SIAM J. ALG. DISC. METH.
Vol. 2, No. 4, December 1981

0196-5212/81/0204-0011 $01.00/0

WEIGHT ENUMERATORS OF SELF-ORTHOGONAL CODES OVER GF(3)*

C. L. MALLOWS† AND N. J. A. SLOANE†

Abstract. The Hamming and complete weight enumerators of maximally self-orthogonal codes over $GF(3)$ of lengths $12m-1$, $12m$ and $12m+1$ are characterized. The results for length $12m+1$ are believed to be new, while those for length $12m-1$ and $12m$ have been considerably simplified.

1. Introduction. Professor Marshall Hall, Jr., recently pointed out to us (in connection with his work on the hypothetical projective plane of order twelve) that there is an omission in [6]: the maximally self-orthogonal ternary codes of length $12m+1$ are not mentioned. An important example of this class is the dual of the code generated by the incidence matrix of the projective plane of order 3, denoted by p_{13} in [1] and [10]. In fact it is incorrect to say (as we do in [6, p.655]) that if C is a maximally self-orthogonal $[n, \frac{1}{2}(n-1)]$ code over $GF(3)$ with $1 \in C^{\perp}$ then the extended code $(C^{\perp})^{+}$ is self-dual and n is congruent to -1 modulo 12. We shall see that the correct conclusion is that either $n \equiv -1 \pmod{12}$ and $(C^{\perp})^{+}$ is self-dual, or $n \equiv +1 \pmod{12}$ and $(C^{\perp})^{+}$ is not self-dual. The present paper gives the weight enumerators for the missing case. While determining these we were able to considerably simplify the weight enumerators in the case $n \equiv -1 \pmod{12}$ and also when C itself is self-dual and $n \equiv 0 \pmod{12}$. One might say that this is an error-correcting paper.

2. Weight enumerators. Let C be a code of length n and dimension k over $GF(3)$. The complete weight enumerator (cwe) of C is

$$E_C(x, y, z) = \sum_{\mathbf{u} \in C} x^{n_0(\mathbf{u})} y^{n_1(\mathbf{u})} z^{n_2(\mathbf{u})},$$

where $n_i(\mathbf{u})$ is the number of components of $\mathbf{u}$ that are congruent to i modulo 3. The ordinary or Hamming weight enumerator of C is

$$W_C(x, y) = E_C(x, y, y).$$

From the MacWilliams theorem the complete weight enumerator of the dual code $C^{\perp}$ is given by

$$E_{C^{\perp}}(x, y, z) = \frac{1}{3^k} E_C(x+y+z, x+\omega y+\omega^2 z, x+\omega^2 y+\omega z), \tag{1}$$

where $\omega = e^{2\pi i/3}$ (see [4], [6]).

A code C is called self-orthogonal if $C \subseteq C^{\perp}$ and self-dual if $C = C^{\perp}$. The maximum dimension of a self-orthogonal code of length n is $\frac{1}{2}n$ if $n \equiv 0 \pmod 4$, $\frac{1}{2}(n-2)$ if $n \equiv 2 \pmod 4$, and $\frac{1}{2}(n-1)$ if n is odd (see [8], [9]). We wish to characterize the Hamming and complete weight enumerators of self-orthogonal codes of maximal dimension. However our method will only work when we can express the cwe of $C^{\perp}$ in terms of the cwe of C. There are two general cases when we can do this:

(i) when C is self-dual, so that

$$E_{C^{\perp}}(x, y, z) = E_C(x, y, z), \tag{2}$$

* Received by the editors October 27, 1980.
† Bell Laboratories, Murray Hill, New Jersey 07974.

(ii) when C is maximally self-orthogonal of odd length and the all-ones vector $\mathbf{1}$ is in $C^\perp$ but not in C.

