Binary Codes Which Are Ideals in the Group Algebra of an Abelian Group

By Mrs. F. J. MacWILLIAMS

(Manuscript received January 13, 1970)

A cyclic code is an ideal in the group algebra of a special kind of Abelian group, namely a cyclic group. Many properties of cyclic codes are special cases of properties of ideals in an Abelian group algebra.

A character of an Abelian group G of order v is, for our purposes, a homomorphism of G into the group of vth roots of unity over $GF(2)$. If G is cyclic with generator x, the character is entirely determined by what it does to x; this effect is kept, and the characters are discarded. If G is not cyclic it is necessary to rehabilitate the characters. Without them the notation is impossible; with them one can prove a number of theorems which reduce in the special case to well-known properties of cyclic codes. Moreover the writer thinks that the general proof is often easier and more suggestive than the proof for the special case. To support this point of view we produce a new theorem, which of course also applies to cyclic codes.

I. INTRODUCTION

A cyclic code is an ideal in the group algebra of a special kind of Abelian group, namely a cyclic group. Many properties of cyclic codes are special cases of properties of ideals in an Abelian group algebra.

A character of an Abelian group G of order v is, for our purposes, a homomorphism of G into the group of vth roots of unity over $GF(2)$. If G is cyclic with generator x, the character is entirely determined by what it does to x; this effect is kept, and the characters are discarded. If G is not cyclic, it is necessary to rehabilitate the characters. Without them the notation is impossible; with them one can prove a number of theorems which reduce in the special case to well-known properties of cyclic codes. Moreover the writer thinks that the general proof is often easier and more suggestive than the proof for the special case. To support this point of view we produce a new theorem, which of course also applies to cyclic codes.

The plan of this paper is as follows: Section II contains a summary of the properties of ideals in an Abelian group algebra. Section III contains a description of the group characters; the reader is assured (and we hope reassured) that an effort has been made to point out the analogies with the cyclic case. In Section IV the characters are extended to the group algebra. This section contains the general cases of several familiar theorems, for example, the dimension of the code, a lower bound on its minimum distance, the Mattson–Solomon mapping, and the identification of the dual code. In Section V the structure of product codes is examined for the general case. Section VI contains the new theorem (which needs too much notation to be explained here) and the special case of this theorem which applies to cyclic codes. The Appendix contains an illustrative example of the smallest possible nontrivial case.

II. GENERAL PROPERTIES OF ABELIAN GROUP ALGEBRAS

Let G be a finite Abelian group of odd order v; the group operation is written as multiplication.

Let $R = FG$ be the group algebra of G over the field $F = GF(2)$. R consists of finite sums

$$A = \sum_{g \varepsilon G} a_g g, \qquad a_g \varepsilon F.$$

In FG we have two operations, addition and multiplication, defined as follows:

$$A + B = \sum_{g \varepsilon G} (a_g + b_g)g,$$

and for $f \varepsilon G$,

$$fA = \sum_{g \varepsilon G} a_g fg = \sum_{g \varepsilon G} a_{f^{-1}g} g.$$

This implies

$$AB = \sum_{h \varepsilon G} \sum_{gf=h} a_g b_f h. \tag{1}$$

We use 1 to denote the unit of G, and $\mathbf{1}$, $\mathbf{0}$ to denote the unit and zero of FG.

From the first of these operations we see that FG has the structure of a vector space F^v of dimension v over F. $\mathbf{0}$ is the zero vector and $\mathbf{1}$ is the vector $(1\ 0\ 0\ \cdots\ 0)$.

An ideal $\mathcal{A}$ in FG is defined as follows

$$\mathcal{A} \text{ is a linear subspace of } F^v,$$

$$A \varepsilon \mathcal{A} \Rightarrow gA \varepsilon \mathcal{A} \quad \text{for all} \quad g \varepsilon G.$$

From the general theory of semi-simple group algebras,[1] we know that FG is a principal ideal ring; that is, every ideal is of the form

$$\mathcal{A} = \{rA, r \varepsilon FG\} \quad \text{for some element} \quad A \varepsilon FG.$$

We denote the ideal with generator A by $\langle A \rangle$. In fact every ideal has an idempotent generator; $\mathcal{A} = \langle N \rangle$, where $N = \sum_{g \varepsilon G} \eta_g g$ has the properties:

$$N^2 = N,$$

$$r \varepsilon \mathcal{A} \Leftrightarrow rN = r. \tag{2}$$

Since the ground field is $GF(2)$, and G is commutative

$$N^2 = \sum_{g \varepsilon G} \eta_g g^2,$$

so that

$$N = \sum_{g \varepsilon G} \eta_g g$$

is idempotent if and only if $\eta_g = \eta_{g^2}$ for all $g \varepsilon G$.

FG is the direct sum of its minimal ideals,

$$FG = \langle \theta_1 \rangle + \cdots + \langle \theta_t \rangle,$$

and every ideal in FG is the direct sum of a subset of these minimal ideals.[1] The idempotents, θ_i, of the minimal ideals are called primitive idempotents and have the additional properties

$$\sum_{i=1}^{t} \theta_i = 1, \tag{3}$$

$$\theta_i \theta_j = 0, \qquad i \neq j, \tag{4}$$

$$\langle \theta_i \rangle \cap \langle \theta_j \rangle = 0, \qquad i \neq j.$$

Every idempotent in FG is the sum of primitive idempotents. Since we are over $GF(2)$ the sum of idempotents is idempotent, and the set of all idempotents is a vector space I; $\theta_1, \cdots, \theta_t$ are a set of linearly independent basis elements for I, which is thus of dimension t.

We also define a set of "trivial" idempotents as follows:

Let $y_1 = 1 \varepsilon G$. Pick $g \varepsilon G$, $g \neq 1$, and set

$$y_2 = \{g, g^2, g^4, \cdots, g^{2^s}\}$$

where $g^{2^{s+1}} = g$ (this must happen since G is finite and of odd order). Pick $f \notin y_1 \cup y_2$ and define the set $y_3 = \{f, f^2, f^4, \cdots, f^{2^r}\}$. In this way G

is partitioned into disjoint classes, which we call cycles

$$G = y_1 \cup y_2 \cup y_3 \cdots . \tag{5}$$

Define $Y_i \varepsilon FG$ by

$$Y_i = \sum_{g \varepsilon y_i} g, \qquad \text{(for example, } Y_2 = g + g^2 + \cdots + g^{2^s}\text{)}.$$

The Y_i are the trivial idempotents. From equation (2) it is clear that every idempotent is the sum of trivial idempotents, and they are obviously linearly independent over F. Hence the trivial idempotents also form a basis for I over F. We have proved the following Lemma:

Lemma 1.1: The number of trivial idempotents is the same as the number of primitive idempotents, and each set is linearly dependent on the other; that is, there exists an invertible $t \times t$ matrix (m_{ij}) over F such that

$$\begin{bmatrix} \theta_1 \\ \vdots \\ \theta_t \end{bmatrix} = (m_{ij}) \begin{bmatrix} Y_1 \\ \vdots \\ Y_t \end{bmatrix}.$$

From a practical point of view it is desirable to find the θ_i. The algorithm for doing this is as described in Ref. 2, except that the group is no longer cyclic. Briefly, we form linear combination of the Y_i in a systematic way until we find t idempotents which satisfy equations (3) and (4). An example is given in Appendix A.

