AUTOMORPHISMS OF ABELIAN CODES*)

by P. DELSARTE

Abstract

By using the characters of the group algebra of a finite abelian group $G$ over a finite field, one derives a method to find the equivalence classes of abelian $G$-codes under the group of automorphisms of $G$, acting as permutations on the coordinates of the codes. In the same manner, one obtains the subgroup of these permutations which transform a given $G$-code into itself. The case where $G$ is an elementary abelian group is examined in detail and some examples are given.

1. Introduction

Cyclic codes can be defined as ideals in the group algebra of a cyclic group over a finite field. Working independently, Berman 6,7), Camion 8) and Mac-Williams 9) introduced a more general class of codes, namely the linear $q$-ary codes of length $n$ that are ideals in the group algebra of a finite abelian group $G$ (of order $n$) over $GF(q)$. Such codes will be referred to as abelian $G$-codes. The representation of $G$ as a regular permutation group of degree $n$ then leaves every $G$-code invariant. When $n$ and $q$ are relatively prime, the structure of these ideals is very similar to that of cyclic codes. In particular, to each ideal corresponds a subset of the group $G$, called the annihilator of the ideal, which entirely specifies the code and which can be identified with the set of zeros of the generator polynomial in the case of cyclic codes.

It can be shown that every automorphism of $G$, acting as a permutation on the coordinates, transforms any $G$-code into another equivalent $G$-code. In this paper is shown how to check whether two $G$-codes are equivalent under a given automorphism of $G$, by using the annihilators of the codes. By this method, the equivalence classes of the abelian codes are easily determined and some automorphisms of these codes are immediately found.

When $G$ is the elementary abelian $s$-group of order $n = s^m$ (where $s$ is a prime number), one proves that the automorphism group of $G$ acts as a transitive permutation group on the nontrivial irreducible $G$-codes. Moreover, in some cases, this group is doubly and even triply transitive. Two examples, namely $n = 25$ and $n = 27$, provide a good illustration of the theory.

2. Definitions

Let $G$ be a finite abelian group of order $n$ and let $C$ denote a linear code of length $n$, over the field $F = GF(q)$, whose coordinates are numbered with the elements of $G$. The code $C$ will be called a $G$-code over $F$ if, for every element $g$ of $G$, the substitution

$$g : x \mapsto g(x) = g \cdot x \quad (x \in G),$$

acting as a permutation on the coordinates of the code, transforms any vector of $C$ into another vector of $C$. In other words, the representation $G$ of $G$ as a regular permutation group is contained in the automorphism group of any $G$-code. Let

$$a = (a(z_1), a(z_2), \ldots, a(z_n)), \quad a(z_i) \in F,$$

be a vector of length $n$ over $F$, where $z_1, z_2, \ldots, z_n$ are the elements of $G$. Next, define

$$a = \sum_{i=1}^{n} z_i a(z_i) = \sum_{x \in G} x \cdot a(x)$$

as the element corresponding to $a$ in the group algebra $FG$ of the group $G$ over the field $F$. It is obvious that the mapping

$$a \in F^n \mapsto a \in FG$$

is an isomorphism between $F^n$ and $FG$, considered as vector spaces over $F$.

**Theorem 1.** There is a one-to-one correspondence between the $G$-codes over $F$ and the ideals in the group algebra $FG$.

**Proof:** Let $C$ be a linear code of length $n$ over $F$, i.e. a subspace of $F^n$, and denote by $R$ the corresponding subspace of $FG$, so that $C = R$. If $g$ is an element of $G$, the substitution $g$ transforms the vector (1) into

$$g(a) = (a(g^{-1} z_1), a(g^{-1} z_2), \ldots, a(g^{-1} z_n))$$

and thus $a$ into

$$g(a) = \sum_{x \in G} x \cdot a(g^{-1} x) = g \cdot a.$$

Next, assume that $C$ is a $G$-code, so that $g(a)$ belongs to $C$ whenever $a$ belongs to $C$. Then, according to (2), one has

$$(a \in R, g \in G) \Rightarrow (g \cdot a \in R)$$

and $R$ is an ideal in $FG$.

