Internat. J. Math. & Math. Sci.
Vol. 4 No. 2 (1981) 279-287

A NOTE OF EQUIVALENCE CLASSES OF MATRICES OVER A FINITE FIELD

J.V. BRAWLEY

Department of Mathematical Sciences, Clemson University
Clemson, South Carolina
and
GARY L. MULLEN
Department of Mathematics, The Pennsylvania State University
Sharon, Pennsylvania

(Received July 16, 1980)

ABSTRACT. Let $F_q^{m\times m}$ denote the algebra of m×m matrices over the finite field F_q of q elements, and let Ω denote a group of permutations of F_q. It is well known that each $\phi\in\Omega$ can be represented uniquely by a polynomial $\phi(x)\in F_q[x]$ of degree less than q; thus, the group Ω naturally determines a relation $\sim$ on $F_q^{m\times m}$ as follows: if $A,B\in F_q^{m\times m}$ then $A\sim B$ if $\phi(A) = B$ for some $\phi\in\Omega$. Here $\phi(A)$ is to be interpreted as substitution into the unique polynomial of degree < q which represents ϕ.

In an earlier paper by the second author [1], it is assumed that the relation $\sim$ is an equivalence relation and, based on this assumption, various properties of the relation are derived. However, if $m \geq 2$, the relation $\sim$ is not an equivalence relation on $F_q^{m\times m}$. It is the purpose of this paper to point out the above erroneous assumption, and to discuss two ways in which hypotheses of the earlier paper can be modified so that the results derived there are valid.

KEY WORDS AND PHRASES. *Equivalence, permutation, automorphism, finite field.*
1980 MATHEMATICS SUBJECT CLASSIFICATION CODES. *Primary 15A33; Secondary 15A24.*

1. INTRODUCTION.

Let F_q denote the finite field of order q and let $F_q^{m\times m}$ denote the algebra of m×m matrices over F_q. If Ω is a group of permutations of F_q, then Ω can

be used to define a relation on $F_q^{m\times m}$ as follows: since each $\phi\in\Omega$ can be expressed uniquely as a polynomial $\phi(x)\in F_q[x]$ of degree $<q$, we take A to be related to B (written $A\sim B$) if $B = \phi(A)$ for some $\phi\in\Omega$ where $\phi(A)$ is the substitution of A into the unique polynomial $\phi(x)$ representing ϕ.

In [1] it is assumed that the relation thus defined is an equivalence relation on $F_q^{m\times m}$ and, based on this assumption, various properties of the relation are derived. However, for $m \geq 2$, the relation is not an equivalence relation. One of the purposes of this note is to point out the above erroneous assumption. Another is to discuss ways in which the hypotheses in [1] can be modified so that the results derived there are valid. In section 2 we discuss why $\sim$ is not an equivalence relation and in section 3 we briefly indicate how the results of [1] can be made valid after a simple modification of the group Ω. In section 4 we keep Ω as defined in [1], but we restrict the domain on which it is acting to be a subset of $F_q^{m\times m}$; namely, the diagonalizable matrices. The relation, thus restricted, becomes an equivalence relation and again the results of [1] are valid provided suitable enumeration formulas for diagonalizable matrices are known. These needed formulas are derived as a part of section 4.

2. THE ERRONEOUS ASSUMPTION.

In [1] it was taken for granted (referring to the relation defined above) that if $B = \phi(A)$ for some $\phi\in\Omega$ then $A = \phi^{-1}(B)$. To explain why this is not necessarily true, consider a particular $\phi\in\Omega$. Let $\phi(x)$ and $\phi^{-1}(x)$ denote the polynomials representing ϕ and ϕ^{-1}. Then for all $a\in F_q$, $\phi(\phi^{-1}(a)) = \phi^{-1}(\phi(a)) = a$. This identity in F_q translates to $F_q[x]$ by the polynomial congruence $\phi(\phi^{-1}(x)) \equiv \phi^{-1}(\phi(x)) \equiv x \pmod{(x^q - x)}$. Thus

$$\phi^{-1}(\phi(x)) = x + h(x)(x^q - x) \tag{2.1}$$

for some $h(x)\in F_q[x]$. Hence, if $A\sim B$ by ϕ(ie; if $\phi(A) = B$), we have

$$\phi^{-1}(B) = \phi^{-1}(\phi(A)) = A + h(A)(A^q - A) \tag{2.2}$$

which is not in general equal to A. Consequently, the relation $\sim$ is not symmetric.

For a specific example, consider $q = 5$ and take ϕ to be the permutation of F_5 represented by $\phi(x) = x^3$. Then the polynomial representing ϕ^{-1} is also $\phi^{-1}(x) = x^3$. Thus for $\Omega = \{x, x^3\}$, $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is related to $B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ as $B = A^3$; however, B is not related to A.