In case (ii) we have

$$\dim C^\perp = \dim C + 1 = \tfrac{1}{2}(n+1),$$

which implies

$$C^\perp = C \cup (\mathbf{1}+C) \cup (\mathbf{2}+C) \tag{3}$$

and

$$E_{C^\perp}(x, y, z) = E_C(x, y, z) + E_C(y, z, x) + E_C(z, x, y) \tag{4}$$

(since the cwe of $\mathbf{1}+C$ is $E_C(y, z, x)$, etc.).

In case (i) the length must be a multiple of 4, and if we make the additional assumption that the all-ones vector is in C then $n \equiv 0 \pmod{12}$. Without this assumption the results are far more complicated (see [6]). In case (ii) it is a consequence of Theorem 3 below that $n \equiv \pm 1 \pmod{12}$. If $n \equiv -1$ we can add an overall parity check to $C^\perp$ so as to make $C^\perp$ self-dual, but if $n \equiv +1 \pmod{12}$ this is impossible.

In order to describe the weight enumerators of these codes we introduce the following polynomials. We apologize for the length of this, but it is essential for our method that we work with homogeneous polynomials in six variables. As far as possible we use the same notation as [6].

First the polynomials in x, y, z:

$$\begin{aligned}
a &= x^3+y^3+z^3,\\
f &= x^2y+y^2z+z^2x,\\
g &= xy^2+yz^2+zx^2,\\
p &= 3xyz,\\
\psi_4 &= x(x^3+8y^3),\\
\phi_4 &= y(x^3-y^3),\\
\xi_4 &= x(y^3-z^3),\\
b &= x^3y^3+y^3z^3+z^3x^3,\\
\beta_6 &= a^2-12b\\
&= x^6+y^6+z^6-10(x^3y^3+y^3z^3+z^3x^3),\\
\upsilon_7 &= x(2x^6-7y^6-7z^6+7x^3y^3+7x^3z^3-56y^3z^3),\\
\pi_9 &= (x^3-y^3)(y^3-z^3)(z^3-x^3),\\
\alpha_{12} &= a(a^3+8p^3)\\
&= \sum^{(3)} x^{12}+4\sum^{(6)} x^9y^3+6\sum^{(3)} x^6y^6+228\sum^{(3)} x^6y^3z^3,\\
\tau_{13} &= xy^6(x^3-y^3)(2x^3+y^3).
\end{aligned}$$

The second set are polynomials in u, v, w, x, y, z:

$$\Lambda_2 = ux + vy + wz,$$
$$\Xi_5 = ux(y^3 - z^3) + vy(z^3 - x^3) + wz(x^3 - y^3),$$
$$\begin{aligned}\Upsilon_8 = {} & ux(2x^6 - 7y^6 - 7z^6 + 7x^3y^3 + 7x^3z^3 - 56y^3z^3) \\ & + vy(2y^6 - 7z^6 - 7x^6 + 7y^3z^3 + 7x^3y^3 - 56x^3z^3) \\ & + wz(2z^6 - 7x^6 - 7y^6 + 7x^3z^3 + 7y^3z^3 - 56x^3y^3).\end{aligned}$$

Note that

$$\pi_9 = g^3 - f^3,$$
$$243\tau_{13} = x\psi_4^3 - 37x\phi_4^3 - \tfrac{1}{2}\beta_6 \upsilon_7\big|_{y=z},$$
$$\xi_4 = \Xi_5(u = 1, v = w = 0),$$
$$\upsilon_7 = \Upsilon_8(u = 1, v = w = 0).$$

We can now state our results.