3. The characters of $G$ over $F$

In the following, we always assume that $n$ and $q$ are relatively prime, so that
Let \( \nu \) be the least integer such that \( x^\nu = 1 \), for every element \( x \) of \( G \). An \( F \)-character \( \psi \) of \( G \) is a homomorphism of \( G \) into the group of \( \nu \)th roots of unity over \( F \). The group \( G' \) of all distinct \( F \)-characters has order \( n \) and is isomorphic to the group \( G \) itself. Moreover, we may number the characters \( \psi_x \) with the elements \( x \) of \( G \) in such a way \(^5\) that
\[
\psi_x(y) = \psi_y(x), \quad \forall \ x, \ y \in G.
\]

We now introduce a useful notation for characters: we define the \( F \)-product of two elements \( x, y \) of \( G \) by
\[
\langle x, y \rangle = \psi_x(y).
\]
By definition, the \( F \)-product has the three following properties (where \( x, x', y, z \) are any elements of \( G \)):
\[
\langle x, yz \rangle = \langle x, y \rangle \langle x, z \rangle, \tag{3}
\]
\[
\langle x, y \rangle = \langle y, x \rangle, \tag{4}
\]
\[
\langle x, y \rangle = \langle x', y \rangle, \quad \forall \ y \in G \leftrightarrow (x = x'). \tag{5}
\]
Moreover, by a well-known theorem \(^5\), one has
\[
\sum_{x \in G} \langle x, y \rangle = \begin{cases} n, & \text{if} \quad y = 1 \\ 0, & \text{if} \quad y \neq 1, \end{cases} \tag{6}
\]
where 1 denotes the unit of \( G \).

We now examine how the automorphisms of \( G \) act on the \( F \)-product. Let
\[
A : x \rightarrow A(x)
\]
be an automorphism of \( G \). Using (3), one easily verifies that the mapping
\[
x \rightarrow \psi(x) = \langle A(x), y \rangle
\]
is a character of \( G \), for every \( y \) in \( G \). In fact \( A(x'x') = A(x)A(x') \) implies \( \psi(x'x') = \psi(x) \psi(x') \). Hence, there exists a unique element \( z = A^T(y) \) in \( G \) such that
\[
\langle A(x), y \rangle = \langle x, A^T(y) \rangle. \tag{7}
\]

**Theorem 2.** If \( A \) is an automorphism of \( G \), the mapping
\[
A^T : y \rightarrow A^T(y) \tag{8}
\]
is also an automorphism of \( G \).
Proof: Assume first that \( A^T(y) = A^T(y') \). By (5) and (7) this implies \( y = y' \) and (8) is a one-to-one mapping. On the other hand, using (3), (4) and (7), one has

\[
\langle x, A^T(y y') \rangle = \langle A(x), y \rangle \langle A(x), y' \rangle = \langle x, A^T(y) \rangle \langle x, A^T(y') \rangle = \langle x, A^T(y) A^T(y') \rangle.
\]

Hence, \( A^T(y y') = A^T(y) A^T(y') \) and the theorem is proved. The automorphism \( A^T \) is called the transpose of \( A \).

**Theorem 3.** The transposition satisfies

\[
(A^T)^T = A \quad \text{and} \quad (AB)^T = B^T A^T,
\]

if \( A \) and \( B \) are two automorphisms of \( G \).

**Proof:** The first part of the theorem immediately follows from the definition (7) of the transposition. In order to prove the second part, we use (7) three times:

\[
\langle x, (AB)^T(y) \rangle = \langle AB(x), y \rangle = \langle B(x), A^T(y) \rangle = \langle x, B^T A^T(y) \rangle.
\]

Let \( r \) be the least integer such that \( r \) divides \( q^r - 1 \). It is easily seen that the \( r \) substitutions

\[
B_i : x \rightarrow x^{q^i} \quad (i = 0, 1, \ldots, r - 1)
\]

are symmetric (i.e. \( B_i^T = B_i \)) and form a normal subgroup of the automorphism group of \( G \). The subsets of \( G \) which are invariant under that subgroup are called the \( q \)-subsets of \( F \). In other words, \( K \) is a \( q \)-subset of \( G \) whenever \( K \subseteq G \) and

\[
(x \in K) \Rightarrow (x^q \in K).
\]