3. A MODIFICATION OF Ω.

It is quite natural to use the polynomial representation of $\phi \in \Omega$ to define the relation $\sim$ on $F_q^{m\times m}$ because polynomial functions can act on $F_q^{m\times m}$, or any algebra over F_q, as easily as on F_q; indeed, this idea is the basis behind most notions of extending functions on a field F to functions on $F^{m\times m}$ (e.g., see [2]). However, permutation polynomials on F do not in general become permutation polynomials on $F^{m\times m}$. The failure to account for this fact led to the error in [1] and the realization of it leads to the following modification.

It is known [3] that there are polynomials $f(x) \in F_q[x]$ in addition to the obvious linear polynomials $ax + b$, $a \neq 0$, which, when acting on $F_q^{m\times m}$ via substitution do indeed define permutations of $F_q^{m\times m}$. These polynomials have been characterized in [3] where it is shown that $f(x)$ and $g(x)$ represent the same function on $F_q^{m\times m}$ if and only if $f(x) \equiv g(x) \pmod{L_m(x)}$ where

$$L_m(x) = (x^{q^m} - x)(x^{q^{m-1}} - x)\cdots(x^q - x).$$

Thus, if G denotes the set of all polynomials of degree less than the degree δ of $L_m(x)$ ($\delta = q^m + q^{m-1} + \cdots + q$) which act as permutations on $F_q^{m\times m}$, then G is a group under composition modulo $L_m(x)$. The group G is studied in [4] where among other things the order $|G|$ is found.

Let Ω be a subgroup of G. Then Ω can be used to define an equivalence relation on $F_q^{m\times m}$ by defining $A \sim B$ if there is a $\phi \in \Omega$ such that $B = \phi(A)$. With this new group playing the role of the group Ω used in [1, section 2], the results and proofs of [1, section 2] are valid. Moreover, if this new Ω is also cyclic, the results and proofs in [1, section 3] are also valid provided the typograph-

ical error in [1, equation (3.1)] is corrected to read

$$M(t,m) = N(E_{\phi^{n/t}},m) - \sum_{t|u|n} M(u,m).$$

Möbius inversion can of course be applied to the above expression to give

$$M(t,m) = \sum_{t|u|n} \mu(\tfrac{u}{t}) N(E_{\phi^{n/u}},m)$$

where μ is the classical Möbius function.

Corollary 3.2 of [1] for the number $\lambda(\Omega)$ of equivalence classes of $\sim$ is now valid with the above modifications. However, a straight forward use of Burnside's lemma (e.g., see [5, p. 136]) together with the results of Hodges [6] perhaps give the simplest expression for the number of equivalence classes; namely,

$$\lambda(\Omega) = \frac{1}{|\Omega|} \sum_{\phi\varepsilon\Omega} \Psi(\phi) \tag{3.1}$$

where $\Psi(\phi)$ is the number of matrix roots of the equation $\phi(x) - x = 0$. In [6] Hodges finds the number of matrix roots of $f(x) = 0$, $f(x)$ arbitrary in $F_q[x]$.

We comment that the main difficulty in using the results of [1] as now corrected or the above formula (3.1) in conjunction with Hodges' formulas is that the polynomials $f(x)$ must be known explicity and in factored form.

As a simple example where this difficulty is readily handled, we take $\Omega = \{ax + b | a, b\varepsilon F_q, a \neq 0\}$. Then $|\Omega| = q(q - 1)$ and it is easily seen (independent of Hodges' work) that

$$\Psi(ax + b) = \begin{cases} 1 \text{ if } a \neq 1 \\ 0 \text{ if } a = 1,\ b \neq 0 \\ q^{m^2} \text{ if } a = 1,\ b = 0 \end{cases}$$

so that

$$\lambda(\Omega) = \frac{q^{m^2} + q(q-2)}{q(q-1)} = \frac{q^{m^2-1} + q - 2}{q - 1}.$$

As an illustration of the theory of [1] in the case where Ω is a cyclic subgroup of G, suppose $m = 2$ and consider $\Omega = \langle\phi\rangle$ where $\phi(x) = 2x + 1$ over F_5. Clearly $\phi(x)$ is a permutation polynomial on $F_5^{2\times 2}$ and $|\Omega| = 4$ so that from Theorem 3.1 of [1] we have $M(1,2) = 624$, $M(2,2) = 0$ and $M(4,2) = 1$. Thus by Corollary 3.2 of [1] there are 156 classes of order 4 and 1 class of order 1 so that $\lambda(\Omega) = 157$, a result which also follows quite readily from (3.1).

4. AN ALTERNATE MODIFICATION.

We now consider another way to modify the hypotheses in [1] in order to obtain a valid equivalence relation. This time, in contrast to the above alternative, we use the same group of [1] but alter the set on which it is acting.

