[14] T. Kasami, S. Lin, and W. W. Peterson, "New generalizations of the Reed–Muller codes—Part I: Primitive codes," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 189–199, Mar. 1968.
[15] J. Riordan, *An Introduction to Combinatorial Analysis*. New York: Wiley, 1958.
[16] E. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
[17] T. Kasami, S. Lin, and W. W. Peterson, "Polynomial codes," Dep. Elec. Eng., Univ. Hawaii, Honolulu, Sci. Rep., 1968.
[18] C. L. Chen and S. Lin, "Further results on polynomial codes," *Inform. Contr.*, vol. 15, pp. 38–60, July 1969.
[19] F. L. Graham and J. MacWilliams, "On the number of parity checks in difference set cyclic codes," *Bell Syst. Tech. J.*, vol. 45, pp. 1046–1070, Sept. 1966.
[20] F. J. MacWilliams and H. B. Mann, "On the p-rank of the design matrix of a difference set," Math. Res. Cen., U.S. Army, Univ. Wisconsin, MRC Tech. Summary Rep. 803, Oct. 1967.
[21] N. Hamada, "The rank of the incidence matrix of points of d-flats in finite geometries," *J. Sci.*, Hiroshima Univ., Hiroshima, Japan, vol. 32, pp. 381–396, 1968.
[22] T. Kasami and S. Lin, "On the minimum distance of BCH codes," *IEEE Trans. Inform. Theory*, to be published.

Generalizations of Gleason's Theorem on Weight Enumerators of Self-Dual Codes

F. JESSIE MACWILLIAMS, COLIN L. MALLOWS, AND NEIL J. A. SLOANE, MEMBER, IEEE

Abstract—**Gleason has recently shown that the weight enumerators of binary and ternary self-dual codes are polynomials in two given polynomials. In this paper it is shown that classical invariant theory permits a straightforward and systematic proof of Gleason's theorems and their generalizations. The joint weight enumerator of two codes (analogous to the joint density function of two random variables) is defined and shown to satisfy a MacWilliams theorem. Invariant theory is then applied to generalize Gleason's theorem to the complete weight enumerator of self-dual codes over $GF(3)$, the Lee metric enumerator over $GF(5)$ (given by Klein in 1884!) and over $GF(7)$ (given by Maschke in 1893!), the Hamming enumerator over $GF(q)$, and over $GF(4)$ with all weights divisible by 2, the joint enumerator of two self-dual codes over $GF(2)$, and a number of other results.**

I. Introduction

In 1963 MacWilliams [20] showed that the weight enumerators of a binary code and of its dual are related by

$$\mathcal{W}_{\mathcal{A}^\perp}(x, y) = \frac{1}{|\mathcal{A}|}\mathcal{W}_{\mathcal{A}}(x + y, x - y). \tag{1}$$

(These terms are defined in Section II.)

It has recently been shown [21] that this identity also holds for nonlinear codes, if the dual is appropriately defined.

A code $\mathcal{A}$ of length n is said to be self-dual if it is linear and $u \cdot v \equiv 0$ (modulo 2) for all $u, v \in \mathcal{A}$, and $|\mathcal{A}| = 2^{n/2}$. Self-dual codes are of considerable interest. For example: they meet the Gilbert bound [22]; many of the best codes known are self-dual; they give rise to dense sphere-packings [19]; and they arise as the linear span of the incidence matrices of projective planes [1], [23].

From (1) it follows that the weight enumerator of a self-dual code satisfies the identity

$$\mathcal{W}(x, y) = \mathcal{W}\left(\frac{x + y}{\sqrt{2}}, \frac{x - y}{\sqrt{2}}\right). \tag{2}$$

In 1970, Gleason [15] showed that all possible weight enumerators satisfying (2) are polynomials in just two weight enumerators

$$x^2 + y^2$$

$$x^8 + 14x^4y^4 + y^8.$$

He also proved similar theorems for binary codes with weights divisible by 4 and for ternary codes. (Alternative proofs of Gleason's theorem have been given by Thompson [34], Feit [13], [14], and Berlekamp *et al.* [4].)

One of the aims of this paper is to show that classical invariant theory allows Gleason's theorems and generalizations to be derived in a straightforward and systematic way. Invariant theory "came into existence about the middle of the nineteenth century somewhat like Minerva: a grown-up virgin, mailed in the shining armor of algebra, she sprang forth from Cayley's Jovian head" (Weyl, 1939 [36]). By 1892, as a result of Hilbert's work (an excellent description is given in Reid's book [30]), the theory was dead. Quite recently, however, it has come back to life (see Dieudonné and Carrell, 1971 [11]).

In Section IV we state the theorems needed from invariant theory and give examples of their application to weight enumerators. Many of the theorems about weight enumerators have been known in another context for a long time. The theorem of Gleason quoted above may be found in effect on p. 362 of Burnside, 1911 [6], although it was certainly known long before. Klein in 1884 [18, p. 236] had already given the theorem that is necessary to characterize the Lee weight enumerators of codes over $GF(5)$! (see Section V-5.3.2).

We begin in Section II by stating the MacWilliams

Manuscript received December 9, 1971; revised June 6, 1972.
The authors are with the Bell Telephone Laboratories, Inc., Murray Hill, N.J. 07974.

theorems for complete, Lee, and Hamming weight enumerators. Section III describes a new kind of enumerator, the joint weight enumerator of two codes. This generalizes the Hamming weight enumerator just as a joint probability-density function generalizes a single density function. The joint weight enumerator of a code with itself, called a biweight enumerator, gives much more information about a code than the weight enumerator does, and seems a more natural way to look at nonlinear codes. Various examples and applications are given. It is shown that the joint weight enumerator satisfies a MacWilliams theorem and this makes it possible to study the joint weight enumerators of self-dual codes.

Finally in Section V we summarize the results of applying invariant theory to weight enumerators. The theorems obtained are all of the type that states that a given weight enumerator is a polynomial in certain specified polynomials. Among others we give such theorems for the complete enumerator of codes over $GF(3)$, the Lee enumerator over $GF(5)$, the Hamming enumerator over $GF(q)$, and over $GF(4)$ with all weights divisible by 2, the joint enumerator of two codes over $GF(2)$, and the biweight enumerator of a code over $GF(2)$.

II. Weight Enumerators

2.1. Codes

Let F be a finite field $GF(q)$, where q is a prime power, and let F^n be a vector space of dimension n over F.

An (n,M,d) *code* over $GF(q)$ is a set of M vectors of length n such that any two differ in at least d places. A code is *linear* if it is a linear subspace of F^n, in which case it contains q^k codewords for some k and is called an $[n,k,d]$ code. If $\mathscr{A}$ is a linear code the *dual* code $\mathscr{A}^\perp$ is $\{\boldsymbol{u} \mid \boldsymbol{u} \cdot \boldsymbol{v} = 0, \text{ for all } \boldsymbol{v} \in \mathscr{A}\}$. If $\mathscr{A} = \mathscr{A}^\perp$ the code is said to be *self-dual*. $|\mathscr{A}|$ denotes the number M of codewords in $\mathscr{A}$. Two codes are said to be *equivalent* if they differ only by a permutation of the coordinates of the codewords.

2.2. Characters

Let $p(x)$ be a primitive irreducible polynomial of degree f over $GF(p)$ and let α be a root of $p(x)$. Any element λ of $GF(q)$, $q = p^f$, has a unique representation as

$$\lambda = \lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \cdots + \lambda_{f-1}\alpha^{f-1}, \qquad \lambda_i \in GF(p). \tag{2.1.1}$$

A *character* of $GF(q)$ is a homomorphism from the additive group of $GF(q)$ to the multiplicative group of the complex numbers. Let χ be the fixed character defined by

$$\chi(\lambda) = \xi^{\lambda_0}, \tag{2.1.2}$$

where $\xi = e^{2\pi i/p}$ and λ_0 is given by (2.1.1).

2.3. Complete Weight Enumerator

Let $\mathscr{A}$ be a linear code of length n over $GF(q)$. We classify the codewords of $\mathscr{A}$ in three ways.

Let the elements of $GF(q)$ be $\omega_0 = 0, \omega_1, \omega_2, \cdots, \omega_{q-1}$ in some fixed order. Then the *composition of a vector* $\boldsymbol{v} \in F^n$ is defined to be $\operatorname{comp}(\boldsymbol{v}) = \boldsymbol{s}(\boldsymbol{v}) = (s_0(\boldsymbol{v}), s_1(\boldsymbol{v}), \cdots, s_{q-1}(\boldsymbol{v}))$ where $s_i(\boldsymbol{v})$ denotes the number of coordinates of $\boldsymbol{v}$ that are equal to ω_i. Clearly

$$\sum_{i=0}^{q-1} s_i(\boldsymbol{v}) = n.$$

In general a *composition* $\boldsymbol{s}$ of n is a vector $\boldsymbol{s} = (s_0, s_1, \cdots, s_{q-1})$ with nonnegative integer components such that

$$\sum_{i=0}^{q-1} s_i = n.$$

Let $A(\boldsymbol{s})$ be the number of codewords $\boldsymbol{v} \in \mathscr{A}$ such that $\operatorname{comp}(\boldsymbol{v}) = \boldsymbol{s}$. Then the *complete weight enumerator* of $\mathscr{A}$ is the polynomial

$$\mathscr{C}_{\mathscr{A}}(z_0, \cdots, z_{q-1}) = \sum_{\boldsymbol{s}} A(\boldsymbol{s}) z_0^{s_0} \cdots z_{q-1}^{s_{q-1}}, \tag{2.3.1}$$

where the z_i are indeterminates and the sum extends over all compositions $\boldsymbol{s}$ of n.

The first MacWilliams identity gives the complete weight enumerator of $\mathscr{A}^\perp$ in terms of that of $\mathscr{A}$.

Theorem 2.3.2—([20, lemma 2.7], [15]):

$$\mathscr{C}_{\mathscr{A}^\perp}(z_0, \cdots, z_{q-1}) = \frac{1}{|\mathscr{A}|} \mathscr{C}_{\mathscr{A}}\left(\sum_{j=0}^{q-1} \chi(\omega_0\omega_j) z_j, \cdots, \sum_{j=0}^{q-1} \chi(\omega_{q-1}\omega_j) z_j\right), \tag{2.3.3}$$

where χ is the fixed character defined in (2.1.2).

2.4. Lee Weight Enumerator

In studying Lee weight enumerators q is assumed to be an odd prime or prime power, since for $q = 2$ this enumerator coincides with the Hamming weight enumerator, and for $q = 2^r$, $r > 1$, it is undefined.