THEOREM 1 (Complete weight enumerator). *If* $C = C^\perp$ *and* $\mathbf{1} \in C$, *then* $n \equiv 0 \pmod{12}$ *and*

$$E_C(x, y, z) \in R \oplus \beta_6 \pi_9^2 R, \tag{5}$$

where

$$R = \mathbf{C}[\beta_6^2, \alpha_{12}, \pi_9^4].$$

In other words the cwe *of* C *can be written uniquely as a polynomial in* β_6^2, α_{12} *and* π_9^4, *plus* $\beta_6\pi_9^2$ *times another such polynomial.*

COROLLARY 2 (Hamming weight enumerator—Gleason [3]). *With the same hypotheses as Theorem* 1,

$$W_C(x, y) \in \mathbf{C}[\psi_4^3, \phi_4^3]. \tag{6}$$

THEOREM 3 (Complete weight enumerator). *If* $C \subset C^\perp$, $\mathbf{1} \in C^\perp \backslash C$, *and* $\dim C^\perp = \dim C + 1$ *then* $n \equiv \pm 1 \pmod{12}$.

(a) *If* $n = 12m + 1$ *then*

$$E_C(x, y, z) \in xR \oplus \beta_6\upsilon_7 R \oplus \xi_4\pi_9 R \oplus \upsilon_7\pi_9^2 R \oplus x\beta_6\pi_9^2 R \oplus \xi_4\beta_6\pi_9^3 R, \tag{7}$$

where R *is defined in Theorem* 1.

(b) *If* $n = 12m - 1$ *then*

$$E_C(x, y, z) \in \bar{\alpha}_{12} R \oplus \bar{\beta}_6\beta_6 R \oplus \bar{\beta}_6\pi_9^2 R \oplus \beta_6\bar{\pi}_9\pi_9 R \oplus \bar{\pi}_9\pi_9^3 \oplus \beta_6\pi_9^2\bar{\alpha}_{12} R, \tag{8}$$

where the bar denotes partial differentiation with respect to x.

COROLLARY 4 (Hamming weight enumerator). *With the same hypotheses as Theorem* 3,

(a) *if* $n = 12m + 1$ *then*

$$W_C(x, y) \in x\mathbf{C}[\psi_4^3, \phi_4^3] \oplus \tau_{13}\mathbf{C}[\psi_4^3, \phi_4^3], \tag{9}$$

and

(b) *if* $n = 12m - 1$ *then*

$$W_C(x, y) \in \bar{\psi}_4\psi_4^2\mathbf{C}[\psi_4^3, \phi_4^3] \oplus \bar{\phi}_4\phi_4^2\mathbf{C}[\psi_4^3, \phi_4^3]. \tag{10}$$

Extremal weight enumerators. Let us consider the extremal weight enumerators (as defined in [5] and [7]) corresponding to Theorem 3(a) and Corollary 4(a). The first nontrivial length is 13, and for simplicity we begin with the Hamming weight enumerator. By Corollary 4(a) the Hamming weight enumerator of any [13, 6] self-orthogonal code (with **1** in the dual code) has the form

$$W(x, y) = c_1 x\psi_4^3 + c_2 x\phi_4^3 + c_3\tau_{13} \tag{11}$$

for appropriate constants c_1, c_2, c_3. Suppose these constants are chosen so that the minimum weight of the corresponding code (if there is one) is as large as possible. We obtain

$$\begin{aligned} W(x, y) &= x\psi_4^3 - 24x\phi_4^3 - 132\tau_{13} \\ &= x^{13} + 572x^4y^9 + 156xy^{12} \\ &= W^* \qquad \text{(say)}. \end{aligned}$$

Since W^* has nonnegative integral coefficients, it could indeed be the weight enumerator of some [13, 6] code C^* with minimum weight 9. On the other hand from Theorem 3(a) the complete weight enumerator of C^* has the form

$$E_{C^*}(x, y, z) = b_1 x\beta_6^2 + b_2 x\alpha_{12} + b_3\beta_6\upsilon_7 + b_4\xi_4\pi_9 \tag{12}$$

for appropriate constants b_i. The condition that C^* has minimum weight 9 determines the b_i uniquely and we find

$$\begin{aligned} E_{C^*}(x, y, z) = {} & x^{13} + 286x^4(y^6z^3 + y^3z^6) \\ & - \tfrac{13}{9}x(y^{12} + z^{12}) + \tfrac{286}{9}x(y^9z^3 + y^3z^9) + \tfrac{286}{3}xy^6z^6. \end{aligned}$$

Since this does not have nonnegative integral coefficients, C^* does not exist.