If \( x \) is an element of \( G \), the minimal \( q \)-subset of \( G \) containing \( x \) is

\[
Q(x) = \{x, x^q, x^{q^2}, \ldots, x^{q^{k(x)-1}} \},
\]

where \( k(x) \) is the smallest integer such that

\[
x^{q^{k(x)-1}} = 1.
\]

Since \( x^{q^r-1} = 1 \), \( k(x) \) divides \( r \). According to the definitions, \( G \) can be written as the union of all its minimal \( q \)-subsets:

\[
G = Q(x_0) \cup Q(x_1) \ldots \cup Q(x_t)
\]

and every \( q \)-subset of \( G \) is the union of some of the \( Q(x_i) \).
4. Structure of the ideals in $FG$

The $F$-characters of $G$ are extended to the group algebra $FG$ in the following manner: The field $F_r = GF(q^r)$ is the smallest extension field of $F$ containing all the $v$th roots of unity. If $a$ belongs to $FG$, the characters of $a$ are defined by

$$\langle x, a \rangle = \sum_{y \in G} \langle x, y \rangle a(y) \in F_r,$$

for each element $x$ of $G$. One easily verifies that

$$\langle x, a + b \rangle = \langle x, a \rangle + \langle x, b \rangle$$

and

$$\langle x, ab \rangle = \langle x, a \rangle \langle x, b \rangle,$$

for $a, b \in FG$ and $x \in G$. Moreover one has (over $F = GF(q)$)

$$\langle x, a \rangle^q = \sum_{y \in G} a(y) \langle x, y \rangle^q,$$

and thus, by (3):

$$\langle x, a \rangle^q = \langle x^q, a \rangle.$$  \hspace{1cm} (13)

From (13) and the definition of $k(x)$, it follows that $\langle x, a \rangle$ belongs to the field $GF(q^{k(x)})$, which is a subfield of $F_r$.

Theorem 4. (i) If $H$ is a subset of $G$, its annihilator in $FG$, defined as

$$H^o = \{ a \in FG | \langle x, a \rangle = 0, \forall x \in H \},$$

is an ideal in $FG$.

(ii) If $R$ is a subset of $FG$, its annihilator in $G$, defined as

$$^oR = \{ x \in G | \langle x, a \rangle = 0, \forall a \in R \},$$

is a $q$-subset of $G$.

Proof: Part (i) of the theorem follows from eqs (12). Part (ii) follows from (13) and the definition (10) of a $q$-subset.

For future use, we now recall the definition and some properties of the Mattson–Solomon mapping $4,5,9)$. To each element $a$ in $FG$ we associate an element

$$a = \sum_{x \in G} x \langle x, a \rangle$$

which belongs to the group algebra $F,G$ of the group $G$ over the field $F_r$. From (13) one deduces

$$a^q = a.$$  \hspace{1cm} (17)

On the other hand, using the properties (3), (4) and (6) of the $F$-product, one obtains the following formula $5$):
\[ a = \frac{1}{n} \sum_{x \in G} x \langle x^{-1}, a \rangle. \]  

(18)

Hence, if \( X \) is defined as the subset of all elements \( \alpha \) in \( F,G \) satisfying (17), we have the following theorem.

**Theorem 5**. The mapping

\[ a \in FG \rightarrow \alpha \in X \]  

(19)

is an isomorphism between \( FG \) and \( X \) (considered as vector spaces of dimension \( n \) over \( F \)); the inverse mapping of (16) is given by (18).

**Proof**: The proof follows from the fact that (17) and (18) imply

\[ (a(x))^q = a(x) \]

so that \( a(x) \) belongs to \( F \) (and thus \( a \in FG \)) whenever \( a \) satisfies (17). We examine in some detail the mapping (19): Condition (17) is equivalent to

\[ \alpha(x) = (\alpha(x))^q, \; \alpha(x) \in GF(q^{k(x)}), \]  

(20)

if \( \alpha = \Sigma \alpha(x) \). According to the decomposition (11) of \( G \) into its minimal \( q \)-subsets, the elements \( \alpha \) of \( X \) are of the form

\[ \alpha = \alpha_0 + \alpha_1 + \ldots + \alpha_t, \]  