III. GROUP CHARACTERS

Since we shall make extensive use of the characters of the group and the group algebra, we give a brief account of their properties.

For our purposes, a character of G is a homomorphism ψ of G into the vth roots of unity over $GF(2)$. These vth roots of unity lie in an extension field $GF(2^s)$ in which the expression $z^v - 1$ splits into linear factors. They form a cyclic subgroup of the (multiplicative) group of non-zero elements of this field.

Formally

$$\psi(f)\psi(g) = \psi(fg). \tag{6}$$

Hence

$$\psi(1) = 1$$

(the unit of G on the left and of $GF(2^s)$ on the right) and

$$\psi(g^{-1}) = [\psi(g)]^{-1}.$$

If G is a cyclic group of order v, with generator x, a character is a map $x \to \beta$, where β is a vth root of unity. In this case one usually does not distinguish between the character and the value it assigns to x. We define multiplication of characters by

$$(\phi\psi)(g) = \phi(g)\psi(g).$$

Under this operation, the characters form a group, $\mathfrak{X}$. The unit of $\mathfrak{X}$, called the principal character ψ_1, is the map

$$g \to 1 \quad \text{for all} \quad g \in G.$$

The group G and the character group $\mathfrak{X}$ are isomorphic in many ways. We construct a particular isomorphism and use it henceforth.

Theorem 2.1: (Reference 3) The Abelian group G has a unique decomposition as the direct product of cyclic groups of prime power order,

$$G = G_1 \times G_2 \times \cdots \times G_s, \qquad G_i \text{ cyclic of order } p_i^{s_i}.$$

(The primes p_i are not necessarily district.)

Pick a generator x_i for G_i, and a fixed primitive p^{s_i}th root of unity, α_i. Let ψ_{x_i} be the character defined on the generators by

$$\psi_{x_i}(x_i) = \alpha_i, \qquad \psi_{x_i}(x_j) = 1, \qquad i \neq j.$$

By equation (6) this is sufficient to define ψ_{x_i} on any $g \in G$. We may by equation (7) define $\psi_{x_i}^2$

$$\psi_{x_i}^2(g) = [\psi_{x_i}(g)]^2.$$

Lemma 2.2: If φ is any character of G, then ϕ can be represented in the form

$$\varphi = \prod_{i=1}^{s} \psi_{x_i}^{a_i}.$$

Proof: Let $\varphi(x_i) = \beta$. Then

$$\beta^{p_i^{s_i}} = \varphi(x_i)^{p_i^{s_i}} = \varphi(x_i^{p_i^{s_i}}) = \varphi(1) = 1.$$

Thus β is a power of α_i, say $\beta = \alpha_i^{a_i}$. We then see that

$$\varphi(\prod_i x_i^{b_i}) = \prod_i \varphi(x_i^{b_i}) = \prod \alpha_i^{a_i b_i}.$$

Hence

$$\varphi = \prod_i \psi_{x_i}^{a_i}.$$

Set $a = \prod_i x_i^{a_i}$ and denote the character $\varphi = \prod_i \psi_{x_i}^{a_i}$ by φ_a. We then have

Lemma 2.3: The mapping $a \Leftrightarrow \varphi_a$ as defined above is an isomorphism between G and $\mathfrak{X}$.

We also use ψ_a to mean the character corresponding to a in this isomorphism.

Lemma 2.4: $\varphi_a(b) = \varphi_b(a)$, *and* $\varphi_{a^{-1}}(b) = \varphi_a(b^{-1})$.

Proof: Let

$$a = x_1^{a_1} \cdots x_s^{a_s}, \qquad b = x_1^{b_1} \cdots x_s^{b_s}.$$

Then

$$\varphi_a(b) = \prod_i [\varphi_{x_i}(b)]^{a_i} = \prod_i \prod_j [\varphi_{x_i}(x_j^{b_j})]^{a_i},$$

$$= \prod \alpha_i^{a_i b_i} = \varphi_b(a).$$

The second statement is proved in a similar way.

We shall need the following theorem which is well known, so the proof is omitted. The skeptical reader may easily construct an elementary proof by using the properties of the roots of unity.

Theorem 2.5:

$$(i) \qquad \sum_{\psi \in \mathfrak{X}} \psi(g) = \begin{cases} v & \text{if} \quad g = 1, \\ 0 & \text{otherwise}. \end{cases}$$

$$(ii) \qquad \sum_{g \in G} \psi(g) = \begin{cases} v & \text{if} \quad \psi = \psi_1, \\ 0 & \text{otherwise}. \end{cases}$$

If G is cyclic, both parts of this theorem reduce to

$$\sum_{i=0}^{v-1} \beta^i = \begin{cases} v & \text{if} \quad \beta = 1, \\ 0 & \text{otherwise}. \end{cases}$$

Let $\mathfrak{X}(g)$ be a matrix whose columns are labeled by the characters ψ and rows by the group elements g. The entry in row ψ, column g is $\psi(g)$. An example is given in Appendix A.

Lemma 2.6: $\mathfrak{X}(g)\mathfrak{X}^T(g^{-1}) =$ *diagonal* $[vv \cdots v] = vI$. *Hence* $\mathfrak{X}(g)$ *is invertible.*

Proof: A typical entry on the main diagonal is

$$\sum_{g \in G} \psi(g)\psi(g^{-1}) = \sum_{g \in G} \psi(1) = v, \quad \text{by Theorem 2.5 } (ii).$$

A typical off-diagonal entry is

$$\sum_{g \in G} \psi_a(g)\psi_b(g^{-1}) = \sum_{g \in G} \psi_g(a)\psi_g(b^{-1}),$$
$$= \sum_{g \in G} \psi_g(ab^{-1}) = 0, \text{ by Theorem 2.5 } (ii) \text{ since } a \neq b.$$

IV. CHARACTERS OF THE GROUP ALGEBRA

If G is a cyclic group of order v, with generator x, and $A = A(x)$ an element of FG (that is, a polynomial of degree less than v in x) then $A(\beta)$ is the value of the character $x \to \beta$ on A. In the general case, for $A = \sum_{g \in G} a_g g$ in FG, we extend the character to the elements of the group algebra by

$$\psi(A) = \sum_{g \in G} a_g \psi(g).$$

Using the notation of Theorem 2.1 and those that follow, we could write an element of FG as a sum of terms of the form $x_1^{j_1} x_2^{j_2} \cdots x_s^{j_s}$, $0 \leq j_i < p^{s_i}$. A is a polynomial in the variables $x_1, \cdots, x_s$ with restrictions on the degree of each variable. A character is a mapping $A(x_1 \cdots x_s) \to A(\beta_1, \cdots, \beta_s)$ where β_i is a (p^{s_i})th root of unity. As pointed out in the introduction, there are certain advantages to using this polynomial notation as little as possible.

