7-1-1978

Codes which are ideals in abelian group algebras.

Patrick R. Coulton

CODES WHICH ARE IDEALS IN ABELIAN GROUP ALGEBRAS

A Thesis

Presented to the

Department of Mathematics

and the

Faculty of the Graduate College

University of Nebraska

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

University of Nebraska at Omaha

by

Patrick R. Coulton

July, 1978

THESIS ACCEPTANCE

Accepted for the faculty of the Graduate College, University of Nebraska, in partial fulfillment of the requirements for the degree Master of Arts, University of Nebraska at Omaha.

Thesis Committee	Name	Department
	J. K. Karlof	Mathematics
	John Konvalina	Mathematics
	Charles Downey	"
	Orville D. Menard	Political Science
	Paul A. Haeder	Mathematics

J K Karlof

Chairman

7-19-78

Date

ACKNOWLEDGEMENTS

I would especially like to thank Dr. John Karlof, whose help and encouragement made this work possible.

I would also like to thank P.D. Sackett for invaluable aid.

TABLE OF CONTENTS

CHAPTER 1

Section 1

Take G to be any multiplicative group. Let $|G| = n$ and choose q to be a prime such that n and q are relatively prime. Let K denote the field of order q (i.e. $GF(q) = K$). We form the group algebra KG defined to be the set of all formal sums

$$\sum_{g \in G} a(g)g \ , \quad a(g) \in K = GF(q)$$

with multiplication and addition defined by

$$\text{i)} \quad \sum_{g \in G} a(g)g + \sum_{g \in G} b(g)g = \sum_{g \in G} (a(g) + b(g))g \ ,$$

$$\text{ii)} \quad \sum_{g \in G} a(g)g \ . \sum_{h \in G} b(h)h = \sum_{g \in h} a(g)b(h) \ g \cdot h \ ,$$

$$= \sum_{k \in G} [\sum_{h \in g} a(kh^{-1}) \ b(h)] \ k \ ,$$

where the coefficient of k is $\gamma(k) = \sum_{h \in G} a(kh^{-1}) \ b(h)$.

A straightforward application of these definitions yields that KG is an associative algebra with multiplicative identity. In fact, the identity in the group G acts as the multiplicative identity in KG.

Definition 1.1.1. A ring is said to satisfy the minimum chain condition if it satisfies the following two properties:

i) The chain of ideals (ascending chain condition)

$$I_1 \subset I_2 \subset I_3 \ldots \subset I_n \subset \ldots$$

always repeats indefinitely after a finite number of steps;

ii) The chain of ideals (descending chain condition)

$$I_1 \supset I_2 \supset I_3 \ldots \supset I_n \supset \ldots$$

always repeats indefinitely after a finite number of steps.

The dimension of KG over K as a vector space is n, and every ideal of KG is a vector subspace. Therefore, KG satisfies the minimum chain condition.

An ideal is nilpotent if $I^k = 0$, for some integer k, (where I^k is the set of all products of k elements in I). The radical of the ring, (denoted Rad(R)), is the sum of all nilpotent left ideals.

Definition 1.1.2. A ring with minimum condition will be called semisimple if Rad(R) is the zero ideal. A ring is said to be simple if the only two-sided ideals are the trivial ones.

Recall that when KG was defined we restricted n to be relatively prime to q. This is a sufficient condition to ensure that KG is a semisimple ring. We state without proof:

Theorem 1.1.3: Let G be a finite group of order n, and let K be an arbitrary field. Then the group algebra KG is semisimple if and only if char K = 0, or char K $\mid$ n.

The proof of this theorem and a lucid development of Theorem 1.2.3 can be found in [2].

Definition 1.1.4. Given $b \in KB$, then b is an idempotent generator if b acts as a multiplicative identity on $< b >$. The set $\{ b_1, \ldots , b_s \}$ is a set of primitive idempotents if $< b_i >$ is a minimal ideal for each i, $b_i \cdot b_j = 0$ whenever $i \neq j$, and $\Sigma\, b_i = 1 \in KG$.

Theorem 1.1.5: Let R be a semisimple ring with identity, which satisfies the minimum chain condition. Then the following are properties of R:

i) Every minimal left ideal has a generating idempotent, and every left ideal can be written as the direct sum of minimal left ideals;

ii) The sum of all left ideals of R that are isomorphic to a given minimal left ideal of R is a simple two-sided ideal;

iii) R can be written uniquely up to ordering as a direct sum of simple two-sided ideals. Any two-sided ideal is a direct sum of simple left-sided ideals;

iv) An ideal I is two-sided if and only if it has a central idempotent generator.

The last three properties imply that KG is a principal ideal domain, and in addition give the properties of elements which generate two-sided ideals. In particular, when G is an abelian group, KG is a commutative associative algebra whose ideals are two-sided. The idempotent generators of minimal ideals act as the multiplicative identity on the ideals they generate.

Section 2

The set of all n-tuples over GF(q) forms a vector space, $V^n(GF(q))$.

Definition 1.2.1. A block code of length n with elements in GF(q) is any subset of $V^n(GF(q))$.

The alphabet of a code are the symbols used to transmit information over a channel. In a block code the alphabet is the field GF(q). An example of an alphabet is the binary alphabet {0,1}, which is just GF(2). An n-tuple consisting of zeros and ones is in $V^n(GF(2))$. Any subset of $V^n(GF(2))$ may be chosen and designated as a block code. Each element in the block code is used for a distinct "message" over the channel. For instance, all n-tubples which have an even number of ones describe a block code. Suppose such a message word is sent over some channel. If there is "noise" in the channel the message may be distorted and the n-tuple received will not necessarily be the one that was originally sent. An error occurs if a zero is changed to a one, or a one is changed to a zero. If any odd combination of these errors occur, it can be detected simply by summing the ones on the message word received. In any case when errors occur there is no way of determining what the original message was.

Under such circumstances we would like to know if we can choose a subset of $V^n(GF(2))$ which gives a "maximal probability" for guessing the actual message word from the information contained in a received word which has been distorted. While the basic problem of mathematical coding is to develop maximal error detection and correction capabilities, there are other engineering problems that also enter into the problem. That is, a code must offer efficient methods for encoding and decoding.

CHAPTER 2

Section 1

Let $K = GF(2)$. Take G to be any cyclic group of odd order, then the order of G and the characteristic of the field K are relatively prime. This implies that the group algebra, KG, is semisimple by Theorem 1.1.3. Furthermore, KG is a commutative ring, which is also a principal ideal domain. KG can be written as the direct sum of minimal two-sided ideals according to Theorem 1.1.5. These ideals are generated by primitive idempotent generators.

Theorem 2.1.1. Let n be any odd integer and let $K = GF(2)$. If G is a cyclic group of order n, then

$$KG \simeq K[x] \,/\, < x^n - 1 > \quad ,$$

where the ismorphism is a ring isomorphism.

Proof: The isomorphism we present is also a K-isomorphism. Define $\phi : KG \to K[x] \,/\, < x^n-1 >$ by

$$\phi: \sum_{i-0}^{n-1} a_i g^i \to \sum a_i x^i + < x^n-1 >$$

where $G = < g >$. Now

$$\begin{aligned}\phi(a + b) &= \sum_{i=0}^{n-1} a_i x^i + \sum_{i=0}^{n-1} b_i x^i + < x^n-1 > . \\ &= \phi(a) + \phi(b)\end{aligned}$$

where $a = \sum_{i=0}^{n-1} a_i g^i$, and $b = \sum_{i=0}^{n-1} b_i g^i$. Also

$$\phi(a \cdot b) = ((\sum_{i=0}^{n-1} a_i g^i)(\sum_{j=0}^{n-1} b_j g^j)) ,$$

$$= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_i x^{i+j} + < x^n - 1 > ,$$

$$= \phi(a) \cdot \phi(b) ,$$

where exponent addition is mod n. Thus ϕ is a ring homomorphism, which is onto $K[x]/< x^n-1 >$. Let $a = \sum_{i=0}^{n-1} a_i g^i \in KG$, such that $\phi(a) = 0 + < x^n-1 >$. So, $\phi(a) = \sum a_i x^i + < x^n-1 >$. But $\deg \phi(a)<n$, which implies a = 0. Therefore, ϕ is a ring isomorphism.

We now introduce a theorem which gives the polynomials which generate minimal ideals in $K[x]/< x^n-1 >$.

Theorem 2.1.2: Let $p_1(x) \cdot p_2(x) \ . \ . \ . \ p_s(x) = x^n-1$ be the factorization of x^n-1 into irreducible monic polynomials in K[x]. We have:

i) Each irreducible monic factor $p_i(x)$ generates a maximal ideal over $K[x]/< x^n-1 >$;

ii) For $p_i(x)$, (an irreducible monic factor of x^n-1), $p_1(x)\ p_2(x) \ . \ . \ . \ \widehat{p_i(x)} \ . \ . \ . \ p_s(x)$ generates a minimal ideal over $K[x]/< x^n-1 >$.