(21)

with

\[ \alpha_t = \sum_{j=0}^{k_t-1} (x_t c_t)^{q^j}, \; c_t \in GF(q^k), \]  

(22)

where \( k_t = k(x_t) \). This immediately follows from (20), if one sets \( c_t = \alpha_t(x_t) = \alpha(x_t) \). The element \( a_t \) in \( FG \) corresponding to \( \alpha_t \) under the Mattson–Solomon mapping is given (see (18)) by

\[ a_t(x) = \frac{1}{n} T_{k_t} (c_t \langle x^{-1}, x_t \rangle), \]  

(23)

where

\[ T_k(z) = z + z^q + \ldots + z^{q^{k-1}} \]

is the trace of \( z \) (a linear mapping from \( GF(q^k) \) onto \( GF(q) \)). Accordingly, the element \( a \) of \( FG \) can be written as

\[ a = a_0 + a_1 + \ldots + a_t. \]  

(24)

From (12) and (16), one also deduces

\[ \langle x, a_i a_j \rangle = a_i(x) \alpha_j(x). \]
For $i \neq j$, the definition (22) implies $\alpha_i(x) \alpha_j(x) = 0$. Hence, $\alpha_i \alpha_j$ corresponds to zero in $X$, so that one has

\[ a_i a_j = 0, \quad \text{if} \quad i \neq j. \]

In fact, the decomposition (24) corresponds to the well-known representation of $FG$ as the direct sum of its minimal ideals\(^2,9\). This will be proved in the following (see theorem 10).

In the rest of this section, we examine how the $q$-subsets of $G$ and the ideals in $FG$ are related together.

Theorem 6. If $H$ is a $q$-subset of $G$, the dimension of the ideal $H^o$ (over $F$) is equal to

\[ \dim (H^o) = n - |H|. \]

Proof: Let $X'$ be the image of $H^o$ under the Mattson-Solomon mapping (19). Since $H^o$ is a subspace of $FG$, $X'$ is a subspace of $X$. The subset $K = G \setminus H$ of $G$ clearly is a $q$-subset, so that we can write

\[ K = \bigcup_{i \in I} Q(x_i), \]

where $I$ is a subset of $J = \{0, 1, \ldots, t\}$. By (14) and (21), the elements $\alpha$ of $X'$ are of the form

\[ \alpha = \sum_{i \in I} \alpha_i, \]

and the number of these elements is equal to

\[ |X'| = \prod_{i \in I} q^{|I|}. \]

Hence, the dimension of $X'$ over $F = GF(q)$ is equal to

\[ k = \sum_{i \in I} k_i = |K|, \]

and the theorem is proved, since $|K| = n - |H|$. 

We now state, without demonstration, the following result due to MacWilliams and Mann\(^5\).

Theorem 7. If $R$ is an ideal in $FG$, its dimension over $F$ is equal to

\[ \dim (R) = n - |^oR|, \]

where $^oR$ denotes the annihilator of $R$ in $G$.

The theorems 6 and 7 can be considered as “dual” of each other. They lead to an important result:
Theorem 8. There is a one-to-one correspondence between the $q$-subsets $H$ of $G$ and the ideals $R$ in $FG$, such that

$$R = H^o, \ H = \circ R.$$  

Moreover, the dimension of $R$ over $F$ is equal to

$$\dim (R) = n - |H|. \quad (25)$$ 

Proof: Let $R$ be an ideal in $FG$ and set $H = \circ R$. By theorem 7, eq. (25) is satisfied. On the other hand, it is obvious by (14) and (15) that $R$ is a subideal of $H^o$. But, according to theorem 6, $\dim (H^o) = n - |H|$; so that $\dim (R) = \dim (H^o)$ and thus $R = H^o$. By the same reasoning, if $H$ is a $q$-subset of $G$, one shows that $R = H^o$ is the unique ideal in $FG$ for which $H = \circ R$.

Corollary 9. A subset $R$ of $FG$ is an ideal if and only if $R = (\circ R)^o$. A subset $H$ of $G$ is a $q$-subset if and only if $H = \circ (H^o)$.

By theorems 4 and 8, it is obvious that the irreducible (or minimal) ideals in $FG$ correspond to the maximal $q$-subsets of $G$ and thus are of the form

$$R_i = (G \setminus \mathcal{Q}(x_i))^o.$$ 

Hence $\dim (R_i) = k_i$, and the elements $a_i$ of $R_i$ are given by (23). Summarizing the above results, we have the following theorem.