Let Ω be a group of permutations of F_q so that each $\phi\varepsilon\Omega$ is represented by a unique polynomial $\phi(x) = \Sigma a_i x^i \varepsilon F_q[x]$ of degree less than q. Let $\mathcal{D}(m,q)$ denote the set of $m \times m$ diagonalizable matrices over F_q; i.e., an $m \times m$ matrix A over F_q is in $\mathcal{D}(m,q)$ if and only if A is similar over F_q to a diagonal matrix. It is shown in [3, Theorem 5] that each $\phi(x)\varepsilon\Omega$ defines, via substitution, a permutation of $\mathcal{D}(m,q)$. This also follows easily from (2·2) since $A^q - A = 0$ for all $A\varepsilon\mathcal{D}(m,q)$. Hence, the relation $\sim$ defined on $\mathcal{D}(m,q)$ by $A\sim B$ if $\phi(A) = B$ for some $\phi(x)\varepsilon\Omega$ is an equivalence relation on $\mathcal{D}(m,q)$.

For this particular equivalence relation on $\mathcal{D}(m,q)$, results identical to those stated in [1] can be derived (using identical proofs) provided the following agreement is made: whenever a formula or statement in [1] calls for the number of matrices $A\varepsilon F_q^{m\times m}$ satisfying $f(x) = 0$ where $f(x) = \phi(x) - x$, $\phi(x)\varepsilon\Omega$, we instead use the number of matrices $A\varepsilon\mathcal{D}(m,q)$ satisfying $f(x) = 0$. The former number was determined by Hodges in [6] while the latter number is given in the next theorem, the proof of which is an adaption of Hodges' methods to our situation.

THEOREM 1. Let $f(x)\varepsilon F_q[x]$ have $t \geq 0$ distinct roots (with various multiplicities) in F_q. Then the number $Z(f(x))$ of matrices $A\varepsilon\mathcal{D}(m,q)$ satisfying $f(A) = 0$ is

$$Z(f(x)) = \sum_{\pi} \frac{\gamma(m)}{\gamma(k_1)\gamma(k_2)\cdots\gamma(k_t)} \tag{4.1}$$

where the sum is over all t-tuples $\pi = (k_1,\ldots,k_t)$ of nonnegative integers satisfying $\Sigma k_i = m$ and where

$$\gamma(r) = (q^r - 1)(q^r - q)\cdots(q^r - q^{r-1}) \tag{4.2}$$

is the well known number of invertible $r \times r$ matrices over F_q.

PROOF. A matrix A is in $\mathcal{D}(m,q)$ and also satisfies $f(x) = 0$ if and only if the minimum polynomial of A factors into distinct linear factors and also divides $f(x)$. This is equivalent to saying A is similar to a unique diagonal matrix of the form

$$\operatorname{diag}(a_1 I_{k_1}, a_2 I_{k_2}, \ldots, a_t I_{k_t}) \tag{4.3}$$

where $(a_1,a_2,\ldots,a_t)$ is a fixed ordering of the t distinct roots of $f(x)$ and where the k_i are nonnegative integers whose sum is m. (If some $k_i = 0$, we understand that the corresponding block does not appear in (4.3)). An $m \times m$

matrix P is invertible and commutes with (2.2) if and only if $P = \operatorname{diag}(P_1, P_2, \ldots, P_t)$ where P_i is $k_i \times k_i$ and invertible. Thus from [6] the number of matrices similar to (4.3) is $\gamma(m)/(\gamma(k_1)\cdots\gamma(k_t))$ and the result follows by summing over all $\pi = (k_1, k_2, \ldots, k_t)$.

We should comment that in case f(x) has no roots in F_q, the sum (4.1) is the empty sum which by convention is zero.

Formula (4.1) can also be used in conjunction with Burnside's lemma [5] to give the following number $\lambda(\Omega)$ of equivalence classes:

$$\lambda(\Omega) = \frac{1}{|\Omega|} \sum_{\phi \in \Omega} Z(\phi(x) - x) \tag{4.4}$$

where $Z(\phi(x) - x)$ is given in (4.1).

If we take Ω to be the trivial group $\Omega = \{\phi(x) = x\}$, then (4.4) counts the number $|\mathcal{D}(m,q)|$ of $m \times m$ diagonalizable matrices over F_q and simplifies using (4.1) to

$$|\mathcal{D}(m,q)| = \sum_{\pi} \frac{\gamma(m)}{\gamma(k_1)\,\gamma(k_2)\cdots\gamma(k_q)} \tag{4.5}$$

where the sum is overall q-tuples $\pi = (k_1, k_2, \ldots, k_q)$ of nonnegative integers with $\Sigma k_i = m$.

