TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 287, Number 1, January 1985

THE ALGEBRA OF THE FINITE FOURIER TRANSFORM AND CODING THEORY

BY
R. TOLIMIERI[1]

ABSTRACT. The role of the finite Fourier transform in the theory of error correcting codes has been explored in a recent text by Richard Blahut. In this work we study how the finite Fourier transform relates to certain polynomial identities involving weight enumerator polynomials of linear codes. These include the generalized MacWilliams identities and theorems originally due to R. Gleason concerning polynomial algebras containing weight enumerator polynomials. The Heisenberg group model of the finite Fourier transform provides certain algebras of classical theta functions which will be applied to reprove Gleason's results.

I. Introduction. This work will place the theory of the finite Fourier transform at center stage in the study of several problems in coding theory, especially those involving the weight enumerator polynomial and its characterization. The emergence of finite Fourier transform theory as an explicit tool in coding theory can be found in R. Blahut's recently published text [**10**] *Theory and practice of error control codes,* where many important aspects of coding theory are viewed within the framework of the finite Fourier transform. That this should be the case should come as no surprise to coding theorists, who often apply the Hadamard transform to coding theory problems. The Blahut text formalizes this cohabitation of ideas and has been a major influence on this work.

In §II we present the theory of the finite Fourier transform on a finite-dimensional vector space over finite fields. We then show how the MacWilliams identities for exact weight enumerator polynomials of linear codes follow (up to rather complicated, but standard, algebraic identifications) from the definition of the Fourier transform.

The second major influence on this work can be found in the work of N. Sloane [**8**]. There he applies theta function theory to the study of weight enumerator polynomials. In [**1**] L. Auslander and the author built an algebra from the finite Fourier transform on n points, $n > 0$, that was related to an algebra of theta functions.

We now introduce some notation and definitions that enable us to review the results in [**1**].

For an integer $m > 0$, denote by Z/m the integers mod m, and by L_m the space of all complex-valued functions on Z/m, along with the inner product $\langle f, g \rangle$ on L_m

Received by the editors August 5, 1982 and, in revised form, February 3, 1984.
1980 *Mathematics Subject Classification.* Primary 22E25, 22E40, 94B05, 43A80.
[1]Partially supported by N.S.F.

defined by

$$\langle f, g \rangle = \sum_{j=0}^{m-1} f(j)\overline{g}(j),$$

where bar denotes complex conjugate.

Let us now introduce two orthogonal bases of the m-dimensional vector space L_m which we need in this work. For each $0 \leq j < m$ let $x_j \in L_m$ be defined by

$$x_j(k) \equiv \begin{cases} 1, & k = j, \\ 0, & k \neq j, \end{cases} \qquad 0 \leq k < m.$$

Direct calculation shows that

$$\langle x_j, x_k \rangle \equiv \begin{cases} 1, & j = k, \\ 0, & j \neq k, \end{cases} \qquad 0 \leq j, k < m,$$

and, hence, $x_0, x_1, \ldots, x_{m-1}$ is an orthonormal basis of L_m.

For each $0 \leq j < m$ define $\Psi_j \in L_m$ by

$$\Psi_j(k) \equiv \exp(2\pi i jk/m), \qquad 0 \leq k < m.$$

It is easy to see that

$$\langle \Psi_j, \Psi_k \rangle = \begin{cases} m, & j = k, \\ 0, & j \neq k, \end{cases} \qquad 0 < j, k < m,$$

and, hence, $\Psi_0, \Psi_1, \ldots, \Psi_{m-1}$ is an orthogonal basis of L_m.

The set

$$\widehat{Z_m} \equiv \{\Psi_j : 0 \leq j < m\}$$

is a group with respect to the multiplication

$$\Psi_j \Psi_k \equiv \Psi_{j+k}, \qquad 0 \leq j, k < m,$$

where $j + k$ is taken mod m. We call $\widehat{Z_m}$ the dual, or character, group of Z_m.

The Fourier transform F_m on Z/m is the linear mapping of L_m defined by setting

$$F_m(x_j) = (1/\sqrt{m})\Psi_j, \qquad 0 \leq j < m.$$

Clearly, F_m is a unitary operator on L_m and, for any $f \in L_m$, we have

$$F_m(f)(k) = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} f(j) \exp\left(2\pi i \frac{jk}{m}\right), \qquad 0 \leq k < m.$$

Consider

$$L = \sum_{m \geq 0} \bigoplus L_m, \qquad L_0 \equiv \mathbf{C},$$

$$F = \sum_{m \geq 0} \bigoplus F_m, \qquad F_0 \equiv \text{identity mapping.}$$

In [**1**] we proved that algebra structures can be defined on L so that F becomes an algebra homomorphism. One of these is isomorphic to the algebra of theta functions on $\mathbf{C}(a + ib)$, $a, b \in Z$. This algebra will play a crucial role in our analysis of Gleason's theorems stated in §IV.

The main coding theorems to be proved by our methods are the MacWilliams identities, Theorems A and B, in §II and the Gleason theorems, Theorems C and D, in §IV. The tools for the MacWilliams identities are contained in §II, while those for Gleason's results appear in §III. Original proofs of these results can be found in [**4** and **3**]. Other proofs of Gleason's results can be found in [**5** and **9**].

II. The Fourier transform and coding theory. Consider a prime p and denote the field of integers mod p by Z/p. Let $n \geq 1$ be an integer and denote n-dimensional vector space over Z/p by V_n. Since, in the first part of this discussion, n will be fixed, we set $V \equiv V_n$. A typical point $v \in V$ will be written $v = (v_1, \ldots, v_n)$, $v_j \in Z/p$.

A linear code in V or a linear code of length n over Z/p is any subspace C of V. The dimension of the linear code C in V is its dimension as a vector space over Z/p.

An inner product on V will now be specified. The inner product of two elements $v,\ w \in V$, denoted by $\langle v, w\rangle$, is defined by

$$\langle v, w\rangle = \sum_{j=1}^{n} v_j w_j. \tag{2.1}$$

The dual $C^{\perp}$ of a linear code C in V is given by

$$C^{\perp} = \{v \in V : \langle v, w\rangle = 0 \text{ for all } w \in C\}. \tag{2.2}$$

It is easy to see that $C^{\perp}$ is also a linear code. We say that C is self-dual whenever

$$C^{\perp} = C. \tag{2.3}$$

Consider V as an abelian group under addition. A character of V is any mapping $\Psi\colon V \to \mathbf{C}^x$ satisfying

$$\Psi(v + w) = \Psi(v) \cdot \Psi(w), \qquad v, w \in V. \tag{2.4}$$

The set of all characters of V, denoted $\hat{V}$, becomes a group under the product rule

$$(\Psi\Psi')(v) \equiv \Psi(v)\Psi(v'), \qquad \Psi, \Psi' \in \hat{V},\ v \in V. \tag{2.5}$$

The mapping Ψ_0, given by $\Psi_0(v) \equiv 1$, $v \in V$, is called the trivial character on V. The following formulas will be used without proof:

$$\sum_{v \in V} \Psi(v) = 0 \quad \text{if } \Psi \text{ is not the trivial character.} \tag{2.6}$$

$$\sum_{\Psi \in \hat{V}} \Psi(v) = 0 \quad \text{if } v \neq 0. \tag{2.7}$$

Up to this point we have made no use of the special nature of V. Definitions (2.4) and (2.5), as well as formulas (2.6) and (2.7), carry over to any finite abelian group A. Although it is true that for any finite abelian A we have A and $\hat{A}$ isomorphic, we use the inner product (2.1) to define an isomorphism between V and $\hat{V}$. This isomorphism is not canonically defined in terms of V as an abelian group, but essentially depends upon our choice of inner product.

For $v \in V$ we define the mapping Ψ_v by the rule

$$\Psi_v(w) \equiv \exp(2\pi i(1/p)\langle v, w\rangle), \qquad v, w \in V, \tag{2.8}$$

where we view an element of Z/p as its representative k in Z such that $0 \leq k < p$. It is easy to verify that $\Psi_v \in \hat{V}$, and the mapping $v \mapsto \Psi_v$, $v \in V$, defines an isomorphism from V onto $\hat{V}$.

