $\mathfrak{G}$ of order $192p$ consisting of the matrices $\begin{pmatrix} \omega^\nu A & \\ & A \end{pmatrix}$, $0 \le \nu \le p-1$, $A \in \mathfrak{G}_{192}$. Then the set $\mathfrak{M}^+$ of relative invariants of $\mathfrak{G}$ with respect to $\chi(M^+) = \chi(J^+) = 1$, $\chi(P) = \omega$ is in 1 – 1 correspondence with $\mathfrak{M}$ up to degree $p-1$. Therefore from (2), for all $p > d$, a_d is the coefficient of λ^{d+1} in

$$\frac{1}{192p} \sum_{B \in \mathfrak{G}} \frac{\bar{\chi}(B)}{|I - \lambda B|} = \frac{1}{192} \sum_{A \in \mathfrak{G}_{192}} \frac{1}{p} \sum_{\nu=0}^{p-1} \frac{\omega^{-\nu}}{|I - \lambda A||I - \lambda \omega^\nu A|}$$

$$\to \frac{1}{192} \sum_{A \in \mathfrak{G}_{192}} \frac{1}{|I - \lambda A|} \frac{1}{2\pi} \int_0^{2\pi} \frac{e^{-i\theta}\, d\theta}{|I - \lambda e^{i\theta} A|}$$

as $p \to \infty$, $|\lambda| < 1$,

$$= \frac{\lambda}{192} \sum_{A \in \mathfrak{G}_{192}} \frac{\operatorname{trace}(A)}{|I - \lambda A|} = \lambda \frac{\lambda^7 + \lambda^{23}}{(1-\lambda^8)(1-\lambda^{24})} \quad \text{from (3).}$$

This proves (iii) and half of part (ii). The case $n = 4m + 1$ is treated similarly, taking $M^+ = \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}$, $J^+ = \begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}$. For part (i) we take $J = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$, obtaining a group of order $16p$.

Proof of Theorem 2(ii). (Part (i) and Theorem 3 are similar.) Let $\mathcal{C}$ satisfy the hypotheses of Theorem 2(ii) and have split weight enumerator $\mathcal{W} = \mathcal{W}(x, y, X, Y)$. We use the same notation as in the proof of Theorem 1. From the hypotheses, eq. (1), and the fact that in each term $x^j y^k X^l Y^m$ of $\mathcal{W}$, $j+k = l+m$, it follows that $\mathcal{W}$ is invariant under M^*, J^*, and

$$T_1 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{pmatrix}, \quad T_2 = \begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix}; \quad T_3 = \begin{pmatrix} \omega & & & \\ & \omega & & \\ & & \omega^{-1} & \\ & & & \omega^{-1} \end{pmatrix}.$$

M^*, J^*, T_1 generate a group of order $16 \cdot 192$ consisting of the matrices $\begin{pmatrix} A & \\ & BA \end{pmatrix}$, $A \in \mathfrak{G}_{192}$, $B \in \mathfrak{D}_{16}$, where $\mathfrak{D}_{16} = \{\delta\begin{pmatrix} 1 & \\ & \pm 1 \end{pmatrix}, \delta\begin{pmatrix} & 1 \\ \pm 1 & \end{pmatrix} : \delta \in \{1, i, -1, -i\}\}$ is a normal subgroup of $\mathfrak{G}_{192}$; and $\mathfrak{G}_{192} = \bigcup_{k=1}^{12} A_k \mathfrak{D}_{16}$, where $A_1, \ldots, A_6$ are

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ & i \end{pmatrix}, 2^{-1/2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, 2^{-1/2}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, 2^{-1/2}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}, 2^{-1/2}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix},$$

and $A_{6+j} = rA_j$, $1 \le j \le 6$. Then M^*, J^*, T_1, T_2, T_3 generate a group $\mathfrak{G}$ of order $6144p$ consisting of the matrices

$$\begin{pmatrix} \omega^\nu A & \\ & \omega^{-\nu} BA \end{pmatrix}, \quad \begin{pmatrix} & \omega^\nu A \\ \omega^{-\nu} BA & \end{pmatrix}, \qquad 0 \le \nu \le p-1,$$
$$A \in \mathfrak{G}_{192}, \quad B \in \mathfrak{D}_{16}.$$