Let the elements of $GF(q)$ be $\omega_0 = 0, \omega_1, \cdots, \omega_\delta, \omega_{-\delta}, \omega_{-\delta+1}, \cdots, \omega_{-1}$ where $\omega_{-i} = -\omega_i$ and $\delta = (q-1)/2$. The Lee weight of a vector $\boldsymbol{v} \in F^n$ is defined to be $\operatorname{Lee}(\boldsymbol{v}) = (l_0(\boldsymbol{v}), l_1(\boldsymbol{v}), \cdots, l_\delta(\boldsymbol{v}))$ where $l_0(\boldsymbol{v}) = s_0(\boldsymbol{v})$ and $l_i(\boldsymbol{v}) = s_i(\boldsymbol{v}) + s_{-i}(\boldsymbol{v})$, for $1 \le i \le \delta$. Let $A^L(\boldsymbol{l})$ be the number of codewords $\boldsymbol{v} \in \mathscr{A}$ such that $\operatorname{Lee}(\boldsymbol{v}) = \boldsymbol{l}$; then the Lee *weight enumerator* of $\mathscr{A}$ is the polynomial

$$\mathscr{L}_{\mathscr{A}}(z_0, \cdots, z_\delta) = \sum_{\boldsymbol{l}} A^L(\boldsymbol{l}) z_0^{l_0}, \cdots, z_\delta^{l_\delta}.$$

Clearly $\mathscr{L}_{\mathscr{A}}$ is obtained from the complete weight enumerator $\mathscr{C}_{\mathscr{A}}$ of (2.3.1) by replacing z_{-i} by z_i for $1 \le i \le \delta$. Applying this same transformation to (2.3.3), we obtain the second MacWilliams identity, giving the Lee weight enumerator of $\mathscr{A}^\perp$.

Theorem 2.4.1—([21]):

$$\mathscr{L}_{\mathscr{A}^\perp}(z_0, \cdots, z_\delta) = \frac{1}{|\mathscr{A}|} \mathscr{L}_{\mathscr{A}}\left(z_0 + \sum_{j=1}^{\delta} (\chi(\omega_0\omega_j) + \chi(-\omega_0\omega_j)) z_j, \cdots, z_0 + \sum_{j=1}^{\delta} (\chi(\omega_\delta\omega_j) + \chi(-\omega_\delta\omega_j)) z_j\right). \tag{2.4.2}$$

The Lee enumerator is a compromise, in that it gives

much more information about a code than the Hamming enumerator of the next section, but has only half as many variables as the complete enumerator. It is also an appropriate measure for codes to be used in phase-modulation communication schemes (see Berlekamp [3, p. 205]).

2.5. Hamming Weight Enumerator

Let the (Hamming) weight wt (v) of a vector $v \in F^n$ be the number of nonzero coordinates of v; then

$$\text{wt}\,(v) = \sum_{i=1}^{q-1} s_i(v).$$

Let $A(i)$ be the number of codewords $v \in \mathscr{A}$ such that wt $(v) = i$. The *Hamming* (or ordinary) *weight enumerator* of $\mathscr{A}$ is the polynomial

$$\mathscr{W}_{\mathscr{A}}(x,y) = \sum_{i=0}^{n} A(i)x^{n-i}y^i.$$

In (2.3.3), if z_0 is replaced by x and z_i by y for $i > 0$, then the third MacWilliams identity is obtained, giving the weight enumerator of $\mathscr{A}^\perp$.

Theorem 2.5.1—([20, theorem 1]):

$$\mathscr{W}_{\mathscr{A}^\perp}(x,y) = \frac{1}{|\mathscr{A}|}\,\mathscr{W}_{\mathscr{A}}(x + (q-1)y,\ x - y). \quad (2.5.2)$$

For binary codes Theorems 2.3.2, 2.4.1, and 2.5.1 coincide, and for ternary codes Theorems 2.4.1 and 2.5.1 coincide.

2.6. Self-Dual Codes

Let $\mathscr{A}$ be a self-dual code over $GF(q)$. Then certainly n must be even and $|\mathscr{A}| = q^{n/2}$. In fact, there are stronger restrictions on n.

Theorem 2.6.1—(Pless [28]): If $q \not\equiv -1 \pmod 4$, self-dual codes exist if and only if n is even; if $q \equiv -1 \pmod 4$, self-dual codes exist if and only if n is a multiple of 4.

From Theorem 2.3.2 the complete weight enumerator of a self-dual code satisfies the identity

$$\mathscr{C}_{\mathscr{A}}(z_0,\cdots,z_{q-1}) = \mathscr{C}_{\mathscr{A}}\left(\frac{1}{\sqrt{q}}\sum_{j=0}^{q-1}\chi(\omega_0\omega_j)z_j,\cdots,\frac{1}{\sqrt{q}}\sum_{j=0}^{q-1}\chi(\omega_{q-1}\omega_j)z_j\right). \quad (2.6.2)$$

That is, $\mathscr{C}_{\mathscr{A}}$ is invariant under the linear transformation

$$T_1\text{: replace } z_i \text{ by } \frac{1}{\sqrt{q}}\sum_{j=0}^{q-1}\chi(\omega_i\omega_j)z_j, \quad \text{for all } i = 0,\cdots,q-1. \quad (2.6.3)$$

Similarly, from Theorems 2.4.1 and 2.5.1, the Lee weight enumerator is invariant under the transformation

$$T_2\text{: replace } z_i \text{ by } \frac{1}{\sqrt{q}}\left(z_0 + \sum_{j=0}^{\delta}(\chi(\omega_i\omega_j) + \chi(-\omega_i\omega_j))z_j\right), \quad \text{for all } i = 0,\cdots,\delta \quad (2.6.4)$$

and the Hamming weight enumerator satisfies the identity

$$\mathscr{W}_{\mathscr{A}}(x,y) = \mathscr{W}_{\mathscr{A}}\left(\frac{1}{\sqrt{q}}(x + (q-1)y),\ \frac{1}{\sqrt{q}}(x - y)\right) \quad (2.6.5)$$

and so is invariant under the transformation

$$T_3(q)\text{: replace } x \text{ by } \frac{1}{\sqrt{q}}(x + (q-1)y), \quad \text{replace } y \text{ by } \frac{1}{\sqrt{q}}(x - y). \quad (2.6.6)$$

Polynomials that are invariant under T_1, T_2, or T_3 we call *formally self-dual weight enumerators.* (These may have coefficients that are not positive integers.) Important examples of such polynomials are the weight enumerators of i) linear codes that have the same weight distribution as, but are not equal to, their duals, ii) certain nonlinear codes, such as the (16,256,6) Nordstrom–Robinson code of [27], or the (8,16,2) code of Fig. 1 of [21], which satisfy (2.6.5).

If in fact $\mathscr{A}$ is linear and equal to $\mathscr{A}^\perp$, then as Gleason [15] has observed, the weight enumerators satisfy additional constraints. First, let β be a generator of the multiplicative group of nonzero elements of $GF(q)$. Then $v \in \mathscr{A}$ implies $\beta v \in \mathscr{A}$ and so $\mathscr{C}_{\mathscr{A}}$ is invariant under the permutation T_4: replace z_0 by z_0 and z_r by $z_{i(r)}$, where

$$\beta\omega_r = \omega_{i(r)},\ r = 1,\cdots,q-1. \quad (2.6.7)$$

Also the same transformation (with r running from 1 to δ) acts on the Lee weight enumerator.

Second, since any codeword v, say of composition s, is orthogonal to itself, it satisfies

$$\sum_{i=0}^{q-1} s_i\omega_i^{\,2} = 0$$

and so $\mathscr{C}_{\mathscr{A}}$ is invariant under the transformation

$$T_5\text{: replace } z_i \text{ by } \chi(\lambda\omega_i^{\,2})z_i, \qquad i = 0,1,\cdots,q-1 \quad (2.6.8)$$

for any $\lambda \in GF(q)$.

2.7. The Problem

Polynomials that are invariant under transformations T_1, T_4, T_5 applied separately are also invariant under any combination of these transformations; i.e., are invariant under the *group* of transformations generated by T_1, T_4, T_5. In Section IV we consider the general problem of characterizing polynomials invariant under a given group of transformations.

III. Joint Weight Enumerators

3.1. Definitions

The joint weight enumerator of two codes $\mathscr{A}$ and $\mathscr{B}$ measures the overlap between the zeros in a typical codeword of $\mathscr{A}$ and those in a typical codeword of $\mathscr{B}$.

Let $u = (u_1,\cdots,u_n)$, $v = (v_1,\cdots,v_n)$ be any pair of vec-

tors of F^n. Then we define

$$\begin{aligned} i(\boldsymbol{u},\boldsymbol{v}) &= \text{number of } r \text{ such that } u_r = v_r = 0;\\ j(\boldsymbol{u},\boldsymbol{v}) &= \text{number of } r \text{ such that } u_r = 0,\ v_r \neq 0;\\ k(\boldsymbol{u},\boldsymbol{v}) &= \text{number of } r \text{ such that } u_r \neq 0,\ v_r = 0;\\ l(\boldsymbol{u},\boldsymbol{v}) &= \text{number of } r \text{ such that } u_r \neq 0,\ v_r \neq 0. \end{aligned}$$

Of course

$$\begin{aligned} i(\boldsymbol{u},\boldsymbol{v}) + j(\boldsymbol{u},\boldsymbol{v}) + k(\boldsymbol{u},\boldsymbol{v}) + l(\boldsymbol{u},\boldsymbol{v}) &= n\\ j(\boldsymbol{u},\boldsymbol{v}) + l(\boldsymbol{u},\boldsymbol{v}) &= \text{wt } (\boldsymbol{v})\\ k(\boldsymbol{u},\boldsymbol{v}) + l(\boldsymbol{u},\boldsymbol{v}) &= \text{wt } (\boldsymbol{u}). \end{aligned}$$

Let $\mathscr{A},\mathscr{B}$ be (linear or nonlinear) codes of length n over $GF(q)$. The *joint* (Hamming) *weight enumerator* of $\mathscr{A}$ and $\mathscr{B}$ is

$$\begin{aligned} \mathscr{J}_{\mathscr{A},\mathscr{B}}(a,b,c,d) &= \sum_{\boldsymbol{u}\in\mathscr{A}} \sum_{\boldsymbol{v}\in\mathscr{B}} a^{i(\boldsymbol{u},\boldsymbol{v})} b^{j(\boldsymbol{u},\boldsymbol{v})} c^{k(\boldsymbol{u},\boldsymbol{v})} d^{l(\boldsymbol{u},\boldsymbol{v})}\\ &= \sum_{i,j,k,l=0}^{n} A_{ijkl} a^i b^j c^k d^l, \end{aligned}$$

where A_{ijkl} is the number of pairs $\boldsymbol{u} \in \mathscr{A}$, $\boldsymbol{v} \in \mathscr{B}$ such that

$$i(\boldsymbol{u},\boldsymbol{v}) = i \qquad j(\boldsymbol{u},\boldsymbol{v}) = j \qquad k(\boldsymbol{u},\boldsymbol{v}) = k \qquad l(\boldsymbol{u},\boldsymbol{v}) = l$$

and a,b,c,d are (complex) indeterminates.