Let $L^2(V)$ denote the set of all complex-valued functions on V made into an inner product space by setting

$$\langle f, g\rangle \equiv \sum_{v \in V} f(v)\bar{g}(v), \qquad f, g \in L^2(V). \tag{2.9}$$

The Fourier transform of V, denoted F_V, is the mapping of $L^2(V)$ to itself defined by

$$F_V(f)(w) \equiv p^{-n/2} \sum_{v \in V} f(v)\Psi_v(w), \tag{2.10}$$

where $w \in V$ and $f \in L^2(V)$. A straightforward verification shows that F_V is a unitary operator of $L^2(V)$. To simplify notation we write F for F_V.

The evaluation function of a subset S of V, denoted E_S, is the function on V given by the rule

$$E_S(v) \equiv \begin{cases} 1, & v \in S, \\ 0, & v \notin S, \end{cases} \qquad v \in V. \tag{2.11}$$

If $\{v\}$ denotes the set v, we let $E_{\{v\}} = E_v$. Clearly, the set of functions

$$E_v, \qquad v \in V, \tag{2.12}$$

determines an orthonormal basis of $L^2(V)$.

THEOREM 2.1. *Let C be a linear code in V. Then*

$$F(E_C) = o(C)p^{-n/2}E_{C^\perp}, \tag{2.13}$$

where F is the Fourier transform of V, and $o(C)$ equals the number of elements in C.

PROOF. By definition,

$$F(E_C)(v) = p^{-n/2} \sum_{w \in C} \Psi_v(w), \qquad v \in V.$$

If $v \in C^\perp$ then $\Psi_v(w) = 1$ for all $w \in C$ and we have

$$F(E_C)(v) = o(C)p^{-n/2}.$$

If $v \notin C^\perp$ then Ψ_v restricted to C is a nontrivial character of the abelian group C and, by (2.6), $\sum_{w \in C} \Psi_v(w) = 0$, which completes the proof of the theorem.

Theorem 2.1 is a disguised version of the MacWilliams identity for the exact weight enumerator polynomial. To recognize (2.13) as a MacWilliams identity, certain well-known identifications will be recalled.

Let $X \equiv L^2(Z/p)$, the space of all complex-valued functions on Z/p. We consider X as a p-dimensional vector space over $\mathbf{C}$. We know that a basis for X is given by the functions

$$x_0, x_1, \ldots, x_{p-1}, \tag{2.14}$$

where

$$x_j(k) \equiv \begin{cases} 1, & k = j, \\ 0, & k \neq j, \end{cases} \qquad 0 \leq j, k < p.$$

We let

$$T_n(X) = \bigotimes_1^n X_j, \qquad X_j = X,\ j = 1, \ldots, n, \tag{2.15}$$

denote the tensor product of n copies of X. In the following discussion we set $T_n \equiv T_n(X)$.

Consider $v \in V$ and let $x^v \in T_n$ be defined by

$$x^v \equiv \bigotimes_{j=1}^n x_{v_j}, \tag{2.16}$$

where $v = (v_1, \ldots, v_n)$ and $v_j \in Z/p$. We call x^v a monomial of degree n. The set of all monomials of degree n,

$$x^v, \qquad v \in V, \tag{2.17}$$

defines a basis of T_n. An arbitrary $f \in T_n$ can be written

$$f \equiv f(x) \equiv \sum_{v \in V} a(v) x^v, \qquad a(v) \in \mathbf{C}, \tag{2.18}$$

and will be called a homogeneous polynomial in the noncommuting variables (2.14) of degree n.

THEOREM 2.2. *Let ϕ_n be the linear mapping $\phi \equiv \phi_n$: $T_n \to L^2(V)$ defined on the basis elements* (2.17) *by the rule*

$$\phi(x^v) \equiv E_v, \qquad v \in V.$$

Then ϕ is an isomorphism of T_n onto $L^2(V)$.

Moreover, for $f \in T_n$ of the form

$$f = \bigotimes_{j=1}^n f_j, \qquad f_j \in X, \tag{2.19}$$

we have

$$\phi(f)(v) = \prod_{j=1}^n f_j(v_j), \tag{2.20}$$

where $v = (v_1, \ldots, v_n) \in V$.

PROOF. Since the set of functions E_v, $v \in V$, defines a basis of $L^2(V)$, ϕ is trivially an isomorphism of T_n onto $L^2(V)$.

Observe that, by definition, f_j is a function on Z/p. Formula (2.20) clearly holds whenever f is of the form $f = x^w$, $w \in V$. In general, write

$$f_j = \sum_{k=0}^{p-1} a_j(k) x_k, \qquad a_j(k) \in \mathbf{C},$$

and use the bilinearity of the tensor product to finish the proof of the theorem.

Consider the Fourier transform $F \equiv F_v$ of V. Since ϕ is a linear isomorphism,

$$F^\phi \equiv \phi^{-1} \circ F \circ \phi \tag{2.21}$$

is a linear isomorphism of T_n. The next theorem describes the action of F^ϕ on T_n. Recall that F_p denotes the Fourier transform on L_p. For the sake of completeness we state and prove the following known result.

THEOREM 2.3. $F = \bigotimes_1^n F_p$.

PROOF. Consider x^v, $v \in V$. By definition

$$\left(\bigotimes_1^n F_p \right) (x^v) = \bigotimes_1^n (F_p(x_j)),$$

and, by §I,

$$F_p(x_j) = p^{-1/2} \sum_{k=0}^{p-1} \exp\left(2\pi i \frac{1}{p} jk \right) x_k.$$

Thus,

$$\begin{aligned} \left(\phi \circ \left(\bigotimes_{j=1}^n F_p \right) \right) (x^v)(w) &= \prod_{j=1}^n F_p(x_{v_j})(w) \\ &= p^{-n/2} \prod_{j=1}^n \exp\left(2\pi i \frac{1}{p} v_j w_j \right) \\ &= p^{-n/2} \exp\left(2\pi i \frac{1}{p} \langle v, w \rangle \right). \end{aligned}$$

Since $(\phi \circ F)(x^v) = F(E_v)$ and

$$F(E_v)(w) = p^{-n/2} \exp(2\pi i (1/p) \langle v, w \rangle),$$

the theorem follows.

Consider $f \in T_n$ and write

$$f = \sum_{v \in V} a(v) x^v, \qquad a(v) \in \mathbf{C}.$$

We can use Theorem 2.3 to explicitly write $F^\phi(f)$. Let

$$y_j = p^{-1/2} \sum_{e=0}^{p-1} \exp\left(2\pi i \frac{1}{p} jk \right) x_k, \qquad 0 \le j < p. \tag{2.22}$$

For $v \in V$ we write

$$y^v = y_{v_1} \otimes \bigotimes y_{v_n}, \qquad v = (v_1, \ldots, v_n). \tag{2.23}$$

An immediate application of Theorem 2.3 gives the following result.

THEOREM 2.4. $F^{\phi}(f) = \sum_{v \in V} a(v) y^{v}$.

We come now to the MacWilliams identities. The exact weight enumerator of a linear code C on V, denoted P_C, is defined by

$$P_C \equiv P_C(x) \equiv \sum_{v \in C} x^{v}. \tag{2.24}$$

By definition of ϕ we have

$$\phi(P_C) = E_C \tag{2.25}$$

and, hence, by Theorem 2.1,

$$F^{\phi}(P_C) = o(C) p^{-n/2} P_{C^{\perp}}. \tag{2.26}$$

The MacWilliams identity for exact enumerator polynomials immediately follows from Theorem 2.4 and is given by the next theorem.

THEOREM A. *If P_C is the exact enumerator polynomial of a linear code C on V, then*

$$P_C(y) = o(C) p^{-n/2} P_{C^{\perp}}(x),$$

where y is given by (2.22).