Now $\mathcal{W}$ is invariant under $\mathfrak{G}$. Let $\mathfrak{M}$ be the set of all invarinats of $\mathfrak{G}$. Clearly $\mathfrak{M}$ contains $\mathfrak{N} = \mathbb{C}[\eta_8, \theta_{16}, \gamma_{24}]$. To show $\mathfrak{M} = \mathfrak{N}$, we define a_d, b_d as before and will show $a_d = b_d$ for all d. We have

$$\sum_0^\infty b_d \lambda^d = 1/(1-\lambda^8)(1-\lambda^{16})(1-\lambda^{24}).$$

From (2), for all $p > d$, a_d is the coefficient of λ^d in

$$\frac{1}{6144p} \sum_{\nu, A, B} \left\{ \frac{1}{|I-\lambda\omega^\nu A|\,|I-\lambda\omega^{-\nu}BA|} + \frac{1}{|I-\lambda^2 ABA|} \right\} = \Sigma_\mathrm{I} + \Sigma_\mathrm{II} \text{ say.}$$

In Σ_I we put $A = A_k B'$:

$$\Sigma_\mathrm{I} = \frac{1}{24p} \sum_{k=1}^{12} \sum_{\nu=0}^{p-1} f(A_k; \lambda\omega^\nu) f(A_k; \lambda\omega^{-\nu}),$$

where

$$f(A_k;\lambda) = f_k = \frac{1}{16} \sum_{B \in \mathfrak{H}_{16}} \frac{1}{|I - \lambda A_k B|}.$$

In fact, $f_1 = (1-\lambda^4)^{-2}$, $f_7 = (1+\lambda^4)^{-2}$, $f_4 = f_5 = (1-\lambda^4+\lambda^8)^{-1}$, $f_{10} = f_{11} = (1+\lambda^4+\lambda^8)^{-1}$, $f_j = (1-\lambda^8)^{-1}$ for $j = 2,3,6,8,9,12$.

$$\Sigma_1 = \frac{1}{24} \sum_{k=1}^{12} \left\{ \text{coefft. of } \omega^0 \text{ in } f(A_k;\lambda\omega) f(A_k;\lambda\omega^{-1}) \right\} + O(\lambda^p)$$

$$= \frac{1}{24} \left\{ \frac{2(1+\lambda^8)}{(1-\lambda^8)^3} + \frac{6}{1-\lambda^{16}} + \frac{4(1+\lambda^8)}{1-\lambda^{24}} \right\} + O(\lambda^p)$$

Similarly,

$$\Sigma_{11} = \frac{1}{24} \sum_{k=1}^{12} f(A_k^2;\lambda^2) + O(\lambda^p)$$

$$= \frac{1}{24} \left\{ \frac{8}{(1-\lambda^8)^2} + \frac{4}{1+\lambda^8+\lambda^{16}} \right\} + O(\lambda^p),$$

$$\Sigma_1 + \Sigma_{11} = \frac{1}{(1-\lambda^8)(1-\lambda^{16})(1-\lambda^{24})} + O(\lambda^p),$$

hence $a_d = b_d$. This completes the proof.

Acknowledgments

We thank Mrs. F.J. MacWilliams for several helpful discussions. Some of the calculations were verified with the help of the ALTRAN system for rational function manipulation [4, 14], and the GRAPPA group theory analysis program [9].

References

[1] E.F. Assmus, Jr., and H.F. Mattson, Jr., New 5-designs, J. Combin. Theory 6 (1969) 122–151.

[2] E.R. Berlekamp, Algebraic Coding Theory (McGraw-Hill, New York, 1968).