If G is cyclic, we know that

$$A(x)B(x)\mid_{x=\beta} = AB(x)\mid_{x=\beta}.$$

Analogously for the general case (and with the same proof, using equation (1)),

$$\psi(AB) = \psi(A)\psi(B).$$

If G is cyclic, it is usually the case that $A(\beta_1)A(\beta_2) \neq A(\beta_1\beta_2)$. There is however a vital exception, namely $A(\beta)^2 = A(\beta^2)$. Similarly, in the general case

$$\psi\varphi(A) \neq \psi(A)\varphi(A), \qquad \text{but}$$

Lemma 3.1: $\psi(A)^2 = \psi^2(A) = \psi(A^2)$.

Proof:

$$[\psi(A)]^2 = [\sum_{g \in G} a_g \psi(g)]^2 = \sum_{g \in G} a_g \psi(g)^2,$$
$$= \sum_{g \in G} a_g \psi(g^2).$$

A cyclic code is an ideal in a cyclic group algebra. It is frequently described as the set of polynomials which vanish on a certain prescribed set S of vth roots of unity:

$$\mathcal{A} = \{A(x): A(\beta) = 0, \beta \in S\}. \tag{7}$$

Similarly, we can characterize an ideal in the group algebra of an Abelian group as the set of elements of FG which vanish at a prescribed set of characters:

$$\mathcal{A} = \{A \in FG: \psi(A) = 0, \psi \in S\}. \tag{7'}$$

From Lemma 3.1 we see that in the general case, as in the special case, the maximal set $\hat{S}$ corresponding to a particular ideal must have a special form; in fact it is the union of sets $\{\psi, \psi^2, \psi^4, \cdots\}$.

It is well known that the dimension of the cyclic code associated by equation (7) with the set $\hat{S}$ is the number of vth roots of unity not contained in $\hat{S}$, that is, the number of nonzeros of the code. Similarly in the general case. The following two theorems are proved in Reference 4; we repeat the proofs here for convenience, and also supply an example in Appendix A. Let $g_1, g_2, \cdots, g_r$ be the elements of G. Associate with the element A the $v \times v$ matrix $(a_{g_i^{-1}g_j})$. The entry in row i column j is the coefficient of g_j in g_iA. The ideal $\mathcal{A} = \langle A \rangle$ is generated as a subspace of $R = F^v$ by the rows of the matrix $(a_{g_i^{-1}g_j})$. The dimension of this ideal is the rank of this matrix.

Theorem 3.2: The dimension of the ideal $\langle A \rangle$ is the number of characters ψ such that $\psi(A) \neq 0$.

Proof: The matrix $\mathfrak{X}^T(g^{-1})(a_{g_i^{-1}g_j})\mathfrak{X}(g)$ has the same rank as $(a_{g_i^{-1}g_j})$, since by Lemma 2.6 $\mathfrak{X}(g)$ is invertible. A typical entry of the product $(a_{g_i^{-1}g_j})\mathfrak{X}(g)$ is of the form

$$n_{ij} = \sum_{g_k \in G} a_{g_i^{-1}g_k} \psi_{g_i}(g_k).$$

Now

$$\sum_{g_k \in G} a_{g_i^{-1}g_k} \psi_{g_j}(g_k) = \sum_{g_k \in G} a_{g_k} \psi_{g_j}(g_i g_k) = \psi_{g_j}(g_i) \cdot \psi_{g_j}(A).$$

Thus

$$n_{ij} = \psi_{g_j}(g_i)\psi_{g_j}(A).$$

In the product $\mathfrak{X}(g^{-1})(n_{ij})$ the diagonal terms are of the form

$$\psi_{g_j}(A) \sum_{\psi \in \mathfrak{X}} \psi(g^{-1})\psi(g) = v\psi_{g_j}(A).$$

The off-diagonal terms are of the form

$$\psi_{g_i}(A) \sum_{\psi \in \mathfrak{X}} \psi(g^{-1})\psi(f) = 0.$$

Thus

$$\mathfrak{X}(g^{-1})^T(a_{g_i^{-1}g_j})\mathfrak{X}(g) = \text{diagonal } [\psi_{g_1}(A), \psi_{g_2}(A), \cdots \psi_{g_v}(A)],$$

and the rank of the matrix $(a_{g_i^{-1}g_j})$ is the number of characters for which $\psi(A) \neq 0$.

We call these characters the non-zeros of the ideal $\langle A \rangle$.

Let D be the $m \times v$ submatrix of $\mathfrak{X}(g)^T$ whose columns are indexed by the group elements and rows by the m characters for which $\psi(A) = 0$. If $\mathbf{a} = (a_1, a_2, \cdots, a_v)$ is a vector of $\langle A \rangle$, then $D\mathbf{a}^T = 0$. If D contains no set of t linearly independent columns, the minimum weight in $\langle A \rangle$ is at least $t + 1$. This is the extension of the BCH bound for cyclic codes. It is generally a very weak lower bound.

Theorem 3.3: (The Mattson-Solomon mapping—see Reference 5.)

(i) *If* $A = \sum a_g g$, then $a_f = \frac{1}{v} \sum_{\psi \in \mathfrak{X}} \psi(A)\psi(f^{-1})$.

(ii) *If* $va_g = \sum_{\psi \in \mathfrak{X}} \beta_g \psi(g^{-1})$, then $\psi_h(A) = \beta_h$.

Proof:

(i)
$$\sum_{\psi \in X} \psi(A)\psi(f^{-1}) = \sum_{\psi \in \mathfrak{X}} \sum_{g \in G} a_g \psi(g)\psi(f^{-1}),$$
$$= \sum_{g \in G} a_g \sum_{\psi \in \mathfrak{X}} \psi(gf^{-1}) = va_f .$$

(ii)
$$v\psi_h(A) = \sum_{g \in G} a_g \psi_h(g),$$
$$= \sum_{g \in G} \sum_{\psi_f \in \mathfrak{X}} \beta_g \psi_f(g^{-1})\psi_h(g),$$
$$= \sum_{g \in G} \beta_g \sum_{\psi_f \in \mathfrak{X}} \psi_f(g^{-1})\psi_h(g),$$
$$= \sum_{g \in G} \beta_g \sum_{f \in G} \psi_g(f^{-1})\psi_g(h),$$
$$= \sum_{g \in G} \beta_g \sum_{f \in G} \psi_g(f^{-1}h),$$
$$= \beta_h .$$

Corollary 3.4: A is uniquely determined by the set of values $\psi(A)$.

We divide the group G as in equation (5) into cycles corresponding to the trivial idempotents of FG, and divide the character group $\mathfrak{X}$ into similar classes by the isomorphism of Lemma 2.3.

$$G = y_1 \cup y_2 \cup \cdots \cup y_t , \tag{5}$$

$$\mathfrak{X} = \Psi_1 \cup \Psi_2 \cup \cdots \cup \Psi_t . \tag{8}$$

$y_1 = 1$ and Ψ_1 contains only the principal character ψ_1. By Lemma 3.1 if $\psi(A) \neq 0$ for some $\psi \in \Psi_i$, then $\psi(A) \neq 0$ for all $\psi \in \Psi_i$. The non-zeros of A are a union of cycles Ψ_i.