Proof: i) K[x] is a principal ideal domain, and if $< \overline{p_i(x)} >$ is not maximal in $K[x]/< x^n-1 >$, then there exists an ideal I such that $< \overline{p_i(x)} > \subsetneq I$. There exists an ideal I in K[x], by correspondence, such that $< p_i(x) >$ I. However, $p_i(x)$ is irreducible and therefore $< p_i(x) >$ is a maximal ideal in $K[x]$. This implies that there are no ideals between $< \overline{p_i(x)} >$ and $K[x]/< x^n-1 >$. Therefore, $< \overline{p_i(x)} >$ is a maximal ideal.

For the proof of ii) we consider $(x^n-1)/p_i(x) = z_i(x)$. Let $\overline{J}$ be a minimal ideal in $< \overline{z_i(x)} >$. Associated with $\overline{J}$ there is an ideal J in $K[x]$; let $g(x)$ be a monic polynomial of minimal degree in J, then in $K[x]$,

$$x^n-1 = k(x)g(x) + r(x)$$

where $\deg r(x) < \deg g(x)$ >. However, $(x^n-1) \in J$, since $\overline{J} \subseteq K[x]/< x^n-1 >$. Therefore

$$(x^n-1) - k(x)g(x) \in J,$$

which implies that $r(x) \in J$. But, since $g(x)$ is of minimal degree $f(x)$ must be zero, and $g(x)$ divides x^n-1. However, the only element of $< z_i(x) >$ which divides x^n-1 is $z_i(x)$. Therefore, $< \overline{z_i(x)} >$ is a minimal ideal in $K[x]/< x^n-1 >$.

Q.E.D.

In addition to the above result we have, $< \overline{z_i(x)} > \cap < \overline{z_j(x)} >$ is $< \overline{z_i(x)z_j(x)} >$, which is the zero ideal if $i \neq j$. This is because x^n-1 divides $z_i(x)z_j(x)$. The dimension of the ideal $< z_i(x) >$ is exactly the degree of $p_i(x)$. Therefore, the dimension of the direct sum of the ideals generated by the $\overline{z_i(x)}$'s is n. Consequently,

$$K[x]/\langle x^n-1 \rangle = \bigoplus_{i=1}^{s} \langle \overline{z_k(x)} \rangle .$$

Example 2.1.3. Let G = σ(3), (i.e., the cyclic group of order three). We consider the polynomial x^3-1. Then

$$K\,\sigma\,(3) = K[x]/\langle x^3-1 \rangle .$$

This ring is semisimple and a principal ideal domain with a mutliplicative identity. Factoring x^3-1 we have

$$x^3-1 = (x^2+x+1)(x-1).$$

There are two minimal ideals. One is $\langle \overline{x-1} \rangle$, which can be written as $\langle \overline{x+1} \rangle$, and $\langle \overline{x^2+x+1} \rangle$. The ideal $\langle \overline{x+1} \rangle$ is composed of elements

$$x^2+x+\langle x^3-1 \rangle ,$$
$$x^2+1+\langle x^3-1 \rangle ,$$
$$x+1+\langle x^3-1 \rangle ,$$
$$0+\langle x^3-1 \rangle .$$

This ideal is of dimension 2 over GF(2). On the other hand the ideal generated by $\overline{x^2+x+1}$ is of dimension one, as is easily verified. Thus,

$$K[x]/\langle x^3-1 \rangle = \langle \overline{x+1} \rangle \oplus \langle x^2+x+1 \rangle ,$$

but $\overline{(x^2+x)}\,\overline{(x^2+x)} = \overline{x^2+x}$, so x^2+x is the idempotent generator of the ideal $\langle \overline{x+1} \rangle$. Finally we can write

$$K[x]/\langle x^3-1 \rangle = \langle \overline{x^2+x} \rangle \oplus \langle \overline{x^2+x+1} \rangle ,$$

where $\overline{x^2+x} + \overline{x^2+x+1} = 1$. This shows that $\overline{x^2+x}$, and $\overline{x^2+x+1}$ are the idempotent generators. Note that in general the method of Theorem 2.1.2 does not yield the idempotent generators of the minimal ideals.

Example 2.1.4. Let G = $\sigma(7)$. Factoring x^7-1 in GF(2) yields,

$$x^7+1 = (x+1)(x^3+x^2+1)(x^3+x+1).$$

There are three minimal ideals, generated by the polynomials

$$(x+1)(x^3+x^2+1) = x^4+x^2+x+1 ,$$

$$(x+1)(x^3+x+1) = x^4+x^3+x^2+1 ,$$

and,

$$(x^3+x^2+1)(x^3+x+1) = x^6+x^5+x^4+x^3+x^2+x+1 .$$

An easy calculation shows that the first and the last determine idempotent generators of the minimal ideals. However, $\overline{x^4+x^3+x^2+1}$ is not an idempotent. In fact, it can be shown that the idempotent generator of the ideal $< \overline{x^4+x^3+x^2+1} >$ is $\overline{x^6+x^5+x^3+1}$. Therefore,

$$K[x]/ < x^7-1 > = < x^4+x^2+x+1 > \oplus < x^6+x^5+x^3+1 > \oplus < x^6+x^5+x^4+x^3+x^2+1>.$$

A direct calculation shows that the pairwise products of these idempotents are zero. It should be noted that the decomposition of x^n-1 into irreducible polynomials over GF(q), in general, is by no means trivial. In case it is accomplished, the decomposition doesn't necessarily yield the idempotent generators. We shall explore a method in Chapter 3, which will provide an algorithm which gives the idempotent generators.

Section 2

We are now ready to discuss some of the practical aspects of cyclic coding.

Definition 2.2.1. i) A subset $\mathcal{C}$ of $V^n(FG(q))$ is called a linear code if it is a vector subspace of $V^n(GF(q))$.

ii) A code is cyclic if it is a linear code, and if every cyclic shift of a code word is a code word.

Example 2.2.2. Let $\mathcal{C}_1 = \{(011),(101),(110),(000)\}$. It is clear that this set satisfies Definition 2.2.1 ii). Thus $\mathcal{C}_1$ is a linear code which is also cyclic. In other words if α is the permutation (123), then $\alpha(101) = (101)$, $\alpha(110) = (011)$, and $\alpha(011)$ is (101). Note that $\mathcal{C}_1$ is exactly the code generated by $\overline{x^2+x}$ given in Example 2.1.3.

Cyclic codes have been important in coding almost from the beginning. Cyclic codes were first identified by Prange in 1956. The first class of cyclic codes was discovered by Hamming and are named after him. They were followed in 1960 by the discovery of the class of BCH codes, which are cyclic codes over GF(2), and contain the Hamming codes as a subclass. The generalization of BCH codes are referred to as Reed-Muller codes. These codes are over the field of GF(q).

Up until now the practical use of error correcting codes has not attained the promise it appeared to hold in the early years of development. The first obstacle encountered in implementing a code is the encoding procedure. An efficient method for encoding information to be sent over a channel must be found. Another obstacle involves decoding the information so that it can be put into useful form.

In 1960 Petersen [7] developed an efficient method decoding BCH codes. For cyclic codes encoding is a simple procedure involving matrix multiplication. If we choose a code which is not cyclic, the encoding procedure is generally much more complicated. It is precisely for this reason that cyclic codes have been emphasized in the field of error correcting codes. But the nice encoding properties of cyclic codes, which are a result of the fact that they are ideals in the group algebra KG, necessarily imply less desirable properties. For instance, cyclic codes do not achieve maximal distance properties. That is because they are a vector subspace; they are also more "tightly" packed than they need be. Petersen's method for decoding cyclic codes is efficient and workable. However, the number of operations needed to decode a word received with an error increases as a small power of the code length.

CHAPTER 3

Section 1

Throughout this chapter, $K = GF(q)$, q prime, and $|G| = n$, where $(q,n) = 1$. If G is an abelian group, then

$$KG = \bigoplus_{j=1}^{s} M_j ,$$

where M_j is a two-sided ideal generated by a primitive orthogonal idempotent. Each M_j is a vector subspace of KG. Each element b M_j can be written as

$$b = \sum_{i=1}^{n} b(g_i)\, g_i , \qquad b(g_i) \in K.$$

This determines a unique n-tuple $(b(g_1), b(g_2), \ldots, b(g_n))$. In this way each M_j determines a linear code. If J is any ideal of dimension k over K in KG, then the ideal J is associated with a (k,n) code.

Section 2

If G is an abelian group, then we can decompose G into the direct product of primary cyclic groups,

$$G = G_{p_1^{\alpha_1}} \times G_{p_2^{\alpha_2}} \quad s \ldots \times G_{p_s^{\alpha_s}} ,$$

each $G_{p_i^{\alpha_i}}$ is cyclic. The number of irreducible representations of G over C is equal to the number of conjugacy classes. Consequently, there are $|G|$ irreducible representations of G over the complex numbers. The set of irreducible characters in this case can be identified with the set of irreducible representations.