The joint weight enumerator of a code $\mathscr{A}$ with itself is called the *biweight enumerator* of $\mathscr{A}$.

3.2. Properties of Joint Weight Enumerators

It follows immediately from the definition that

$$\begin{aligned} \mathscr{J}_{\mathscr{A},\mathscr{B}}(1,1,1,1) &= |\mathscr{A}||\mathscr{B}|\\ \mathscr{J}_{\mathscr{B},\mathscr{A}}(a,b,c,d) &= \mathscr{J}_{\mathscr{A},\mathscr{B}}(a,c,b,d). \end{aligned} \tag{3.2.1}$$

The single weight enumerators are given by

$$\mathscr{W}_{\mathscr{A}}(x,y) = \frac{1}{|\mathscr{B}|}\mathscr{J}_{\mathscr{A},\mathscr{B}}(x,x,y,y)$$

$$\mathscr{W}_{\mathscr{B}}(x,y) = \frac{1}{|\mathscr{A}|}\mathscr{J}_{\mathscr{A},\mathscr{B}}(x,y,x,y)$$

$$\mathscr{W}_{\mathscr{A}}(x,y) = \mathscr{J}_{\mathscr{A},\mathscr{B}}(x,0,y,0), \qquad \text{if } \mathbf{0} \in \mathscr{B}$$

$$\mathscr{W}_{\mathscr{B}}(x,y) = \mathscr{J}_{\mathscr{A},\mathscr{B}}(x,y,0,0), \qquad \text{if } \mathbf{0} \in \mathscr{A}.$$

If $\mathscr{A} = \mathscr{A}_1 \cup \mathscr{A}_2$ where $\mathscr{A}_1$ and $\mathscr{A}_2$ are disjoint sets, then

$$\mathscr{J}_{\mathscr{A},\mathscr{B}} = \mathscr{J}_{\mathscr{A}_1,\mathscr{B}} + \mathscr{J}_{\mathscr{A}_2,\mathscr{B}}. \tag{3.2.2}$$

3.3. Examples (All Are Binary Codes)

Example 3.3.1: $\mathscr{A} = \{\mathbf{0},\mathbf{1}\}$ = repetition code of length n

$$\mathscr{J}_{\mathscr{A},\mathscr{A}}(a,b,c,d) = a^n + b^n + c^n + d^n.$$

Example 3.3.2: $\mathscr{A} = \{\mathbf{0}\}$, $\mathscr{B}$ arbitrary

$$\mathscr{J}_{\mathscr{A},\mathscr{B}}(a,b,c,d) = \mathscr{W}_{\mathscr{B}}(a,b).$$

Example 3.3.3: $\mathscr{A}$ = {single vector of weight e}, $\mathscr{B} = F^n$ (= all codewords of length n)

$$\mathscr{J}_{\mathscr{A},\mathscr{B}}(a,b,c,d) = (a+b)^{n-e}(c+d)^e.$$

Example 3.3.4: $\mathscr{A}$ arbitrary, $\mathscr{B} = F^n$

$$\mathscr{J}_{\mathscr{A},\mathscr{B}}(a,b,c,d) = \mathscr{W}_{\mathscr{A}}(a+b, c+d)$$

[use (3.2.2) and (3.3.3)].

Example 3.3.5: $\mathscr{A}$ arbitrary, $\mathscr{B}$ = {all even weight vectors}

$$\mathscr{J}_{\mathscr{A},\mathscr{B}}(a,b,c,d) = \tfrac{1}{2}\mathscr{W}_{\mathscr{A}}(a+b, c+d) + \tfrac{1}{2}\mathscr{W}_{\mathscr{A}}(a-b, c-d).$$

3.4. Generalized MacWilliams Identities

Theorem 3.4.1: Let $\mathscr{A}$ be a linear code, $\mathscr{A}^\perp$ its dual, and $\mathscr{B}$ an arbitrary code, all of length n over $GF(q)$. Then the joint weight enumerators of $\mathscr{A},\mathscr{B}$ and $\mathscr{A}^\perp,\mathscr{B}$ are related by

$$\mathscr{J}_{\mathscr{A}^\perp,\mathscr{B}}(a,b,c,d) = \frac{1}{|\mathscr{A}|}\mathscr{J}_{\mathscr{A},\mathscr{B}}(a+\gamma c, b+\gamma d, a-c, b-d), \tag{3.4.2}$$

where $\gamma = q - 1$.

Corollary 3.4.3: For $\mathscr{A}$ arbitrary and $\mathscr{B}$ linear,

$$\mathscr{J}_{\mathscr{A},\mathscr{B}^\perp}(a,b,c,d) = \frac{1}{|\mathscr{B}|}\mathscr{J}_{\mathscr{A},\mathscr{B}}(a+\gamma b, a-b, c+\gamma d, c-d).$$

[For proof use (3.2.1).]

Corollary 3.4.4: For $\mathscr{A}$ and $\mathscr{B}$ linear,

$$\begin{aligned} \mathscr{J}_{\mathscr{A}^\perp,\mathscr{B}^\perp}(a,b,c,d) &= \frac{1}{|\mathscr{A}||\mathscr{B}|}\mathscr{J}_{\mathscr{A},\mathscr{B}}(a+\gamma(b+c)+\gamma^2 d, a-b+\gamma(c-d),\\ &\qquad a-c+\gamma(b-d), a-b-c+d). \end{aligned}$$

Theorem 2.5.1 is another corollary. The proof of the following lemma and the deduction of Theorem 3.4.1 from it parallel the proof of Theorem 2.5.1 given by Van Lint [35]; we omit the details.

Lemma 3.4.5: Let A be a vector space over the complex numbers, let $f: F^n \times F^n \to A$ be any mapping, and for any $\boldsymbol{v} \in F^n$ define $g: F^n \times F^n \to A$ by

$$g(\boldsymbol{u},\boldsymbol{v}) = \sum_{\boldsymbol{u}'\in F^n} f(\boldsymbol{u}',\boldsymbol{v})\chi(\boldsymbol{u}'\boldsymbol{u}^T)$$

where $\boldsymbol{u}'\boldsymbol{u}^T \in GF(q)$. Then for any linear code $\mathscr{A}$,

$$\sum_{\boldsymbol{u}'\in\mathscr{A}^\perp} f(\boldsymbol{u}',\boldsymbol{v}) = \frac{1}{|\mathscr{A}|}\sum_{\boldsymbol{u}\in\mathscr{A}} g(\boldsymbol{u},\boldsymbol{v}).$$

Corollary 3.4.4 can also be established for nonlinear codes by defining the dual in the appropriate way.

3.5. Further Examples of Biweight Enumerators

Example 3.5.1: The $[n = 2^m - 1, m, 2^{m-1}]$ simplex code = dual of Hamming code, for $m \geq 2$

$$\begin{aligned} \mathscr{J}_{\mathscr{A},\mathscr{A}}(a,b,c,d) = a^n + na^{\frac{1}{2}(n-1)}(b^{\frac{1}{2}(n+1)} + c^{\frac{1}{2}(n+1)}\\ + d^{\frac{1}{2}(n+1)}) + \frac{n(n-1)}{a}(abcd)^{\frac{1}{2}(n+1)}. \end{aligned}$$

Example 3.5.2: The $[n = 2^m - 1, 2^m - m - 1, 3]$ Ham-

ming code, for $m \geq 2$

$$\mathcal{J}_{\mathcal{A},\mathcal{A}}(a,b,c,d) = \frac{1}{(n+1)^2}\left[\sigma_1{}^n + \frac{n(n-1)}{\sigma_1}(\sigma_4 - 2\sigma_{22} + 8\sigma_{1111}) + n\sigma_1^{\frac{1}{2}(n-1)}\{(a-b+c-d)^{\frac{1}{2}(n+1)} + (a+b-c-d)^{\frac{1}{2}(n+1)} + (a-b-c+d)^{\frac{1}{2}(n+1)}\}\right],$$

where σ denotes a symmetric function of a,b,c,d:

$$\sigma_i = a^i + b^i + c^i + d^i$$

$$\sigma_{ij} = a^i(b^j + c^j + d^j) + b^i(a^j + c^j + d^j) + \cdots, \quad i \neq j,$$

$$\sigma_{ii} = a^ib^i + a^ic^i + a^id^i + b^ic^i + b^id^i + c^id^i$$

$$\cdots$$

$$\sigma_{iiii} = a^ib^ic^id^i.$$

(This example is obtained from Example 3.5.1 using Corollary 3.4.4.)

Example 3.5.3: The $[n = 2^m, m+1, 2^{m-1}]$ first-order Reed–Muller code, for $m \geq 2$

$$\mathcal{J}_{\mathcal{A},\mathcal{A}}(a,b,c,d) = \sigma_n + 2(n-1)\sigma_{n/2,n/2} + 4(n-1)(n-2)\sigma_{1111}^{\frac{1}{4}n}.$$

Example 3.5.4: To emphasize that the biweight enumerator gives more information about a code than does the weight enumerator, we exhibit three examples of a pair of codes with the same weight enumerator and different biweight enumerators

i) $\mathcal{A}_1 = \{100,011\}$, $\mathcal{A}_2 = \{100,110\}$.

ii) $\mathcal{A}_1$ is the linear code generated by {110000,001100, 000011} and $\mathcal{A}_2$ is generated by {110000,011000,001111}.

iii) $\mathcal{A}_1$ is the [32,16,8] self-dual Reed–Muller code, $\mathcal{A}_2$ the quadratic residue code with the same parameters (cf. [5]).

Other examples are given in Section IV-4.9.