The minimal ideals have the smallest possible dimension, so that by Theorem 3.2 the non-zeros of a minimal ideal are, if possible, the characters in a single class Ψ_i. (This is in fact possible; an explicit construction is given in Section V.) If θ_i is the idempotent of this minimal ideal we may define θ_i by the property

$$\psi(\theta_i) = \begin{cases} 1 & \psi \in \Psi_i , \\ 0 & \text{otherwise.} \end{cases} \tag{9}$$

Theorem 3.5: The dimension of the ideal $\langle \theta_i \rangle$ *is* $|\Psi_i|$, *the number of elements in* Ψ_i.

Since every ideal in FG is the direct sum of minimal ideals, every idempotent is of the form $C = \sum_i \epsilon_i \theta_i$, $i = 0$ or 1. The dimension of C is $\sum \epsilon_i \, |\Psi_i|$. From equations (2) and (4) we have immediately:

Theorem 3.6: If C_1, C_2 *are idempotents with non-zeros* Φ_1 *and* Φ_2, *and* $\Phi_1 \subset \Phi_2$, *then* $\langle C_1 \rangle$ *is a subideal of* $\langle C_2 \rangle$.

The dual code of $\langle N \rangle$ is the set of vectors $b_1, \cdots, b_v$ such that $\sum_{i=1}^{v} a_i b_i = 0$ for all vectors $a_1, \cdots, a_v$ in $\langle N \rangle$. The dimension of the dual code is $v - \dim \langle N \rangle$.

If N is idempotent, the dimension of $\langle (1 + N) \rangle$ is $v - \dim \langle N \rangle$. This follows at once from the fact that $1 = \sum_{i=1}^{t} \theta_i$. For $A = \sum a_g g$, set $A^* = \sum a_g g^{-1}$.

Theorem 3.7: The dual code of $\langle N \rangle$ *is* $\langle (1 + N)^* \rangle$.

Proof: Let $\sum b_{g^{-1}} g \in \langle (1+N)^* \rangle$; then $\sum b_g g \in \langle (1+N) \rangle$. Since $N(1+N) = 0$, for any $\sum a_g g \in \langle N \rangle$ we have

$$(\sum a_g g)(\sum b_g g) = 0.$$

From the coefficient of 1 in this product

$$\sum a_g b_{g^{-1}} = 0.$$

Therefore, $\langle (1 + N)^* \rangle$ is contained in the dual code of $\langle N \rangle$, and has dimension $v - \dim \langle N \rangle$. Thus it is the dual code.

V. QUASI-CYCLIC AND PRODUCT CODES

Let H be a proper subgroup of order u of the Abelian group G; and let

$$G = k_1H \cup k_2H \cup \cdots \cup k_wH \qquad (k_1 = 1, v = uw)$$

be the decomposition of G into cosets of H. In this section we suppose the coordinate places in FG to be arranged in the order

$$k_1h_1, k_1h_2, \cdots, k_1h_u, k_1h_1, \cdots, k_2h_u, \cdots, k_wh_1, \cdots, k_wh_u.$$

Let $\mathfrak{a}$ be an ideal of FG, and denote by $\mathfrak{a}_i$ the part of $\mathfrak{a}$ which lies in the coordinate places $k_ih_1, \cdots, k_ih_u$. $\mathfrak{a}_1$ is an ideal of FH (usually several repetitions of an ideal of FH), and since $k_i\mathfrak{a}_1 = \mathfrak{a}_i$ the codes $\mathfrak{a}_i$ are all repetitions of $\mathfrak{a}_1$. Each vector of $\mathfrak{a}$ consists of w vectors of $\mathfrak{a}_1$; these are not in general the same vector, and some of them may be zero. If H is a cyclic group, $\mathfrak{a}$ has the structure of a quasi-cyclic code. Since G contains cyclic subgroups of order p for every prime p which divides v, $\mathfrak{a}$ may have this structure in several different ways.

We make the additional assumption that G is the direct product $G = H \times K$ of subgroups H, K. This means that $H \cap K = 1$, and each element of G can be expressed uniquely as $g = kh$, $k \in K$, $h \in H$. The character group $\mathfrak{X}$ is correspondingly a direct product

$$\mathfrak{X} = \mathfrak{X}_H \times \mathfrak{X}_K,$$

where $\mathfrak{X}_H$, $\mathfrak{X}_K$ are the images of H, K under the isomorphism of Lemma 2.3. Every character can be expressed uniquely as

$$\psi = \varphi_H\varphi_K, \qquad \varphi_H \in \mathfrak{X}_H, \qquad \varphi_K \in \mathfrak{X}_K.$$

We shall need the following result.

Lemma 4.1: $\varphi_H\varphi_K(hk) = \varphi_H(h)\varphi_K(k)$.

Proof: From the isomorphism of Lemma 2.3,

$$\varphi_H(k) = 1, \qquad \varphi_K(h) = 1.$$

Let $A = \sum_{h \in H} a_h h$, $B = \sum_{k \in K} b_k k$ be idempotents in the group algebras FH, FK. Let Φ_H, Φ_K be the non-zeros of A, B respectively. Φ_H, Φ_K correspond to cycles of $\mathfrak{X}_H$, $\mathfrak{X}_K$ which are, of course, also cycles of $\mathfrak{X}$.

The Kronecker product of matrices, M, N, is denoted by $M \dot{\times} N$ (an example is given in Appendix A).

Theorem 4.2: (*i*) *$C = AB$ is an idempotent of FG.*

(*ii*) *The codes $\langle C \rangle$ is the direct product of codes $\langle A \rangle$, $\langle B \rangle$.*
(*iii*) *The non-zeros of $\langle C \rangle$ are $\varphi_H \varphi_K$, $\varphi_H \in \Phi_H$, $\varphi_K \in \Phi_K$.*
(*iv*) *The minimum distance of $\langle C \rangle$ is the product of those of $\langle A \rangle$, $\langle B \rangle$.*

Proof: (*i*) It is clear that $C = \sum_{k \in K} b_k k \sum_{h \in H} a_h h$ is idempotent.

(*ii*) The first row of the Kronecker product

$$(a) \dot{\times} (b) = (a_{h_q^{-1} h_r}) \dot{\times} (b_{k_s^{-1} k_t})$$

consists of the coefficients of C. The second row contains the coefficients of $h_1 C$, and the $(u + 1)$st row the coefficients of $k_2 C$. Without further notation, we see that the rows of this Kronecker product generate the code $\langle C \rangle$ as a subspace of F^v.