[3] E.R. Berlekamp, F.J. MacWilliams and N.J.A. Sloane, Gleason's theorem on self-dual codes, IEEE Trans. Information Theory 18 (1972) 409–414.

[4] W.S. Brown, ALTRAN User's Manual, 2nd ed. (Bell Laboratories, Murray Hill, N.J., 1972).

[5] W. Burnside, Theory of Groups of Finite Order, 2nd ed. (Dover, New York, 1955).

[6] J.H. Conway, A group of order 8,315,553,613,086,720,000, Bull. London Math. Soc. 1 (1969) 79–88.

[7] J.H. Conway, A characterization of Leech's lattice, Invent. Math. 7 (1969) 137–142.

[8] J.H. Conway, Groups, lattices, and quadratic forms, in: Computers in Algebra and Number Theory, SIAM-AMS Proc. IV (Am. Math. Soc., Providence, R.I., 1971) 135–139.

[9] L.A. Dimino, GRAPPA Basic User's Manual (Bell Laboratories, Murray Hill, N.J., 1972).

[10] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in: Actes, Congrès Internl. de Mathématique, 3, 1970 (Gauthier-Villars, Paris, 1971) 211–215.

[11] J.-M. Goethals, On the Golay perfect binary code, J. Combin. Theory 11(A) (1971) 178–186.

[12] J.-M. Goethals, F.J. MacWilliams and C.L. Mallows, Further remarks on extremal self-dual codes, to appear.

[13] J.-M. Goethals and S.L. Snover, Nearly perfect binary codes, Discrete Math. 3 (1972) 65–88.

[14] A.D. Hall, Jr., The ALTRAN system for rational function manipulation – A survey, Comm. Assoc. Comput. Mach. 14 (1971) 517–521.

[15] M. Karlin, New binary coding results by circulants, IEEE Trans. Information Theory 15 (1969) 81–92.

[16] J. Leech and N.J.A. Sloane, Sphere packings and error-correcting codes, Can. J. Math. 23 (1971) 718–745.

[17] F.J. MacWilliams, Combinatorial problems of elementary abelian groups, Ph.D. Thesis, Dept. of Mathematics, Harvard University, Cambridge, Mass., May 1962.

[18] F.J. MacWilliams, A theorem on the distribution of weights in a systematic code, Bell System Tech. J. 42 (1963) 79–94.

[19] F.J. MacWilliams, C.L. Mallows and N.J.A. Sloane, Generalizations of Gleason's theorem on weight enumerators of self dual codes, IEEE Trans. Information Theory 18 (1972) 794–805.

[20] F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, Good self-dual codes exist, Discrete Math. 3 (1972) 153–162.

[21] F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, On the existence of a projective plane of order 10, J. Combin. Theory 14(A) (1973) 66–78.

[22] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, Information and Control 22 (1973) 188–200.

[23] G.A. Miller, H.F. Blichfeldt and L.E. Dickson, Theory and Applications of Finite Groups (Dover, New York, 1961).

[24] T. Molien, Über die Invarianten der linear Substitutionsgruppe, S.-B. König. Preuss. Akad. Wiss. (1897) 1152–1156.

[25] A.W. Nordstrom and J.P. Robinson, An optimum nonlinear code, Information and Control 11 (1967) 613–616.

[26] V. Pless, A classification of self-orthogonal codes over GF(2), Dicrete Math. 3 (1972) 209–246.

[27] V. Pless and J.N. Pierce, Self-dual codes over GF(*q*) satisfy a modified Varshamov bound, Information and Control 23 (1973) 35–40.

[28] E.P. Shaughnessy, Codes with simple automorphism groups, Arch. Math. 22 (1971) 459–466.

[29] N.J.A. Sloane and D.S. Whitehead, New family of single-error correcting codes, IEEE Trans. Information Theory 16 (1970) 717–719.

[30] J.H. Van Lint, Coding Theory, Lecture Notes in Math. 201 (Springer, Berlin, 1971).