3.6. Applications to the Study of Code Constructions

3.6.1. Joint Weight Enumerator of Direct Sum Codes: Let $\mathcal{A}_i$ be an (n_i,M_i,d_i) code over $GF(q)$ for $i = 1,2$. The *direct sum* $\mathcal{A}_1 \oplus \mathcal{A}_2$ consists of all vectors $(\boldsymbol{u},\boldsymbol{v})$ where $\boldsymbol{u} \in \mathcal{A}_1$, $\boldsymbol{v} \in \mathcal{A}_2$, and is an $(n_1 + n_2, M_1M_2, d = \min(d_1,d_2))$ code [3, p. 347]. Since wt $(\boldsymbol{u},\boldsymbol{v})$ = wt $(\boldsymbol{u})$ + wt $(\boldsymbol{v})$,

$$\mathcal{W}_{\mathcal{A}_1\oplus\mathcal{A}_2}(x,y) = \mathcal{W}_{\mathcal{A}_1}(x,y)\mathcal{W}_{\mathcal{A}_2}(x,y).$$

Similarly it follows that if $\mathcal{B}_i$ is an (n_i,M_i',d_i') code for $i = 1,2$, then

$$\mathcal{J}_{\mathcal{A}_1\oplus\mathcal{A}_2,\mathcal{B}_1\oplus\mathcal{B}_2}(a,b,c,d) = \mathcal{J}_{\mathcal{A}_1,\mathcal{B}_1}(a,b,c,d)\mathcal{J}_{\mathcal{A}_2,\mathcal{B}_2}(a,b,c,d).$$

3.6.2. The Weight Enumerator of the $(u, u+v)$ Construction: This construction is of interest because it generates all Reed–Muller codes, an infinite family of nonlinear single-error-correcting codes that are better than linear codes, as well as other nonlinear codes [33].

Let $\mathcal{A}_i$ be an (n,M_i,d_i) binary code, for $i = 1,2$. Then the code $\mathcal{A} = \{(\boldsymbol{u}, \boldsymbol{u}+\boldsymbol{v}): \boldsymbol{u} \in \mathcal{A}_1, \boldsymbol{v} \in \mathcal{A}_2\}$ is a $(2n, M_1M_2, d = \min(2d_1,d_2))$ code. (Notice the improvement in d over the direct sum construction.) The joint weight enumerator of $\mathcal{A}_1,\mathcal{A}_2$ is exactly what is required for the weight enumerator of $\mathcal{A}$. Since

$$\text{wt}(\boldsymbol{u}, \boldsymbol{u}+\boldsymbol{v}) = j(\boldsymbol{u},\boldsymbol{v}) + 2k(\boldsymbol{u},\boldsymbol{v}) + l(\boldsymbol{u},\boldsymbol{v})$$

$$\mathcal{W}_{\mathcal{A}}(x,y) = \mathcal{J}_{\mathcal{A}_1,\mathcal{A}_2}(x^2,xy,y^2,xy).$$

One may similarly write down the weight enumerators for codes obtained by the constructions $(\boldsymbol{u}, \boldsymbol{u}$ AND $\boldsymbol{v})$ $(\boldsymbol{u}, \boldsymbol{u}$ OR $\boldsymbol{v})$, where the logical operations AND, OR are applied componentwise.

3.7. The Joint Weight Enumerator of Self-Dual Codes

Let $\mathcal{A} = \mathcal{A}^\perp$ and $\mathcal{B} = \mathcal{B}^\perp$ be self-dual codes. It follows from (3.4.1)–(3.4.4) that their joint weight enumerator $\mathcal{J}_{\mathcal{A},\mathcal{B}}(a,b,c,d)$ is invariant under the transformation

$$\text{replace} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \text{ by } T \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \tag{3.7.1}$$

for the following values of T:

$$T_6 = \frac{1}{\sqrt{q}}\begin{pmatrix} 1 & 0 & \gamma & 0 \\ 0 & 1 & 0 & \gamma \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

$$T_7 = \frac{1}{\sqrt{q}}\begin{pmatrix} 1 & \gamma & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & \gamma \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$T_8 = T_6T_7 = \frac{1}{q}\begin{pmatrix} 1 & \gamma & \gamma & \gamma^2 \\ 1 & -1 & \gamma & -\gamma \\ 1 & \gamma & -1 & -\gamma \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{3.7.2}$$

If $\mathcal{A},\mathcal{B}$ are binary self-dual codes, then $\mathcal{J}_{\mathcal{A},\mathcal{B}}$ is invariant under some additional transformations. Let $\boldsymbol{u} \in \mathcal{A}$, $\boldsymbol{v} \in \mathcal{B}$. Then $n = i(\boldsymbol{u},\boldsymbol{v}) + j(\boldsymbol{u},\boldsymbol{v}) + k(\boldsymbol{u},\boldsymbol{v}) + l(\boldsymbol{u},\boldsymbol{v})$, wt $(\boldsymbol{u}) = k(\boldsymbol{u},\boldsymbol{v}) + l(\boldsymbol{u},\boldsymbol{v})$, and wt $(\boldsymbol{v}) = j(\boldsymbol{u},\boldsymbol{v}) + l(\boldsymbol{u},\boldsymbol{v})$ must all be even. Therefore i,j,k,l are either all odd or all even, and so $\mathcal{J}_{\mathcal{A},\mathcal{B}}$ is invariant under the transformation (3.7.1) for the following values of T:

$$T_9 = \text{diag}(-1,-1,1,1)$$

$$T_{10} = \text{diag}(-1,1,-1,1)$$

$$T_{11} = \text{diag}(-1,1,1,-1),$$

using the usual abbreviation for a diagonal matrix.

Finally, consider the biweight enumerator $\mathcal{J}(a,b,c,d)$ of a binary self-dual code $\mathcal{A}$. Since $l(\boldsymbol{u},\boldsymbol{v})$ must be even for $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{A}$, $\mathcal{J}(a,b,c,d)$ is invariant under all changes of sign of a,b,c,d. Furthermore, it is invariant under all permutations of a,b,c,d. In fact replacing each codeword $\boldsymbol{v}$ in $\mathcal{A}$ by

its complement $\bar{v}$ leaves $\mathscr{A}$ unchanged, and so

$$\mathscr{J}(a,b,c,d) = \sum_{u \in \mathscr{A}} \sum_{v \in \mathscr{A}} a^{i(u,\bar{v})} b^j c^k d^l$$
$$= \sum_{u \in \mathscr{A}} \sum_{v \in \mathscr{A}} a^{j(u,v)} b^i c^l d^k = \mathscr{J}(b,a,d,c),$$

where the omitted arguments of the exponents of b,c,d agree with those of a.

Similarly $\mathscr{J}(a,b,c,d) = \mathscr{J}(c,d,a,b)$. Furthermore we may write $\mathscr{J}(a,b,c,d)$ as

$$\sum_{v \in \mathscr{A}} a^{i(\mathbf{0},v)} b^{j(\mathbf{0},v)} + \sum_{\substack{u \in \mathscr{A} \\ u \neq \mathbf{0}}} \sum_{v \in \mathscr{A}_u} (a^{i(u,v)} b^j c^k d^l + a^{i(u,u+v)} b^j c^k d^l),$$

where for each $u \neq \mathbf{0}$ we have partitioned $\mathscr{A}$ into $\mathscr{A}_u \cup (u + \mathscr{A}_u)$, $\mathscr{A}_u \cap (u + \mathscr{A}_u) = \phi$. But $k(u, u + v) = l(u,v)$, $l(u, u + v) = k(u,v)$, so the double sum is equal to

$$\sum_{\substack{u \in \mathscr{A} \\ u \neq \mathbf{0}}} \sum_{v \in \mathscr{A}_u} (a^{i(u,v)} b^j c^k d^l + a^{i(u,v)} b^j c^l d^k),$$

which is a symmetric function of c and d. Therefore $\mathscr{J}(a,b,c,d) = \mathscr{J}(a,b,d,c)$. Iterating these three permutations shows that $\mathscr{J}(a,b,c,d)$ is invariant under all permutations of its arguments.

Therefore to characterize the biweight enumerators of binary self-dual codes, we must characterize polynomials $\mathscr{J}(a,b,c,d)$ that are invariant under the transformations T_6, T_7, all sign changes, and all permutations of the arguments.

IV. Invariants

The problems described in Sections II and III are special cases of the general problem of finding the invariant polynomials of a group of linear transformations. The classical statement and solution of this problem are as follows (see [6, ch. 17], [25, part II], [37]).

4.1. The Problem

Let G be a finite group of linear transformations on n (complex) variables $x_1,x_2,\cdots,x_n$; that is, G is a multiplicative group of nonsingular complex $n \times n$ matrices. Let g be the order of G, and let I denote the identity matrix.

A typical element $A = (a_{ij})$ of G thus stands for the linear transformation

$$\text{replace } x_i \text{ by } \sum_{j=1}^{n} a_{ij} x_j, \qquad i = 1,2,\cdots,n. \quad (4.1.1)$$

We use the same symbol A both for a transformation and for the matrix describing it.

If $f(\boldsymbol{x}) = f(x_1,\cdots,x_n)$ is any polynomial, $f(A\boldsymbol{x})$ denotes the polynomial obtained by applying the transformation (4.1.1) to the variables $x_1,\cdots,x_n$.

Definition: $f(\boldsymbol{x})$ is an *invariant* polynomial of G if

$$f(A\boldsymbol{x}) = f(\boldsymbol{x}), \qquad \text{for all } A \in G.$$

Clearly if f,g are invariants so are $f + g$ and fg; therefore the invariants of G form a ring $\mathscr{J}(G)$.

The main problem is to characterize $\mathscr{J}(G)$. It is sufficient to characterize the invariants that are homogeneous polynomials, since any invariant is a sum of homogeneous invariants.

4.2. Existence of a Basic Set of Invariants for Finite Groups

Definition: Polynomials $f_1(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x})$ are *algebraically dependent* if there is a polynomial p with complex coefficients, not all zero, such that $p(f_1(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x})) \equiv 0$. Otherwise $f_1(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x})$ are *algebraically independent.*

Theorem 4.2.1—([17, p. 154]): Any $n + 1$ polynomials in n variables are algebraically dependent.

Theorem 4.2.2—([6, p. 357]): There always exist n algebraically independent invariants $f_1,\cdots,f_n$ in $\mathscr{J}(G)$; and so (by Theorem 4.2.1) any invariant is a root of a polynomial equation in $f_1,\cdots,f_n$.

Theorem 4.2.3—([6, p. 359]): There always exist $n + 1$ invariants $f_1,\cdots,f_{n+1}$ in $\mathscr{J}(G)$ such that any invariant is a rational function in $f_1,\cdots,f_{n+1}$.

However, by far the most convenient description of $\mathscr{J}(G)$ is a set of invariants $f_1,\cdots,f_m$ such that any invariant is a *polynomial* in $f_1,\cdots,f_m$. Then $f_1,\cdots,f_m$ is called a *polynomial basis* for $\mathscr{J}(G)$. By Theorem 4.2.1 if $m > n$ there will be polynomial equations, which are called *syzygies*, relating $f_1,\cdots,f_m$.

Theorem 4.2.4—(*Noether; see* [37, pp. 275–276]): $\mathscr{J}(G)$ has a polynomial basis consisting of not more than $\binom{g+n}{n}$ invariants, of degree not exceeding g.

Theorem 4.2.4 says that a polynomial basis for $\mathscr{J}(G)$ can always be found. Finding invariants is fairly easy using the following theorem.