(*iii*) $\mathfrak{X}(G) = \mathfrak{X}_H(h) \dot{\times} \mathfrak{X}_K(k)$. By Theorem 3.2, the non-zeros of C are given by

$$[\mathfrak{X}_H(h^{-1}) \dot{\times} \mathfrak{X}_K(k^{-1})]^T[(a) \dot{\times} (b)][\mathfrak{X}_H(H) \dot{\times} \mathfrak{X}_K(K)]$$
$$= \mathfrak{X}_H^T(h^{-1})(a)\mathfrak{X}_H(H) \dot{\times} \mathfrak{X}_K^T(k^{-1})(b)\mathfrak{X}_K(K).$$

The triple matrix products are diagonal matrices with ones in the places corresponding to $\varphi \in \Phi_H$ ($\varphi \in \Phi_K$) and zeros elsewhere. Their Kronecker product is a diagonal matrix with ones in the places corresponding to $\varphi_H \varphi_K$, $\varphi_H \in \Phi_H$, $\varphi_K \in \Phi_K$.

(*iv*) This is a well-known property of direct product codes.

Given an idempotent C of FG we would like to know how, if possible, to find subgroups H, K such that $G = H \times K$, and $C = AB$. The following theorem is sometimes helpful.

Theorem 4.3: Let Ψ be the set of non-zeros of C; suppose Ψ can be expressed as the product of two sets of cycles Φ_1, Φ_2 where $\Phi_1 \in \mathfrak{X}_H$, $\Phi_2 \in \mathfrak{X}_K$ and $\mathfrak{X} = \mathfrak{X}_H \times \mathfrak{X}_K$. (Consequently, $G = H \times K$.)

Then $C = AB$, where A, B are idempotents in FH and FK, with non-zeros Φ_1, Φ_2; consequently the code $\langle C \rangle$ is the direct product of codes $\langle A \rangle$ and $\langle B \rangle$.

Proof:

$$C = \sum_{kh \in G} a_{kh} kh = k_1 \sum_{h \in H} a_{k_1 h} h + k_2 \sum_{h \in H} a_{k_2 h} h + \cdots + k_w \sum_{h \in H} a_{k} f_h h.$$

By Theorem 3.3 (*i*)

$$a_{k_i h} = \sum_{\psi \in \mathfrak{X}} \psi(C) \psi(k_i^{-1} h^{-1}) = \sum_{\varphi_1 \in \Phi_1} \sum_{\varphi_2 \in \Phi_2} \varphi_1 \varphi_2(k_i h^{-1}),$$

since by hypothesis

$$\psi(C) = \begin{cases} 1 & \text{if} \quad \psi = \varphi_1\varphi_2 \\ 0 & \text{otherwise.} \end{cases}$$

$$= \sum_{\varphi_2 \varepsilon \Phi_2} \varphi_2(k_i^{-1}) \sum_{\varphi_1 \varepsilon \Phi_1} \varphi_1(h^{-1})$$

by Lemma 4.1. Set $a_h = \sum_{\psi \varepsilon \mathfrak{X} H} \alpha_h \psi(h^{-1})$, where

$$\alpha_h = \begin{cases} 1 & \psi \varepsilon \Phi_1 \\ 0 & \text{otherwise.} \end{cases}$$

Set $A = \sum_{h \varepsilon H} a_h h$; then

$$\psi(A) = \alpha_h = \begin{cases} 1 & \psi \varepsilon \Phi_1 \\ 0 & \text{otherwise} \end{cases}$$

by Lemma 3.5 (*ii*). Define B similarly for K. Then A, B are idempotents in FH, FK, and $C = AB$.

If H, K are cyclic groups whose orders are relatively prime, then G is also cyclic. The codes $\langle A \rangle$, $\langle B \rangle$ are cyclic codes in FH, FK respectively, and $\langle C \rangle$ is a cyclic code in FG.

This special case has been thoroughly investigated by Burton and Weldon[6] and Goethals.[7]

The extension to direct products of more than two subgroups is theoretically obvious, but rather hard to visualize. An example for the cyclic case is given in Appendix 2.

VI. A NEW THEOREM

Everything in this paper so far is a natural extension of known results about cyclic codes. This section is not; the special case of Theorem 5 for G cyclic is new and interesting (at least the writer thinks so).

The primitive idempotents θ_i of FG have been defined by the property

$$\psi(\theta_i) = \begin{cases} 1 & \psi \varepsilon \Psi_i \, , \\ 0 & \psi \notin \Psi_i \, . \end{cases} \tag{10}$$

We recall that the trivial idempotents are defined by the property

$$Y_i = \sum_{g \varepsilon G} a_g g, \; a_g = \begin{cases} 1 & g \varepsilon y_i \, , \\ 0 & g \notin y_i \, . \end{cases} \tag{11}$$

Since these properties look remarkably symmetrical, one expects to find some symmetry in the matrix (m_{ij}) (Lemma 1.1) which relates θ_i to Y_i. This in fact exists, as follows.

We recall that

$$A^* = \sum_{g \varepsilon G} a_g g^{-1}.$$

Theorem 5.1:

$$\theta_i = \sum_{k=1}^{t} r_k Y_k \leftrightarrow Y_i^* = \sum_{k=1}^{t} r_k \theta_k .$$

Proof: Let

$$\theta_i = \sum_{g \varepsilon G} b_g g$$

$$= \sum_{g \varepsilon G} \sum_{\psi \varepsilon \mathfrak{X}} \psi(\theta_i)\psi(g^{-1})g \quad \text{by Lemma 3.3 } i$$

(Note that $1/v = 1$ in characteristic 2.)

$$= \sum_{g \varepsilon G} \Big(\sum_{\psi \varepsilon \Psi_i} \psi(g^{-1})\Big)g \quad \text{by (10).}$$

From definition (8) of Ψ_i, we may suppose that $\Psi_i = \{\psi_f, \psi_{f^2}, \cdots, \psi_{f^{2^s}}\}$. Then the inner sum is

$$\psi_f(g^{-1}) + \psi_{f^2}(g^{-1}) + \cdots + \psi_{f^{2^s}}(g^{-1})$$

$$= \psi_g(f^{-1}) + \psi_g(f^{-2}) + \cdots + \psi_g(f^{-2^s}) \quad \text{by Lemma 2.4,}$$

$$= \psi_g(Y_i^*).$$

Thus

$$\theta_i = \sum_{g \varepsilon G} \psi_g(Y_i^*)g. \tag{12}$$

(This is the explicit construction for θ_i.) Now suppose

$$Y_i^* = \sum_{k=1}^{t} r_k \theta_k , \qquad r_k \varepsilon GF(2).$$

$$\psi_g(Y_i^*) = \sum_{k=1}^{t} r_k \psi_g(\theta_k),$$

$$\psi_g(\theta_k) = \begin{cases} 1, & g \varepsilon Y_k , \\ 0, & g \notin Y_k . \end{cases} \quad \text{from (9).}$$

Hence $\psi_{g_1}(Y_i^*) = r_1$, $\psi_g(Y_i^*) = r_k$ for all $g \varepsilon Y_k$. Substituting in equation (11), we obtain

$$\theta_i = r_1 + r_2 \sum_{g \varepsilon Y_2} g + \cdots + r_t \sum_{g \varepsilon Y_t} g,$$
$$= \sum_{i=1}^{t} r_i Y_i .$$

Let $\psi_k(Y_j)$ be the common value of $\psi(Y_j)$ for $\psi \,\varepsilon\, \Psi_k$. Equation (12) then becomes

$$\theta_i = \sum_{k=1}^{t} \psi_k(Y_i^*) Y_k ,$$
$$= \sum_{k=1}^{t} r_k Y_k . \tag{13}$$

With a slight change of notation, let

$$\theta_i = \sum_{k=1}^{t} m_{ik} Y_k .$$

Let P be a permutation matrix such that P acting on the column vector $(Y_1, Y_2, \cdots, Y_t)^T$ produces $(Y_1^*, Y_2^*, \cdots, Y_t^*)^T$.