Theorem 10. The decomposition (24) corresponds to the representation of $FG$ as the direct sum of its minimal ideals, i.e.

$$FG = R_0 + R_1 + \ldots + R_t.$$ 

Moreover, any ideal in $FG$ is of the form

$$R = \sum_{i \in I} R_i,$$

where $I$ is a subset of $J = \{0, 1, \ldots, t\}$. The annihilator $H = \circ R$ of $R$ is

$$H = \cup_{i \in J} \mathcal{Q}(x_i).$$

This theorem leads to the following method for the analysis of ideals in $FG$ (or, equivalently, of $G$-codes over $F$): Given a subset $I$ of $J$, one calculates the components $a_i$ ($i \in I$) of each element $a$ in the ideal $R$ by using eq. (23). This method is an extension of that of Mattson and Solomon 4) for cyclic codes.

Remark. For $x_0 = 1$, $\mathcal{Q}(x_0) = \{1\}$, the irreducible ideal $R_0$ has dimension 1
and is called the \textit{trivial ideal}. It is easily seen that the elements of $R_0$ are of the form

$$a = c \sum_{x \in G} x,$$

where $c$ is any element of $F$. If $R$ is an ideal in $FG$, one deduces from theorem 10 that

$$(R_0 \nsubseteq R) \iff (1 \in ^oR).$$

The condition $(1 \in ^oR)$ means that the "coordinate sum" $\sum a(x)$ of every element $a$ in $R$ is equal to zero. In the binary case ($q = 2$), all vectors $a$ of the $G$-code $R$ then have an even weight.

5. Automorphisms of $G$-codes

In sec. 2, we have seen that the regular permutation group $G$ leaves any $G$-code invariant. We now examine how the automorphism group of $G$ acts on the $G$-codes.

\textbf{Lemma 11.} If $A$ is an automorphism of $G$, the mapping

$$a = \sum_{x \in G} x a(x) \rightarrow A(a) = \sum_{x \in G} A(x) a(x)$$

is an automorphism of the algebra $FG$.

\textit{Proof:} One easily verifies that

$$A(a + b) = A(a) + A(b), \quad \text{and} \quad A(ab) = A(a) A(b),$$

if $a$ and $b$ are any two elements of $FG$.

\textbf{Theorem 12.} Every automorphism of $G$, acting as a permutation on the coordinates of the codes, transforms a $G$-code into another \textit{equivalent} $G$-code.

\textit{Proof:} Let $C$ be a code of length $n$ over $F$, and let $R$ be the subset of $FG$ corresponding to $C$. If $A$ is an automorphism of $G$, the element $a$ of $R$ is transformed into $A(a)$ by the permutation $A$. Lemma 11 then shows that $A(R)$ is an ideal in $FG$ whenever $R$ is an ideal in $FG$, so that the theorem is proved.

In the following, we assume that $n$ and $q$ are relatively prime and we examine how the annihilators of the ideals $R$ and $A(R)$ are related to each other. We first need a lemma:

\textbf{Lemma 13.} Let $A$ be an automorphism of $G$, then

$$\langle x, A(a) \rangle = \langle A^T(x), a \rangle,$$

for every $x$ in $G$ and $a$ in $FG$.

\textit{Proof:} From (7) and (26) one deduces
As a consequence of theorem 8, we then have the following theorem.

**Theorem 14.** The automorphism $A$ of $G$ transforms the ideal $R$ (in $FG$) into the ideal $R'$ if and only if the automorphism

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

transforms the annihilator of $R$ in $G$ into the annihilator of $R'$.

**Proof:** By (15) and lemma 13, with $R' = A(R) = \{A(a)|a \in R\}$, one has

$$\text{o}(R') = \{a \in FG|\langle x, A^{-1}(a) \rangle = 0, \forall x \in H\}$$

$$= \{a \in FG|\langle A'(x), a \rangle = 0, \forall x \in H\}.$$ 

Hence $\text{o}(R') = A'(H)$, where $A' = (A^{-1})^T$. By theorem 3, one also has $A' = (A^T)^{-1}$.