For $G_{p_i^{\alpha_i}} = < a_i >$, consider the mappings defined by

$$\chi_{a_i}(a_i) = \xi \text{ , a primitive } p_i^{\alpha_i} \text{ th root of unity,}$$

and

$$\chi_{a_i}(a_j) = 1 \text{ , for } i \neq j.$$

For each i, χ_{a_i} can be extended to an irreducible representation of G in an extension field L of K. which is algebraically closed. Any irreducible character from G into L can be written as the product of some of the χ_{a_i}'s. For example, if χ is an irreducible character, where

$$\chi(a_i) = \zeta \text{ , } i = 1, 2, \ldots, s \text{ ,}$$

then

$$\begin{aligned}(\chi(a_i))^{p_i^{\alpha_i}} &= (\zeta)^{p_i^{\alpha_i}} \\ &= \chi(a_i^{p_i^{\alpha_i}}) \\ &= 1.\end{aligned}$$

This implies that ξ is a $p_i^{\alpha_i}$ th root of unity. Thus,

$$\chi(a_i) = \xi^{\beta_i} , \ 0 \leq \beta_i < p_i^{\alpha_i} ,$$

and for $g = a_1^{k_1} a_2^{k_2} \ . \ . \ . \ a_s^{k_s}$,

$$\chi(g) = \chi(a_1^{k_1} \ . \ . \ . \ a_s^{k_s})$$

$$= \prod_{i=1}^{s} (\xi)^{\beta_i k_i}$$

$$= \prod_{i=1}^{s} \chi_{a_i^{\beta_i}} (a_1^{k_1} a_2^{k_2} \ . \ . \ . \ a_s^{k_s}) ,$$

where $\chi_{a_i^{\beta_i}} (a_i) = \xi^{\beta_i} = (\chi_{a_i}(a_i))^{\beta_i}$.

Consider the isomorphism $\psi : G \to G^*$, (where G^* is the group of all irreducible characters on G into L), defined by

$\psi : g \to \chi_g$.

That is, if $g = \prod_{i=1}^{s} a_i^{k_i}$, then

$$\chi_g(x) = \chi_{a_1^{k_1}}(x) \ \chi_{a_2^{k_2}}(x) \ . \ . \ . \ \chi_{a_s^{k_s}}(x) , \quad x \in G.$$

Since multiplication of characters is defined according to the generators of G, it is easy to verify that ψ is an isomorphism. From this point on G and G* will be identified with each other. We list some properties of the irreducible characters of abelian groups.

Theorem 3.2.1:

$$\text{i)} \quad \sum_{g\in G} \chi_g(h) = \begin{cases} |G| & \text{if } h = 1 \\ 0, & \text{otherwise} \end{cases} \quad ;$$

$$\text{ii)} \quad \sum_{g\in G} \chi_h(g) = \begin{cases} |G| & \text{if } h = 1 \\ 0, & \text{otherwise} \end{cases}$$

Proof: If h = 1, then $\chi_g(h) = 1 \quad g \in G$. Therefore, $\sum_{g\in G} \chi_g(1) = |G|$.

If $h \neq 1$, assume

$$\sum_{g\in G} \chi_g(h) = \alpha \ , \ \alpha \in L,$$

then

$$\chi_k(h)\ \alpha = \sum_{g\in G} \chi_k(h)\ \chi_g(h) \ ,$$

$$= \sum_{g\in G} \chi_{kg}\ (h) = \sum_{g} \chi_g(h) = \alpha \ .$$

This implies that $\alpha = 0$.

For the proof of ii), consider $g = \prod_{i=1}^{s} a_i^{k_i}$, and

$$h = \prod_{i=1}^{s} a_i^{l_i} \ ,$$

then

$$\chi_g(h) = \prod_{i=1}^{s} \chi_{a_i^{k_i}}(a_i^{l_i}) = \prod_{i=1}^{s} \chi_{a_i^{l_i}}(a_i^{k_i}) \ ,$$

and

$$\chi_g(h) = \chi_h(g). \tag{3.1}$$

Using i) and (3.1) yields ii).

Q.E.D.

From the development of the group characters $\chi_{g_1}(h)\chi_{g_2}(h)=\chi_{g_1 g_2}(h)$. This fact along with (3.1) implies

$$\chi_h(g_1)\ \chi_h(g_2) = \chi_h(g_1 g_2) \tag{3.2}$$

As in [5] we adopt the notation

$$\chi_h(g) = < h,g > .$$

The first position specifies the character and the second position specifies the element being operated on.

We extend the characters to a set of linear functions from KG into L. Define for $a \in KG$.

$$\chi_h(a) = < h,a > = < h, \sum_{g \in G} \alpha_g g > ,$$

$$= \sum_{g \in G} \alpha_g < h,g > .$$

Section 3

MacWilliams [6] was first to investigate abelian codes over GF(2). In her paper, she formulates the method for constructing the orthogonal idempotent generators. In the cyclic case, the idempotent generators were written as polynomial in $K[x]/< x^n-1 >$. Camion [4] also investigated the structure of the ideals of the group algebra, and discusses in some detail how the structure of the polynomials, which generate the ideals, relates to the structure of a code.

From the theory of semisimple algebras there exists a set of orthogonal idempotent generators $\{e_1,\ldots,e_s\}$ such that

$$< e_1 > \oplus < e_2 > \oplus \ldots \oplus < e_s > = KG ,$$

and

$$e_1 + e_2 + \ldots + e_s = 1,$$

with $e_i \cdot e_j = 0$, for $i \neq j$. If $a \in < e_i >$, then

$$a \cdot 1 = a(e_1 + \ldots + e_i + \ldots + e_s) = a \cdot e_i . \quad (3.3)$$

Thus, e_i acts as the identity on the ideal $< e_i >$. Furthermore,

$$(e_i)^q = e_i , \quad (3.4)$$

and $\forall\ a \in KG$

$$(\sum_{i=1}^{n} \alpha_i g_i)^q = (\alpha_1 g_1)^q + a(\alpha_1 g_1)^{q-1}(\sum_{i=2}^{n} \alpha_i g_i) + \ldots + (\sum_{i=1}^{n} \alpha_i g_i)^q ,$$

but since we are over $GF(q)$, $q = 0$. So

$$(\sum_{i=1}^{n} \alpha_i g_i)^q = (\alpha_1 g_1)^q + (\sum_{i=2}^{n} \alpha_i g_i)^q .$$

By induction,

$$(\Sigma\ \alpha_i g_i)^q = \sum_{i=1}^{n} (\alpha_i g_i)^q ,$$

$$= \sum_{i=1}^{n} \alpha_i g_i^q \ .$$

Let ν be the exponent of G, then $(q, \nu) = 1$, since q and the order of G are relatively prime. Therefore,

$$q^r \equiv 1 \bmod \nu \text{ , for some integer } r \ . \tag{3.5}$$

Definition 3.3.1: The minimal q-power subset of $x \in G$ is

$$Q(x) = \{ x, x^q, x^{q^2}, \ . \ . \ . \ , x^{q^{k(x)-1}} \} ,$$

where $k(x)$ is the least integer, such that

$$q^{k(x)} \equiv 1 \bmod (\text{the order of } x). \tag{3.6}$$

Each q-power subset is closed under the operation of raising elements fo the q-power. Hence,

$$G = Q(1) \cup Q(x_1) \cup . \ . \ . \cup Q(x_t) \ ,$$

where each x_{i+1} is chosen from $G \setminus Q(1) \cup Q(x_1) \cup . \ . \ . \cup Q(x_i)$.

Now from (3.6), $x^{q^{k(x)}} = x$, and $k(x)$ is the smallest integer for which this is true. On the other hand, the next smallest integer for which this is true is $2k(x)$, and in fact, r must be a multiple of $k(x)$, for each $x \in G$. Otherwise,

$$x^{q^r} = s^{q^{mk(x)+b}} \quad , \ 0 \leq b < k(x),$$

and

$$x = (x^{q^{mk(x)}})^{q^b}$$

$$= x^{q^b} .$$

But since k(x) is minimal, b = 0, and k(x) divides r.