Theorem 5.2:

$$(m_{ij})^2 = P.$$

Proof: By Theorem 5.1,

$$Y_i^* = \sum_{k=1}^{t} m_{ik}\theta_k = \sum_{k=1}^{t} m_{ik} \sum_{j=1}^{t} m_{kj} Y_j ,$$
$$= \sum_{j=1}^{t} \left(\sum_{k=1}^{t} m_{ik} m_{kj} \right) Y_j .$$

Hence

$$\sum_{k=1}^{t} m_{ik} m_{kj} = \begin{cases} 1 & Y_i^* = Y_j , \\ 0 & \text{otherwise.} \end{cases}$$

We give a brief description of the special case G cyclic of prime order p. FG is now the polynomial ring $R = F[x]/x^p + 1$. Let f be the order of 2 mod p. If $p - 1 = ef$, then

$$2 = g^e$$

for some generator g of the integers mod p. The trivial idempotents, other than 1, are of the form

$$x^i + x^{i \cdot 2} + x^{i \cdot 4} + \cdots + x^{i \cdot 2^{f-1}}.$$

Let σ be the automorphism of R induced by $x \to x^g$; define

$$X_0 = x + x^2 + x^4 + \cdots + x^{2^{f-1}}, \quad X_i = X_{i-1}\sigma, \quad i = 1, \cdots, e - 1.$$

Then

$$X_i = x^a + x^{a\cdot 2} + \cdots + x^{a\cdot 2^{f-1}}, \qquad a = g^i.$$

Since the trivial idempotents were previously called $Y_1, \cdots, Y_t$ we have changed notation; now

$$Y_1 = 1, \qquad Y_2 = X_0, \cdots, Y_t = X_{e-1}.$$

We rename the primitive idempotents correspondingly,

$$\theta_1 = J, \qquad \theta_2 = \eta_0, \cdots, \theta_t = \eta_{e-1}.$$

The characters of G are defined by

$$\psi_{x^k}(x) = \alpha^k,$$

where α is a primitive pth root of unity; thus η_i is defined by

$$\psi_{x^k}(\eta_i) = \begin{cases} 1 & \text{if} \quad k = g^{es+i}, \\ 0 & \text{otherwise.} \end{cases}$$

This may be rewritten as

$$\eta_i(\alpha^{g^{es+k}}) = \begin{cases} 1 & i = k, \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

In particular

$$J(\alpha^i) = \begin{cases} 1 & \alpha^i = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Hence

$$J = \sum_{i=0}^{p-1} x^i.$$

Write

$$\eta_i = m_i + \sum_{k=0}^{e-1} m_{ik} X_k ;$$

$$m_i = X_i^*(J) = f,$$

$$m_{ik} = X_i^*(\alpha^{es+k}).$$

Since $-1 = g^{ef/2}$ we have

$$X_i^* = \begin{cases} X_i , & f \quad \text{even}, \\ X_{i+e/2} & f \quad \text{odd}. \end{cases} \tag{15}$$

Now

$$\eta_i \sigma = f + \sum_{k=0}^{e-1} m_{ik} X_{k+1} ,$$

and

$$m_{ik} = X_i^*(\alpha^{g^{es+k}}) = X_{i-1}^*(\alpha^{g^{es+k+1}}),$$

by equation (14) and the definition of X_i . Hence

$$m_{ik} = m_{i-1,k+1} ,$$

and

$$\eta_i \sigma = f + \sum_{j=0}^{e-1} m_{i-1,j} X_j = \eta_{i-1} .$$

Set

$$\theta_0 = f + \sum_{k=0}^{e-1} m_k X_k ;$$

then

$$\theta_1 = \theta_0 \sigma^{e-1} = f + \sum_{k=0}^{e-1} m_{k+1} X_k .$$

Clearly

$$J = 1 + \sum_{k=0}^{e-1} X_k .$$

The matrix corresponding to the (m_{ij}) of Theorem 5.2 is of the form

$$\begin{pmatrix} 1 & \mathbf{J} \\ \mathbf{f}^T & M \end{pmatrix},$$

where **J**, **f** are now vectors of length e and

$$M = \begin{bmatrix} m_0 , & m_1 , & \cdots , & m_{e-1} \\ m_1 , & m_2 , & \cdots , & m_0 \\ m_{e-1} , & m_0 , & \cdots , & m_{e-2} \end{bmatrix}.$$

Let P be the permutation matrix which turns the column vector $(1, X_0, \cdots, X_{e-1})^T$ into $(1, X_0^*, \cdots, X_{e-1}^*)^T$. By equation (14)

$$P = I \quad \text{for} \quad f \text{ even},$$

$$P = \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0}^T & Q^{e/2} \end{bmatrix} \quad \text{for} \quad f \quad \text{odd}$$

where

$$Q = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix} \quad \text{of size} \quad (e-1) \times (e-1).$$

From Theorem 5.2 we have

$$\begin{bmatrix} 1 + ef, & \mathbf{J} + \mathbf{1}M \\ \mathbf{f}^T + M\mathbf{f}^T & \mathbf{f}^T\mathbf{1} + M^2 \end{bmatrix} = P.$$

For f even, $\mathbf{f}^T\mathbf{1}$ is an $e \times e$ matrix of zeros, hence

$$M^2 = I \quad \text{if } f \text{ is even};$$

for f odd, $\mathbf{f}^T\mathbf{1}$ is an $e \times e$ matrix of ones, which we denote by K.

$$M^2 = K + Q^{e/2} \quad \text{if } f \text{ is odd}.$$

The matrix M, which is symmetric and circulant in the wrong direction, can be made circulant in the usual way by multiplication by a suitable permutation matrix. Skipping the obvious details we have the following theorem.

Theorem 5.3: With η_i, X_i defined as above, and

$$\eta_0 = m_\infty + \sum_{i=0}^{e-1} m_k X_k ,$$

(i)

$$X_0^* = m_\infty + \sum_{i=0}^{e-1} m_k \eta_k .$$

(ii) Set

$$m(y) = m_0 + m_1 y + m_2 y^2 + \cdots + m_{e-1} y^{e-1},$$

$$m(y)^T = m_0 + m_{e-1} y + m_{e-2} y^2 + \cdots + m_1 y^{e-1}.$$

Then

(*i*) $$m_\infty = \begin{cases} 0 & f \text{ even}, \\ 1 & f \text{ odd}. \end{cases}$$

(*ii*) $$m(y)m(y)^T = 1 \mod y^e + 1, \quad f \text{ even},$$
$$= \sum_{i=0}^{e-1} y^i + y^{e/2}, \quad f \text{ odd}.$$

Theorem 5.3 has several interesting corollaries of which we mention one.

