* This research was done while the author was visiting the Department of Statistics, University of North Carolina at Chapel Hill, in May, 1970, and was partially sponsored by the Army Research Office, Durham, under Grant No. DA-ARO-D-31-124-G910 and by the United States Air Force Office of Scientific Research under Contract No. AFOSR-68-1406.

COMBINATORIAL
MATHEMATICS
YEAR

February 1969 - June 1970

ABELIAN CODES*

by

P. Camion**
University of Toulouse

Department of Statistics
University of North Carolina at Chapel Hill

Institute of Statistics Mimeo Series No. 600.32

July, 1970

** and M. R. C, University of Wisconsin.

Abelian Codes*

P. Camion**
Department of Statistics
University of North Carolina at Chapel Hill

ABSTRACT

B.C.H. Codes are ideals of the K-algebra K[G], where K is a finite field and G is a cyclic group. We call "Abelian Codes" the ideals of K[G] when G is any finite abelian group. For studying such ideals, we introduce a tool which we have already used in [4] as "The Fundamental Isomorphism", in the case where G was cyclic. We call it here a Fourier Transform, briefly F.T., referring to [6]. The definition of the F.T., in the general case, requires, with a slight modification, the H. Mann's treatment of "Characters of Finite Abelian Groups" [8] of which use in [7] is rather close to the present.

This leads to a generalization of B.C.H. theorem ot Abelian Codes, giving their dimension and a lower bound for their distances. It is proved that all Abelian Codes are neither isomorphic nor trivially obtained from Kronecker products of cyclic codes.

Several classes of codes are given for which the exact values of distances are established. Finally, an example is worked out of binary code with length 49, dimension 18 and distance 12, which requires a special proof.

* *This research was done while the author was visiting the Department of Statistics, University of North Carolina at Chapel Hill, in May, 1970, and was partially sponsored by the Army Research Office, Durham, under Grant No. DA-ARO-D-31-124-G910 and by the United States Air Force Office of Scientific Research under Contract No. AFOSR-68-1406.*

** *University of Toulouse and M.R.C., University of Wisconsin.*

The proofs which are omitted here will be found in the paper "Abelian Codes" submitted to *Information and Control.*

1. Characters of Abelian Groups. *(Based on H. Mann [3].)*

1.1. The dual group of an abelian group.

Let G be an additive group and let $[a] = \{a,\dots,a^i,\dots,a^e=1\}$ be a multiplicative cyclic group of order e, where e is the exponent of G. $|G| = v$ is the order of G. A *character* χ of G is a homomorphism of G into $[a]$. We define the *sum* of two characters χ and χ'

(1) $$(\chi+\chi')(g) = \chi(g)\chi'(g), \quad \forall\, g \in G.$$

$[a]$ being an abelian group, the sum of two characters is a character.

Proposition 1. *The set of characters of a finite abelian group G is an additive group G^*, isomorphic to G; G is itself the group of characters of G^*.*

Outline of the argument.

G is the direct sum of cyclic groups

(2) $$G = G_1 \oplus \dots \oplus G_s \;;$$

and if g_i is a generator of G_i, $i = 1,\dots,s$, every g in G may be written uniquely as

(3) $$g = \ell_1 g_1 + \dots + \ell_s g_s$$

where ℓ_i is an integer modulo v_i $(v_i = |G_i|)$. We then define s distinct characters χ_j, $j = 1,\dots,s$, by

(4) $$\chi_j(g_i) = a^{\delta_{ij} e/v_i}, \quad i,j = 1,\dots,s.$$

So every character may be written uniquely

(5) $\quad \chi = h_1\chi_1 + \ldots + h_s\chi_s$

where h_i is an integer modulo v_i, and the announced isomorphism is defined by

(6) $\quad g_i \mapsto \chi_i, \quad i = 1,\ldots,s.$

1.2. The monomial representation of G and G*.

From (2), G is isomorphic with the group of s-tuples with the form

(1) $\quad (\ell_1,\ldots,\ell_s)$

where ℓ_i runs over the set of integers modulo v_i and we may thus represent an element of G by the monomial

(2) $\quad X_1^{\ell_1} X_2^{\ell_2} \ldots X_s^{\ell_s}$, (briefly X^g).

To the sums of elements of G will correspond the product of monomials; and so G* is represented by a group of monomials with the form

$$U_1^{h_1} \ldots U_s^{h_s} \quad \text{(briefly } U^\chi\text{)}.$$

Now let $r_i = e/v_i$. If we substitute $a^{h_i r_i}$ to X_i in (2), we obtain

(3) $\quad \prod_i a^{\ell_i h_i r_i} = a^{\sum_i \ell_i h_i r_i}$

and so do we by substituting $a^{\ell_i r_i}$ to U_i in (3).

g considered as a character of G* is thus the monomial function (2), and χ is the function (3). We shall now write χg or $g\chi$ for $\chi(g) = g(\chi)$.

