EQUIVALENCE CLASSES OF MATRICES OVER A FINITE FIELD

GARY L. MULLEN
Department of Mathematics
The Pennsylvania State University
Sharon, Pennsylvania 16146

(Received October 26, 1978)

ABSTRACT. Let $\mathbb{F}_q = GF(q)$ denote the finite field of order $q$ and $F(m,q)$ the ring of $m \times m$ matrices over $\mathbb{F}_q$. Let $\Omega$ be a group of permutations of $\mathbb{F}_q$. If $A, B \in F(m,q)$ then $A$ is equivalent to $B$ relative to $\Omega$ if there exists $\phi \in \Omega$ such that $\phi(A) = B$ where $\phi(A)$ is computed by substitution. Formulas are given for the number of equivalence classes of a given order and for the total number of classes induced by a cyclic group of permutations.

KEY WORD AND PHRASES. Equivalence, permutation, automorphism, finite field.

1980 MATHEMATICS SUBJECT CLASSIFICATION CODES. Primary 15A33; Secondary 15A24.

1. INTRODUCTION.

In the series of papers [2], [4], [8], and [9], L. Carlitz, S. Cavior, and the author studied several forms of equivalence of functions over a finite field. In this paper we study a form of equivalence defined on the ring of $m \times m$ matrices over a finite field.
Let $F_q = GF(q)$ denote the finite field of order $q$ and $F(m,q)$ the ring of $m \times m$ matrices over $F_q$. Let $\Omega$ be a group of permutations on $F_q$ so that $\Omega$ is isomorphic to a subgroup of $S_q$, the symmetric group on $q$ letters.

2. GENERAL THEORY.

A permutation $\phi$ of $F_q$ is a function from $F_q$ onto $F_q$ and so by the Lagrange Interpolation Formula [6,p.55], is expressible as a polynomial of degree less than $q$. Suppose $\phi(x) = a_n x^n + \ldots + a_1 x + a_0$ where each $a_i \in F_q$ and $n \leq q-1$. Then by substitution we may compute the $m \times m$ matrix $\phi(A) = a_n A^n + \ldots + a_1 A + a_0 I_m$ where $I_m$ is the $m \times m$ identity matrix. If $\Omega$ is a group of permutations then we can make

**DEFINITION 1.** If $A, B \in F(m,q)$ then $A$ is equivalent to $B$ relative to $\Omega$ if $B = \phi(A)$ for some $\phi \in \Omega$.

As this relation is an equivalence relation on $F(m,q)$ we let $\nu(A,\Omega)$ denote the order of the class of $A$ relative to $\Omega$ and $\lambda(\Omega)$ denote the number of classes induced by $\Omega$.

**DEFINITION 2.** If $A \in F(m,q)$ then a permutation $\phi \in \Omega$ is an automorphism of $A$ relative to $\Omega$ if $\phi(A) = A$.

Let $\text{Aut}(A,\Omega)$ and $\nu(A,\Omega)$ denote the group and number of automorphisms of the matrix $A$ relative to $\Omega$. If $\phi(A) = B$ for some $\phi \in \Omega$ then

$$\text{Aut}(B,\Omega) = \phi \text{Aut}(A,\Omega) \phi^{-1}$$

(2.1)

so that $\nu(B,\Omega) = \nu(A,\Omega)$. Thus the number of automorphisms depends only upon the class and not on the particular matrices within the class. One can now easily prove:

**THEOREM 2.1.** Let $A \in F(m,q)$. Then for any group $\Omega$

$$\nu(A,\Omega) \nu(A,\Omega) = |\Omega|$$

(2.2)

where $|\Omega|$ denotes the order of the group $\Omega$.

If $\phi$ is a permutation let $I(\phi,m)$ denote the number of $m \times m$ matrices $A$
such that $\phi(A) = 0$. Suppose $\phi(x) = a_n x^n + \ldots + a_1 x + a_0$ where each $a_i \in F_q$ and $a_n \neq 0$. Then if $\phi(A) = A$ we have the matrix equation

$$A^n + \frac{a_{n-1}}{a_n} A^{n-1} + \ldots + \frac{(a_1 - 1)}{a_n} A + \frac{a_0}{a_n} I_m = 0.$$  

(2.3)

Consider the monic polynomial

$$E_\phi(x) = x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \ldots + \frac{(a_1 - 1)}{a_n} x + \frac{a_0}{a_n}$$

over $GF(q)$. Hodges in [7] gives a formula for the number $N(E_\phi, m)$ of $m \times m$ matrices $A$ over $GF(q)$ such that $E_\phi(A) = 0$. Clearly $I(\phi, m) = N(E_\phi, m)$ and moreover this number can be computed as follows.