Theorem 4.2.5: If $f(\boldsymbol{x})$ is any polynomial then the average of $f(\boldsymbol{x})$ over the group G,

$$h(\boldsymbol{x}) = \frac{1}{g} \sum_{A \in G} f(A\boldsymbol{x})$$

is an invariant of G.

Proof: For any $A' \in G$,

$$h(A'\boldsymbol{x}) = \frac{1}{g} \sum_{A \in G} f(A'A\boldsymbol{x}) = \frac{1}{g} \sum_{A \in G} f(A\boldsymbol{x}) = h(\boldsymbol{x})$$

since the last sum is a rearrangement of the one before. Q.E.D.

Furthermore, it is clear that all invariants of G can be obtained in this way. In fact the proof of Theorem 4.2.4 shows that a polynomial basis for the invariants of G can be obtained by averaging over G all monomials

$$x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$$

of total degree

$$\sum b_i \leq g.$$

More generally, any symmetric function of the g polynomials $\{f(A\boldsymbol{x}); A \in G\}$ is an invariant of G.

Finally, Theorems 4.2.6 and 4.2.7 enable one to determine when enough invariants have been found to make a basis.

Theorem 4.2.6—([25, p. 258]): The number of linearly independent invariants of G of the first degree is

$$\frac{1}{g}\sum_{A\in G}\text{trace }(A).$$

Theorem 4.2.7—(*Molien*, [26], [6, p. 301], [25, p. 259]): The number of linearly independent invariants of G of degree ν is the coefficient of λ^ν in the expansion of

$$\Phi(\lambda)=\frac{1}{g}\sum_{A\in G}\frac{|A|}{|A-\lambda I|}. \tag{4.2.8}$$

We call $\Phi(\lambda)$ the *Molien series* of G.

Remark 4.2.9: In all the examples considered in this paper, it is possible to put the Molien series into the form

$$\Phi(\lambda)=\frac{1+\sum_{i=1}^{m}c_i\lambda^{\delta_i}}{\prod_{i=1}^{n}(1-\lambda^{d_i})}, \tag{4.2.10}$$

where $c_i\in Z^+=\{0,1,2,\cdots\}$. Furthermore, whenever the Molien series is put into this form, it is then possible to find a polynomial basis for the invariants of G consisting of n algebraically independent invariants $f_1,\cdots,f_n$ of degrees $d_1,\cdots,d_n$ (equal to the degrees of the denominator factors), together with c_1 invariants of degree $\delta_1,\cdots,c_m$ of degree δ_m, say $g_1,\cdots,g_k$ (corresponding to the terms in the numerator), which are algebraically dependent on $f_1,\cdots,f_n$, and such that any invariant of G is a sum of terms of the form

$$f_1^{l_1}\cdots f_n^{l_n}g_i^{\varepsilon}, \tag{4.2.11}$$

where $l_j\in Z^+$, $\varepsilon=0$ or 1, and $1\le i\le k$. That is, there are syzygies expressing g_i^2 and g_ig_j in terms of $f_1,\cdots,f_n$, $g_1,\cdots,g_k$, so that there is at most one g_i in each term (4.2.11).

This is a desirable state of affairs, since then the degrees of the invariants can be read off the Molien series (4.2.10). This happens for all Abelian groups (Section IV-4.4), for the groups known as u.g.g.r. (Section IV-4.8), and for all the other groups considered in this paper. But the exact determination of the groups for which it is true is an unsolved problem. (Partial answers to this question have been obtained and will appear elsewhere.)

In the rest of the paper the invariants $g_1,\cdots,g_k$ that need never be used more than once in any term are denoted by an asterisk *.

4.3. An Example

Consider a formally self-dual Hamming weight enumerator $\mathcal{W}(x,y)$ over $GF(q)$. By (2.6.6) this is invariant under the group G generated by

$$T_3(q)=\frac{1}{\sqrt{q}}\begin{pmatrix}1 & q-1\\ 1 & -1\end{pmatrix}.$$

In fact $G=\{I,T_3\}$, since $T_3(q)^2=I$.

Using (4.2.5) with $f(x)=x$ we obtain the invariant $x+(1/\sqrt{q})(x+(q-1)y)$, or equivalently $\phi_1=x+(\sqrt{q}-1)y$. Using (4.2.5) with $f(x)=x^2$ we obtain the invariant $x^2+(1/q)(x+(q-1)y)^2$, or equivalently, subtracting $(1+1/q)\phi_1^2$, $\phi_2=y(x-y)$.

Any polynomial in ϕ_1,ϕ_2 is of course an invariant of G, and the number of products $\phi_1^i\phi_2^j$ of degree ν is equal to the number of solutions of $i+2j=\nu$, which is the coefficient of λ^ν in

$$(1+\lambda+\lambda^2+\cdots)(1+\lambda^2+\lambda^4+\cdots)=1/\{(1-\lambda)(1-\lambda^2)\}. \tag{4.3.1}$$

To see if this includes all the invariants of G we compute the Molien series (4.2.8). This is found to be

$$\Phi(\lambda)=\frac{1}{2}\left(\frac{1}{(1-\lambda)^2}+\frac{1}{1-\lambda^2}\right)=\frac{1}{(1-\lambda)(1-\lambda^2)},$$

which agrees with (4.3.1)! We conclude that ϕ_1,ϕ_2 are a polynomial basis for the invariants of G.

For coding applications we are interested in invariants of even degree. This corresponds to extending the group by adding the matrix $-I$ and the Molien series becomes

$$\Phi_e(\lambda)=\tfrac{1}{2}(\Phi(\lambda)+\Phi(-\lambda))=\frac{1}{(1-\lambda^2)^2}$$

and as a basis we may take ϕ_1^2,ϕ_2, or equivalently $\phi_3=x^2+(q-1)xy$, $\phi_4=x^2+(q-1)y^2$. Any formally self-dual weight enumerator over $GF(q)$ of even degree is a polynomial in ϕ_3,ϕ_4.

For example, the code generated by $\{01\}$, which is equivalent to its dual, has weight enumerator ϕ_3, and the code generated by $\{11\}$, which is self-dual if q is even and otherwise has the same weight enumerator as its dual, has weight enumerator ϕ_4.

4.4. Invariants of Abelian Groups

We show that the invariants and Molien series of Abelian groups have the desirable properties described in Remark 4.2.9.

Let G be a finite Abelian group of order g acting on variables $x_1,\cdots,x_n$. By [25, p. 213, Theorem 8], it is possible to redefine (by a linear transformation) the variables $x_1,\cdots,x_n$ so as to simultaneously diagonalize all the transformations of G. Thus each $A\in G$ has the form diag $(\lambda_1,\cdots,\lambda_n)$, where the λ_i are the eigenvalues of A and are gth roots of unity. Let ω be a primitive gth root of unity.

Since G is Abelian, it is the direct product of cyclic groups:

$$G=c_1\times c_2\times\cdots\times c_m,$$

where c_i is a cyclic group generated by diag $(\omega^{a_{i1}},\omega^{a_{i2}},\cdots,\omega^{a_{in}})$, for $i=1,\cdots,m$.

Since G is diagonalized, any invariant polynomial for G is a sum of invariant monomials. Furthermore a monomial $x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ is invariant iff

$$\sum_{j=1}^{n}a_{ij}b_j\equiv 0\ (\text{mod } g),\qquad i=1,\cdots,m,\ b_j\in Z^+,\ j=1,\cdots,n. \tag{4.4.1}$$

Any solution $(b_1,\cdots,b_n)$ of (4.4.1) can be written as

$$(b_1,\cdots,b_n) = (b_1',\cdots,b_n') + (gl_1,\cdots,gl_n),$$

where $0 \le b_i' < g$, $l_i \in Z^+$. To every solution $(b_1',\cdots,b_n')$ with $0 \le b_i' < g$ there corresponds the invariant $x^{b_1'}\cdots x^{b_n'}$. Let these monomials be called $g_1,\cdots,g_k$, of degrees $d_1,\cdots,d_k$. Then a basic set of invariants consists of the n algebraically independent monomials

$$x_1{}^g, x_2{}^g, \cdots, x_n{}^g$$

together with $g_1,\cdots,g_k$. Any invariant can be written as a sum of terms of the form

$$(x_1{}^{l_1}\cdots x_n{}^{l_n})^g g_i{}^\varepsilon$$

where $l_j \in Z^+$, $\varepsilon = 0$ or 1 and $1 \le i \le k$. The number of linearly independent invariants of degree v is equal to the number of solutions of

$$v = g(l_1 + \cdots + l_n) + \varepsilon d_i.$$

These numbers have the generating function

$$\Phi(\lambda) = \frac{1 + \sum_{i=1}^{k} \lambda^{d_i}}{(1-\lambda^g)^n}, \qquad (4.4.2)$$

which is therefore the Molien series (4.2.8) for G.

Often it is possible to find a simpler set of invariants than this, in which case there will be cancellation of a common factor in the numerator and denominator of (4.4.2).

4.5. *Example: Formally Self-Dual Complete Weight Enumerators over GF(3)*

Let the exponents of x,y,z count the occurrences of 0,1,2 in a codeword. Then by (2.6.3), the complete weight enumerator $\mathscr{C}(x,y,z)$ is invariant under the group generated by

$$A = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \qquad \omega = e^{2\pi i/3} \qquad (4.5.1)$$

a cyclic group of order 4. Take new variables

$$a = (\sqrt{3}+1)x + y + z$$
$$b = (\sqrt{3}-1)x - y - z$$
$$f = y - z$$

so A becomes diag $(1,i^2,i)$. The monomial $a^\alpha b^\beta f^\gamma$ is invariant iff $2\beta + \gamma \equiv 0$ (modulo 4); and a basic set of invariants is given by $a, b^2, bf^2{}^*, f^4$ with the syzygy $(bf^2)^2 = b^2 \cdot f^4$. The Molien series is

$$\Phi(\lambda) = \frac{1+\lambda^3}{(1-\lambda)(1-\lambda^2)(1-\lambda^4)}. \qquad (4.5.2)$$

(Direct application of the theory of the previous section gives a more complicated set of basic invariants, corresponding to writing the Molien series (4.5.2) as

$$\Phi(\lambda) = \frac{1+\lambda+2\lambda^2+3\lambda^3+2\lambda^4+3\lambda^5+2\lambda^6+\lambda^7+\lambda^8}{(1-\lambda^4)^3},$$

which is of the form (4.4.2).)

The invariants of even degree have Molien series

$$\Phi_e(\lambda) = \frac{1+\lambda^4}{(1-\lambda^2)^2(1-\lambda^4)};$$

and as basic polynomials we may take a^2, b^2, f^4, and $abf^2{}^*$, with the syzygy $(abf^2)^2 = a^2 \cdot b^2 \cdot f^4$.