2. The Fourier Transform of Albebras of Abelian Groups over Integer Domains.

2.1. Integer Domain L.

Given an abelian group with exponent e, we consider any integral domain L whose multiplicative monoid contains a cyclic subgroup H of order e. *The characteristic of such a ring could not divide* e.

We now consider the convolution L-algebra $L[G]$.

2.2. The Fourier Transform.

Referring again to H. Mann [3], we represent an element of $K[G]$

(1) $$x \equiv \sum_g x_g X^g, \quad x_g \in K, \quad g \in G.$$

for any subring K of L.

So, every character is extended into a K-homomorphism of $K[G]$ into L, by

(2) $$\chi(x) \equiv \sum_g x_g \chi g.$$

Now we define the Fourier Transform x^t (briefly F.T.) of $x \in K[G]$ by

(3) $$x^t \equiv \sum_\chi x^t_\chi U^\chi,$$

where $x^t_\chi \equiv \chi(x)$ as defined by (2).

According to the structure involved, x^t may be understood to be the second member of (3) or the e-tuple $(x^t_\chi)_{\chi \in G^*} \in L^{G^*}$.

Proposition 2.1. *For every subring K of L_1, the F.T. is a K-isomorphism of $K[G]$ into L^{G^*}.*

2.3. The inversion formula.

The element $\sum_g x_g X^g$ of $K[G]$ may be obtained from its F.T. by the inversion formula

$$\frac{1}{v} \sum_{\chi} x_{\chi}^{t}(\chi g)^{-1} = x_{g}.$$

Remark. By 2.2 (3) and 1.2 (3), vx_g may be obtained as the image of the polynomial function 2.2 (3) for the argument corresponding to $-g$.

2.4. Injectivity of the Fourier Transform.

The following statements are easily proved:

THEOREM 2.1. *For every subring K of L, the F.T. is a K-isomorphism of $K[G]$ into L^{G*}.*

COROLLARY. *If v^{-1} belongs to L, μ^{-1} is the F.T. and is an L-isomorphism of $L[G]$ onto L^{G*}.*

2.4. The ideals of $K[G]$, when L is a field, algebraic over K.

We have

THEOREM 2.3. *Every ideal of $K[G]$ is the direct sum of the minimal ideal that it contains, considered as subspaces of $K[G]$ over K.*

Every minimal ideal, considered as a subring of $K[G]$ is isomorphic to some subfield of $K(a)$. The dimension over K of an ideal T of $K[G]$ is

$$v - \min_{x \in T} |\{\chi | \chi(x) = o\}| .$$

THEOREM 2.4. *A polynomial belongs to the F.T. of $K[G]$ if and only if it is fixed by every Galois K-automorphism of L extended to $L[G]$.*

COROLLARY. *The minimal supports of G^* are the orbits of G^* under the subgroup of the Euler group of e isomorphic to the Galois group of L over K.*

Theorem 2.4 was proved for G cyclic in [4].

3. Abelian Codes.

3.1. Introduction.

Let $K = F_2$ and let G be the abelian group of type $(3,3)$. It follows from the corollary of Theorem 2.4 that G^* is partitioned into five minimal supports and hence that $K[G]$ has 2^5 ideals. Now the number of distinct ideals having a generator with the form

$$(1) \qquad g(X_1,\ldots,X_s) = g_1(X_1)g_2(X_2)\ldots g_s(X_s)$$

is 2^4. A code generated by a polynomial with the form (1), we shall call a *separate code*.

3.2. Separate codes.

3.2.1. The support polynomial.

To every ideal C of $K[G]$ corresponds a polynomial $\sum_{\chi\in J} U^{\chi}$ where J is the support of the ideal $\mu^{-1}C$. We shall call such a polynomial the *support polynomial of the code C as well as of its F.T. C^t.*

We have

Theorem 3.1. *The three following statements are equivalent.*

1. *An abelian code is separable.*
2. *An abelian code is the Kronecker product of cyclic codes.*
3. *The support polynomial of an abelian code has the form*

$$f(U_1,\ldots,U_s) = \prod_{1\le j\le s} f_j(U_j).$$

Corollary. *Burton and Weldon (1965) [3]. Let $(n_1,n_2) = 1$. A is a cyclic code of length n_1 generated by $a(X)$. B is a cyclic code of length n_2 generated by $b(Y)$. Then the Kronecker product of A and B is a cyclic code of length n_1n_2 generated by*

$$g(Z) = a(Z^{p_2n_2})b(Z^{p_1n_1})\,mod(Z^{n_1n_2}-1),$$

where $n_1p_1+n_2p_2 = 1$.

