ACTA ARITHMETICA
XLI (1982)

Matrix equivalence over finite fields

by

Gary L. Mullen (Sharon, Pa.)

1. Introduction. In a series of papers [1]–[4], [6], [8]–[10] L. Carlitz, S. Cavior, J. Durbin, and the author studied various forms of equivalence of functions over finite fields. In [11] the author studied a similar notion of equivalence for matrices over a finite field. In particular, two matrices A and B were said to be *equivalent* if $b_{ij} = \varphi(a_{ij})$ for some $\varphi \in \Omega$ where Ω is a group of permutations on $\mathrm{GF}(q)$. In the present paper we study a generalization of this definition which corresponds to the notion of weak equivalence of functions considered in [10] and [6]. We study this form of matrix equivalence by using the Pólya–deBruijn Theorem instead of the techniques employed by the author in [8]–[10].

In Section 2 we develop some general theory while in Section 3 we determine the number of equivalence classes induced by various permutation groups. In Section 4 we show that in the case of a cyclic group the results from the Pólya–deBruijn theory agree with those obtained for cyclic groups in Section 4 of [11] while in Section 5 we conclude with several examples.

Let $F = \mathrm{GF}(q)$ denote the finite field of order $q = p^b$, p a prime and $b \geqslant 1$. Let $F_{m\times n}$ denote the ring of $m \times n$ matrices over F so that $|F_{m\times n}| = q^{mn}$. Let $D = \{1, \ldots, mn\}$ and let F^D be the set of all functions from D into F so that $|F^D| = q^{mn}$. We now define a 1-1 correspondence between the mn ordered pairs of indices and the set D. To a given pair (i, j) we associate the number $n(i-1)+j \in D$. Conversely given $k \in D$, by the division algorithm we may write $k = n(i-1)+j$ where $0 \leqslant j < n$ so that to k we associate the pair (i, j) if $j \neq 0$ and $(i-1, n)$ if $j = 0$. We use this correspondence by saying that $l_{ij} \in D$ corresponds to the pair (i, j).

We use this correspondence to construct a 1-1 correspondence between $F_{m\times n}$ and F^D. To each $A \in F_{m\times n}$ we associate a function $f_A \in F^D$ as follows. Suppose $A = (a_{ij})$ has k distinct elements $a_1, \ldots, a_k$. For each $t = 1, \ldots, k$ let $A_t = \{l_{ij} \in D \mid a_{ij} = a_t\}$ and define $f_A\colon D \to F$ by $f_A(A_t) = a_t$. Then $A \leftrightarrow f_A$ gives a 1-1 correspondence between $F_{m\times n}$ and F^D.

2. General theory. Let G be a permutation group acting on D and H a permutation group acting on F so that G is a subgroup of S_{mn} and H

is isomorphic to a subgroup of S_q, the symmetric group on q letters. We now make

DEFINITION 1. If $A, B \in F_{m\times n}$ then B is *equivalent* to A relative to G and H if $\beta A\alpha = B$ for some $\alpha \in G$ and $\beta \in H$ where if $A = (a_{ij})$ then $\beta A\alpha = \big(\beta(a_{\alpha(l_{ij})})\big)$.

Thus G permutes the indices of A using the above correspondence while H permutes the elements of F. We note that if $G = \{\mathrm{id.}\}$ then this definition reduces to Definition 1 of [11].

Motivated by Durbin in [6] and the notion of weak equivalence considered by the author in [10] we may use G and H to induce an equivalence relation on F^D if we say f is equivalent to g if $\beta f\alpha = g$ for some $\alpha \in G, \beta \in H$. Moreover, if $A, B \in F_{m\times n}$, $A \leftrightarrow f_A$, and $B \leftrightarrow f_B$ then A is equivalent to B relative to G and H if and only if f_A is equivalent to f_B relative to G and H. The Pólya–deBruijn Theorem may now be used to calculate the number of equivalence classes induced by G and H in F^D and consequently, by the above remark, the number of equivalence classes induced by G and H in $F_{m\times n}$.

Suppose a permutation group K acts on a set S of r elements. If $\pi \in K$ consider the monomial $x_1^{b_1}x_2^{b_2}\ldots x_r^{b_r}$ where for $t = 1, \ldots, r$, b_t denotes the number of cycles of π of length t. The polynomial

$$P_K(x_1, \ldots, x_r) = |K|^{-1}\sum_{\pi\in K} x_1^{b_1}x_2^{b_2}\ldots x_r^{b_r} \tag{2.1}$$

is called the *cycle index* of K.