The following examples of complete weight enumerators of codes over $GF(3)$ show that all four polynomials are necessary.

Generators for Code	Enumerator
{01}	$\phi_5 = x(x+s) = (1/4\sqrt{3})(a^2 - b^2)$, where $s = y + z$
{0111,1210}	$\psi = \phi_5{}^2 - \phi_5\phi_6 = x(x^3 + s^3)$, where $\phi_6 = s(2x - s)$ $= (1/2\sqrt{3})\{(2-\sqrt{3})a^2 - (2+\sqrt{3})b^2\}$
{0011,1210}	$\psi + \frac{1}{8}(\phi_6{}^2 + f^4) + \frac{1}{4}abf^2$
{0011,1200}	$\psi + \frac{1}{4}(\phi_6{}^2 - f^4)$

The second code is self-dual, the others equivalent to their duals.

4.6. *Invariants of Large Groups*

If the invariants of a subgroup H are known, then the invariants of G may be found from the following theorem.

Theorem 4.6.1: Let the decomposition of G into cosets of H be

$$G = A_1H \cup A_2H \cup \cdots \cup A_rH,$$

where $r = |G|/|H|$. Then if $\phi(\boldsymbol{x})$ is an invariant of H,

$$\frac{1}{r}\sum_{i=1}^{r} \phi(A_i\boldsymbol{x})$$

is an invariant of G, and all invariants of G may be obtained in this way.

If in addition H is a normal subgroup of G (written $H \lhd G$), then the application of Theorem 4.6.1 is simplified because of the following.

Theorem 4.6.2: Suppose $H \lhd G$ and $f_1(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x})$ are a polynomial basis for the invariants of H. Then $f_i(A\boldsymbol{x})$ is a polynomial in $f_1(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x})$, for any $A \in G$, $1 \le i \le m$.

Proof: For any $B \in H$, $f_i(BA\boldsymbol{x}) = f_i(AB'\boldsymbol{x}) = f_i(A\boldsymbol{x})$ for some $B' \in H$. Thus $f_i(A\boldsymbol{x})$ is an invariant of H and so is a polynomial in $f_i(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x})$.

So to find the invariants of a large composite group G it is usually easiest to choose a subnormal series [31, p. 107] for G, i.e., a chain of subgroups

$$G_1 \lhd G_2 \lhd \cdots \lhd G$$

and to successively find the invariants for $G_1, G_2, \cdots, G$ using Theorems 4.6.1 and 4.6.2.

Another technique for finding invariants of large groups,

* See Remark 4.2.9.

illustrated by Maschke [23b], is first to find the invariants separately for two subgroups and then to find all combinations of these which are invariants of the large group.

4.7. Example: Complete Weight Enumerators of Self-Dual Codes Over GF(3)[1]

We continue Example 4.5, imposing the additional requirement that the code be self-dual. By (2.6.3), (2.6.7), and (2.6.8), the complete weight enumerator $\mathscr{C}(x,y,z)$ is invariant under the transformations A of (4.5.1) and $B = \text{diag}(1,\omega,\omega)$. A and B generate a group G of order 96 that has a subnormal series

$$G_1 \lhd G_2 \lhd G_3 \lhd G.$$

First, G_1 consists of I and

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

has Molien series $(1+\lambda^2)/\{(1-\lambda)(1-\lambda^2)^2\}$, and has basic invariants $f = y - z$, $\theta_2 = x^2$, $\theta_3 = xs^*$, $\theta_4 = s^2$, where $s = y + z$, with syzygy ${\theta_3}^2 = \theta_2\theta_4$.

Second, G_2 consists of the 4 cosets of G_1 with coset representatives

$$I, \quad -iA, \quad \lambda\begin{pmatrix}1&\omega&\omega\\\omega^2&\omega&\omega^2\\\omega^2&\omega^2&\omega\end{pmatrix}, \quad -\lambda\begin{pmatrix}1&\omega^2&\omega^2\\\omega&\omega^2&\omega\\\omega&\omega&\omega^2\end{pmatrix},$$

where $\lambda = 1/(i\sqrt{3})$. The Molien series is $(1+\lambda^6)/\{(1-\lambda)\cdot(1-\lambda^4)^2\}$ and basic invariants are f, $\psi = x(x^3+s^3) = {\theta_2}^2 + \theta_3\theta_4$, $\theta_5 = s(s^3 - 8x^3) = {\theta_4}^2 - 8\theta_2\theta_3$, and ${\theta_6}^* = s^6 + 20x^3s^3 - 8x^6 = {\theta_4}^3 + 20\theta_2\theta_3\theta_4 - 8{\theta_2}^3$, with syzygy ${\theta_6}^2 = {\theta_5}^3 + 64\psi^3$. The invariants $\psi,\theta_5,{\theta_6}^*$ are obtained by averaging x^4,s^4,x^6 over the cosets, using Theorem 4.6.1.

Third, G_3 consists of the 3 cosets of G_2 with coset representatives I,B,B^2, and has Molien series $\Phi_3 = (1+\lambda^6+\lambda^9)/\{(1-\lambda^3)(1-\lambda^4)(1-\lambda^6)\}$. Clearly the invariants of G_3 are exactly those invariants of G_2 in which each term $x^iy^jz^k$ has $j + k \equiv 0 \pmod 3$. Basic invariants are $f^3,\psi,\theta_6,f^2\theta_5{}^*,f{\theta_5}^{2*}$, with syzygies $(f^2\theta_5)^2 = f^3\cdot f{\theta_5}^2$, $f^2\theta_5\cdot f{\theta_5}^2 = f^3({\theta_6}^2 - 64\psi^3)$, $(f{\theta_5}^2)^2 = f^2\theta_5({\theta_6}^2 - 64\psi^3)$.

Finally G consists of the 4 cosets of G_3 with coset representatives $\pm I, \pm iI$, and has Molien series $\Phi(\lambda) = \frac{1}{4}\{\Phi_3(\lambda) + \Phi_3(i\lambda) + \Phi_3(-\lambda) + \Phi_3(-i\lambda)\} = (1+4\lambda^{12}+\lambda^{24})/\{(1-\lambda^4)(1-\lambda^{12})^2\}$. The invariants are all invariants of G_3 in which the degree is a multiple of 4, and so a set of basic invariants is $\psi,f^{12},{\theta_6}^2,f^6{\theta_6}^*,f^2\theta_5\theta_6{}^*,f^4{\theta_5}^{2*},f^8\theta_5{}^*,f^{10}{\theta_5}^2{\theta_6}^*$. (We omit the 15 syzygies.)

If these invariants are denoted by $f_1,f_2,f_3,g_1,\cdots,g_5$, we conclude [in agreement with Remark (4.2.9)] that the complete weight enumerator of any self-dual code over $GF(3)$ is a sum of terms of the form ${f_1}^{l_1}{f_2}^{l_2}{f_3}^{l_3}{g_i}^{\varepsilon}$, where $l_j \in Z^+$, $\varepsilon = 0$ or 1, and $1 \le i \le 5$. For example, ψ is the enumerator of a code given in Section IV-4.5, and the [12,6,6] Golay code has enumerator $\mathscr{C}(x,y,z)$ given by

$$\begin{aligned}\mathscr{C} &= x^{12}+y^{12}+z^{12}+22(x^6y^6+x^6z^6+y^6z^6)\\&\quad+220(x^6y^3z^3+x^3y^6z^3+x^3y^3z^6)\\&= 2^{-11}\{1280\psi^3+12(f^{12}+{\theta_6}^2)+660(f^4{\theta_5}^2+f^8\theta_5)\\&\quad+704f^6\theta_6\}.\end{aligned}$$

4.8. Unitary Groups Generated by Reflections

For the finite groups known as *unitary groups generated by reflections* (u.g.g.r.) the ring of invariants has a particularly simple structure. We need not give their definition here, but just remark that there are 37 types of irreducible u.g.g.r., a complete list being given in [32], and that they include the symmetry groups of the regular polytopes [8], [9, table 10]. For our purposes their important property is given by the following theorem.

Theorem 4.8.1—(Shephard and Todd [32]): A group G acting on n variables is a u.g.g.r. iff G has a set of basic invariants consisting of n algebraically independent polynomials $f_1,\cdots,f_n$. Furthermore the product of the degrees $m_1,\cdots,m_n$ of these invariants is equal to the order of G.

Thus the Molien series for a u.g.g.r. has the form

$$1\Big/\prod_{i=1}^{n}(1-\lambda^{m_i}).$$

The numbers m_i are tabulated in [32]; see also [7].

4.9. Example: Biweight Enumerators of Self-Dual Codes

By Section III-3.7 the biweight enumerator $\mathscr{J}(a,b,c,d)$ of a binary self-dual code is invariant under the group G_2 generated by the matrices T_6,T_7, all sign changes, and all 4×4 permutation matrices. G_2 has a subnormal series $G_0 \lhd G_1 \lhd G_2$.

First, G_0 is generated by the 24 permutations and the 16 matrices $\text{diag}(\pm1,\pm1,\pm1,\pm1)$, has order 384, and the invariants are all symmetric functions in a^2,b^2,c^2,d^2.

Second, G_1 is generated by G_0 and $T_8 = T_6T_7$. It is not difficult to show that G_1 is the u.g.g.r. [3,4,3], which is the symmetry group of the 24-cell [8, p. 149], and has order 1152.

A set of basic invariants for G_1 is, in the symmetric function notation of (3.5.2):

$$\begin{aligned}A &= \sigma_2\\B &= 6\sigma_{222} - \sigma_{22}\sigma_2 + \tfrac{1}{8}{\sigma_2}^3\\C &= 12\sigma_{1111}^2 - \tfrac{3}{2}\sigma_{222}\sigma_2 + {\sigma_{22}}^2 - \tfrac{1}{4}\sigma_{22}{\sigma_2}^2 + \tfrac{1}{16}{\sigma_2}^4\\D &= -4\sigma_{1111}^2\sigma_{22} + \tfrac{5}{4}\sigma_{1111}^2{\sigma_2}^2 + \tfrac{3}{4}\sigma_{222}^2 + \tfrac{1}{9}{\sigma_{22}}^3\\&\quad - \tfrac{1}{24}{\sigma_{22}}^2{\sigma_2}^2 - \tfrac{1}{4}\sigma_{222}\sigma_{22}\sigma_2 + \tfrac{1}{96}\sigma_{22}{\sigma_2}^4 - \frac{1}{9\cdot 2^7}{\sigma_2}^6\end{aligned}$$

and the product of their degrees is $2\cdot6\cdot8\cdot12 = 1152$, verifying Theorem 4.8.1. (These were found with the help of the symmetric function tables in [10].)