The exact weight enumerator polynomial P_C of the linear code C specifies the code uniquely but, involving as it does noncommuting variables, it is difficult to handle. A related polynomial, the complete weight enumerator polynomial, contains less information, but still reflects essential features of the code and has the advantage of involving commuting variables only.

We begin by a direct definition of the complete weight enumerator polynomial of a code. Consider a linear code C in $V \equiv V_n$ over Z/p. For any element $v = (v_1, \ldots, v_n) \in V$ and any k, $0 \leq k < p$, we set $w_k(v)$ equal to the number of v_j, $1 \leq j \leq n$, satisfying $v_j \equiv k \bmod p$. The complete weight enumerator polynomial, $W \equiv W_C$, of C is defined by setting

$$W_C(x) = \sum_{v \in C} x^{w(v)},$$

where $x^{w(v)} = x_0^{w_0(v)} \cdots x_{p-1}^{w_{p-1}(v)}$.

We observe that $W_C(x)$ is a homogeneous polynomial of degree n in the p commuting variables $x_0, \ldots, x_{p-1}$. Also, if C is a self-dual code, then n must have been even.

Let us now define the complete weight enumerator polynomial in terms of the exact weight enumerator polynomial. Consider the vector space defined by

$$T \equiv \sum_{m \geq 0} \bigoplus T_m.$$

We briefly review the definition of the tensor algebra over X and how it is isomorphic to the polynomial algebra over $\mathbf{C}$ in p noncommuting variables.

For $m \geq 1$ the monomials of degree m, x^{v}, $v \in V_m$, form a basis of T_m. Take $v \in V_l$ and $u \in V_m$, $l, m \geq 1$, and define the product $x^{v} \cdot x^{u}$ by the rule

$$x^{v} \cdot x^{u} = x^{w}, \tag{2.27}$$

where $w = (v, u) \in V_{l+m}$. Extending (2.27) to a product on the vector space

$$\sum_{m \geq 1} \bigoplus T_m \tag{2.28}$$

by linearity and the distributive law determines a unique algebra structure on (2.28). Since $T_0 \equiv \mathbf{C}$, this algebra product extends to an algebra product on T.

Suppose the algebra T is given as above. Consider the ideal I of T generated by the relations

$$x_j x_k = x_k x_j, \qquad 0 \leq j, k < p. \tag{2.29}$$

I is homogeneous relative to the decomposition of T, given by (2.26), in the sense that

$$I = \sum_{m \geq 0} \bigoplus I_m, \tag{2.30}$$

where $I_m = I \cap T_m$. Note $I_0 = I_1 = (0)$.

It follows that the quotient algebra T/I is isomorphic to $\mathbf{C}[x_0, \ldots, x_{p-1}]$, the polynomial algebra over $\mathbf{C}$ in the commuting variables $x_0, \ldots, x_{p-1}$, and as vector spaces,

$$T/I = \sum_{m \geq 0} \bigoplus T_m / I_m. \tag{2.31}$$

We call T/I the full symmetric algebra of X.

Consider the natural map η of T_n onto T_n/I_n. Let P_C be the exact enumerator polynomial of the linear code C in $V = V_n$. Then $P_C \in T_n$. The complete weight enumerator polynomial of C, denoted W_C, is defined by setting

$$W_C = \eta(P_C).$$

The MacWilliams identity for the complete weight enumerator polynomial of a linear code immediately follows from Theorem A.

THEOREM B. *Let C be a linear code and W_C its complete weight enumerator polynomial. Then,*

$$W_C(y) = o(C) p^{-n/2} W_{C^\perp}(x),$$

where y is given by (2.22).

III. The algebra of the Fourier transform. A prime p is fixed for the remainder of this section. We also set $L_m \equiv L(Z/m)$, $m \geq 1$. The Fourier transform of L_m is denoted by F_m.

As a prelude to Gleason's results, we now relate the Fourier transform to the algebras introduced in the previous section.

Take a fixed integer $n \geq 1$. Let F denote the Fourier transform of $V \equiv V_n$, and let ϕ be the linear isomorphism from T_n onto $L^2(V)$ defined in Theorem 2.2. Consider the linear isomorphism $F^\phi \equiv \phi^{-1} \circ F \circ \phi$ of T_n. A typical element in I_n is the sum of elements of the form $f(x)(x_j x_k - x_k x_j) g(x)$, where $f, g \in T$, of proper degrees. Applying F^ϕ to this element, by Theorem 2.4, implies $f(y)(y_j y_k - y_k y_j) g(y)$, where y is given by (2.22). Expanding this, we easily see that this latter element is in I_n. Thus,

$$F^\phi(I_n) \subset I_n \tag{3.1}$$

and F induces a linear homomorphism of the vector space T_n/I_n. We denote the induced linear isomorphism of T_n/I_n by $F(n)$.

The Fourier transform of T/I, denoted by F_S, is defined by

$$F_S = \sum_{n\geq 0} \bigoplus F(n), \tag{3.2}$$

where $F(0)$ is the identity mapping. The definition of tensor products immediately implies the next result.

THEOREM 3.1. *F_S is an algebra homomorphism of $S = T/I$ and is uniquely determined by its action on the free generators $x_0, \ldots, x_{p-1}$ of S. The rule for this action is*

$$F_S x_j = \frac{1}{\sqrt{p}} \sum_{e=0}^{p-1} \exp\left(2\pi i \frac{1}{p} jk\right) x_k, \qquad 0 \leq j, k < p. \tag{3.3}$$

We introduce at this time two other important algebra homomorphisms of S. Since $x_0, \ldots, x_{p-1}$ freely generate S, it suffices to define the homomorphism action on these generators.

We define the algebra homomorphisms R_S and U_S of S by the formulas

$$R_S x_j \equiv x_{j+1}, \tag{3.4}$$

$$U_S x_j \equiv \exp(2\pi i j/p) x_j, \tag{3.5}$$

where $0 \leq j < p$. If $j = p - 1$ in (3.4), then $j + 1 = p$ is set equal to 0.

THEOREM 3.2. $F_S R_S F_S^{-1} = U_S$.

PROOF. By Definitions (3.3) and (3.4) we have

$$F_S R_S x_j = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \exp\left(2\pi i \frac{1}{p}(j+1)k\right) x_k,$$

and by Definition (3.5),

$$\begin{aligned} U_S F_S x_j &= \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \exp\left(2\pi i \frac{1}{p} jk\right) U_S x_k \\ &= \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \exp\left(2\pi i \frac{1}{p} jk\right) \exp\left(2\pi i \frac{1}{p} k\right) x_k \\ &= F_S R_S x_j, \end{aligned}$$

which proves the theorem.

The algebra $T/I \equiv S$ is too 'big' for our purposes, in a sense described below. We now define other algebras upon which a Fourier transform acts. The first of these was introduced in [1], and we briefly outline the results needed.

Consider the vector space

$$L \equiv \sum_{m\geq 0} \bigoplus L_m \tag{3.6}$$

and the linear mapping of L,

$$F_L \equiv \sum_{m \geq 0} \bigoplus F_m. \tag{3.7}$$

We call F_L the Fourier transform of L.

The following two theorems can be found in [**1**].