Section 4

If L is an extension field of K = GF(q), which contains all of the ν the roots of unity, then the smallest such field is $GF(q^r)$. This is true since r is the smallest integer such that $\nu | q^r - 1$, (that is the multiplicative group of the field $GF(q^r)$ contains an element of order ν). So let $L = GF(q^r)$. For each $x \in G$ $< x,a > \in GF(q^r)$ where $a \in KG$. Also,

$$< x, a \cdot b > = < x, \sum_g \sum_h \alpha_g \beta_h \; g \cdot h > ,$$

$$= \sum_g \sum_h \alpha_g \beta_h < x,gh >$$

$$= < x,a > < x,b > .$$

Denote by L^G the space of all formal sums $\sum_g a(g)g$, where $a(g) \in L$, with addition defined as in LG. We define two multiplications ($\cdot$, *). The "dot" multiplication is as defined for LG, but the "star" multiplication is componentwise. For instance,

$$(\sum_g a(g)g) * (\sum_g b(g)g) = \sum a(g) \, b(g)g .$$

We will denote the ring consisting of the set LG with multiplication by "star" as L_*^G .

We introduce the Mattson Solomon mapping. Define $\mu : KG \to L_*^G$, where $\forall$ $a \in KG$

$$\mu(a) = \sum_{x \in G} < x, a > x$$

$$= \sum_{x \in G} \Big(\sum_{y \in G} a(y) < x, y > \Big) x .$$

Theorem 3.4.1.: The M-S mapping is a ring isomorphism from KG into L_*^G .

Proof: It is clear that μ is a vector space isomorphism since

$$\mu(\lambda_1 a + \lambda_2 b) = \sum_{x \in G} < x, \lambda_1 a + \lambda_2 b > x ,$$

$$= \sum_{x \in G} < x, \lambda_1 a > x + \sum_{x \in G} < x, \lambda_2 b > x ,$$

$$= \lambda_1 \mu(a) + \lambda_2 \mu(b) .$$

We define the mapping μ^{-1} from L_*^G into LG by

$$\mu^{-1}(\alpha) = 1/n \sum_{x \in G} < x^{-1}, \alpha > x ,$$

for each $\alpha \in L_*^G$. Let $a = \sum_{z \in G} a(z)x \in KG$, then

$$\mu(a) = \sum_{x \in G} < x, a > x ,$$

and

$$\mu^{-1}(\mu(a)) = 1/n \sum_{y \in G} < y^{-1}, \sum_{x \in G} < x, a > x > y ,$$

$$= 1/n \sum_{y \in G} \sum_{x \in G} < x,a > < y^{-1},x > y \ ,$$

$$= 1/n \sum_{y \in G} \sum_{x \in G} < x,ay^{-1} > y \ ,$$

$$= 1/n \sum_{y \in G} \sum_{z \in G} a(z) \ y \sum_{x \in G} < x,y^{=1}z > \ .$$

The sum is nonzero if and only if y = z, so

$$\mu^{-1}(\mu(a)) = \sum_{z \in G} a(z)z \ .$$

Thus μ is one-to-one. In addition,

$$\mu(a \cdot b) = \sum_{x \in G} < x,ab > x \ ,$$

$$= \sum_{x \in G} < x,a > < x,b > x \ ,$$

$$= \mu(a) * \mu(b) \ .$$

Q.E.D.

In fact, if $g_1 = 1$, then

$$\mu(g_.) = \sum_{x \in G} < x,g_1 > x,$$

$$= \sum_{x \in G} x$$

This is the identity under "*" multiplication. To denote the "*" product of $\mu(a)$ with itself k times we write

$$(\mu(a))^{*k} \ .$$

Whereas, $\mu(a)$ to the k-th power under the "dot" product will be

$$(\mu(a))^k .$$

Let $\alpha = \mu(a)$, for some a in KG, then

$$\alpha^q = \left(\sum_{i=1}^{n} \langle g_i,a \rangle g_i\right)^q$$

$$= \sum_{i=1}^{n} < g_i,a >^q g_i^q ,$$

since we are over $GF(q^r)$. Thus,

$$\alpha^q = \sum_{i=1}^{n} < g_i,a >^q g_i^q ,$$

$$= \sum_{i=1}^{n} < g_i^q,a > g_i^q ,$$

$$= \sum_{i=1}^{n} < g_i^q,a > g_i^q .$$

But this is simply the sum over the elements in G, so $\alpha^q = \alpha$. Therefore, whenever α is an image under the M-S mapping, the "dot" product of α with itself q times is α . On the other hand, suppose $\alpha^q = \alpha$, for some α in L_*^G , then

$$< x,\alpha >^q = < x, \sum_{y \in G} \alpha(y)y >^q ,$$

$$= \sum_{y \in G} \alpha(y)^q < x,y^q >$$

$$= < x,\alpha^q > ,$$

which is $< x,\alpha >$ for each $x \in G$.

Lemma 3.4.2. Let $\alpha \in L_*^G$, such that $\alpha^q = \alpha$, (under the "dot" product), then $\mu^{-1}(\alpha)$ KG.

Proof: Let $\alpha^q = \alpha$, and let $a \in LG$, such that

$$a = 1/n \sum_{x \in G} < x^{-1}, \alpha > x ,$$

but

$$a(x) = \frac{< x^{-1}, \alpha > x}{n} ,$$

$$= \frac{< x^{-1}, \alpha^q >}{n} ,$$

$$= a(x)^q .$$

Thus $a(x) \in GF(q)$, (i.e., $\alpha(x)^q \Rightarrow \alpha(x) \in GF(q)$, since the multiplication group of GF(q) is the only subgroup of the multiplication group of $GF(q^r)$ of order q - 1). This implies $a \in KG$, and μ^{-1} is the inverse mapping from the image of μ onto KG. Let $\mu[KG]_*$ denote the subspace of L_*^G which is the image of KG under the M-S mapping. From Theorem 3.4.1., KG and $\mu[KG]_*$ are isomorphic as rings.

Theorem 3.4.3. The minimal ideals of $\mu[KG]_*$ are generated by elements of the form

$$\eta_i = \sum_{j=1}^{k_i - 1} (x_i)^{q^j} ,$$

where the x_i's are taken from the decomposition of G into minimal q-power subsets.

Proof: Note that, $\eta_i^q = \eta_i$, so $\eta_i \in \mu[KG]_*$, since η_i is just the sume of elements in a q-power subset. The elements in the ideal $< \eta_1 >$ are of the form

$$\beta_i = \sum_{j=0}^{k_i - 1} (x_i c_i)^{q^j} \ , \quad c_i \in GF(q^{k_i}) \ ,$$

where $k_i = k(x_i)$. It is clear that this sum is in $\mu[KG]_*$, since $\alpha_i^q = \alpha_i$. Furthermore, there are no ideals properly contained in $< \eta_i >_*$. Since, if there were, its idempotent would not contain all of the elements of $Q(x_i)$ in its formal sum. In this case, it could not be in $\mu[KG]_*$. In addition,

$$\eta_1 + \eta_2 + \ldots + \eta_s = \sum_{x \in G} x \ , \tag{3.7}$$

which is the "*" multiplication identity in $\mu[KG]_*$, and $\eta_i * \eta_j = 0$. Therefore, the η_i's generate minimal ideals and

$$\mu[KG]_* = < \eta_1 >_* \oplus < \eta_2 >_* \oplus \ldots \oplus < \eta_s >_*$$

by (3.7).

Q.E.D.

Corollary 3.4.4. The minimal ideals of KG are generated by orthogonal idempotents of the form

$$\mu^{-1}(\eta_i) = 1/n \sum_{g \in G} \left(\sum_{j=1}^{k_i - 1} < g^{-1}, x_i >^{q^j} \right) g \ .$$

Proof: Since $\mu[KG]_* \simeq KG$. The result is an immediate consequence of the isomorphism μ^{-1} .

Q.E.D.

Let $e_i = \mu^{-1}(\eta_i)$, then

$$\begin{aligned} e_1 + e_2 + \ldots + e_s &= \mu^{-1}(\eta_1) + \mu^{-1}(\eta_2) + \ldots + \mu^{-1}(\eta_s) \\ &= \mu^{-1}(\eta_1 + \eta_2 + \ldots + \eta_s) \\ &= 1 \ . \end{aligned}$$

Also,

$$\begin{aligned} e_i \cdot e_j &= \mu^{-1}(\eta_i) \cdot \mu^{-1}(\eta_j) \\ &= \mu^{-1}(\eta_i * \eta_j) \\ &= 0 \end{aligned}$$

and

$$\begin{aligned} e_i^{\ 2} &= \mu^{-1}(\eta_i^{\ 2}) \\ &= e_i \ . \end{aligned}$$

Therefore, we have found the set of primitive orthogonal idempotents of KG.

Section 5

Definition 3.5.1.

i. Let H be a q-power subset, the annihilator of H is

$$A[H] = \{b \in KG \mid < x,b > = 0 \;\forall x \in H\} .$$

ii. Let R be a subset of KG, the annihilator of R in G is

$$An[R] = \{x \in G \mid < x,a > = 0 \;\forall a \in R\} .$$

If $a \in KG$ and H is a q-power subset with $b \in A[H]$, then

$$< x,ba > = 0, \;\forall x \in H.$$

Therefore, $A[H]$ is an ideal. If $x \in An[R]$, then

$$< x,a > = 0 , \quad \forall a \in R.$$

Therefore, $< x,a >^q = 0$, and this implies that $< x^q,a > = 0$, which in turn implies that $x^q \in An[R]$. So An[R] is a q-power subset. The annihilator of any q-power subset is an ideal, and the annihilator of any subset of KG is a q-power subset.