**Remark:** The mapping $A \rightarrow A'$ satisfies

$$(A')' = A \quad \text{and} \quad (AB)' = A' B',$$

if $A$ and $B$ are two automorphisms of $G$. This is an immediate consequence of theorem 3.

As a corollary of theorem 14, we have:

**Corollary 15.** The automorphism $A$ of $G$ transforms the ideal $R$ into itself if and only if the automorphism $A'$ transforms the annihilator of $R$ into itself.

Let $L(G)$ denote the automorphism group of $G$ and $L_q(G)$ the greatest subgroup of $L(G)$ all of whose elements transform any ideal in $FG$ into itself. Obviously, $L_q(G)$ is a normal subgroup of $L(G)$.

**Theorem 16.** (i) The group $L_q(G)$ has order $r$; it consists of all automorphisms $B_i$ of the form (9).

(ii) The factor group $L(FG) = L(G)/L_q(G)$ acts as a permutation group on the minimal ideals $R_j$ in $FG$.

**Proof:** Let $A$ be an element of $L_q(G)$. By corollary 15, the automorphism $A'$ transforms any $q$-subset of $G$ into itself. In particular, it transforms $Q(x)$ into itself and thus satisfies
\[ A'(x) = x^{i_f(x)}, \quad \text{for some } i(x) < k(x). \]

Since \( A' \) is an automorphism of \( G \), there must exist a (unique) integer \( i \) such that
\[ i \equiv i(x) \pmod{k(x)}, \quad 0 \leq i < r. \]

Hence (see (9)), \( A' = B_i \) and, since \( B_i \) is symmetric, one has \( A = B_i^{-1} \). This proves the first part of the theorem. Next, let \( R_j \) be a minimal ideal in \( FG \) and \( A \) an automorphism of \( G \). If \( x_k = A'(x_j) \), it is obvious that
\[ x_k^{q^s} = A'(x_j^{q^s}), \quad (s = 0, 1, 2, \ldots). \]

Therefore \( A'(Q(x_j)) = Q(x_k) \) and, by theorem 14, \( A(R_j) = R_k \). This completes the proof, since \( L_q(G) \) can be defined as the set of automorphisms \( A \) such that \( A(R_j) = R_j, \forall j \in J \).

Remark: From the fact that \( A'(1) = 1, \forall A' \in L(G) \), it follows that every automorphism \( A \) of \( G \) transforms the trivial ideal \( R_0 \) into itself.

6. Elementary abelian codes

Let \( s \) be a prime integer and denote by \( G \) the elementary abelian \( s \)-group of order \( n = s^m \). The order of each element \( x \) in \( G \) (other than \( x_0 = 1 \)) is then equal to \( v = s \). If \( q = p^e \) is a power of a prime number \( p \), distinct from \( s \), the parameter \( r \), which is the order of \( q \) (mod \( s \)), is a divisor of \( s - 1 \). On the other hand, one has \( k(1) = 1 \) and
\[ (x \in G, \ x \neq 1) \Rightarrow (k(x) = r), \]
so that the nontrivial irreducible ideals all have dimension \( r \) over \( F \) and the number of these ideals is
\[ t = (s^m - 1)/r. \]

The minimal \( q \)-subsets of \( G \) (other than \( Q(x_0) = \{1\} \)) in fact are of the form
\[ Q(x_j) = \{x_j, x_j^q, \ldots, x_j^{q^{r-1}}\} \quad (1 \leq j \leq t). \]  

(27)