ALGEBRA THEOREM. *Up to isomorphism, L admits exactly three algebra structures, denoted by L^α, $x = 1, 2, 3$, satisfying:*

(1) *if $f \in L_m$ and $g \in L_n$, then $fg \in L_{m+n}$;*

(2) *L^α has no zero divisors; and*

(3) *F_L is an algebra homomorphism of L^α.*

Consider the action of F_L on L_j, $j = 1, 2, 3$. A direct computation shows that, up to constant multiple, there exist unique elements

$$z_j \in L_j, \qquad j = 1, 2, 3, \tag{3.8}$$

satisfying

$$F_L(z_1) = z_1, \quad F_L(z_2) = -z_2, \quad F_L(z_3) = iz_3. \tag{3.9}$$

REPRESENTATION THEOREM. *The algebra L^α is generated by the elements z_1, z_2 and z_3. The homomorphism of algebras π^α: $\mathbf{C}[Z_1, Z_2^2, Z_3^3] \to L^\alpha$, defined by requiring $\pi^\alpha(Z_j^j) \equiv z_j$, $j = 1, 2, 3$, induces an isomorphism $\mathbf{C}[Z_1, Z_2^2, Z_3^3]/p_\alpha \cong L^\alpha$, where we can take*

$$p_1 = Z_3^6 + Z_2^6, \quad p_2 = Z_3^6 + Z_1^4 Z_2^2 + Z_2^6, \quad p_3 = Z_3^6 + Z_1^4 Z_2^2.$$

In L^α the set of monomials given by

$$z^a = z_1^{a_1} z_2^{a_2} z_3^{a_3}, \qquad a = (z_1, a_2, a_3),\ a_j \geq 0, \tag{3.10}$$

spans the vector space L. Thus, z^a, where $m = a_1 + a_2 + a_3$, spans the subspace L_m, $m \geq 1$, of L^α. Moreover, since F_L is an algebra homomorphism of L, we have

$$F_L(z^a) = (-1)^{a_2 \cdot a_3} z^a. \tag{3.11}$$

For each $m \geq 1$, a basis $B(m)$ of L_m can be defined inductively, consisting of monomials z^a, $m = a_1 + a_2 + a_3$. Let $B(1) \equiv \{z_1\}$. Suppose a basis $B(m-1)$ of L_{m-1} has been constructed. We define $B(m)$ to be the set of functions of L_m given by

$$B(m) = \begin{cases} \{z_1 B(m-1), z_2^{m/2}\}, & m \text{ even}, \\ \{z_1 B(m-1), z^{(m-3)/2} \cdot z_3\}, & m \text{ odd}. \end{cases} \tag{3.12}$$

It follows from the discussion in [**1**] that $B(m)$ is a basis of L_m.

Consider L_p as a subspace of the algebra L^α. The basis elements $x_0, \ldots, x_{p-1}$ of L_p need not be free on L^α, in the sense that some polynomial in $x_0, \ldots, x_{p-1}$, $F(x)$, given by $f(x) = \sum a(v) x^v$, can be 0 in L^α with some $a(v) \neq 0$. In fact, some linear combination must already exist between the monomials $x_j x_k$, $0 \leq j, k < p$, and there are $p(p+1)/2$ such monomials which all lie in L_{2p}, a vector space of dimension $2p$.

Denote by $A^\alpha(p)$ the subalgebra of L generated by L_p. Then $x_0, \ldots, x_{p-1}$ generate $A^\alpha(p)$. The next result is an immediate consequence of F_L being an algebra homomorphism.

THEOREM 3.3. *The Fourier transform F_L maps $A^\alpha(p)$ onto itself and is uniquely determined by its action on the generators $x_0, \ldots, x_{p-1}$. This action is given by* (3.3).

Since the algebra $S \equiv T/I$ is freely generated by $x_0, \ldots, x_{p-1}$, we can define an algebra homomorphism Ψ^α of S onto $A^\alpha(p)$ by requiring $\Psi^\alpha(x_j) \equiv x_j$, $0 \leq j < p$. It follows automatically from Theorems 3.1 and 3.2 that the next result holds.

THEOREM 3.4. $F_L \Psi^\alpha = \Psi^\alpha F_S$.

Observe that Theorem 3.4 implies

$$(T_1) \qquad F_S(\ker \Psi^\alpha) \subset \ker \Psi^\alpha.$$

We would like the algebra homomorphisms R_S and U_S of S to induce, under Ψ^α, algebra homomorphisms of $A^\alpha(p)$. Necessary and sufficient conditions for this to occur are

$$(T_2) \qquad R_S(\ker \Psi^\alpha) \subset \ker \Psi^\alpha,$$

$$(T_3) \qquad U_S(\ker \Psi^\alpha) \subset \ker \Psi^\alpha.$$

From the discussion in [**1**] we can prove that, for at least one $\alpha = 1, 2, 3$, these conditions hold. Even more can be said, which we develop below.

For an integer $r \geq 1$ we define the subalgebra $L^\alpha[r]$ of L^α by

$$(3.13) \qquad L^\alpha[r] \equiv \sum_{m \geq 1} \bigoplus L_{rm}.$$

Observe that $A^\alpha(p) \subset L^\alpha[p]$.

On $L^\alpha[p]$ we define the linear homomorphisms R and U as follows. For each $m \geq 1$ we define the linear homomorphisms R_m and U_m of L_{pm} by

$$(3.14) \qquad (R_m f)(k) \equiv f(k - m),$$

$$(3.15) \qquad (U_m f)(k) \equiv \exp(2\pi i k/p) f(k),$$

where $f \in L_{pm}$ and $0 \leq k < pm$. Define R and U by

$$(3.16) \qquad R \equiv \sum_{m \geq 1} \bigoplus R_m,$$

$$(3.17) \qquad U \equiv \sum_{m \geq 1} \bigoplus U_m.$$

The analogue of Theorem 3.2 holds on $L^\alpha[p]$. We state it without proof.

THEOREM 3.5. $F_L R F_L^{-1} = U$ *on* $L^\alpha[p]$.

One of the algebras L^α is classical, in that it can be realized as the algebra of theta functions of period i relative to the standard lattice $Z + iZ$ in $\mathbf{C}$. The proof can be found in [**1**]. Let L^* denote this algebra. The proof of the following result can also be found in [**1**]. We adopt the notational rule that we replace α by $*$ when referring to concepts based on L^*.

HOMOMORPHISM THEOREM. *R and U are algebra homomorphisms of $L^*[p]$ whose actions on $x_0, \dots, x_{p-1}$ are given by* (3.4) *and* (3.5), *respectively.*

Observe that since F_L restricts to an algebra homomorphism of $L^*[p]$, by Theorem 3.5, U is an algebra homomorphism if and only if R is.

The following result immediately follows from the homomorphism theorem.

THEOREM 3.6. *$A^*(p)$ is R- and U-invariant. Moreover, we have*
(1) $R\Psi^* = \Psi^* R_S$,
(2) $U\Psi^* = \Psi^* U_S$,
where Ψ^* is the algebra homomorphism of S onto the subalgebra $A^*(p)$ of $L^*[p]$.

Consider the subalgebra $L^*[p^2]$ of $L^*[p]$. Clearly F_L restricts to an algebra homomorphism of $L^*[p^2]$. Also by the Homomorphism Theorem, R and U restrict to algebra homomorphisms of $L^*[p^2]$. Let

$$\Theta \equiv \{f \in L^*[p^2] : R(f) = U(f) = f\}. \tag{3.18}$$

THEOREM 3.7. *Θ is a subalgebra of L^* and*

$$F_L(\Theta) = \Theta. \tag{3.19}$$

PROOF. Since R and U are algebra homomorphisms, Θ is a subalgebra. Theorem 3.5 implies (3.19).

Θ plays a fundamental role in our approach to Gleason's theorems. Consider the subspace Θ_m of $L_{p^2 m}$, defined by

$$\Theta_m \equiv \Theta \cap L_{p^2 m}. \tag{3.20}$$

Since $L_{p^2 m}$ is both R- and U-invariant, it is easy to see that

$$\Theta = \sum_{m \geq 0} \bigoplus \Theta_m. \tag{3.21}$$

Θ satisfies the following properties:

(3.22) (1) Θ has no zero divisors.

(2) If $f \in \Theta_m$ and $g \in \Theta_m$, then $f \cdot g \in \Theta_{m+n}$. By Theorem 3.7 we also have

(3.23) (3) Θ is invariant under F_L.

Hence the restriction of F_L to Θ is an algebra homomorphism.

Thus, Θ has properties similar to those satisfying the Algebra Theorem. The following important theorem implies it is, in fact, the algebra L^* up to isomorphism. Thus, L^* contains, as a proper subalgebra, an isomorphic copy of itself.