Lemma 3.5.2. If H is a q-power subset of G, then the dimension of the ideal $A[H]$ over K is $n - |H|$.

Proof: Consider $X = \mu(A[H])$, since $A[H]$ is an ideal, X is a subspace of $\mu[KG]_*$. By definition,

$$A[H] = \{b \in KG \mid < x,b > = 0 \;\forall x \in H\} .$$

If $b \in A[H]$ and $x \in H$, then $< x,b > = 0$. This implies that $\mu(b)$ doesn't contain x in its formal sum. For $G = Q(x_0) \cup Q(x_1) \ldots \cup Q(x_s)$, let $H = \quad Q(x_i)$, where $I \subset \{0, 1, \ldots , s\}$.
Elements in X have the form

$$\beta = \sum_{i \notin I} \beta_i ,$$

where β_i is defined as

$$\beta_i = \sum_{j=0}^{k_i - 1} (c_i x_i)^{q^j} , \quad c_i \in GF(q^{k_i}) .$$

Accordingly, the number of unique β_i's is $|GF(q^{k_i})|$, since each unique element of the field defines a unique β_i . Therefore, the number of unique elements in X is

$$|X| = \prod_{i \notin I} q^{k_i} = q^l$$

where $l = \sum_{i \notin I} k_i$. But

$$\sum_{i \notin I} k_i = |G| - |H| = n - |H| .$$

Q.E.D.

Theorem 3.5.3. (MacWilliams and Mann): If $\mathbb{R}$ is an ideal in KG, its dimension over K is equal to

$$\dim(\mathbb{R}) = n - | An[Q] | .$$

Proof: Let $\mathbb{R}$ be an ideal of KG, and let $a \in \mathbb{R}$, such that $< a > = \mathbb{R}$. Let d be the dimension of $\mathbb{R}$ over K. Define the matrix Λ by

$$\Lambda = (\lambda_{ij}) = (< g_i, g_j >) .$$

Clearly,

$$\Lambda^t = \Lambda$$

and

$$\Lambda^{-1} = (1/n < g_k{-1}, g_j >).$$

The set $\{ag_1, ag_2, \ldots , ag_n\}$ spans $\mathbb{R}$ as a vector space over K, since $< a > = \mathbb{R}$. A typical vector in the set is

$$ag_i = \sum_{j=1}^{n} a(g_j)\ g_j g_i$$

$$= \sum_{j=1}^{n} a(g_i^{-1}\ g_k)\ g_k$$

where $g_k = g_i g_j = g_j g_i$. Define

$$M = (a(g_i^{-1}\ g_j))$$

then

$$(M\cdot\Lambda)_{ij} = \sum_{k=1}^{n} a(g_i^{-1}\ g_k)\quad g_k, g_j$$

$$= \sum_{l=1}^{n} a(g_l) < g_i g_l, g_j >$$

$$= \sum_{l=1}^{n} a(g_l) < g_i, g_j > < g_l, g_j >$$

$$= < g_i, g_j > < a, g_j > .$$

Next,

$$(\Lambda^{-1} \cdot M \cdot \Lambda)_{m,j} = 1/n \sum_{i=1}^{n} < g_m^{-1}, g_i > < g_j, g_i > < g_j, a >$$

$$= 1/n \sum_{i=1}^{n} < g_m^{-1} g_j, g_i > < a, g_j > .$$

But $\sum_{i=1}^{n} < g_m^{-1} g_j, g_i >$ is nonzero if and only if $g_m = g_j$, which yields

$$(\Lambda^{-1} M \Lambda)_{mj} = < a, g_m > \delta_{mj} .$$

The resultant matrix is zero off the diagonal and nonzero along the diagonal if and only if $< a, g_m > \neq 0$. Therefore the rank of M is the same as the number of characters which are nonzero on a. Hence

$$\dim \mathbb{R} = n - | An[\mathbb{R}] | .$$

Q.E.D.

Theorem 3.5.4. (Delsarte): There is one-to-one correspondence between the q-subsets H of G, and the ideals $\mathbb{R}$ in KG. The correspondence is

$$\mathbb{R} = A[H] \text{ and } H = An[\mathbb{R}] .$$

Proof: Let $\mathbb{R}$ be an ideal in KG. Let $H = An[\ \mathbb{R}\ ]$, then

$$\dim\ \mathbb{R} = n - |H|$$

by Theorem 3.5.3., but

$$\dim\ A[H] = n - |H|$$

by Lemma 3.5.2. Since $\mathbb{R}$ is annihilated by H, $\mathbb{R} \subset A[H]$, which implies that $\mathbb{R} = A[H]$.

On the other hand, if H is a q-power subset, we let $\mathbb{R} = A[H]$. Now

$$\dim\ A[H] = n - |H|$$

$$= n - |\ An[\ A[H]\ ]\ |$$

by Theorem 3.5.3. So

$$H = An[\ A[H]\ ]\ .$$

Q.E.D.

For any $x \in G$, $G \setminus Q(x)$ is a maximal q-power subset, in the sense that there are no q-power subsets between G and $G \setminus Q(x)$. If $\mathbb{R} = A[G \setminus Q(x)]$, then $\mathbb{R}$ is a minimal ideal. This follows directly from the fact that $G \setminus Q(x)$ is maximal, and any ideal contained in $\mathbb{R}$ is annihilated by $G \setminus Q(x)$. The only q-power subset which properly contains $G \setminus Q(x)$ is G, which corresponds to the zero ideal according to Theorem 3.5.4.

CHAPTER 4

Section 1

One reason for considering the class of abelian codes is that they contain, as a subclass, the cyclic codes. MacWilliams was able to demonstrate some properties of cyclic codes by using machinery developed for abelian codes. In addition, we can extend our discussion of cyclic codes to Tensor product codes, and we shall demonstrate some of the properties of these codes.

As in Chapter 3, take G to be an abelian group of order n. Let S be a subgroup of G. Let $|S| = n_s$. Consider the coset decomposition of G,

$$G = k_1 S \cup k_2 S \quad . . . \cup k_w S \quad ,$$

where $n = wn_s$. For each $a \in KG$,

$$a = \sum_{i=1}^{w} \sum_{j=1}^{n_s} \alpha_{ij} \; k_i s_j \quad .$$

Next, consider the projection mapping π_i from $KG \rightarrow KG$, with

$$\pi_i(a) = \sum_{j=1}^{n_s} \alpha_{ij} \; k_i s_j \quad . \qquad (4.1)$$

Lemma 4.1.1. If we let $\mathfrak{a}_i$ be the image of an ideal $\mathfrak{a}$ under the mapping π_i, then $\mathfrak{a}_i$ is isomorphic to an ideal of KS.

Proof: First, note that (4.1) is strictly a sum over the elements of S. Next, $\forall\, s \in S$

$$s\,\pi_i(a) = k_i \sum_{j=1}^{n_s} \alpha_{ij}\, s_j\, s \quad ,$$

$$= \pi_i(s \cdot a) \; .$$

Also, $\forall\, a,b \in \mathfrak{A}$, π_i acts as a homomorphism under addition, that is

$$\pi_i(a) + \pi_i(b) = \pi_i(a + b) \quad ,$$

which is in $\mathfrak{A}_i$. Therefore, $\mathfrak{A}_i$ is an ideal in KS.

Q.E.D.

It is also clear, from (4.1), that

$$k_i\,\mathfrak{A}_1 = \mathfrak{A}_i \; , \tag{4.2}$$

whenever k_1 is the identity in G. Furthermore,

$$a = \sum_{i=1}^{w} \pi_i(a) = \sum_{i=1}^{w} k_i k_i^{-1}\, \pi_i(a) \; , \tag{4.3}$$

but $k_i^{-1}\,\pi_i(a)$ is in $\mathfrak{A}_1$. When we write vectors of KG as n-tuples as in (4.1), the ordering produces n-tuples which contain w n_s-tuples of $\mathfrak{A}_1$ placed end to end. In particular, choose H to be a cyclic subgroup of G, where $H = < h >$ is of order n_H . For $\mathfrak{A}$ an ideal of KG, $\mathfrak{A}_1$ determines a cyclic code of KH. Now, $\forall a \in \mathfrak{A}$, by (4.3), $k_i^{-1} \pi_i(a) \in \mathfrak{A}_1$, and

$$k_i^{-1} \pi_i(a) = \sum_{j=1}^{n_H} \beta_{ij} h^j ,$$

we have

$$a = \sum_{i=1}^{w} \sum_{j=1}^{n_H} \beta_{ij} h^j k_i . \tag{4.4}$$

Definition 4.1.2. A quasicyclic code is a linear subspace of $V(GF(q))^n$ in which $\lambda | n$, and λ cyclic shifts of a code word is another code word.