In this case we already knew from the enumeration in [1] that the highest minimum weight attainable is 6, and furthermore that there is a unique code with minimum weight 6, namely the projective plane code p_{13} mentioned in §1. For this code

$$\begin{aligned} W_{p_{13}}(x, y) &= x^{13} + 156x^7y^6 + 494x^4y^9 + 78xy^{12} \\ &= x\psi_4^3 - 24x\phi_4^3 - 54\tau_{13}, \end{aligned} \tag{13}$$

and

$$\begin{aligned} E_{p_{13}}(x, y, z) &= x^{13} + 156x^7y^3z^3 + 13x^4(y^9 + 18y^6z^3 + 18y^3z^6 + z^9) + 78xy^6z^6 \\ &= \tfrac{5}{72}x\beta_6^2 + \tfrac{17}{24}x\alpha_{12} + \tfrac{1}{9}\beta_6\upsilon_7 + 3\xi_4\pi_9 \end{aligned} \tag{14}$$

(which are of the forms (11) and (12)). Although the extremal weight enumerators did not tell us anything new in this example, it is nevertheless interesting to find a situation where the cwe leads to a contradiction not apparent from the Hamming weight enumerator.

For codes of greater length the extremal cwe will probably always contain a negative coefficient (compare [5] and [7]).

Relationship with [6]. The basis for cwe's given in Theorem 1 is simpler than that given in [6, Thm. 1]. The old basis is expressed in terms of the new one by

$$\gamma_{18} = -\tfrac{1}{2}\beta_6^3 + \tfrac{3}{2}\beta_6\alpha_{12} + 216\pi_9^2,$$

and

$$256\delta_{36} = -\beta_6^6 + 6\beta_6^4\alpha_{12} - 9\beta_6^2\alpha_{12}^2 + 4\alpha_{12}^3 + 864\beta_6^3\pi_9^2 - 2592\beta_6\pi_9^2\alpha_{12} - 186624\pi_9^4.$$

The syzygy $\gamma_{18}^2 = \alpha_{12}^3 - 64\delta_{36}$ has been replaced by the trivial identity

$$(\beta_6\pi_9^2)^2 = \beta_6^2 \cdot \pi_9^4.$$

3. The proofs.

Proof of Theorem 1. Since this is parallel to the proofs given in [11] and [12] our treatment will be brief. Suppose C is a self-dual code of length $n = 12m$ containing $\mathbf{1}$. Let G be the subgroup of $GL(3, \mathbf{C})$ of order 2952 generated by the matrices

$$M = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}, \qquad J = \begin{bmatrix} 1 & & \\ & \omega & \\ & & 1 \end{bmatrix},$$

and all 3×3 permutation matrices. The matrices in G are listed below, in the proof of Lemma 6. In [11] and [12] it is shown that the cwe $E_C(x, y, z)$ is invariant under G. If a_n denotes the number of linearly independent homogeneous invariants for G of degree n, it is also shown in [11] and [12] that the Molien series $\sum_{n=0}^{\infty} a_n\lambda^n$ is equal to

$$\frac{1+\lambda^{24}}{(1-\lambda^{12})^2(1-\lambda^{36})}. \tag{15}$$

To find a basis for the invariants we proceed as follows. Let $s = e^{2\pi i/12}$. Under the action of M we have

$$\beta_6 \xrightarrow{M} -\beta_6, \qquad \alpha_{12} \xrightarrow{M} \alpha_{12}, \qquad x^3 - y^3 \xrightarrow{M} s^{11}(f - \omega^2 g) \xrightarrow{M} -(z^3 - x^3),$$

$$y^3 - z^3 \xrightarrow{M} s^3(f - g) \xrightarrow{M} -(y^3 - z^3), \qquad z^3 - x^3 \xrightarrow{M} s^7(f - \omega g) \xrightarrow{M} -(x^3 - y^3).$$