Berlekamp in [1] has given an algorithm for factoring polynomials over $F_q$ in terms of solving a system of linear equations over $F_q$. Suppose $E_\phi$ has the prime factorization $E_\phi = p_1^{h_1} \ldots p_s^{h_s}$ where the $p_i$'s are distinct monic polynomials, $h_1 \geq 1$ and the degree of $p_i$ is $d_i$ for $i = 1, \ldots, s$. Let $g(t, d)$ represent the number of non-singular matrices of order $t > 1$ over $GF(q^d)$ so that, as is well known, $g(t, d) = \frac{t(t-1)}{d} (q^d - q^d)$. We also set $g(o, d) = 1$.

Let $\pi$ be a partition of $m$ defined by

$$m = \sum_{i=1}^{s} \frac{h_i}{d_i} \sum_{j=1}^{k_{ij}} j, k_{ij} \geq 0.$$  

(2.5)

For $i = 1, \ldots, s$ let

$$b_i(\pi) = \sum_{u=1}^{h_i} \left[ k_{iu}^2 (u-1) + 2uk_{iu} \sum_{v=u+1}^{h_i} k_{iv} \right]$$  

(2.6)

and set $a(\pi) = \sum_{i=1}^{s} d_i b_i(\pi)$. Then as shown by Hodges in [7],

$$I(\phi, m) = N(E_\phi, m) = g(m, 1) \sum_{i=1}^{s} g(k_{ij}, d_i)^{-1}$$

(2.7)

where the sum is over all partitions $\pi$ of $m$ given by (2.5).

3. CYCLIC GROUPS.

Let $\Omega$ be a cyclic group of order $n$, say $\Omega = \langle \phi \rangle$, and let $H(t)$ denote
the subgroup of \( \Omega \) of order \( t \), where \( t | n \). It follows that \( H(t) = \langle \phi^n | t \rangle \).

Let \( M(t,m) \) denote the number of \( m \times m \) matrices \( A \) such that \( \text{Aut}(A,\Omega) = H(t) \).

**THEOREM 3.1.** For each divisor \( t \) of \( n \)

\[
M(t,m) = N(E_{\phi^n/t},m) - \sum N(E_{\phi^n/u},m)
\]

where the sum is over all \( u \) for which \( u | n, t | u, \) and \( t \neq u \).

**PROOF.** The number of \( m \times m \) matrices \( A \) such that \( H(t) \leq \text{Aut}(A,\Omega) \) is given by \( N(E_{\phi^n/t},m) \). From this we subtract those for which the containment is proper.

**COROLLARY 3.2.** For all \( t | n \) there are \( tM(t,m)/n \) classes of order \( n/t \) and

\[
\lambda(\Omega) = \frac{1}{n} \sum_{t | n} tM(t,m).
\]

Following Definition 3.1 of [8] we say that two groups \( \Omega_1 \) and \( \Omega_2 \) induce *equivalent* decompositions of \( F(m,q) \) if they induce the same number of classes of the same size. It is easy to see that if \( \Omega = \langle \phi_1 \rangle \) and \( \Omega_2 = \langle \phi_2 \rangle \) are cyclic groups of order \( n \) then \( \Omega_1 \) and \( \Omega_2 \) will induce equivalent decompositions of \( F(m,q) \) if for each \( t | n \), \( \phi_1^{n/t} \) and \( \phi_2^{n/t} \) have the same number of distinct prime factors of the same degree and multiplicity.

As a simple illustration of the above theory let \( m = 2 \) and consider \( \phi(x) = x^3 \) over \( \text{GF}(5) \) so that if \( \Omega = \langle \phi \rangle \) then \( |\Omega| = 2 \). We have

\[
E_{\phi}(x) = x^3 - x = x(x-1)(x+1) \quad \text{so that} \quad s = 3, \ P_1 = x, \ P_2 = x-1, \ P_3 = x+1 \quad \text{and} \quad h_i = d_i = 1 \quad \text{for} \quad i = 1,2,3.
\]

There are six partitions defined by (2.5) which are given by \( 2 = k_{11} + k_{21} + k_{31} \) where \( 0 \leq k_{ij} \leq 2 \). Clearly \( b_1(\pi) = 0 \) for \( i = 1,2,3 \) so that \( a(\pi) = 0 \) for each partition \( \pi \). One checks that \( g(2,1) = (q^2 - 1)(q^2 - q) = 480, g(1,1) = q-1 = 4 \) and \( g(0,1) = 1 \). Hence using (2.7) it is not difficult to check that \( N(E_{\phi},2) = 93 \) so that by (3.1), \( M(2,2) = 93 \) and thus \( M(1,2) = 532 \). Hence by Corollary 3.2 there are 93 classes of order one and 266 classes of order two so that by (3.2) \( \lambda(\Omega) = 359 \).
REFERENCES


Submit your manuscripts at http://www.hindawi.com