Under this construction, it follows that if the n-tuples of G are "properly ordered" , then the code associated with the ideal $\mathfrak{A}$ is quasicyclic. As MacWilliams points out the quasicyclic nature can be seen in many ways. For instance, consider the ordering from (4.4)

$$(hk_1, h^2k_1, \ldots , h^{n_H}k_1, hk_2, \ldots , h^{n_H}k_w) ,$$

then n_H cyclic shifts of

$$\sum_{i=1}^{w} \sum_{j=1}^{n_H} \beta_{i,j} h^j k_i$$

accomplishes

$$\sum_{j=1}^{n_H} \beta_{w,j}\, h^j k_1 + \sum_{i=1}^{w-1} \sum_{j=1}^{n_H} \beta_{i-1,j}\, h^j k_i \quad . \qquad (4.5)$$

We note that $\Sigma\ \beta_{i,j}\ h^j$ is an element of $\mathfrak{A}_1$, for each i, therefore (4.5) represents an element of $\mathfrak{A}$.

Section 2

Definition 4.2.1. If $\mathfrak{A}$ is an ideal generated by $a \in KG$, then we define the generator matrix of $\mathfrak{A}$ as

$$M(\mathfrak{A}) = (a_{g_i^{-1} g_j}) \quad , \qquad (4.6)$$

where $a = \Sigma\ a_{g_i} g_i$, $a_{g_i} \in K$.

The first row of $M(\mathfrak{A})$ is

$$(a_{g_1},\ a_{g_2},\ .\ .\ .\ ,\ a_{g_n}) \quad ,$$

This is just the n-tuple associated with a. The second row of $M(\mathfrak{A})$ is

$$(a_{g_2^{-1} g_1},\ a_{g_2^{-1} g_2},\ .\ .\ .\ ,\ a_{g_2^{-1} g_n}) \quad ,$$

which is the n-tuple associated with $g_2 \cdot a$. But $g_1 a$, $g_2 a$, . . . , $g_n a$ span < a > in KG. Therefore, the matrix $M(\mathfrak{A})$ generates all of the n-tuples associated with the ideal < a >.

Definition 4.2.2. Given two matrices A and B, with

$$A = (a_{ij}) \ , \qquad B = (b_{lk}) \ ,$$

then the tensors or kronecker product of A with B is the matrix

$$A \dot{x} B = \begin{bmatrix} a_{11}B & . & a_{12}B & . & . & . & . & . & a_{1s}B \\ . & . & . & . & . & . & . & . & . \\ a_{21}B & . & a_{22}B & . & . & . & . & . & a_{2s}B \\ . & . & . & . & . & . & . & . & . \\ . & . & . & & & & & . & \\ . & . & . & & & & & . & \\ . & . & . & & & & & . & \\ . & . & . & . & . & . & . & . & . \\ a_{t1}B & . & a_{t2}B & . & . & . & . & . & a_{ts}B \end{bmatrix} \quad (4.6)$$

The tensor product of the vectors

$$v_1 = (a_1, \ . \ . \ . \ , a_s) \quad \text{and} \quad v_2 = (b_1, b_2, \ . \ . \ . \ , b_t)$$

is denoted by the vector

$$(a_1b_1, a_1b_2, \ . \ . \ . \ , a_1b_t, a_2b_1, \ . \ . \ . \ , a_2b_t, \ . \ . \ . \ , a_sb_1, \ . \ . \ , a_sb_t)$$

Definition 4.2.3. Let $\Omega(a) = \{ g \in G \mid \chi_g(a) \neq 0 \}$.

Theorem 4.2.4. (MacWilliams): Suppose G is the direct product of subgroups S and T. Suppose a is an idempotent of KS, and b is an idempotent of KT, then the ideal formed by the kronecker product

$$< a > \dot{x} < b > = \{ x \dot{x} y \mid x \in < a > , y \in < b > \} \ .$$

in KG, is < ab > .

Proof: If a is idempotent in KS and b is idempotent in KT, then

$$(a \cdot b)(a \cdot b) = a \cdot b \cdot b \cdot a = a \cdot b \cdot a = a \cdot b$$

So ab is idempotent. Let $\mathfrak{A} = < a >$ and $\mathfrak{B} = < b >$.
Let $n_s = |S|$ and $n_t = |T|$. The first row of $M(\mathfrak{A})$ is the n_s-tuple associated with the vector a. On the other hand the first row of $M(\ )$ is the n_t-tuple associated with b in KT. Thus, the first row of $M(\mathfrak{A}) \dot{\times} M(\mathfrak{B})$ is the n-tuple associated with $a \cdot b$ in KG. The second row of $M(\mathfrak{A}) \dot{\times} M(\mathfrak{B})$ is the n-tuple associated with $a \cdot t_2 b$. The third is associated with $a \cdot t_3 b$, and the $n_s + 1$ th row is the n-tuple associated with $s_2 a \cdot t_1 b$, and so on. Therefore, this matric generates the ideal < ab > . But $M(\mathfrak{A})$ generates < a > , and $M(\mathfrak{B})$ generates < b > . Therefore $M(\mathfrak{A}) \dot{\times} M(\mathfrak{B})$ necessarily generates $< a > \dot{\times} < b >$ as a vector space. Thus

$$< ab > = < a > \dot{\times} < b > .$$

Q.E.D.

Let $\Lambda(G)$ be defined as in Chapter 3, Section 5. Similarly, for S < G, the matrix

$$\Lambda(S) = (\psi_{s_i}(s_j)) \quad ,$$

where the ψ_{s_i} represents the irreducible characters of S.

Corollary 4.2.5. The set of nonzero characters of $a \cdot b$ is

$$\Omega(ab) = \{ \psi_{s_i} \phi_{t_j} \mid \psi_{s_i} \in \Omega(a) \text{ and } \phi_{t_j} \in \Omega(b) \} , \qquad (4.7)$$

where $\psi_{s_i} \dot{\times} \phi_{t_j} = \chi_{s_i t_j}$.

If we order the elements of G according to

$$s_1 t_1, s_1 t_2, \ldots , s_1 t_{n_T}, s_2 t_1, s_2 t_2, \ldots , s_2 t_{n_T}, \ldots , s_{n_S} t_{n_T},$$

then for $g = s_i t_j$, g is the $[(i-1)n_T + j]$ th element in the listing. The (ℓ,k) th element in $\Lambda(G)$ is $\chi_{g_\ell}(g_k)$, whereas the (ℓ,k) th element of $\Lambda(S) \dot{\times} \Lambda(T)$ is found by taking

$$\ell = (i_\ell - 1)n_T + j_\ell \quad ,$$

which implies since $j < n_T$

$$i_\ell = [\; l/n_T \;] + 1 \quad ,$$

and

$$j_\ell = l - n_T[\; l/n_T \;] \; .$$

Therefore,

$$\chi_{g_\ell}(g_k) = \chi_{s_i t_j}(s_\mu t_\nu) \quad ;$$

$$= \psi_{s_i}(s_\mu)\ \phi_{t_j}(t_\nu)\ ,$$

which is the (ℓ,k) th element of $\Lambda(S)\ \dot{x}\ \Lambda(T)$. Now, $\Lambda(G) \cdot \langle ab \rangle \cdot \Lambda^{-1}(G)$ is

$$[\Lambda(S)\ \dot{x}\ \Lambda(T)]\ [\langle a \rangle\ \dot{x}\ \langle b \rangle]\ [\Lambda^{-1}(S)\ \dot{x}\ \Lambda(T)]\ , \tag{4.8}$$

which is

$$[\Lambda(S) \langle a \rangle \Lambda^{-1}(S)]\ \dot{x}\ [\Lambda(T) \langle b \rangle \Lambda^{-1}(T)]\ .$$

The left hand side of the product is a diagonal matrix with nonzero's in those places associated with the nonzero characters of a. The right hand side of the product is also diagonal and has nonzeroes in those places corresponding to nonzero characters of b. Their kronecker product is diagonal and has nonzeroes in those places corresponding to the characters of (4.7).

Q.E.D.

Remark 4.2.6. This corollary and Theorem 4.2.4. imply that

$$\dim \langle ab \rangle = \dim \langle a \rangle \cdot \dim \langle b \rangle\ .$$

The method of kronecker products allows the construction of abelian codes with some desirable properties from cyclic codes.