Therefore

$$\pi_9 = (x^3 - y^3)(y^3 - z^3)(z^3 - x^3) = g^3 - f^3 \xrightarrow{M} i\pi_9.$$

All of β_6, π_9 and α_{12} are invariant under J, and the permutations fix β_6 and α_{12} and send π_9 to $\pm\pi_9$. Thus β_6^2, α_{12}, $\beta_6\pi_9^2$ and π_9^4 are indeed invariant under G. It only remains to show that β_6^2, α_{12} and π_9^4 (or equivalently β_6, α_{12} and π_9) are algebraically independent. This is verified by computing the Jacobian of β_6, α_{12} and π_9, which is

$$-2592x^2y^2z^{20} + \cdots.$$

Since this does not vanish, the polynomials are indeed algebraically independent [2, Thm. 2.3]. Therefore the ring of invariants of G has the form shown on the right-hand side of (5). This completes the proof of Theorem 1.

Proof of Corollary 2. We set $y = z$ in Theorem 1, making π_9 vanish, and then replace β_6^2 and α_{12} by the equivalent but simpler pair ψ_4^3 and ϕ_4^3.

Proof of Theorem 3. Suppose C is an $[n, \frac{1}{2}(n-1)]$ self-orthogonal code with $\mathbf{1} \in C^{\perp}\backslash C$. This implies that the cwe of C is a polynomial in x, y^3 and z^3, and also satisfies

(4). From the MacWilliams identity (1) we have

$$\begin{aligned} M \circ E_C(x, y, z) &= 3^{-n/2} E_C(x+y+z, x+\omega y+\omega^2 y, x+\omega^2 y+\omega z) \\ &= 3^{-1/2} E_{C^\perp}(x, y, z) \\ &= 3^{-1/2}\{E_C(x, y, z)+E_C(y, z, x)+E_C(z, x, y)\}, \end{aligned} \tag{16}$$

using (4). Also

$$\begin{aligned} M \circ E_{1+C}(x, y, z) &= M \circ E_C(y, z, x) \\ &= 3^{-n/2} E_C(x+\omega y+\omega^2 z, x+\omega^2 y+\omega z, x+y+z) \\ &= 3^{-1/2} E_{C^\perp}(x, \omega y, \omega^2 z) \qquad \text{(from (16))} \\ &= 3^{-1/2}\{E_C(x, \omega y, \omega^2 z)+E_C(\omega y, \omega^2 z, x)+E_C(\omega^2 z, x, \omega y)\} \\ &= 3^{-1/2}\{E_C(x, y, z)+\omega^n E_C(y, z, x)+\omega^{2n} E_C(z, x, y)\}, \end{aligned} \tag{17}$$

where in the last step we used the fact that $n_0(\mathbf{u}) \equiv n \pmod 3$ and $n_1(\mathbf{u}) \equiv n_2(\mathbf{u}) \equiv 0 \pmod 3$ for all $\mathbf{u} \in C$. Similarly,

$$M \circ E_C(z, x, y) = 3^{-1/2}\{E_C(x, y, z)+\omega^{2n} E_C(y, z, x)+\omega^n E_C(z, x, y)\}. \tag{18}$$

Since n is odd we have to consider the possibilities $n \equiv \pm 1, \pm 3$ and $\pm 5 \pmod{12}$.

Case 1. $n \equiv \pm 3 \pmod{12}$. The last expressions in (16) and (17) are now identical, implying $E_C(x, y, z) = E_C(y, z, x)$. Since C always contains $\mathbf{0}$, this implies that $\mathbf{1} \in C$, a contradiction. Thus $n \not\equiv \pm 3 \pmod{12}$.