THEOREM 3.8. *There exists an algebra isomorphism D of Θ onto L^* such that*
(1) $D(\Theta_m) \subset L_m$,
(2) $DF_L = F_L D$ *on* Θ.

Once we have the identification of L^* with the theta function algebra, an easy proof would be available. However, we outline a proof without resorting to this identification.

We begin by describing the functions $f \in \Theta_m$. Since $Uf = f$ we have

$$f(k) = \exp(2\pi i k/p) f(k), \qquad 0 \leq k < mp^2,$$

and, hence, f is "decimated"; i.e., $f(k) = 0$ unless

$$k = pj, \qquad 0 \leq j < mp, \tag{3.24}$$

in Z/p^2m. The condition $Rf = f$ implies f satisfies the periodicity property

$$f(k) = f(k + mp), \qquad 0 \leq k < p^2m. \tag{3.25}$$

It follows that f is completely determined by its values on the m points

$$0, p, zp, \ldots, (m-1)p. \tag{3.26}$$

Conversely, if $g \in L_m$ we can define a function $f \in \Theta_m$ by setting $f(jp) \equiv g(j)$, $0 \leq j < m$, and requiring

$$f(k + mp) \equiv f(k), \qquad 0 \leq k < mp^2,$$
$$f(k) \equiv 0, \qquad p/k.$$

This motivates the following definition. For $f \in \Theta_m$ define the function $D_m(f) \in L_m$ by the rule

$$D_m(f)(j) \equiv f(jp), \qquad 0 \leq j < m. \tag{3.27}$$

We have shown that D_m is a linear isomorphism from H_m onto L_m. Thus, setting

$$D \equiv \sum_{m \geq 1} \bigoplus D_m, \tag{3.28}$$

we have that D is a linear isomorphism from Θ onto L.

The Fourier transform F_L acts on L and, by Theorem 3.7, maps Θ onto itself. We will now see how F_L acts relative to D.

Consider $f \in \Theta_m$. Since $F_L(f) \in \Theta_m$, it is determined by its values on the m points (3.26). For $0 \leq j < m$ we have, using (3.24),

$$F_L(f)(pj) = \frac{1}{p\sqrt{m}} \sum_{k=0}^{pm-1} f(kp) \exp\left(2\pi i \frac{kj}{m}\right). \tag{3.29}$$

Write $k = k' + k''m$, $0 \leq k' < m$, $0 \leq k'' < p$, and substitute in (3.29) to obtain

$$(F_L f)(pj) = \frac{1}{\sqrt{m}} \sum_{k'=0}^{m-1} f(k'p) \exp\left(2\pi i \frac{k'j}{m}\right).$$

This implies

$$D_m(F_L(f)) = F_m(D_m(f)). \tag{3.30}$$

Therefore,

$$D \circ F_L = F_L \circ D \tag{3.31}$$

on Θ.

It remains to show that D is an algebra isomorphism of Θ onto L^*. There is a unique algebra structure on L, denoted $L\#$, such that D is an algebra isomorphism of Θ onto $L\#$. But conditions (3.22) and (3.23), along with the preceding discussion, imply $L\#$ satisfies the conditions of the Algebra Theorem. Thus, $L\# \cong L^\alpha$ for some $\alpha = 1, 2, 3$. Since Θ is a subalgebra of L^*, it follows from the Representation Theorem that $L\# \cong L^*$. This completes the proof of Theorem 3.8.

The subalgebra Θ of $L^*[p^2] \subseteq L^*$ and certain of its subalgebras will play important roles in the study of weight enumerator polynomials. We introduce these subalgebras in the following discussion.

By Theorem 3.8 we know there exist uniquely determined, up to constant multiple, elements $w_1 \in \Theta_1$, $w_2 \in \Theta_2$, $w_3 \in \Theta_3$ such that

$$F_L(w_1) = w_1, \quad F_L(w_2) = -w_2, \quad F_L(w_3) = iw_3,$$

and Θ is generated as an algebra by w_1, w_2, w_3.

Moreover, we can choose a basis of Θ_m from the monomials $w^a = w_1^a w_2^a w_3^a$, $a = (a_1, a_2, a_3)$, where $m = a_1 + 2a_2 + 3a_3$. Observe that the basis monomials always have $a_3 = 0$ or $a_3 = 1$. It follows from (3.11) that w^a is an eigenvector of F_L of eigenvalue ± 1 if $a_3 = 0$; in addition, if a_2 is even, the eigenvalue is ± 1.

Denote by Θ' the subalgebra of all $f \in H$ such that

$$F_L(f) = f. \tag{3.32}$$

Since each subspace Θ_m is F_L-invariant, we can write

$$\Theta' = \sum_{m \geq 0} (H_m \cap \Theta'). \tag{3.33}$$

A basis of $\Theta_m \cap \Theta'$ is given by the monomials

$$w_1^{a_1} w_2^{2a_2}, \qquad a_1, a_2 \in Z, \tag{3.34}$$

where $a_1 + 4a_2 = m$. We also have, by the Representation Theorem, that w_1, w_2 freely generate. This proves

THEOREM 3.9. *$\Theta' = \mathbf{C}[w_1, w_2^2]$, where w_1, w_2^2 freely generate.*

We need a slightly more general result.

THEOREM 3.10. *Choose $y_1 \in \Theta_1$ and $y_2 \in \Theta_4 \cap \Theta'$ such that y_1^4 and y_2 are linearly independent. Then $\Theta' = \mathbf{C}[y_1, y_2]$, where y_1, y_2 are free.*

PROOF. Θ_1 is one dimensional. Without loss of generality we can assume $y_1 = w_1$. By (3.32) w_1^4, w_2^2 define a basis of $\Theta_4 \cap \Theta'$ and we can write $w_2^2 = ay_1^4 + by_2$, $b \neq 0$. Replacing w_2^2 by $aw_1^2 + by_2$ in (3.32), we get a polynomial in w_1, y_2. This implies w_1, y_2 generate Θ'.

To prove w_1, y_2 freely generate, we write $y_2 = b^{-1}(w_2^2 - aw_1^4)$ and argue as in the Appendix.

Two subalgebras of Θ', defined by

$$\Theta'' = \left(\sum_{m \geq 0} \bigoplus \Theta_{2m} \right) \cap \Theta', \tag{3.35}$$

$$\Theta''' = \left(\sum_{m \geq 0} \bigoplus \Theta_{4m} \right) \cap \Theta', \tag{3.36}$$

play an important role in §IV.

Arguing as in the preceding theorem, we have the following two results.

THEOREM 3.11. *If $y_1 \in \Theta_2 \cap \Theta'$ and $y_2 \in \Theta_4 \cap \Theta'$ satisfy the property that y_1^2, y_2 are linearly independent, then y_1, y_2 freely generate and $\Theta'' = \mathbf{C}[y_1, y_2]$*

THEOREM 3.12. *Choose $y_1, y_2 \in \Theta_4 \cap \Theta'$ such that they are linearly independent. Then y_1, y_2 freely generate Θ'''.*

For the rest of this section, C denotes a self-dual code of length n over Z/p containing $1_n = (1, 1, \ldots, 1)$. The existence of a self-dual code on the vector space $V \equiv V_n$ implies n is even because, as is easy to show, as vector spaces $C \cong V/C^{\perp} \cong V/C$ and $n = 2 \dim C$. The condition $1_n \in C$ is equally important as a constraint on n The inner product $\langle 1_n, 1_n \rangle = n$ must vanish mod p and, hence, p divides n. In particular, if p is odd, then $2p$ divides n.

Let $W = W_C$ be the complete weight enumerator polynomial of C. In general, W is a homogeneous polynomial of degree n in the commuting variables $x_0, \ldots, x_{p-1}$. This means that each monomial on W has degree n divisible by 2 and p.