Example 4.2.6. Consider the code of Example 2.2.2. The matrix generator of the code $\mathcal{C}_1$ is

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

The knonecker product of this code with itself is

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \dot{\times} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} =$$

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

This matrix generates a code of dimension four over a vector space of dimension nine. The code can correct all single errors, and some double errors. The original code $\mathcal{C}_1$ corrects no errors. Sending the code $\mathcal{C}_1$ over a channel twice is more efficient than the kronecker product code and still corrects all single errors. The idempotent generator of $\mathcal{C}_1$

is $x + x^2$. The kronecker product code is generated by the idempotent $(x^2 + x)(y^2 + y)$ in KG, where $G = \sigma(3) \times \sigma(3)$, according to Theorem 4.2.5, (where we have taken x and y to be generators of G and K = GF(2)). If there is imposed, upon the group G, an ordering such that

$$g_1 = 1, \quad g_2 = x, \quad g_3 = x^2, \quad g_4 = y, \quad g_5 = yx, \quad g_6 = yx^2$$

$$g_7 = y^2, \quad g_8 = y^2x \quad g_9 = y^2x^2$$

then the ideal generated by $(xy + x^2y^2)$ has the generator matrix

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

Under the decomosition $G = \langle x \rangle \times \langle y \rangle$, it is clear that the above code is not a knonecker product of an ideal in $K\langle x \rangle \otimes K\langle y \rangle$, but if we let $G = \langle xy \rangle \otimes \langle y \rangle$, then it is a kronecker product of the ideal $< xy + x^2y^2 >$ in $K< xy >$ with the ideal $K< y >$. Camion shows that every abelian code is a kronecker product code when we observe the code under a proper decomposition of G.

Definition 4.2.7. A code is separable if it can be written as the kronecker product of cyclic codes.

Camion showed that not all abelian codes are separable, but on the other hand, every abelian code is equivalent to a separable code. Therefore, it is sufficient for our purposes to consider the class of separable codes.

Theorem 4.2.8. (MacWilliams): Let $c \in KG$, and $\Omega_{KG}(c)$ be the set associated with the nonzero characters of $< c >$ in KG. Let $G = S \times T$, with $n_S = |S|$ and $n_T = |T|$. Let a and b be idempotents of KS and KT respectively. If

$$\Omega_{KS}(a)\ \Omega_{KT}(b) = \Omega_{KG}(c)$$

then $c = ab$.

Proof: Let $c = \sum_{i=1}^{n_S} \sum_{j=1}^{n_T} \gamma_{ij}\, s_i t_j$. From the M-S mapping

$$n\gamma_{i,j} = \sum_{g\ \Omega(c)} \chi_g(c)\ \chi_g(s_i t_j)^{-1} \quad .$$

Thus, since $\chi_g(c) = 1$,

$$n\gamma_{i,j} = \sum_{x \in \Omega(a)} \sum_{y \in \Omega(b)} \psi_x(s_i^{-1})\, \phi_y(t_j^{-1}) \quad .$$

Let

$$a = 1/n_S \sum_{i=1}^{n_S} \sum_{x \in \Omega(a)} \psi_x(s_i^{-1})\, s_i \quad ,$$

and let

$$b = 1/n_T \sum_{j=1}^{n_T} \sum_{y \in \Omega(b)} \phi_y(t_j^{-1})\, t_j$$

We have that a and b are idempotents of KS and KT respectively, from Theorem 3.4.3. Thus $c = ab$.

Q.E.D.

Section 3

Let G be a finite group of order n.

Definition 4.3.1. A linear code $\mathcal{C}$ will be called a G-code if for $\mathcal{C}$ an n-tuple code, the vectors of $\mathcal{C}$ are labled with elements of G, and for each n-tuple code word

$$(a_{g_1}, a_{g_2}, \ldots, a_{g_n}) \quad ,$$

we have

$$(a_{g_1 g^{-1}}, a_{g_2 g^{-1}}, \ldots, a_{g_n g^{-1}})$$

is also a code word.

All codes obtained from the ideals of group algebras are G-codes. In fact, Delsarte shows that the G-codes can be identified with the ideals of KG. Abelian codes are a special case of G-codes. If A is an automorphism of G, then the mapping

$$a = \sum_{g \in G} a(g)g \rightarrow A(a) = \sum_{g \in G} a(g)\ A(g) \qquad (4.9)$$

is an automorphism of KG.

Theorem 4.3.2: Let $\mathcal{C}$ be a G-code of G. Every automorphism, acting as a permutation on the coordinates of the code words transforms $\mathcal{C}$ into an equivalent G-code.

Proof: Since $\mathcal{C}$ is a G-code, there exists an ideal $\mathcal{Q} \subset KG$, which corresponds to $\mathcal{C}$. If A is an automorphism of G, then $A(\mathcal{Q})$ is an ideal of KG isomorphic to $\mathcal{Q}$. Also, $A(\mathcal{Q})$ is only a permuatation on the coordinates. Thus, the distance and weight properties of the code $\mathcal{Q}'$, associated with $A(\mathcal{Q})$, must be the same as those of the code $\mathcal{Q}$.

Q.E.D.

Let A be an automorphism of G, and consider for $h \in G$

$$< g, A(h) > = \chi_g\ (A(h)) \quad .$$

From our definition of irreducible characters

$$\chi_g(A(h)) = \chi_{g'}(h)$$

for some $g' \in G$. This relation defines a mapping which we call A^T, (i.e. $A^T(g) = g'$, $\forall g \in G$). This is written symbolically as

$$< g, A(h) > = < A^T(g), h > . \qquad (4.10)$$

Theorem 4.3.3:

i) If A is an automorphism of G, then A^T is an automorphism of G.

ii) $(A^T)^T = A$ and $(AB)^T = B^T A^T$.

Proof: i) Suppose $A^T(y) = A^T(y')$, then

$$< A^T(y), g > = < A^T(y'), g > ,$$

$\forall g \in G$, and

$$< y, A(g) > = < y', A(g) > ,$$

$\forall g \in G$. But this is true if and only if $y = y'$. Thus, A^T is one-to-one. Next, for $g, g' \in G$,

$$< x, A^T(gg') > = < A(x), gg' > ,$$

$$= < A(x), g > < A(x), g' > ,$$

$$= < x, A^T(g) > < x, A^T(g') > ,$$

$$= < x, A^T(g)\, A^T(g') > .$$

Hence, $A^T(gg') = A^T(g)\, A^T(g')$, and A^T preserves products.

Thus, A^T is an automorphism. To prove the second part of theorem, we note that A^T is an automorphism which implies

$$< A^T(x),y > = < x,(A^T)^T(y) >. \qquad (4.11)$$

On the other hand,

$$< A(y),x > = < y,A^T(x) > = < A^T(x),y > . \qquad (4.12)$$

Thus, (4.11) and (4.12) imply that

$$< x,A(y) > = < x,(A^T)^T(y) > ,$$

$\forall x,y \in G$. In addition,

$$< x,(AB)^T(y) > = < AB(x),y > ,$$

$$= < B(x),A^T(y) > ,$$

$$= < x,B^T(A^T(y)) > .$$

Which is what we set out to prove.

Q.E.D.

Again let r be the least integer such that the exponent of G divides q^r-1. Define

$$B_i : x \to x^{q^i} , \qquad 0 \leq i < r .$$

Then the B_i's are automorphisms of G, and

$$< x^{q^i}, y > = < x, y >^{q^i} = < x, y^{q^i} > .$$

Thus $B_i = B_i^{\ T}$, and if A is any automorphism of G, $A^{-1}B_iA(x) = x^{q^i}$. Thus, the B_i's are contained in the center of the group of automorphisms of G. Furthermore, the inverse automorphism of B_i is B_{r-i}, and $B_iB_j(x) = x^{q^{i+j}} = B_{i+j}(x)$, where addition is mod r. The set of B_i's is clearly a normal subgroup in the group of automorphisms on G. The subsets of G, which are invariant under the automorphism subgroup containing the B_i's, are the sets we have defined as q-power subsets of G.

Lemma 4.3.4. If A is an automorphism of G, then

$$< g, A(a) > = < A^T(g), a > ,$$

$\forall g \in G$ and $\forall a \in KG$.

Proof: For $g \in G$ and $a \in KG$,

$$< g, A(a) > = \sum_{k\ G} a(k) < g, A(k) > ,$$

$$= \sum_{k\ G} a(k) < A^T(g), k > ,$$

$$= < A^T(g), a > .$$

Q.E.D.

From this proof it is also clear that

$$< A(g),a > = < g,A^T(a) > ,$$

$\forall g \in G$ and $\forall a \in KG$.

Theorem 4.3.5. (Delsarte): The automorphism A of G transforms the ideal $\mathcal{Q}$ in KG, into the ideal $\mathcal{Q}'$ if and only if the automorphism defined by

$$A' = (A^{-1})^T = (A^T)^{-1}$$

transforms the annihilator of $\mathcal{Q}$ into the annihilator of $\mathcal{Q}'$.