Finally $G_2 = G_1 \cup T_6G_1$ has order 2304, Molien series $(1+\lambda^{18})/\{(1-\lambda^2)(1-\lambda^8)(1-\lambda^{12})(1-\lambda^{24})\}$, and basic invariants A,C,B^2,BD^*,D^2 of degrees 2,8,12,18,24, with syzygy $(BD)^2 = B^2\cdot D^2$.

Thus the biweight enumerator of any binary self-dual code

[1] This section is essentially due to McEliece [24].

is a polynomial in A,C,B^2,BD^*,D^2. The following examples of self-dual codes show that all five polynomials are necessary. For generators of these codes see Pless's list [29].

Code	Biweight Enumerator[a]
$C_2 = \{00,11\}$	A
$A_8 =$ [8,4,4] Hamming code	$16C$
$B_{12} =$ [12,6,4]	$-\frac{5}{16}A^6 + 20A^2C + 4B^2$
$I_{18} =$ [18,9,4]	$-\frac{45}{128}A^9 + \frac{25}{2}(A^5C + A^3B^2) + \frac{320}{3}AC^2 - \frac{1}{8}BD_2$
The [24,12,8] Golay code	$\frac{1}{18}(11C_2^3 + 7D_2^2)$

[a] Where $C_2 = 16C$, $D_2 = 576(D + \frac{1}{48}A^3B)$.

V. Characterization of Weight Enumerators of Self-Dual Codes

5.1. Introduction

For each weight enumerator, we describe the group G of transformations under which it is invariant by giving the generators (enclosed within diamond brackets) and the degree n (the number of variables on which G acts). Then we give the Molien series $\Phi(\lambda)$ (4.2.8), and where possible a set of basic polynomial invariants $f_1,\cdots,f_n,g_1,\cdots,g_m$, the g_i being indicated by asterisks. Any weight enumerator is a sum of terms $f_1^{l_1},\cdots,f_n^{l_n}g_i^{\varepsilon}$, $l_j \in Z^+$, $\varepsilon = 0$ or 1, $1 \le i \le m$.

5.2. Formally Self-Dual Weight Enumerators (Section II-2.6)

5.2.1. Complete Weight Enumerators over GF(q): $G = \langle T_1 \rangle$, a cyclic group of order 4; $n = q$. If q is a prime, $4\Phi(\lambda)$ is

$$(1-\lambda)^{-q} + 2(1-\lambda^4)^{-(q+1)/4} + (1-\lambda)^{-1} \cdot (1-\lambda^2)^{-(q-1)/2}, \qquad q \equiv -1 \pmod 4$$

$$(1-\lambda)^{-q} + 2(1-\lambda)^{-1}(1-\lambda^4)^{-(q-1)/4} + (1-\lambda)^{-1}(1-\lambda^2)^{-(q-1)/2}, \qquad q \equiv 1 \pmod 4.$$

For the case $q = 3$ it was shown in Section IV-4.5 that for invariants of even degree there are four basic polynomials, which in the notation of that section are $a^2,b^2,c^4,abc^2{}^*$. Basic invariants are not known for $q > 3$.

5.2.2. Lee Weight Enumerators over GF(q): $G = \langle T_2 \rangle$, a cyclic group of order 2; $n = \frac{1}{2}(q+1)$. If q is a prime, $2\Phi(\lambda)$ is

$$(1-\lambda)^{-n} + (1-\lambda^2)^{-n/2}, \qquad q \equiv -1 \pmod 4$$

$$(1-\lambda)^{-n} + (1-\lambda)^{-1}(1-\lambda^2)^{-(n-1)/2}, \qquad q \equiv 1 \pmod 4$$

For $q = 5$, let the exponents of x,y,z count the occurrences of $0, \pm 1, \pm 2$ in a codeword. Then basic polynomials are $f = y - z$, $\psi_2 = x + \frac{1}{2}(\sqrt{5} - 1)(y + z)$, $\psi_3 = x^2 + 4yz$. For invariants of even degree, basic polynomials are $f^2,f\psi_2{}^*,\psi_2{}^2,\psi_3$. Basic invariants are not known for $q > 5$.

5.2.3. Hamming Weight Enumerators over GF(q): $G = \langle T_3(q) \rangle$, a cyclic group of order 2; $n = 2$. For invariants of even degree, $\Phi_e(\lambda) = (1-\lambda^2)^{-2}$ and basic polynomials are $\phi_3 = x^2 + (q-1)xy$, $\phi_4 = x^2 + (q-1)y^2$ (see Section IV-4.3).

5.3. Weight Enumerators of Self-Dual Codes

5.3.1. Complete Weight Enumerators over GF(q): $G = \langle T_1,T_4,T_5 \rangle$, $n = q$. Gleason [15] and McEliece *et al.* [24] have determined the order of G and the Molien series in the general case.

For the case $q = 3$ a set of eight basic polynomials were given in Section 4.7.

5.3.2. Lee Weight Enumerators over GF(q): $G = \langle T_2,T_4,T_5 \rangle$, $n = \frac{1}{2}(q+1)$. Again McEliece *et al.* [24] have determined the order of G and the Molien series in the general case.

For the case $q = 5$, G is generated by $A = \operatorname{diag}(1,\omega,\omega^4)$,

$$B = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 & 2 & 2 \\ 1 & \omega+\omega^4 & \omega^2+\omega^3 \\ 1 & \omega^2+\omega^3 & \omega+\omega^4 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

where $\omega^5 = 1$. Now the subgroup G_1 generated by A and BC is the classical 3-dimensional representation of the alternating group of order 60, and has Molien series $(1+\lambda^{15})/\{(1-\lambda^2)(1-\lambda^6)(1-\lambda^{10})\}$. A set of basic invariants of G_1, of degrees 2,6,10,15, is given by Klein [18, pp. 236–243]. G itself is the u.g.g.r. [3,5], the symmetry group of the icosahedron, and has order 120. Basic invariants of G are, as given by Klein and writing Y for $2y$ and Z for $2z$,

$$A = x^2 + YZ,$$

$$B = 8x^4YZ - 2x^2Y^2Z^2 + Y^3Z^3 - x(Y^5 + Z^5),$$

$$C = 320x^6Y^2Z^2 - 160x^4Y^3Z^3 + 20x^2Y^4Z^4 + 6Y^5Z^5 - 4x(Y^5 + Z^5)(32x^4 - 20x^2YZ + 5Y^2Z^2) + Y^{10} + Z^{10}.$$

Gleason and Pierce [16] independently found this basis and have very kindly supplied the following examples of codes.

Generators for Code	Lee Weight Enumerator
{12}	A
{100133,010313,001331}	$A^3 - \frac{3}{8}B$
{1122000000,0000100122,0000010213, 1414141414,2420430100}	$A^5 - \frac{5}{8}A^2B + \frac{1}{256}C$

For the case $q = 7$, G is generated by $A = \operatorname{diag}(1,\omega,\omega^4,\omega^2)$,

$$B = \frac{1}{\sqrt{7}}\begin{pmatrix} 1 & 2 & 2 & 2 \\ 1 & \omega+\omega^6 & \omega^2+\omega^5 & \omega^3+\omega^4 \\ 1 & \omega^2+\omega^5 & \omega^3+\omega^4 & \omega+\omega^6 \\ 1 & \omega^3+\omega^4 & \omega+\omega^6 & \omega^2+\omega^5 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Since the length of the code must be a multiple of 4, we are only interested in invariants of degree divisible by 4.

These invariants are unchanged if B is replaced by iB. The group generated by A, iB, and C has order 336 and is important in elliptic function theory and in geometry. (Maschke [23b], Edge [12].) A set of basic invariants was given by Maschke in 1893. For completeness and to correct some errors in Maschke's work (and also because of the inaccessibility of [23b]), we reproduce them here. Let the exponents of t_1,x,y,z count the occurrences of $0, \pm 1, \pm 2, \pm 3$ in a codeword; and write t_2 instead of $2x$, t_3 instead of $2y$, and t_4 instead of $2z$.

Let $a = t_2t_3t_4$, $b = {t_2}^3t_3 + {t_3}^3t_4 + {t_4}^3t_2$, $c = {t_2}^2{t_3}^3 + {t_3}^2{t_4}^3 + {t_4}^2{t_2}^3$, $d = a^2 + t_2{t_3}^5 + t_3{t_4}^5 + t_4{t_2}^5$, $e = 7ab + {t_2}^7 + {t_3}^7 + {t_4}^7$.

Then there are 7 basic invariants, of degrees 4,6,8,8,10, 12,14, as follows:

$$\Phi_4 = 2{t_1}^4 + 6at_1 + b$$

$$\Phi_6 = 8{t_1}^6 - 20a{t_1}^3 - 10b{t_1}^2 - 10ct_1 - 14a^2 - d$$

$$\Phi_8 = {t_1}^8 - 2a{t_1}^5 + b{t_1}^4 + 2c{t_1}^3 + (6a^2 + d){t_1}^2 + 2abt_1 + ac$$

$$\Gamma_8 = {t_1}^8 + 14a{t_1}^5 - 7b{t_1}^4 + 14c{t_1}^3 - 7d{t_1}^2 + et_1$$

$$\Phi_{10} = -8{t_1}^{10} - 20a{t_1}^7 + 14b{t_1}^6 + 14c{t_1}^5 + 7(16a^2 - d){t_1}^4 + (42ab - e){t_1}^3 + 7(b^2 + 3ac){t_1}^2 + 7(7a^3 + bc)t_1 + ae$$

$$\Phi_{12} = 26{t_1}^{12} + 202a{t_1}^9 - 33b{t_1}^8 + 120c{t_1}^7 + 14(13a^2 + d){t_1}^6 + (378ab - 23e){t_1}^5 + 7(35ac - 2b^2){t_1}^4 + 14(49a^3 - 10ad + 5bc){t_1}^3 + 2a(10e + 49ab){t_1}^2 + (49a^2c + 49ab^2 - 7cd + 2be)t_1 + ce$$

$$\Phi_{14} = 48{t_1}^{14} + 7.24a{t_1}^{11} + 7.44b{t_1}^{10} - 28.57c{t_1}^9 + 63(84a^2 + 22d){t_1}^8 - 8(37e + 490ab){t_1}^7 + 4.49(12ac + 5b^2){t_1}^6 + 196(15ad - 13bc){t_1}^5 + 14(13.14c^2 - 86ae - 7bd){t_1}^4 + 28(11be - 42cd){t_1}^3 + 14(21d^2 - 16ce){t_1}^2 + 14det_1 - e^2.$$

(There are 5 syzygies, of degrees 20, 22, 24, 24, and 26.)

For example, the code generated by {1112,0231} has Lee enumerator $\frac{1}{2}\Phi_4$.