Let w be the weight (the number of non-zero coordinates) of $m(y)$. The following statements come from Theorem 5.3.

The weight of X_i = The dimension of $\langle \eta_i \rangle = f$.

The weight of η_i = The dimension of $\langle X_i \rangle = wf$, $f = 0(2)$, $wf + 1$, $f = 1(2)$.

Corollary 5.4: If $p = 2^k - 1$, $\langle X_i \rangle$ *is a* $(2^k - 1, 2^{k-1})$ code, with minimum weight $\leq k$.

Proof: For $p = 2^k - 1$, we have $f = k$. Clearly the minimum weight in $\langle X_i \rangle$ is bounded above by that of X_i, which is k.

The minimal ideal $\langle \eta_i \rangle$ is the dual of a Hamming code. Hence η_i (and every other non-zero code word) has weight $(p + 1)/2 = ef/2 + 1$.

Thus $w = e/2$, and the dimension of $\langle X_i \rangle$ is $(p + 1)/2$.

We can use Theorem 5.3 to discover some other remarkably poor cyclic codes; for example

$$p = 251, e = 16, f = 16, w = 9,$$
$$p = 1801, e = 72, f = 25, w = 39.$$

[After the completion of this paper, the writer discovered that Abelian Group Codes have also been investigated by Berman (KIBERNETIKA, vol. 3, no. 3, 1967) and by Paul Camion (to appear).]

VII. CONCLUSION

The writer regretfully admits that she has made no attempt whatsoever to find out whether general Abelian group codes are of any practical value. One obvious thing to do is to make a computer search; the algorithm for finding the primitive idempotents is quite easy to implement. Another direction of research is to look for a class of groups, not cyclic, which produce codes with some desirable practical properties.

VIII. ACKNOWLEDGMENTS

The writer is grateful to her colleagues, especially N. J. A. Sloane, for several excellent suggestions which greatly increased the clarity of this paper.

APPENDIX A

An Example of a Non-Cyclic Abelian Group

Let G be the group of order 9 which is the direct product of two groups of order 3. The elements of G are

$$1,\ x,\ x^2,\ y,\ xy,\ x^2y,\ y^2,\ xy^2,\ x^2y^2, \qquad x^3 = y^3 = 1.$$

Let α be a primitive third root of unity over $GF(2)$; then

$$1 + \alpha + \alpha^2 = 0.$$

The matrix $\mathfrak{X}(g)$ is:

	ψ_1	ψ_x	ψ_{x^2}	ψ_y	ψ_{xy}	ψ_{x^2y}	ψ_{y^2}	ψ_{xy^2}	$\psi_{x^2y^2}$
1	1	1	1	1	1	1	1	1	1
x	1	α	α^2	1	α	α^2	1	α	α^2
x^2	1	α^2	α	1	α^2	α	1	α^2	α
y	1	1	1	α	α	α	α^2	α^2	α^2
xy	1	α	α^2	α	α^2	1	α^2	1	α
x^2y	1	α^2	α	α	1	α^2	α^2	α	1
y^2	1	1	1	α^2	α^2	α^2	α	α	α
xy^2	1	α	α^2	α^2	1	α	α	α^2	1
x^2y^2	1	α^2	α	α^2	α	1	α	1	α^2

It is symmetric because the characters are written in the same order as the group elements to which they correspond; the argument does not use the symmetry of $\mathfrak{X}(g)$.

The trivial idempotents are

$Y_1 = 1;\ Y_2 = x + x^2;\ Y_3 = y + y^2;\ Y_4 = xy + x^2y^2;\ Y_5 = x^2y + xy^2.$

In order to find the primitive idempotents we need the multiplication table for the Y_i. This also is symmetric and we write only half of it.

	Y_2	Y_3	Y_4	Y_5
Y_2	Y_2	—	—	—
Y_3	$Y_4 + Y_5$	Y_3	—	—
Y_4	$Y_3 + Y_5$	$Y_2 + Y_5$	Y_4	—
Y_5	$Y_3 + Y_4$	$Y_2 + Y_4$	$Y_2 + Y_3$	Y_5

We have then

$$1 = Y_2 + (1 + Y_2); \qquad Y_3 = Y_3Y_2 + Y_3(1 + Y_2);$$
$$(1 + Y_3) = (1 + Y_3)Y_2 + (1 + Y_3)(1 + Y_2).$$

Thus

$$Y_3 = (Y_4 + Y_5) + (Y_3 + Y_4 + Y_5),$$
$$1 + Y_3 = (Y_2 + Y_4 + Y_5) + (1 + Y_2 + Y_3 + Y_4 + Y_5).$$
$$1 = Y_3 + (1 + Y_3) = (Y_4 + Y_5) + (Y_3 + Y_4 + Y_5)$$
$$+ (Y_2 + Y_4 + Y_5) + (1 + Y_2 + Y_3 + Y_4 + Y_5).$$

We multiply this equation by Y_4 and $(1 + Y_4)$:

$$Y_4 = (Y_2 + Y_3 + Y_4) + (Y_3 + Y_4 + Y_5) + (Y_2 + Y_4 + Y_5) + 0,$$
$$1 + Y_4 = (Y_2 + Y_3 + Y_5) + 0 + 0 + (1 + Y_2 + Y_3 + Y_4 + Y_5).$$

Finally,

$$1 = Y_4 + (1 + Y_4) = (Y_2 + Y_3 + Y_4) + (Y_3 + Y_4 + Y_5)$$
$$+ (Y_2 + Y_4 + Y_5) + (Y_2 + Y_3 + Y_5) + (1 + Y_2 + Y_3 + Y_4 + Y_5).$$

This is a decomposition of 1 into five mutually orthogonal idempotents, which are therefore the primitive idempotents. Set

$$A = Y_2 + Y_3 + Y_4 = x + x^2 + y + y^2 + xy + x^2y^2.$$

We use the table $\mathfrak{X}(g)$ to check that

$$\psi_x(A) = \psi_{x^2}(A) = \psi_y(A) = \psi_{y^2}(A) = \psi_{x^2y}(A) = \psi_{xy^2}(A) = 0$$
$$\psi_{xy}(A) = \psi_{x^2y^2}(A) = 1.$$

Hence

$$Y_2 + Y_3 + Y_4 = \theta_4 .$$

Similarly

$$Y_3 + Y_4 + Y_5 = \theta_3 ,$$

$$Y_2 + Y_4 + Y_5 = \theta_2 ,$$

$$Y_2 + Y_3 + Y_5 = \theta_5 ,$$

$$1 + Y_2 + Y_3 + Y_4 + Y_5 = \theta_1 .$$

The matrix $(a_{g_j^{-1}g_i})$ for the trivial idempotent Y_2 is

	1	x	x^2	y	xy	xy^2	y^2	xy^2	x^2y^2
1	0	1	1	0	0	0	0	0	0
x	1	0	1	0	0	0	0	0	0
x^2	1	1	0	0	0	0	0	0	0
y	0	0	0	0	1	1	0	0	0
xy	0	0	0	1	0	1	0	0	0
xy^2	0	0	0	1	1	0	0	0	0
y^2	0	0	0	0	0	0	0	1	1
xy^2	0	0	0	0	0	0	1	0	1
x^2y^2	0	0	0	0	0	0	1	1	0

To save space we write this as the Kronecker product

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \dot{\times} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} b & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & b \end{bmatrix}, \qquad b = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

and also write $\mathfrak{X}(g)$ as the Kronecker product.