Proof: We let $A(\mathcal{Q}) = \mathcal{Q}' = \{A(a) \mid a \in \mathcal{Q}\}$. Then

$$An[\mathcal{Q}'] = \{x \in G \mid < x,A(a) > = 0, \ \forall \ a \in \mathcal{Q}\},$$

$$An[\mathcal{Q}] = \{x \in G \mid < x,A^{-1}(b) > = 0, \ \forall \ b \in \mathcal{Q}'\} ,$$

$$= \{x \in G \mid < (A^{-1})^T(x),b > = 0, \ \forall \ b \in \mathcal{Q}'\} .$$

Thus, if $x \in An[\mathcal{Q}]$, then $(A^{-1})^T(x)$ is in the annihilator of $\mathcal{Q}'$. In fact, this argument is reversible.

Q.E.D.

Remark: $(((A^T)^{-1})^T)^{-1} = (((A^{-1})^T)^T)^{-1} = A$, and $(AB)' = ((AB)^{-1})^T = A'B'$, for A and B automorphisms of G.

From the above theorem, an ideal is mapped to itself under A if and only if its annihilator is mapped to itself under A'.

Definition 4.3.6. Let L(G) denote the automorphism group of G, and $L_q(G)$ the largest subgroup of L(G) whose elements all transform every ideal of KG into itself.

Let $B \in L_q(G)$, and $A \in L(G)$, and suppose $B(\mathfrak{A}) = \mathfrak{A}$. Let $x \in A(\mathfrak{A})$, then

$$ABA^{-1}(x) \in A(\mathfrak{A}).$$

Thus, ABA^{-1} transforms $A(\mathfrak{A})$ into $A(\mathfrak{A})$ and is therefore in $L_q(G)$, which is thereby normal in L(G). We state without proof:

Theorem 4.3.7:

i) The group $L_q(G)$ has order r; it consists of all automorphisms of the form $\mathfrak{B}_i$;

ii) The factor group $L(KG) = L(G)/L_q(G)$ acts as a permutation group on the minimal ideals $\mathfrak{A}_j$ in KG.

CHAPTER 5

Example 5.1.1. Let G = (8), and let K= GF(3). Then $G = \; g_0, g_1, \ldots, g_7$, where $g_0=1$. The 3-power subsets are 1 , g, g_3 , g_2, g_6 , g_4 , and g_5, g_7 . Therefore, there are three minimal ideals of dimension 2 and two of dimension 1. Now , $3^2 = 1$ mod8, and so L= K( )= GF(9), where is a primitive eighth root of unity. The field GF(9) consists of the elements 0,1,2, , +1, +2,2 +1, 2 +2 , where $^2 =$ +1. The group characters are

$g_0(g)=1$, $\quad g_{\cdot}(g)=$, $\quad g_2(g)=$ +1 , $\quad g_3(g)=2$ +1

$g_4(g)=2$, $\quad g_5(g)=2$ $\quad g_6(g)=$ +2 $\quad g_7(g)=$ +2.

According to the M-S mapping

$$e_0 = 2(\quad g_i^{-1}, g_0 \quad g_i),$$

$$= 2(g_0+g_1+g_2+g_3+g_4+g_5+g_6+g_7),$$

$$e_1 = 2(\quad g_i^{-1}, g+g_3 \quad g_i),$$

appling the above characters to this formula yields,

$$e_1 = g_0+ \; g_1+ g_3+ 2g_4+ 2g_5 + 2g_7.$$

The other idempotents are found similarly, and are

$$e_2 = g_0+2g_2+g_4+2g_6,$$

$$e_3 = 2g_0+g_1+2g_2+g_3+2g_4+g_5+2g_6+g_7,$$

$$e_4 = g_0+2g_1+2g_3+2g_4+g_5+g_7,$$

and $e_0+e_1+e_2+e_3+e_4 = 1$ in KG. The minimum Hamming weight of e_1 is 6. The minimum weight of $\langle e_2 \rangle$ is 4, and the minimum weight of $\langle e_4 \rangle$ is 6.

Example 5.1.2. Let G = $\sigma(2)$ $\sigma(2)$ $\sigma(2)$. Let K = GF(3), then for $g_0=1$, the multiplication is defined as follows

TABLE I

	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7
g_0	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7
g_1	g_1	g_0	g_4	g_5	g_2	g_3	g_7	g_6
g_2	g_2		g_0	g_6	g_1	g_7	g_3	g_5
g_3	g_3			g_0	g_7	g_1	g_2	g_4
g_4	g_4				g_0	g_6	g_5	g_3
g_5	g_5					g_0	g_4	g_2
g_6	g_6						g_0	g_1
g_7	g_7							g_0

The exponent of G is 2, and $3 = 1 \bmod 2$. Therefore, the M-S mapping is from $KG \to KG$. The 3-power subsets are $\{g_0\}, \{g_1\}, \{g_2\}, \ldots \{g_7\}$.

$$e_0 = 2\,(\,g_0 + g_1 + g_2 + g_4 + g_5 + g_6 + g_7\,)$$

$$e_j = 2\,(\sum_{i\neq j} g_i\,) + g_j\ .$$

All minimal ideals are of dimension 1. The minimum weight of the ideal $\langle e_j \rangle \oplus \langle e_k \rangle$ is 2, for $j,k \neq 0$. Therefore, this group generates poor codes over GF(3).

Example 5.1.3. Let $G = \sigma(4)\ \ \sigma(2)$, and let K=GF(3). Consider $\sigma(4) = \langle g_1 \rangle$ and $\sigma(2) = \langle g_4 \rangle$. The exponent of G is 4, and $3^2 = 1 \bmod 4$, so r=2, and L = GF(9). The 3-power subsets are $\{g_0\},\{g_1,g_3\},\{g_2\},\{g_5,g_7\},\{g_6\}$. The idempotents are

$$e_0 = 2\,(\,g_0 + g_1 + g_2 + g_3 + g_4 + g_5 + g_6 + g_7\,),$$

$$e_1 = g_0 + 2g_2 + g_4 + 2g_6\ ,$$

$$e_2 = 2g_0 + g_1 + 2g_2 + g_3 + 2g_4 + g_5 + 2g_6 + g_7\ ,$$

$$e_3 = 2g_0 + 2g_1 + 2g_2 + 2g_3 + g_4 + g_5 + g_6 + g_7\ ,$$

$$e_4 = g_0 + 2g_2 + 2g_4 + g_6\ ,$$

and

$$e_5 = 2g_0 + g_1 + 2g_2 + g_3 + 2g_4 + 2g_5 + g_6 + 2g_7\ .$$

The ideals $\langle e_1 \rangle$ and $\langle e_4 \rangle$ are both of dimension 2 over GF(3), and both have minimum Hamming weight 4.

Up until now, we have discussed only abelian G-codes. We consider G to be the group of quaternions of order 8. So, $G = \{1,i,i^2,i^3,j,j^3,k,k^3\}$ with ij=k, jk=i, ki=j, and ji=k^3. Let K= GF(3), then

$$e_1 = 2 + 2i^2 + 2i + 2i^3 + 2j + 2j^3 + 2k + 2k^3\ ,$$

$$e_2 = 2 + i^2\ ,$$

$$e_3 = \quad i + i^3 + j + j^3 + k + k^3$$

are the idempotents generators of the minimal two sided ideals in KG. The minimum weight of $< e_2 >$ is 2, while the minimum weight of $< e_3 >$ is 4.

The other group of order 8 is the dihedral group. The minimal two sided ideals of the group algebra generated by the dihedral group of order 8 have the same properties as the quaternion group algebra. This exhausts all possible G-codes which are ideals in group algebras of dimension 8 over GF(3). The cyclic group $\sigma(8)$ afforded the best distance properties. The ideals of Example 5.1.1 were of dimension 2 with minimum weight 6. The next best code is given by Example 5.1.4. The minimum weight of the code of dimension 3 was 4, which is less than the weights of the code given in Example 5.1.1, but the code of Example 5.1.4 can send three times as many different messages.

BIBLIOGRAPHY

1. Berlekamp, E. : Algebraic Coding Theory. 1968, New York, San Fransisco : McGraw-Hill.

2. Blake, I.F. : Algebraic Coding Theory. 1973, Stroudsburg, Pennsylvania : Dowden, Huchingson, and Ross, Inc.

3. Blake, I.F. : The Mathematical Theory of Coding. 1975, 111 Fifth Avenue, New York, New York : Academic Press.

4. Camion, P. : MRC Summary Report No. 1059,University of Wisconsin, Madison, Wisconsin, 1970.

5. Delsarte, P. : Automorphisms of Abelian Codes. 1970, Philips Res. Repts. 25, 389-403.

6. McWlliams, F.J. : Binary Codes Which Are Ideals in the Group Algebra of an Abelian Group. Bell System Tech. J,, 49 (1970) ,987-1011.

7. Peterson, W.W. : Encoding and Error Correction Procedures for the Bose-Chaudhuri Codes. I.R.E. Trans. Inform. Theory, IT-6, (1960), 459-470.