The condition $1_n \in C$ further restrains the form of W. If $a = (a_0, \ldots, a_{p-1})$ is a p-tuple of integers with $n = \sum_{j=0}^{p-1} a_j$, then the coefficient of the monomial $x^a \equiv x_0^{a_0} \cdots x_{p-1}^{a_{p-1}}$ in W is equal to the number of code words $v \in C$ having, for each j, $a \leq j < p$, exactly a_j components equal to j. Let S denote the subset of such elements in C. Then $1_n + S$ is the subset of C consisting of all code words $v \in C$ having, for each j, $0 \leq j < p$, exactly a_j components equal to $j + 1 \bmod p$. Thus, the coefficient of x^a on W equals the coefficient of the monomial $x_0^{a_{p-1}} x_1^{a_0} \cdots x_{p-1}^{a_{p-2}}$ in W. This implies W is invariant under the action of the shift R_S. We summarize in the following theorem what we have just shown about W.

THEOREM 3.13. *Let $W \equiv W_C$ be the complete weight enumerator polynomial of the self-dual code C in V_n containing $1_n = (1, \ldots, 1)$. Then W is a homogeneous polynomial of degree n satisfying:*

(1) *2 and p divide n;*
(2) $W = R_S(W)$;
(3) $W = F_S(W)$.

We note condition (3) is the MacWilliams identity, and (2) and (3) imply, by Theorem 3.2, that $W = U_S(W)$.

Certain subalgebras A', A'', A''' of S will now be introduced.

Let $S[p]$ be the subalgebra of S defined by

$$S[p] = \sum_{m \geq 0} \bigoplus T_{pm} / I_{pm},$$

and consider the subalgebra A' of $S[p]$ defined as the set of all $fS[p]$ satisfying

(1) $R_S(f) = U_S(f) = f$, and
(2) $F_S(f) = f$.

Consider the algebra homomorphism Ψ^*: $S \to L^*[p]$.

THEOREM 3.14. *Ψ^* maps A' onto Θ'.*

PROOF. Theorems 3.4 and 3.5, along with the definition of A', imply

$$\Psi^*(f) = U(\Psi^*(f)) = R(\Psi^*(f)) = F_L(\Psi^*(f))$$

whenever $f \in A'$. We are done if we can show $\Psi^*(f) \in L^*[p^2]$ for all $f \in A'$. It suffices to show that if $f \in A'$ is a monomial given by $f = x^v$, where $q = \sum_{j=0}^{p-1} v_j$

is divisible by p, then $\Psi^*(f) \in L^*[p^2]$. Since $\Psi^*(f) = x^v$, where the product x^v is taken in L^*, the theorem follows from observing that $\Psi^*(f) \in L_{pq} \subset L^*[p^2]$.

Consider the subalgebras

$$S[2p] \equiv \sum_{m \geq 0} \bigoplus T_{2pm}/I_{2pm}, \quad S[4p] \equiv \sum_{m \geq 0} \bigoplus T_{4pm}/I_{4pm},$$

$A'' \subset S[2p]$, and $A''' \subset S[4p]$ such that

(1) $2p$ divides n,

(2) $W = R_S(W)$.

The following theorem has a proof analogous to that of Theorem 3.14.

THEOREM 3.15. *Ψ^* maps A'' onto Θ'' and A''' into Θ'''.*

Gleason's theorems are related to the structure of the algebras A', A'', A''' in cases $p = 2$ or $p = 3$. We present these results in the next section.

IV. Gleason's theorems. Take $p = 2$ and consider the algebra homomorphism Ψ^*: $S \to L^*$. Arguing, as in the Appendix, it is easy to show that the elements $x_0, x_1 \in L_2 \subset L^*$ generate a free subalgebra of L^*. This implies Ψ^* is a monomorphism. We note that 2 is the only prime for which we will be so lucky.

THEOREM C. *The algebra homomorphism Ψ^* maps A' isomorphically onto Θ'. If $f, g \in S$ are defined by*

$$f = x_0^2 + x_1^2, \qquad g = x_0^2 x_1^2 (x_0^2 - x_1^2)^2,$$

then $f, g \in A'$ freely generate and $A' = \mathbf{C}[f, g]$.

PROOF. The above discussion implies Ψ^* is an algebra monomorphism of A' into Θ'. We want to prove Ψ^* maps A' onto Θ'. At the same time we specify free generators of A'. Since F_S maps

$$F_S(x_0) = \frac{1}{\sqrt{2}}(x_0 + x_1) \quad \text{and} \quad F_S(x_1) = \frac{1}{\sqrt{2}}(x_0 - x_1),$$

we have

$$F_S(x_0^2 + x_1^2) = x_0^2 + x_1^2, \quad F_S(x_0 x_1 (x_0^2 - x_1^2)) = x_0 x_1 (x_0^2 - x_1^2).$$

It follows that $f, g \in A'$.

Note. $x_0 x_1 (x_0^2 - x_1^2)$ is not R_S-invariant and, hence, does not belong to A'.

Let $y_1 \equiv \Psi^*(f)$ and $y_2 \equiv \Psi^*(g)$. Since f^4, g are linearly independent and Ψ^* is an isomorphism, y_1, y_2 satisfy the hypothesis of Theorem 3.10. This implies they freely generate Θ', and f, g freely generate A', which completes the proof of the theorem.

Since $W \equiv W_C \in A'$, whenever C is a self-dual code over $Z/2$, we have proved Gleason's theorem for the case $p = 2$.

GLEASON'S THEOREM FOR $p = 2$. *Let C be a self-dual code over $Z/2$ and W its complete weight enumerator polynomial. Then $W \in \mathbf{C}[f, g]$ where $f = x_3^2 + x_1^2$ and $g = x_0^2 x_1^2 (x_0^2 - x_1^2)^2$.*

We now consider the case $p = 3$ and take a self-dual linear code C on $V \equiv V_n$ satisfying $1_n \in C$. It is well known that 12 divides n and, hence, $W \equiv W_C$ lies in A'''. Gleason's theorem describes the structure of A'''.

We begin by noting that the algebra homomorphism Ψ^*: $A''' \to \Theta'''$, is not a monomorphism. Let K be the kernel of Ψ^* on A'''. The description of A''' will be of a more complicated nature than the corresponding description of A' in the $p = 2$ case. From our approach the reason for this is the existence of the nontrivial kernel K.

We require the following notation. Let

$$a \equiv x_0^3 + x_1^3 + x_2^3, \quad p \equiv 3x_0x_1x_2, \quad b \equiv x_0^3x_1^3 + x_0^3x_2^3 + x_1^3x_2^3, \tag{4.1}$$

and

$$\begin{aligned} &\alpha_{12} = a(a^3 + 8p^3), \quad \beta_6 = a^2 - 12b, \quad \nu_{18} = a^6 - 20a^3p^3 - 8p^6, \\ &\delta_{36} = p^3(a^3 - p^3) = -\frac{1}{64}(\nu_{18}^2 - \alpha_{12}^3). \end{aligned} \tag{4.2}$$

A direct computation shows that, under the action of F_S, we have

$$a \to \frac{1}{\sqrt{3}}(a + 2p), \quad p \to \frac{1}{\sqrt{3}}(a - p), \quad b \to -b + \frac{1}{9}(a^2 + ap + p^2), \tag{4.3}$$

from which we infer that the action of F_S has the following effect:

$$\alpha_{12} \to \alpha, \qquad \beta_6^2 \to \beta_6^2, \qquad \alpha_{36} \to \alpha_{36}, \tag{4.4}$$

$$\beta_6 \to -\beta_6, \qquad r_{18} \to -r_{18}. \tag{4.5}$$

By (4.4) it follows that $\alpha_{12}, \beta_6^2, \alpha_{36}$ lie in A''' and they can be shown to freely generate.