It is well known \(^1\) that the group \( L(G) \) has order
\[ |L(G)| = (s^m - 1) \ (s^m - s) \ldots (s^m - s^{m-1}) \]
and is isomorphic to the group \( GLH(m,s) \) of linear substitutions in \( m \) variables over the field \( E = GF(s) \). The isomorphism is as follows: Let \( z_1, z_2, \ldots, z_m \) be a set of independent generators of \( G \). Each element \( x \) of \( G \) then admits a unique representation as
\[ x = z_1^{i_1} z_2^{i_2} \ldots z_m^{i_m}, \quad 0 \leq i_k \leq s - 1. \]
To \( x \) we associate the vector \( \omega \) of \( E^m \), defined by
\[
\omega = (\omega_1, \omega_2, \ldots, \omega_m)^T, \quad \text{with} \quad \omega_k \equiv i_k \pmod{s}.
\]
The mapping
\[
x \in G \to \omega \in E^m
\] (28)
clearly is an isomorphism between \( G \) and the additive group in \( E^m \). Now, let \( A \) be an automorphism of \( G \) and assume that
\[
A(z_i) = z_1^{a_{1i}} z_2^{a_{2i}} \cdots z_m^{a_{mi}}, \quad 0 \leq a_{ji} < s - 1.
\]
To \( A \) thus corresponds a nonsingular square matrix \( A = |a_{ij}| \) of order \( m \) over \( E \); and the mapping (29) becomes
\[
A(x) \in G \to A \omega \in E^m.
\]
This follows from the fact that \( A(x) = \Pi (A(z_k))^{\xi k} \).

Remark: The generators \( z_1, z_2, \ldots, z_m \) of \( G \) can be chosen in such a way that the transpose \( A^T \) of an automorphism \( A \) corresponds to the usual transpose \( A^T \) of the matrix \( A \).

Let \( \zeta \) be the residue of \( q \) mod \( s \). Obviously \( \zeta \) is a primitive \( r \)th root of unity in \( E \) and the subset \( Q(x_j) \) of \( G \) corresponds to
\[
Q(\omega_j) = \{\omega_j, \zeta \omega_j, \ldots, \zeta^{r-1} \omega_j\} \subseteq E^m. \tag{29}
\]

**Theorem 17.** The group \( L(FG) \) acts as a transitive permutation group of degree \( t \) on the nontrivial irreducible ideals in \( FG \). More precisely, \( L(FG) \) contains a cyclic permutation of order and degree \( t \).

**Proof:** The subgroup \( H_t \) of \( GLH(s,m) \) corresponding to \( L_q(G) \) is the cyclic group of matrices (see (9))
\[
\overline{B}_i = \zeta^i I \quad (i = 0, 1, \ldots, r - 1),
\]
where \( I \) is the unit matrix. It is well known \(^3\) that the group
\[
G_r(s,m) = GLH(s,m)/H_r,
\]
acting as a permutation group on the \( t \) subsets (29) of \( E^m \) contains a cyclic permutation \( \overline{B} \) of order \( t \). The automorphism \( B \) of \( G \) then acts as a cyclic permutation on the \( t \) subsets (27) of \( G \). Hence, by theorems 14 and 16, \( B' \) permutes cyclically the \( t \) irreducible ideals \( R_j \) (\( 1 \leq j \leq t \)).

**Theorem 18.** When \( q \) is primitive mod \( s \), the group \( L(FG) \) acts as a doubly transitive group of degree \( t \) on the nontrivial irreducible ideals in \( FG \). If \( m = 2 \), \( L(FG) \) is in fact triply transitive.
Proof: If \( r = s - 1 \), \( \zeta \) is a primitive element of \( E \) and the subsets (29) of \( E^m \) can be identified with the \( t = (s^n - 1)/(s - 1) \) points of an \((m - 1)\)-dimensional projective geometry \( PG(m - 1, s) \) over \( E = GF(s) \). It is well known \(^1\) that the group \( G_\zeta(s, m) \) acts as a doubly transitive permutation group on these points and that the group is in fact triply transitive when \( m = 2 \). By the same reasoning as in theorem 17, one has the desired result.

Examples. To illustrate the theory, we now study two examples of elementary abelian codes over the binary field \( F = GF(2) \).

First, let \( G \) be the elementary abelian group of order \( n = 25 \), so that \( s = 5 \), \( m = 2 \). Since 2 is primitive mod 5, the nontrivial irreducible ideals in \( FG \) have dimension \( r = 4 \) over \( F \). Let \( R_1, R_2, \ldots, R_6 \) be these ideals. By theorem 18, the group \( L(FG) \), which has order 120, acts as a triply transitive group on the \( R_i \) (\( 1 \leq i \leq 6 \)) and any binary \( G \)-code is equivalent to one of the 6 following ideals:

\[ S_i = R_1 + R_2 + \ldots + R_i \quad (i = 1, 2, \ldots, 6), \]

if all vectors of the code have an even weight. The parameters of the codes \( C_i = S_i \), of length \( n = 25 \), are given in table I, where \( d \) denotes the minimum distance and \( k \) the dimension of the code.

