Internat. J. Math. & Math. Sci.
Vol. 2 #3 (1979) 487-491

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 $F_q = GF(q)$ denote the finite field of order q and $F(m,q)$ the ring of $m \times m$ matrices over F_q. Let Ω be a group of permutations of F_q. If $A, B \in F(m,q)$ then A is equivalent to B relative to Ω 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 Ω be a group of permutations on F_q so that Ω is isomorphic to a subgroup of S_q, the symmetric group on q letters.

2. GENERAL THEORY.

A permutation ϕ 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 $\phi(x) = a_n x^n + \ldots + a_1 x + a_o$ where each $a_i \in F_q$ and $n \leq q-1$. Then by substitution we may compute the $m \times m$ matrix $\phi(A) = a_n A^n + \ldots + a_1 A + a_o I_m$ where I_m is the $m \times m$ identity matrix. If Ω is a group of permutations then we can make

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

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

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

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

$$Aut(B,\Omega) = \phi Aut(A,\Omega)\phi^{-1} \tag{2.1}$$

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 Ω

$$\mu(A,\Omega)\ \nu(A,\Omega) = |\Omega| \tag{2.2}$$

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

If ϕ is a permutation let $I(\phi,m)$ denote the number of $m \times m$ matrices A

such that $\phi(A) = 0$. Suppose $\phi(x) = a_n x^n + \ldots + a_1 x + a_o$ where each $a_i \in F_q$ and $a_n \neq o$. Then if $\phi(A) = A$ we have the matrix equation

$$A^n + \frac{a_{n-1}}{a_n} A^{n-1} + \ldots + \frac{(a_1 - 1)}{a_n} A + \frac{a_o}{a_n} I_m = 0. \tag{2.3}$$

Consider the monic polynomial

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

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_ϕ has the prime factorization $E_\phi = P_1^{h_1} \ldots P_s^{h_s}$ where the P_i's are distinct monic polynomials, $h_i \geq 1$ 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 $t \geq 1$ over $GF(q^d)$ so that, as is well known, $g(t,d) = \prod_{i=o}^{t-1}(q^{dt} - q^{di})$. We also set $g(o,d) = 1$.

Let π be a partition of m defined by

$$m = \sum_{i=1}^{s} d_i \sum_{j=1}^{h_i} jk_{ij}\ ,\ k_{ij} \geq o. \tag{2.5}$$

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

$$b_i(\pi) = \sum_{u=1}^{h_i} [k_{iu}^2 (u-1) + 2uk_{iu} \sum_{v=u+1}^{h_i} k_{iv}] \tag{2.6}$$

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

$$I(\phi,m) = N(E_\phi,m) = g(m,1) \sum_{\pi} g^{-a(\pi)} \prod_{i=1}^{s} \prod_{j=1}^{h_i} g(k_{ij},d_i)^{-1} \tag{2.7}$$

where the sum is over all partitions π of m given by (2.5).

3. CYCLIC GROUPS.

Let Ω be a cyclic group of order n, say $\Omega = \langle\phi\rangle$, and let $H(t)$ denote

the subgroup of Ω 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 $\mathrm{Aut}(A,\Omega) = H(t)$.

THEOREM 3.1. For each divisor t of n

$$M(t,m) = N(E_{\phi^{n/t}},m) - \Sigma\, N(E_{\phi^{n/u}}, m) \tag{3.1}$$

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 $H(t) \leq \mathrm{Aut}(A,\Omega)$ is given by $N(E_{\phi^{n/t}}, m)$. From this we subtract those for which the containment if proper.

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

$$\lambda(\Omega) = \frac{1}{n} \sum_{t|n} tM(t,m). \tag{3.2}$$

Following Definition 3.1 of [8] we say that two groups Ω_1 and Ω_2 induce <u>equivalent</u> decompositions of $F(m,q)$ is 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 Ω_1 and Ω_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 $GF(5)$ so that if $\Omega = \langle\phi\rangle$ then $|\Omega| = 2$. We have $E_\phi(x) = x^3 - x = x(x-1)(x+1)$ so that $s = 3$, $P_1 = x$, $P_2 = x-1$, $P_3 = x+1$ and $h_i = d_i = 1$ for $i = 1,2,3$. There are six partitions defined by (2.5) which are given by $2 = k_{11} + k_{21} + k_{31}$ where $o \leq k_{ij} \leq 2$. Clearly $b_i(\pi) = o$ for $i = 1,2,3$ so that $a(\pi) = o$ for each partition π. One checks that $g(2,1) = (q^2 - 1)(q^2 - q) = 480$, $g(1,1) = q-1 = 4$ and $g(o,1) = 1$. 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

1. Berlekamp, E. R., "Factoring polynomials over finite fields," Bell System Technical J. 46 (1967), 1853-1859.

2. Carlitz, L., "Invariantive theory of equations in a finite field," Trans. Amer. Math. Soc. 75 (1953), 405-427.

3. Carlitz, L., "Invariant theory of systems of equations in a finite field," J. Analyse Math. 3 (1953-54), 382-413.

4. Cavior, S. R., "Equivalence classes of functions over a finite field," Acta Arith. 10 (1964), 119-136.

5. Cavior, S. R., "Equivalence classes of sets of polynomials over a finite field," Journ. Reine Angew. Math. 225 (1967), 191-202.

6. Dickson, L. E., Linear Groups with an Exposition of the Galois Field Theory, Dover Publications, Inc., New York, 1958.

7. Hodges, J. H., "Scalar polynomials equations for matrices over a finite field," Duke Math. J. 25 (1958), 291-296.

8. Mullen, G. L., "Equivalence classes of functions over a finite field," Acta Arith. 29 (1976), 353-358.

9. Mullen, G. L., "Equivalence classes of polynomials over finite fields," Acta Arith. 31 (1976), 113-123.

10. Mullen, G. L., "Equivalence classes of sets of polynomials over finite fields," To appear, Bull. Calcutta Math. Soc.