Case 2. $n \equiv +1$ or $-5 \pmod{12}$. Now (17) becomes

$$M \circ E_C(y, z, x) = 3^{-1/2}\{E_C(x, y, z)+\omega E_C(y, z, x)+\omega^2 E_C(z, x, y)\}.$$

We introduce new indeterminates u, v, w and define

$$F(u, v, w, x, y, z) = uE_C(x, y, z)+vE_C(y, z, x)+wE_C(z, x, y).$$

Let G^* denote the group of 6×6 matrices

$$\left\{A^* = \begin{pmatrix} \bar{A} & 0 \\ 0 & A \end{pmatrix}; A \in G\right\}$$

of order 2592, where $\bar{A}$ acts on the variables u, v, w and A acts on x, y, z. From (16), (17) and (18) it follows that F is invariant under M^* and thus under all of G^*. (Compare the proof of [6, Thm. 9].) We indicate this by writing

$$F(\bar{A}\mathbf{u}, A\mathbf{x}) = F(\mathbf{u}, \mathbf{x}) \quad \text{all } A \in G. \tag{19}$$

At this point we need the following analogue of [6, Thm. 8]. (The proof is essentially the same and is omitted.)

THEOREM 5. *Let G be any finite subgroup of $GL(m, \mathbf{C})$, and let Φ_d denote the set of all polynomials $F(\mathbf{u}, \mathbf{x}) = F(u_1, \cdots, u_m, x_1, \cdots, x_m)$ which are*

(i) *homogeneous of total degree d,*

(ii) *linear in the u_i, and*

(iii) *satisfy* (19).

Let a_d denote the number of linearly independent polynomials in Φ_d. Then a generating function for the numbers a_d is

$$\sum_{d=0}^{\infty} a_d \lambda^d = \frac{\lambda}{|G|} \sum_{A \in G} \frac{\operatorname{tr}(\bar{A})}{\det(I - \lambda A)}. \tag{20}$$

The next step is to compute the sum on the right-hand side of (20) for our group.

LEMMA 6. *If G is the subgroup of $GL(3, \mathbf{C})$ of order 2592 defined at the beginning of this section,*

$$\frac{\lambda}{|G|}\sum_{A\in G}\frac{\operatorname{tr}(\bar{A})}{\det(I-\lambda A)}=\lambda\cdot\frac{\lambda+\lambda^{13}}{(1-\lambda^{12})^3} \tag{21}$$
$$=\lambda\cdot\frac{\lambda+2\lambda^{13}+2\lambda^{25}+\lambda^{37}}{(1-\lambda^{12})^2(1-\lambda^{36})}.$$

Proof. We know from [11] and [12] that there are (I) 1944 elements of G of the form

$$\begin{bmatrix} & 1 & \\ s^\nu & & \omega^a \\ & & & \omega^b \end{bmatrix} M^e \begin{bmatrix} 1 & & \\ & \omega^c & \\ & & \omega^d \end{bmatrix}$$

and (II) 648 elements of the form

$$\begin{bmatrix} & 1 & \\ s^\nu & & \omega^a \\ & & & \omega^b \end{bmatrix} P,$$

where $0\leqq\nu\leqq 11$, $0\leqq a, b, c, d\leqq 2$, $e=1$ or 3 and P is any 3×3 permutation matrix. Instead of (20) we shall work out

$$\frac{1}{\lambda}\sum_{A\in G}\frac{\operatorname{tr}(\bar{A})}{\det(I-\lambda A)}=\sum_{A\in G}\frac{\operatorname{tr}(\lambda A)^{-1}}{\det(I-\lambda A)}$$