5.3.3. Hamming Weight Enumerators over GF(q): In going from formally self-dual enumerators to self-dual codes, for general q nothing can be added to what was said in (5.2.3). But for small q we can study the effect of imposing the restriction that the Hamming weights of all codewords be divisible by a constant. According to the following theorem there are four cases in which this can happen.

Theorem 5.3.4—(Gleason and Pierce [2]): If $\mathscr{A}$ is a self-dual code over $GF(q)$ in which all Hamming weights are divisible by c, then the only possible values for the pair (q,c) are (2,2), (2,4), (3,3), and (4,2).

We consider these cases separately.

5.3.5. Binary Codes: A binary self-dual code automatically has all weights divisible by 2. The weight enumerator is invariant under $G = \langle T_3(2), \text{diag } (1,-1)\rangle$, a dihedral group of order 16, and a u.g.g.r. Basic invariants are $\psi_1 = x^2 + y^2$, $\psi_2 = x^8 + 14x^4y^4 + y^8$, the latter being the enumerator of the [8,4,4] Hamming code (Burnside [6, p. 362], Gleason [15]).

5.3.6. Binary Codes With Weights Divisible by 4: $G = \langle T_3(2), \text{diag } (1,i)\rangle$, a u.g.g.r. of order 192. Basic invariants are ψ_2 and $\psi_3 = x^4y^4(x^4 - y^4)^4$ (Shephard and Todd [32], Gleason [15]). The [24,12,8] Golay code has enumerator ${\psi_2}^3 - 672\psi_3$.

5.3.7. Ternary Codes: A ternary self-dual code automatically has all weights divisible by 3. $G = \langle T_3(3), \text{diag } (1,e^{2\pi i/3})\rangle$, a u.g.g.r. of order 48. Basic invariants are $\psi_4 = x^4 + 8xy^3$, $\psi_5 = y^3(x^3 - y^3)^3$ (Shephard and Todd [32], Gleason [15]). The [12,6,6] Golay code has enumerator ${\psi_4}^4 + 24\psi_5$. As a verification, we observe that the 8 basic invariants of Section IV-4.7 reduce to ψ_4,ψ_5 when $y = z$.

5.3.8. Quaternary Codes With Weights Divisible by 2: $G = \langle T_3(4), \text{diag } (1,-1)\rangle$, a dihedral group of order 12, and a u.g.g.r. Basic invariants are $\psi_6 = x^2 + 3y^2$, $\psi_7 = y^2(x^2 - y^2)^2$. The code generated by $\{11\omega00\omega,1\omega1\omega00, 10\omega1\omega0\}$, where $\omega^2 + \omega + 1 = 0$, has enumerator ${\psi_6}^3 - 9\psi_7$.

5.4. Joint Weight Enumerators of Binary Codes (Section III-3.1)

5.4.1. Joint Enumerator of Self-Dual Codes: Let $\mathscr{A},\mathscr{B}$ be binary self-dual codes. By Section III-3.7 their joint weight enumerator $\mathscr{J}(a,b,c,d)$ is invariant under $G = \langle T_6,T_7,T_9, T_{10},T_{11}\rangle$, of order 128, and

$$\Phi(\lambda) = \frac{1 + \lambda^8 + \lambda^{10} + \lambda^{18}}{(1 - \lambda^2)(1 - \lambda^4)(1 - \lambda^8)^2}.$$

The seven invariants have been calculated.

5.4.2. Biweight Enumerator of a Binary Self-Dual Code: The five basic polynomials are given in Section IV-4.9.

Acknowledgment

The authors wish to thank A. M. Gleason, R. J. McEliece, and J. N. Pierce for telling them about their work, J. H. Conway and R. P. Kurshan for very helpful discussions, and L. A. Dimino for computing the orders of many of the groups for them with his group theory analysis system GRAPPA.

References

[1] E. F. Assmus, Jr., and H. F. Mattson, Jr., "The algebraic theory of codes II," Sylvania Electron. Syst., Needham Heights, Mass., Rep. AFCRL-71-0013, Oct. 15, 1970 (especially Part II).

[2] E. F. Assmus, Jr., H. F. Mattson, Jr., and R. Turyn, "Cyclic Codes," Sylvania Electron. Syst., Waltham, Mass., Rep. AFCRL-65-332, pp. 77–79, Apr. 28, 1965.

[3] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[4] E. R. Berlekamp, F. J. MacWilliams, and N. J. A. Sloane, "Gleason's theorem on self-dual codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 409–414, May 1972.

[5] E. R. Berlekamp and L. R. Welch, "Weight distributions of the cosets of the (32,6) Reed–Muller code," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 203–207, Jan. 1972.

[6] W. Burnside, *Theory of Groups of Finite Order*, 2nd ed., 1911. New York: Dover, 1955.
[7] H. S. M. Coxeter, "The product of the generators of a finite group generated by reflections," *Duke Math. J.*, vol. 18, pp. 765–782, 1951.
[8] H. S. M. Coxeter, *Regular Polytopes*, 2nd ed. New York: Macmillan, 1963.
[9] H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, 2nd ed. New York: Springer, 1965.
[10] F. N. David, M. G. Kendall, and D. E. Barton, *Symmetric Function and Allied Tables*. Cambridge: Cambridge Univ. Press, 1966.
[11] J. A. Dieudonné and J. B. Carrell, *Invariant Theory, Old and New*. New York: Academic Press, 1971.
[12] W. L. Edge, "The Klein group in three dimensions," *Acta Math.*, vol. 79, pp. 153–223, 1947.
[13] W. Feit, "Some remarks on weight functions of spaces over $GF(2)$," to be published.
[14] ——, "On weight functions of self orthogonal spaces over $GF(3)$," to be published.
[15] A. M. Gleason, "Weight polynomials of self-dual codes and the MacWilliams identities," in *1970 Act. Congr. Int. Math.*, vol. 3, pp. 211–215. Paris: Gauthier-Villars, 1971.
[16] A. M. Gleason and J. N. Pierce, private communication.
[17] N. Jacobson, *Lectures in Abstract Algebra*, vol. 3. Princeton, N.J.: Van Nostrand, 1964.
[18] F. Klein, *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*, 2nd rev. ed., 1913. New York: Dover, 1956, 1st German ed., 1884.
[19] J. Leech and N. J. A. Sloane, "Sphere packing and error-correcting codes," *Can. J. Math.*, vol. 23, pp. 718–745, 1971.
[20] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell Syst. Tech. J.*, vol. 42, pp. 79–84, 1963.
[21] F. J. MacWilliams, N. J. A. Sloane, and J.-M. Goethals, "The MacWilliams identities for nonlinear codes," *Bell Syst. Tech. J.*, vol. 51, pp. 803–819, Apr. 1972.
[22] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, "Good self-dual codes exist," *Discr. Math.*, to be published.
[23] a.——, "On the existence of a projective plane of order ten," *J. Combinatorial Theory*, to be published.
b. H. Maschke, "Invariants of a group of $2 \cdot 168$ linear quaternary substitutions," presented at the 1893 Int. Math. Congr. New York: MacMillan, 1896, pp. 175–186.
[24] R. J. McEliece, E. R. Rodemich, and H. C. Rumsey, Jr., private communication.
[25] G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, *Theory and Applications of Finite Groups*, 1st ed., 1916. New York: Dover, 1961.
[26] T. Molien, "Über die Invarianten der linear Substitutionsgruppen," *Sitzungsber. König Preuss. Akad. Wiss.*, pp. 1152–1156, 1897.
[27] A. W. Nordstrom and J. P. Robinson, "An optimum nonlinear code," *Inform. Contr.*, vol. 11, pp. 613–616, 1967.
[28] V. S. Pless, "On the uniqueness of the Golay codes," *J. Combinatorial Theory*, vol. 5, pp. 215–228, 1968.
[29] ——, "A classification of self-orthogonal codes over $GF(2)$," to be published.
[30] C. Reid, *Hilbert*. New York: Springer, 1970.
[31] J. R. Rotman, *The Theory of Groups*. Boston, Mass.: Allyn and Bacon, 1965.
[32] G. C. Shephard and J. A. Todd, "Finite unitary reflection groups," *Can. J. Math.*, vol. 6, pp. 274–304, 1954.
[33] N. J. A. Sloane and D. S. Whitehead, "New family of single-error correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 717–719, Nov. 1970.
[34] J. G. Thompson, "A note on a theorem of Gleason," to be published.
[35] J. H. van Lint, "Coding theory," in *Lecture Notes in Mathematics*, vol. 201. Berlin: Springer, 1971.
[36] H. Weyl, "Invariants," *Duke Math. J.*, vol. 5, pp. 489–502, 1939.
[37] ——, *The Classical Groups*, 2nd ed. Princeton, N.J.: Princeton Univ. Press, 1953.

Correspondence

Correlation Properties of the Zero-Crossing Intervals of Gaussian Processes

TADASI MIMAKI

***Abstract*—An experimental study is reported of the correlation properties of the intervals between zero crossings of a Gaussian process. The validity of an assumption under which McFadden derived certain theoretical results is examined. It is found that the assumption is valid only for processes with narrow-band spectra. For broad-band spectra, the correlation coefficients of the intervals decay slowly and oscillate with increasing separation between intervals.**

I. Introduction

Heretofore, little has been known about the correlations between the lengths of the zero-crossing intervals of a real-valued stationary random process, either theoretically or experimentally. McFadden [1] derived two relations among the correlation coefficients κ_i of the 0th and ith zero-crossing interval lengths. Earlier, McFadden [2] had derived expressions for the κ_i and for the variance σ^2 of the interval lengths, under the assumption that the successive zero-crossing intervals form a Markov chain in the wide sense. Rainal [3] experimentally obtained κ_1 for Gaussian processes and reported that in some cases the comparisons with the theoretical approximations by McFadden were unsatisfactory.

In this correspondence the experimental values of κ_i are given for Gaussian processes having seventh-order Butterworth spectra. It is shown that the Markov assumption is not valid except for a narrow-band spectrum. For a relatively broad-band spectrum, the coefficients κ_i oscillate and slowly decay as i increases.

II. Fundamental Identities

McFadden [1] derived the following expressions about the correlation coefficients κ_i between zero-crossing interval lengths:

$$\sum_{i=1}^{\infty} (-1)^i \kappa_i = \frac{\mu_0 A}{\sigma^2} - \frac{1}{2} \tag{1}$$

and

$$\sum_{i=1}^{\infty} \kappa_i = \left(B + \frac{1}{2}\right) \frac{\mu_0^2}{\sigma^2} - \frac{1}{2}, \tag{2}$$

Manuscript received November 30, 1971; revised April 14, 1972.
The author was with the Department of Physics, Faculty of Science, Tokyo University, Tokyo, Japan. He is now with the University of Electro-communications, Chofu-Shi, Tokyo, Japan.