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha \end{bmatrix} \dot{\times} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha \end{bmatrix} = \begin{bmatrix} a & a & a \\ a & \alpha a & \alpha^2 a \\ a & \alpha^2 a & \alpha a \end{bmatrix}, \qquad a = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha \end{bmatrix}.$$

$$\mathfrak{X}(g^{-1}) = \begin{bmatrix} a' & a' & a' \\ a' & \alpha^2 a' & \alpha a' \\ a' & \alpha a' & \alpha^2 a' \end{bmatrix}$$

where

$$a' = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha \\ 1 & \alpha & \alpha^2 \end{bmatrix}.$$

It is then easy to calculate that

$$\mathfrak{X}(g^{-1})(a_{g_i^{-1}g_i})\mathfrak{X}(g) = \begin{bmatrix} aba' & 0 & 0 \\ 0 & aba' & 0 \\ 0 & 0 & aba' \end{bmatrix}$$

where

$$aba' = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Theorem 3.4 then says that the non-zeros of Y_2 are

$$\psi_x\,,\ (\psi_x)^2,\ \psi_{xy}\,,\ (\psi_{xy})^2,\ \psi_{x^2y}\,,\ (\psi_{x^2y})^2$$

which is obvious from the array $\mathfrak{X}(g)$.

This is also an illustration, though a rather trivial one, of Theorem 4.2. H is the group $(1, x, x^2)$; K is the group $(1, y, y^2)$. A is the ideal $x + x^2$ in FH, and B the ideal 1 in FK. The non-zeros of A are ψ_x, ψ_x^2 and the non-zeros of B are ψ_1, ψ_y, ψ_y^2. Clearly $Y_2 = AB$, and the non-zeros of Y_2 are the products $\psi_H \psi_K$, as above.

We can also check Theorems 5.1 and 5.2 from the following table:

$$\begin{aligned}
\theta_1 &= Y_1 + Y_2 + Y_3 + Y_4 + Y_5\,, \\
\theta_2 &= \phantom{Y_1 + {}} Y_2 \phantom{{} + Y_3} + Y_4 + Y_5\,, \\
\theta_3 &= \phantom{Y_1 + Y_2 + {}} Y_3 + Y_4 + Y_5\,, \\
\theta_4 &= \phantom{Y_1 + {}} Y_2 + Y_3 + Y_4\,, \\
\theta_5 &= \phantom{Y_1 + {}} Y_2 + Y_3 \phantom{{} + Y_4} + Y_5\,.
\end{aligned}$$

It is clear that

$$\begin{aligned}
Y_1 &= \theta_1 + \theta_2 + \theta_3 + \theta_4 + \theta_5\,, \\
Y_2 &= \phantom{\theta_1 + {}} \theta_2 \phantom{{} + \theta_3} + \theta_4 + \theta_5\,, \quad \text{and so on;}
\end{aligned}$$

and

$$(m_{ij})^2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}^2 = I.$$

APPENDIX B

An Example of the Product of Three Cyclic Codes

Let H, K, L be cyclic groups of orders 3, 5, 7 respectively. Their direct product G is cyclic of order 105. (Unfortunately, this is the smallest possible example.)

Write

$$H = 1, x, x^2; \quad K = 1, y, y^2, y^3, y^4; \quad L = 1, z, z^2, z^3, z^4, z^5, z^6.$$

Let $\langle A_1 \rangle$ (3, 2) and $\langle A_2 \rangle$ (5, 4) be the single parity check codes in FH, FK, with idempotents

$$A_1 = x + x^2; \qquad A_2 = y + y^2 + y^3 + y^4.$$

Let $\langle A_3 \rangle$ (7, 4) be the Hamming code in FL, with idempotent

$$A_3 = 1 + z + z^2 + z^4.$$

The direct product code has idempotent $C = A_1 A_2 A_3$. $\langle C \rangle$ is a (105, 32) cyclic code, with minimum distance 12. Each vector of C can be represented as a three-dimensional array of ones and zeros, which are situated at the lattice points corresponding to $x^i y^j z^k$ in Fig. 1. (The origin is $x^0 y^0 z^0$.) The lines of this array which are parallel to the x-axis are vectors of $\langle A_1 \rangle$; those parallel to the y-axis belong to $\langle A_2 \rangle$, and those parallel to the z-axis to $\langle A_3 \rangle$.

It has been suggested (see Ref. 8) that an array like this be used for simultaneous burst and random error correction. It must however be borne in mind that such a code will be highly redundant.

To express C as a cyclic code we write the lattice points in order $1, \mu, \mu^2, \mu^3, \cdots \mu^{104}$, where μ is a generator of the cyclic group G, for example $\mu = xyz$. With this choice $x^i y^j z^k$ becomes μ^n where n is the least integer such that

$$n - i \equiv 0(3); \qquad n - j \equiv 0(5); \qquad n - k \equiv 0(7)$$

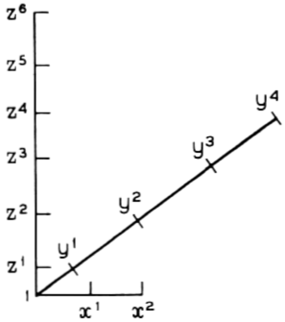

Fig. 1—$x^i y^j z^k$.

for example:

$$x^2 y^3 z^4 = (xyz)^{53}.$$

REFERENCES

1. Curtis, C. W., and Reiner, I., *Representation Theory of Finite Groups and Associative Algebras*, New York: John Wiley, 1962.
2. MacWilliams, Jessie, "The Structure and Properties of Binary Cyclic Alphabets," B.S.T.J., *44*, No. 2 (February 1965), pp. 303–332.
3. Speiser, Andreas, *Die Theorie der Gruppen von Endlicher Ordnung*, New York: Dover, 1945, Chapter 3.
4. MacWilliams, Jessie, and Mann, H. B., "On the p-Rank of the Design Matrix of a Difference Set," Information and Control, *12*, No. 5–6 (May–June 1968), pp. 474–488.
5. Mattson, M. F., and Solomon, G., "A New Treatment of Bose-Chaudhuri Codes," J. SIAM, *9*, No. 4 (December 1961), pp. 654–669.
6. Burton, H. O., and Weldon, E. J., Jr., "Cylic Product Codes," IEEE Trans. Information Theory, *IT-11*, No. 3 (July 1965), pp. 443–440.
7. Goethals, Jean-Marie, "Factorization of Cylic Codes," IEEE Trans. Information Theory, *IT-13*, No. 2 (April 1967), pp. 242–246.
8. Bridwell, J. D., "Burst Distance and Multiple Burst Correction," B.S.T.J., *49*, No. 5 (May–June 1970), pp. 889–909.