As a second illustration, if $\phi(x) = x^3$ over F_5 and $\Omega = \langle \phi \rangle$ so that $|\Omega| = 2$, then as was pointed out in section 2, ϕ is a permutation on F_5 but $\sim$ is not an equivalence relation on $F_5^{2\times 2}$. However, by restricting Ω to act on the $|\mathcal{D}(2,5)| = 305$ diagonalizable 2×2 matrices over F_5, we do indeed have a bonafide equivalence relation on $\mathcal{D}(2,5)$. Using (4.1) it is not difficult to show that $Z(x^3 - x) = 93$ so that by (4.4) $\lambda(\Omega) = 1/2(93 + 305) = 199$ distinct equivalence classes.

For $\Omega = S_q$ (the symmetric group of all permutations of F_q), rather than use formula (4.4) which results in a complicated expression, we shall give an independent derivation which utilizes the following theorem whose proof resembles

that of Theorem 1 and will thus be omitted.

Theorem 2. The number of diagonalizable matrices over F_q with exactly t eigenvalues is

$$E(m,t) = \sum_{\pi(m,t)} \binom{q}{t} \binom{t}{s_1,s_2,\ldots,s_m} \frac{\gamma(m)}{\gamma(1)^{s_1}\gamma(2)^{s_2}\cdots\gamma(m)^{s_m}} \tag{4.6}$$

where the sum is over all partitions $\pi(m,t) = [1^{s_1}2^{s_2}\cdots m^{s_m}]$ of m into exactly t parts ($\Sigma i s_i = m$, $\Sigma s_i = t$) where $\gamma(r)$ is given in (4.2) and where $\binom{q}{t}$ and $\binom{t}{s_1,s_2,\ldots,s_m}$ are binomial and multinomial coefficients, respectively.

Now consider a matrix $A\varepsilon\mathcal{D}(m,t)$ with exactly t distinct eigenvalues, and let P be a fixed matrix such that $P^{-1}AP = D$ where D is a diagonal matrix. Let s_i be the number of eigenvalues of A (or diagonal entries of D) of multiplicity i so that $\Sigma i s_i = m$ and $\Sigma s_i = t$. Hence, associated with A (or D) there is a partition $\pi(m,t) = [1^{s_1}2^{s_2}\cdots m^{s_m}]$ of m into t parts. As $\phi(x)$ runs over $S_q = \Omega$, $\phi(D)$ runs over all diagonal matrices related to D of which there are clearly $q(q-1)\cdots(q-t+1) = q!/t!$. Since $P\phi(D)P^{-1} = \phi(PDP^{-1}) = \phi(A)$, it follows that the number of matrices related to A is also $q!/t!$ and each such matrix has exactly t distinct eigenvalues. Hence, the number of equivalence classes determined by those matrices with exactly t eigenvalues is $t!E(m,t)/q!$ where $E(m,t)$ is given by (4.6). Thus, $\lambda(S_q) = \sum_{t=1}^{m} t!E(m,t)/q!$ is the number of equivalence classes and this simplifies to

$$\lambda(S_q) = \sum_{\pi} \frac{\gamma(m)}{\gamma(1)^{s_1}s_1!\gamma(2)^{s_2}s_2!\cdots\gamma(m)^{s_m}s_m!} \tag{4.7}$$

where the sum is over all partitions $\pi = [1^{s_1}2^{s_2}\cdots m^{s_m}]$ of m.

It is interesting to note the similarity in appearance of (4.7) to Cauchy's formula for the number m! of elements in S_m; namely,

$$|S_m| = \sum_{\pi} \frac{m!}{1^{s_1}s_1!2^{s_2}s_2!\cdots m^{s_m}s_m!}$$

where $\pi = [1^{s_1}2^{s_2}\cdots m^{s_m}]$ again ranges over all partitions of m.

ACKNOWLEDGED: A portion of this work was completed while the first author was a visiting professor in the Department of Mathematics, University of Tennessee, Knoxville, Tennessee.

REFERENCES

1. MULLEN, G.L. Equivalence Classes of Matrices Over a Finite Field, Internat. J. Math. & Math. Sci. 2 (1979), 487-491.

2. LANCASTER, P., Theory of Matrices, Academic Press, New York, 1969.

3. BRAWLEY, J.V., CARLITZ, L., and LEVINE, J., Scalar Polynomial Functions on the n×n Matrices Over a Finite Field, Linear Alg. and its Appl. 10 (1975), 199-217.

4. BRAWLEY, J.V., The Number of Polynomial Functions Which Permute the Matrices Over a Finite Field, J. Comb. Theory 21 (1976), 147-154.

5. LIU, C.L., Introduction to Combinatorial Mathematics, McGraw Hill, New York, 1968.

6. HODGES, J.H., Scalar Polynomial Equations for Matrices Over a Finite Field, Duke Math. J. 25 (1958), 291-296.