(since G is a unitary group). Our strategy is to keep $\nu=0$ as long as possible, finally summing over ν by replacing λ by λs^ν and adding. For type (I) we can ignore c and d (and just multiply the final sum by 9) since c can be combined with a and d with b in both $\operatorname{tr}(\lambda A)^{-1}$ and $\det(I-\lambda A)$. The sum on a, b and e is equal to

$$\frac{2}{1-\lambda^4}+\frac{2\sqrt{3}/\lambda+6^*+\sqrt{3}\lambda+3\lambda^2}{1+\lambda^6}+\frac{2\sqrt{3}/\lambda+4^*+2\sqrt{3}\lambda^3+2\lambda^4}{(1+\lambda^2+\lambda^4)(1-\lambda^2+\lambda^4)}$$
$$+\frac{2\sqrt{3}/\lambda+6^*+\sqrt{3}\lambda-3\lambda^2-\sqrt{3}\lambda^3-3\lambda^{4^*}-3\sqrt{3}\lambda^5-3\lambda^{6^*}}{(1-\lambda^2+\lambda^4)(1+\lambda^6)}.$$

We replace λ by λs^ν and sum over ν; to do this we put everything over powers of $1-\lambda^{12}$ and ignore all terms that are not powers of λ^{12} (those not marked with an asterisk). This gives

$$\frac{24}{1-\lambda^{12}}+\frac{72}{1-\lambda^{12}}+\frac{48}{1-\lambda^{12}}+\frac{12(6+6\lambda^{12}+6\lambda^{12}+6\lambda^{12})}{(1-\lambda^{12})^2}$$

and multipling by 9 to account for the summation over c and d we find that the contribution from the type (I) terms is

$$\frac{9\cdot 144}{1-\lambda^{12}}+\frac{108(6+8\lambda^{12})}{(1-\lambda^{12})^2}. \tag{22}$$

Next we consider the type (II) terms. When $P = I$ the sum on a and b gives

$$\frac{9}{\lambda}\frac{1+2\lambda}{(1-\lambda)(1-\lambda^3)^2}. \tag{23}$$

For

$$P=\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}$$

the contribution is

$$\frac{9}{\lambda}\frac{1}{(1-\lambda)(1-\lambda^6)}, \tag{24}$$

and for

$$P=\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix} \text{ or } \begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}$$

we get

$$\frac{9}{(1-\lambda^3)(1-\lambda^6)} \quad \text{(twice)}. \tag{25}$$

Finally

$$P=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix} \text{ and } \begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$$

have trace 0. Adding (23)–(25) we obtain

$$\frac{9}{\lambda}\frac{2+4\lambda-2\lambda^2+2\lambda^4}{(1-\lambda)(1-\lambda^3)(1-\lambda^6)},$$

and we sum over ν as before, by multiplying top and bottom by $(1+\lambda+\lambda^2)(1+\lambda^3)^2(1+\lambda^6)^3$, to get

$$\frac{9\cdot 12}{(1-\lambda^{12})^3}(6+36\lambda^{12}+6\lambda^{24}). \tag{26}$$

The grand total is the sum of (22) and (26):

$$2596\frac{1+\lambda^{12}}{(1-\lambda^{12})^3}.$$

We multiply by $\lambda^2/2596$ to obtain (21). The final step is to multiply the top and bottom by $1+\lambda^{12}+\lambda^{24}$ to make the denominator agree with that of (15). This completes the proof of Lemma 6.

Since only exponents of the form $12m+1$ appear in (21), we see that n cannot be of the form $12m-5$. It remains to find a basis for the sets Φ_d defined in Theorem 5. We compute

$$\Xi_5 \xrightarrow{M} -\Xi_5, \qquad \Upsilon_8 \xrightarrow{M} -\Upsilon_8$$

and deduce the following theorem from (21).