THEOREM 4.1. *$A''' = \mathbf{C}[\alpha_{12}, \beta_6^2] \oplus K$, where K is the kernel of Ψ^* in A'''.*

PROOF. Clearly, $\Psi^*(a), \Psi^*(p)$ are elements in Θ_1. Since Θ_1 is one dimensional and F_L acts by the identity mapping on Θ_1, we have

$$\Psi^*(p) = \mu \cdot \Psi^*(a), \quad \mu \in C, \qquad F_L(\Psi^*(a)) = \Psi^*(a).$$

By (4.3) we determine $\mu = (-1+\sqrt{3})/2$. This implies $\Psi^*(\alpha_{12}) = (1+8U^2)\Psi^*(a)^4 \neq 0$, so $\Psi^*(\alpha_{12}) \in \Theta_4 \cap \Theta'$. Let $y_1 = \Psi^*(a)^2$, $y_2 = \Psi^*(\beta_6)$. Then $F_L(y_1) = y_1$, $F_L(y_2) = -y_2$, which, by the Appendix, implies y_1, y_2 freely generate. Thus, y_1^2, y_2^2 are linearly independent in $\Theta_4 \cap \Theta'$ and, by Theorem 3.12, freely generate Θ'''. This completes the proof of the theorem.

Consider a polynomial $f(x_0, x_1, x_2)$ on A'''. Since $f(x_0, x_1, x_2)$ is R- and F_S^2-invariant, where F_S^2 is given by the permutation of variables $x_0 \mapsto x_0$, $x_1 \mapsto x_2$, $x_2 \mapsto x_1$, we have that $f(x_0, x_1, x_2)$ is a symmetric polynomial in x_0, x_1, x_2. In addition, $f(x_0, x_1, x_2)$ is U-invariant. The above remarks imply that f is also invariant under the transformations $x_j \mapsto e^{2\pi i/3}x_j$ for each $j = 0, 1, 2,$. Thus, $f(x_0, x_1, x_2)$ is a symmetric polynomial in x_0^3, x_1^3, x_2^3. The theory of elementary symmetric polynomials implies we can write $F(x_0, x_1, x_2)$ as a polynomial on a, p^3, b.

We let $f(x_0, x_1, x_2) \equiv f'(a, p^3, b)$. The degree of each monomial $x^r = x_0^{r_0}x_1^{r_1}x_2^{r_2}$ appearing in $F(x_0, x_1, x_2)$ is divisible by 12. This implies that a monomial $a^{s_0}p^{3s_1}b^{s_2}$, which appears as a term in $f'(a, p^3, b)$, must satisfy $4/s_0 + 3s_1 + 2s_2$.

The algebra A''' can be described as the space of all polynomials $f'(a, p^3, b)$ in the linear span of monomials $a^{s_0}p^{3s_1}b^{s_2}$ satisfying

$$4/s_0 + 3s_1 + 2s_2, \tag{4.6}$$

which are invariant under the transformations given by (4.3).

We want to describe A''' and we know that $A''' = \mathbf{C}[\alpha_{12}, \beta_6^2] \oplus K$, where K is the kernel of Ψ^* in A'''. Hence, we begin by giving a characterization of K.

Let K' be the collection of all polynomials $f'(a, p^3, b) \in \mathbf{C}[a, p^3, b]$ such that

$$\gamma_{18} \cdot f(a, p^3, b) \in A''' . \tag{4.7}$$

In particular, we observe that because $F_S(\gamma_{18}) = -\gamma_{18}$, we have $F_S(f(a, p^3, b)) = -f(a, p^3, b)$.

THEOREM 4.2. $K = \gamma_{18} \cdot K'$.

PROOF. From $\gamma_{18} = a^6 - 20a^3p^3 - 8p^6$, it follows that

$$\psi^*(\gamma_{18}) = (1 - 20u^3 - 8u^6)\Psi^*(a),$$

where $u = (-1 + \sqrt{3})/2$. A direct calculation shows that $1 - 20u^3 - 8u^6 = 0$. This implies $\gamma_{18}K' \subset K$.

Consider $k(a, p^3, b)K$ and let $k'(a, b) = k(a, u^3a^3, b)$. Then

$$k'(\Psi^*(a), \Psi^*(b)) = k(\Psi^*(a), \Psi^*(p^3), \Psi^*(b)) = 0,$$

which implies, since $\Psi^*(a)$, $\Psi^*(b)$ are freely generating, that $k'(a, b) = 0$. Thus, $(ua - p) | k(a, p^3, b)$ in $\mathbf{C}[a, p, b]$.

Since $k(a, p^3, b)$ is invariant under the action, $p \to wp$, $w = \exp(2\pi i/3)$, it follows that $ua - wp$, $ua - w^2p$ are factors of $k(a, p^3, b)$. Thus, since $ua - p$, $ua - wp$, $ua - w^2p$ are relatively prime, we have $u^3a^3 - p^3 = (ua - p)(ua - wp)(ua - w^2p)$ is a factor of $k(a, p^3, b)$.

Consider the factor $ua - wp$. Since $k(a, p^3, b)$ is invariant under F_S, we have $F_S(ua - wp)$ is a factor of $k(a, p^3, b)$. This implies, by a direct calculation, that $va - p$, $v = (-1 - \sqrt{3})/2$, is a factor of $k(a, p^3, b)$. Arguing as above, we have

$$\gamma_{18} = (-8)(u^3a^3 - p^3)(v^3a^3 - p^3)$$

is a factor of $k(a, p^3, b)$. This completes the proof of the theorem.

The final stage in the proof of Gleason's theorem when $p = 3$ is to describe K'. We quickly outline how this is done. For $f(a, p^3, b) \in K'$ we have $F_S(f) = -f$. Also, each monomial in $f(a, p^3, b)$, $a^{s_0}p^{3s_1}b^{s_2}$, has the property that $(s_0 + 3s_1 + 2s_2)/2$ is odd.

Arguing as in the remarks leading to the description of A''' in Theorem 4.1, we can prove

THEOREM 4.3. *If* $f(a, p^3, b) \in K'$ *then*

$$f(a, p^3, b) = \beta_6 g(\alpha_{12}, \beta_6^2) + \gamma_{18} f'(a, p^3, b),$$

where $f'(a, p^3, b) \in A'''$.

We come now to the main theorem in the case $p = 3$.

THEOREM D. $A''' = \mathbf{C}[\alpha_{12}, \beta_6^2, \delta_{36}] \oplus \beta_6\gamma_{18}\mathbf{C}[\alpha_{12}, \beta_6^2, \delta_{36}]$, *where* $\alpha_{12}, \beta_6^2, \delta_{36}$ *freely generate.*

PROOF. Assume $\alpha_{12}, \beta_6^2, \delta_{36}$ freely generate. Also, the sum on the right is trivially a direct sum contained in A'''.

Consider $f(a,p^3,b) \in A'''$. Without loss of generality we assume that $f(a,p^3,b)$ is homogeneous in x_0, x_1, x_2 of degree m. Thus, each monomial $a^{s_0}p^{3s_1}b^{s_2}$ occurring in $f(a,p^3,b)$ satisfies $m = 3s_0 + 9s_1 + 6s_2$. We use induction on m.

By Theorem 4.1 we can write

$$f(a,p^3,b) = g(\alpha_{12},\beta_6^2) + k(a,p^3,b),$$

where $k(a,p^3,b) \in K$. Applying Theorem 4.2 we can write

$$k(a,p^3,b) = \gamma_{18}k'(a,p^3,b),$$

where $k'(a,p^3,b) \in K'$. Theorem 4.3 implies

$$k'(a,p^3,b) = \beta_6 g'(\alpha_{12},\beta_6^2) + \gamma_{18}f'(a,p^3,b),$$

where $f'(a,p^3,b) \in A'''$. The degree of f' as a polynomial in x_0, x_1, x_2 is strictly less than m, which implies by induction that

$$f'(a,p^3,b) \in \mathbf{C}[\alpha_{12},\beta_6^2,\delta_{36}] \oplus \beta_6\gamma_{18}\mathbf{C}[\alpha_{12},\beta_6^2,\delta_{36}].$$

Putting all this together we get

$$f(a,p^3,b) = g(\alpha_{12},\beta_6^2) + \gamma_{18}^2 f'(a,p^3,b) + \gamma_{18}\beta_6 g'(\alpha_{12},\beta_6^2).$$

Since $\gamma_{18}^2 = -64\delta_{36} + \alpha_{12}^3$, the theorem is proved.