4. A General Statement for the B.C.H. Theorem.

Let $f(U)$ be the support polynomial of an abelian code. Let $f^{(\chi)}(U) = U^{\chi}f(U)$. $d^{(\chi)}$ denotes the degree of $f^{(\chi)}$ in U_j and $f_j^{(\chi)}$ is the coefficient of $U_j^{d_j^{(\chi)}}$ in $f^{(\chi)}(U)$

The *apparent distance* $d^*(f)$ of a polynomial $f(U)$ is defined by

$$d^*(f) = \max_{\chi\in G^*} \max_{1\le j\le s} d^*(f_j^{(\chi)})(v_j-d_j^{(\chi)}) .$$

Now, given an abelian code C with support polynomial u_J, we denote by F the set of all terms f that may be obtained by writing $U_J = f+g$, with $f \neq o$ and $\sigma f = f$ for every Galois automorphism. Then the *apparent distance* $d^*(C)$ of a code C with support polynomial u_J will be

$$(3) \qquad \min_{f\in F} d^*(f)$$

where $d^*(f)$ is given by (2).

Theorem 4.1. *$d^*(C)$ is a lower bound for the distance of C.*

5. Examples of Abelian Codes.

5.1. Generalized first order Reed-Muller Codes.

The general support polynomial of such a code is

$$u_J = \sum_{1\le i\le s} \sum_{o\le j\le \nu} U_i^{q^j}$$

for $K = F_q$, $L = F_{q^\nu}$. $v_1 = v_2 = \dots = v_s = q^\nu-1$.

STATEMENT 5.1. *The generalized first order Reed-Muller codes, ideals of* $F_q[G]$, *where* G *is the direct sum of* s *cyclic groups of order* $q^\nu-1$ *have length* $(q^\nu-1)^s$, *and dimension* νs. *The* $q^{\nu s}$ *vectors of the code are partitioned into* $s+1$ *classes. The* i*-th class,* $i = o,\dots,s$, *contains*

(2) $\binom{s}{i}(q^\nu-1)^i$ *vectors of weight* $(q^\nu-1)^{s-i}(q-1)\dfrac{(q^\nu-1)^i-(-1)^i}{q}$.

The distance of the code is

(3) $q^{\nu-1}(q^\nu-2)(q^\nu-1)^{s-2}(q-1)$.

COROLLARY 5.1. *If* $(\nu,q-1) = 1$, *there exists a linear code over* F_q *with length* $(q^\nu-1)^s/(q-1)$, *dimension* νs *and weights and distances given by dropping the factor* $q-1$ *in (2) and (3).*

EXAMPLES. For $q = 3$, $\nu = 3$, $s = 2$, Corollary 5.1 gives a code over F_3 with length $n = 338$, dimension $k = 6$ and distance $d = 225$.

Here k reaches the Plotkin bound.

5.2. A binary non separable abelian code C of length 49, dimension 18 and distance 12.

The support polynomial of the code is

$$\sum_{o\le\ell,h<\nu} U^{q^\ell} V^{-q^h} + \sum_{o\le\ell,h<\nu} U^{-q^\ell} V^{q^h}$$

where $q = 2$, $\nu = 3$, $s = 2$.

A last remark. *(After discussion with H. Mann.)*

H. Mann observes that an ideal of $K[G]$ which is not a Kronecker product of cyclic codes may become so by an automorphism of the group G^* of characters which would correspond to replacing each U_i by a monomial in the support polynomial.

Now, for Example 5.2, it may be seen that it is certainly not possible to exhibit such an automorphism of G^*.

REFERENCES

[1] Albert, A., "Fundamental Concepts of Higher Albegra", The University of Chicago Press, 1956.

[2] Assmus, E.F., Jr. and H.F. Mattson, 1966, "Perfect Codes and the Mathieu Groups", Arch. Math. 17, 121-135.

[3] Berlekamp, E.R., "Algebraic Coding Theory", 1968, McGraw-Hill Book Company, New York.

[4] Camion, P., 1968, "A Proof of Some Properties of R.M. Codes by Means of the Normal Basis Theorem", Proceed. of the Conf. on Comb. Math. (April 10-14, 1967), The Univ. of N.C. Press, Chapel Hill, N.C.

[5] Camion, P., 1966, "Codes correcteurs d'erreur", Revue du CETHEDEC 3ime Trimestre 1966 - Numero special.

[6] Loomis, L.H., 1953, "Abstract Harmonic Analysis", New York, Van Nostrand.

[7] MacWilliams, F.J. and H.B. Mann, 1968, "On the p-Rank of the Design Matrix of a Difference Set".

[8] Mann, H.B., 1965, "Addition Theorems", Wiley & Sons.

[9] Peterson, W.W., "Error-Correcting Codes", Wiley, 1962.