THEOREM 7. *The solutions of* (19) *that are linear in u, v, w belong to*

$$\Lambda_2 R \oplus \beta_6 \Upsilon_8 R \oplus \Xi_5 \pi_9 R \oplus \Upsilon_8 \pi_9^2 R \oplus \Lambda_2 \beta_6 \pi_9^2 R \oplus \Xi_5 \beta_6 \pi_9^3 R.$$

Finally, setting $u = 1$ and $v = w = 0$ in Theorem 7, we obtain (7) and thus prove Theorem 3(a).

Case 3. $n \equiv -1$ or $+5 \pmod{12}$. Now $F(u, v, w, x, y, z)$ is invariant under

$$G^{**} = \left\{ \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}; A \in G \right\}.$$

The proof in this case is essentially given in [6, p. 657].

This completes the proof of theorem 3.

Proof of Corollary 4. We set $y = z$ in Theorem 3, making ξ_4 and π_9 vanish, and replace $\beta_6 \upsilon_7$ by τ_{13}.

Remark. The Taylor series expansion of (21) is

$$\lambda \sum_{m=0}^{\infty} (m+1)^2 \lambda^{12m+1}.$$

Therefore the number of linearly independent homogeneous polynomials of degree $12m+1$ in the right-hand side of (7) is $(m+1)^2$. Similarly the number of degree $12m-1$ in (8) is $m(m+1)$.

Acknowledgments. We are grateful to Professor Marshall Hall Jr. for pointing out the omission in [6] which led to this work. During this investigation we have made use of two computer programs for symbolic manipulation: the MACSYMA system at the Massachusetts Institute of Technology Laboratory for Computer Science, and the ALTRAN system at the Bell Laboratories Murray Hill Computation Center.

REFERENCES

[1] J. H. CONWAY, V. PLESS AND N. J. A. SLOANE, *Self-dual codes over GF*(3) *and GF*(4) *of length not exceeding* 16, IEEE Trans. Information Theory, IT-25 (1979), pp. 312–322.

[2] L. FLATTO, *Invariants of finite reflection groups*, L'Enseignement mathématique, 24 (1978), pp. 237–292.

[3] A. M. GLEASON, *Weight polynomials of self-dual codes and the MacWilliams identities*, in Actes, Congrès International des Mathématiciens 1970, Vol. 3, Gauthiers–Villars, Paris, 1971, pp. 211–215.

[4] F. J. MACWILLIAMS AND N. J. A. SLOANE, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam and Elsevier/North-Holland, New York, 1977.

[5] C. L. MALLOWS, A. M. ODLYZKO AND N. J. A. SLOANE, *Upper bounds for modular forms, lattices and codes*, J. Algebra, 36 (1975), pp. 68–76.

[6] C. L. MALLOWS, V. PLESS AND N. J. A. SLOANE, *Self-dual codes over GF*(3), SIAM J. Applied Math., 31 (1976), pp. 649–666.

[7] C. L. MALLOWS AND N. J. A. SLOANE, *An upper bound for self-dual codes*, Inform. and Control, 22 (1973), pp. 188–200.

[8] V. PLESS, *The number of isotropic subspaces in a finite geometry*, Rend. Cl. Scienze Fisiche, Matematiche e Naturali, Acc. Naz. Lincei, 39 (1969), pp. 418–421.

[9] ———, *On the uniqueness of the Golay codes*, J. Combinatorial Theory, 5 (1968), pp. 215–228.

[10] V. PLESS, N. J. A. SLOANE AND H. N. WARD, *Ternary codes of minimum weight* 6 *and the classification of the self-dual codes of length* 20, IEEE Trans. Information Theory, IT-26 (1980), pp. 305–316.

[11] N. J. A. SLOANE, *Weight enumerators of codes*, in Combinatorics, M. Hall Jr. and J. H. van Lint, eds., Reidel, Dordrecht and Mathematical Centre, Amsterdam, 1974, pp. 115–142.

[12] N. J. A. SLOANE, *Error-correcting codes and invariant theory: new applications of a nineteenth-century technique*, Amer. Math. Monthly, 84 (1977), pp. 82–107.