GLEASON'S THEOREM FOR $p = 3$. *Let C be a self-dual code over $Z/3$ and W its weight enumerator polynomial. Suppose $\mathbf{1} \in C$. Then*

$$W \in \mathbf{C}[\alpha_{12},\beta_6^2,\delta_{36}] \oplus \beta_6\gamma_{18}\mathbf{C}[\alpha_{12},\beta_6^2,\delta_{36}].$$

Appendix. The structure of the algebra L^*, especially the relationship of this structure to the action of the algebra homomorphism F_L, is the central tool in the second part of this work. In this Appendix we review the results we need.

We begin with the direct sum decomposition for L^*, $L^* = \sum_{m\geq 0}\bigoplus L_m$, and the elements $z_1 \in L_1$, $z_2 \in L_2$, $z_3 \in L_3$, where

$$F_L(z_1) = z_1, \quad F_L(z_2) = -z_2, \quad F_L(z_3) = iz_3,$$

and $L^* = \mathbf{C}[z_1,z_2,z_3]$. The elements z_1, z_2, z_3 do not freely generate.

Consider the action of F_L on L^*. Denote the subspace of L^* spanned by the eigenvectors of F_L having eigenvalues ± 1 by M and the eigenvalue one subspace of F_L on L^* by M'. Then M is a subalgebra of L^*, and M' is a subalgebra of M. In fact, we have $M = M' \oplus z_2M'$, where M' is generated freely by z_1, z_2^2, and M is generated freely by z_1, z_2.

These results, along with those mentioned below, are immediate consequences of the following tables. Let $M_n \equiv L_n \cap M$, $M'_m \equiv L_m \cap M'$.

Subspace	Basis	
	$+1$	-1
M_1	z_1	
M_2	z_1^2	z_2
M_3	z_1^3	z_1z_2
M_4	z_1^4, z_2^2	$z_1^2z_2$
M_5	$z_1^5, z_1z_2^2$	$z_1^3z_2$
M_6	$z_1^6, z_1^2z_2^2$	$z_1^4z_2, z_2^3$
M_7	$z_1^7, z_1^3z_2^2$	$z_1^5z_2, z_1z_2^3$
M_8	$z_1^8, z_1^4z_2^2, z_2^4$	$z_1^6z_2, z_1^2z_2^3$.

In general, we distinguish four cases for M_m:

	$+$	$-$
$m \equiv 0 \bmod 4$	$z_1^m, z_1^{m-4}z_2^2, \ldots, z_2^{m/2}$	$z_1^{m-2}z_2, z_1^{m-6}z_2^3, \ldots, z_1^2 z_2^{(m-2)/2}$
$m \equiv 1 \bmod 4$	$z_1^m, z_1^{m-4}z_2^2, \ldots, z_1 z_2^{(m-1)/2}$	$z_1^{m-2}z_2, z_1^{m-6}z_2^3, \ldots, z_1^3 z_2^{(m-3)/2}$
$m \equiv 2 \bmod 4$	$z_1^m, z_1^{m-4}z_2^2, \ldots, z_1^2 z_2^{(m-2)/2}$	$z_1^{m-2}z_2, z_1^{m-6}z_2^3, \ldots, z_2^{m/2}$
$m \equiv 3 \bmod 4$	$z_1^m, z_1^{m-4}z_2^2, \ldots, z_1^3 z_2^{(m-3)/4}$	$z_1^{m-2}z_2, z_1^{m-6}z_2^3, \ldots, z_1 z_2^{(m-1)/2}$

From the pattern established by these tables, statements (1)–(3) easily follow.

(1) $M \cap \sum_{m\geq 0} \bigoplus L_{2m}$ is generated by z_1^2, z_2.

(2) $M' \cap \sum_{m\geq 0} \bigoplus L_{2m}$ is generated by z_1^2, z_2^2.

(3) $M' \cap \sum_{m\geq 0} \bigoplus L_{4m}$ is generated by z_1^4, z_2^2.

We consider generalizations of these results, which are continually used in this work. Although more general results can be appealed to, the grading in L^*, i.e., the direct sum decomposition of L^*, makes the proofs especially simple.

Let $y_2 \in M_2$ and $y_4, y_4' \in M_4'$ in the following statements:

(1) If z_1^2, y_2 are linearly independent, then z_1, y_2 freely generate M.

(2) If z_1^4, y_4 are linearly independent, then z_1, y_4 freely generate M'.

(3) If $y_2 \in M'$ and y_2^2, y_4 are linearly independent, then y_2, y_4 freely generate $M' \cap \sum_{m\geq 0} \bigoplus L_{2m}$.

(4) If y_4, y_4' are linearly independent, they freely generate $M' \cap \sum_{m>0} \bigoplus L_{4m}$.

We prove only the first statement. The others follow in much the same way. Write $y_2 = cz_1^2 + dz_2$, where, by assumption, $d \neq 0$. M is generated freely by z_1, z_2, and since every monomial $z_1^{a_1}z_2^{a_2}$ can be written $z_1^{a_1}z_2^{a_2} = z_1^{a_1}[(y_2 - cz_1^2)d^{-1}]^{a_2}$ upon expanding, we have M generated by z_1, y_2.

Consider any polynomial $f(z_1, y_2)$ satisfying $f(z_1, y_2) = 0$. Write

$$f(z_1, y_2) = \sum_{r=0}^{N} f_r(z_1) y_2^r,$$

where we assume $f_N(z_1) \neq 0$. Replace y_2 by $cz_1^2 + dz_2$ in this expression and form

$$g(z_1, z_2) = f(z_1, cz_1^2 + dz_2) = \sum_{r=0}^{N} f_r(z_1)(cz_1^2 + dz_2)^r.$$

The highest power of z_2 which occurs upon expanding is z_2^N and its coefficient is $f_N(z_1)d^N$. Since $d \neq 0$, z_1, z_2 freely generate, and $g(z_1, z_2) = 0$, we must have $f_N(z_1) = 0$, a contradiction. Thus, z_1, y_2 freely generate.

REFERENCES

1. L. Auslander and R. Tolimieri, *Algebraic structures for* $\bigoplus \sum_{n \geq 1} L^2(Z/n)$ *compatible with the finite Fourier transform,* Trans. Amer. Math. Soc. **244** (1978), 263–272.
2. ——, *Is computing with the finite Fourier transform pure or applied mathematics,* Bull. Amer. Math. Soc. (N.S.) **1** (1979), 847–897.
3. A. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities,* Actes Congrès Internat. Math., Vol. 3, Gauthier-Villars, Paris, 1971, pp. 211–215.
4. F. J. MacWilliams, *A theorem on the distribution of weights in a systematic code,* Bell System Tech. J. **42** (1963), 79–84.
5. F. J. MacWilliams, C. Mallows and N. Sloane, *Generalizations of Gleason's theorem on weight enumerators of self-dual codes,* IEEE Trans. Inform. Theory **18** (1972), 794–805.
6. F. MacWilliams and N. Sloane, *The theory of error correcting codes,* North-Holland, Amsterdam, 1978.
7. J. P. Serre, *A course in arithmetic,* Graduate Texts in Math., Springer-Verlag, New York.
8. N. J. Sloane, *Weight enumerators of codes,* Combinatorics (M. Hall, Jr. and J. H. van Lont, eds.), Reidel, Dordrecht, 1975, pp. 115–142.
9. ——, *Error-correcting codes and invariant theory,* Amer. Math. Monthly **84** (1977), 82–107.
10. R. E. Blahut, *Theory and practice of error control codes,* Addison-Wesley, Reading, Mass., 1983.

DEPARTMENT OF ELECTRICAL ENGINEERING, CITY COLLEGE OF NEW YORK, CUNY, NEW YORK, NEW YORK 10031