<table>
<thead>
<tr>
<th>( C )</th>
<th>( C_1 )</th>
<th>( C_2 )</th>
<th>( C_3 )</th>
<th>( C_4 )</th>
<th>( C_5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( k )</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
</tr>
<tr>
<td>( d )</td>
<td>10</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

In fact, the codes \( C_1 \) and \( C_5 \) are equivalent to cyclic codes.

Next, let \( G \) be the elementary abelian group of order \( n = 27 \), so that \( s = 3 \), \( m = 3 \). The nontrivial irreducible ideals in \( FG \) have dimension \( r = 2 \) over \( F \). Let \( R_1, R_2, \ldots, R_{13} \) be these ideals. By theorem 18, the group \( L(FG) \), which has order \( N = 13.12.36 \), acts as a doubly transitive group on the \( R_i \). Therefore, any two ideals of dimension 4 necessarily are equivalent to each other. We now consider the ideals of dimension 6; they are of the form

\[ R(i) = R_{i_1} + R_{i_2} + R_{i_3} \quad (1 \leq i_1 < i_2 < i_3 \leq 13). \]

The annihilator of \( R(i) \) in \( G \) is then \( G \setminus K(i) \), with

\[ K(i) = Q(x_{i_1}) \cup Q(x_{i_2}) \cup Q(x_{i_3}). \]
Let $\omega_j$ be the element of $E^3$ which corresponds to $x_j$ (see (28)), where $E = GF(3)$. To the ideal $R(i)$ corresponds the square matrix $X_i$ of order 3 (and rank 2 or 3) over $E$ whose columns are the vectors $\omega_{i_k}$ ($k = 1, 2, 3$). Using (28) and theorem 14, one sees that the ideals $R(i)$ and $R(j)$ are equivalent if there exists a nonsingular matrix $\overline{B}$ of order 3 over $E$ and a generalized permutation matrix $P$ satisfying

$$\overline{B} X_i = X_j P.$$ (30)

The automorphism $A = B'$ of $G$ then transforms $R(i)$ into $R(j)$. For fixed matrices $X_i$ and $X_j$, one easily verifies that eq. (30) admits a solution $(\overline{B}, P)$ if and only if the matrices $X_i$ and $X_j$ have the same rank. Accordingly, there are only two nonequivalent $G$-codes of dimension 6. The first one, denoted by $C_2$, corresponds to a matrix $X_i$ of rank 2 and the second one, denoted by $C_3$, to a matrix $X_i$ of rank 3. In fact, among the $\binom{13}{3}$ $G$-codes of dimension 6, there are $N_2 = 52$ which are equivalent to $C_2$ and $N_3 = 234$ which are equivalent to $C_3$. Hence (see corollary 15), the subgroup $L_i$ of $L(G)$ which transforms $C_i$ into itself has order $|L_i| = 2N_i/N_i$, so that

$$|L_2| = 216, \quad |L_3| = 48.$$ 

Table II gives the weight distribution of the codes $C_2$ and $C_3$; $n_i(w)$ denotes the number of code vectors of weight $w$ in $C_i$ (in fact, $C_2$ is equivalent to a cyclic code).

<table>
<thead>
<tr>
<th>$w$</th>
<th>0</th>
<th>6</th>
<th>12</th>
<th>14</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n_2(w)$</td>
<td>1</td>
<td>9</td>
<td>27</td>
<td>0</td>
<td>27</td>
</tr>
<tr>
<td>$n_3(w)$</td>
<td>1</td>
<td>0</td>
<td>27</td>
<td>27</td>
<td>9</td>
</tr>
</tbody>
</table>

Acknowledgment

The writer is very grateful to Mrs F. J. MacWilliams, of Bell Telephone Laboratories, Murray Hill, for calling attention to group algebras and for communicating her results. Thanks are also due to J. M. Goethals for many interesting discussions.

MBLE Research Laboratory Brussels, June 1970
REFERENCES

3) P. Delsarte, J. M. Goethals and F. J. MacWilliams, Information and Control, to be published.