THEOREM (Pólya–deBruijn). *The number of equivalence classes of functions of D into F induced by permutation groups G of D and H of F is*

$$P_G\left(\frac{\partial}{\partial z_1}, \frac{\partial}{\partial z_2}, \ldots\right)P_H\left(e^{z_1+z_2+\cdots}, e^{2(z_2+z_4+\cdots)}, \ldots\right)\Big|_{z_1=z_2=\ldots=0}. \tag{2.2}$$

The Pólya–deBruijn theory may also be used to determine the number of classes relative to G and H of 1-1 functions from D into F if we calculate

$$P_G\left(\frac{\partial}{\partial z_1}, \frac{\partial}{\partial z_2}, \ldots\right)P_H(1+z_1, 1+2z_2, \ldots)\Big|_{z_1=z_2=\ldots=0}. \tag{2.3}$$

We observe that the 1-1 functions from D into F correspond to those matrices with mn distinct elements so that we must have $mn \leqslant p^b$ in order to have such functions.

In [6] Durbin computed the cycle index for any subgroup of $\mathrm{Aut}(\mathrm{GF}(p^b))$, the automorphism group of $\mathrm{GF}(p^b)$. In particular, if a is any generator of the multiplicative group of $\mathrm{GF}(p^b)$ and the mapping θ is defined by $\theta(0) = 0$ and $\theta(a^k) = a^{pk}$ for $0 \leqslant k < v = p^b-1$ then $\mathrm{Aut}(\mathrm{GF}(p^b)) = \langle\theta\rangle$ and has order b. Let $M(i, t)$ denote the number of elements in $\mathrm{GF}(p^b)$ that belong to a t-cycle of θ^i for $0 \leqslant i < b$. Durbin has shown in Lemma 2.1 of [6] that if $r\,|\,b$ then the cycle index of a subgroup $H = \langle\theta^r\rangle$ of $\mathrm{Aut}(\mathrm{GF}(p^b))$ is

$$P_H(x_1, \ldots, x_q) = \frac{r}{b}\sum_{i=0}^{(b/r)-1}\prod_t x_t^{M(ir,t)/t}. \tag{2.4}$$

While an explicit formula for $M(i, t)$ seems difficult to obtain in general, Lemma 2.2 of Durbin shows that $M(i, 1) = p^{(b,i)}$ while if $t > 1$ $M(i, t)$ is the number of k $(0 \leqslant k < v)$ such that t is the order of $p^i \bmod \big(v/(v, k)\big)$.

3. In this section we apply the above theory to obtain the number of equivalence classes induced by various permutation groups G and H. Let $\lambda(G, H)$ denote the number of classes induced by the groups G and H and let $\lambda'(G, H)$ be the number of classes of matrices with mn distinct elements induced by G and H.

THEOREM 3.1 *If $G = \{\mathrm{id}\}$ and $H = \langle\theta^r\rangle$ is a subgroup of $\mathrm{Aut}(\mathrm{GF}(p^b))$ then*

$$\lambda(G, H) = \frac{r}{b}\sum_{i=0}^{(b/r)-1} p^{(b,ir)mn} \tag{3.1}$$

and

$$\lambda'(G, H) = \frac{r}{b}\sum_{i=0}^{(b/r)-1} (p^{(b,ir)})_{mn} \tag{3.2}$$

where $(q)_t = q(q-1)\ldots(q-t+1)$ is the falling factorial with t terms.

Proof. Clearly $P_G = x_1^{mn}$ and P_H is given by (2.4). Substituting P_G and P_H into (2.2) we obtain a sum over $0 \leqslant i \leqslant (b/r)-1$ with general term

$$\frac{r}{b}\frac{\partial^{mn}}{\partial z_1^{mn}} e^{M(ir,1)(z_1+z_2+\ldots)+M(ir,2)(z_2+z_4+\ldots)+\cdots}\Big|_{z_1=z_2=\ldots=0} = \frac{r}{b}[M(ir, 1)]^{mn}$$

from which (3.1) follows. Similarly we obtain (3.2) upon evaluation of (2.3).

THEOREM 3.2. *If G is cyclic of order mn and $H = \langle\theta^r\rangle$ is a subgroup of $\mathrm{Aut}(\mathrm{GF}(p^b))$ then*

$$\lambda(G, H) = \frac{r}{mnb}\sum_{i=0}^{(b/r)-1}\sum_{t|mn}\varphi(t)\Big[\sum_{u|t} M(ir, u)\Big]^{mn/t} \tag{3.3}$$

where $\varphi(t)$ is Euler's totient function and

$$\lambda'(G, H) = \frac{r}{mnb}\sum_{i=0}^{(b/r)-1}\sum_{t|mn}\varphi(t)\,t^{mn/t}\big(M(ir, t)/t\big)_{mn/t}. \tag{3.4}$$

Proof. It is not difficult to show that

$$P_G(x_1, \ldots, x_{mn}) = (1/mn) \sum_{t|mn} \varphi(t) x_t^{mn/t}.$$

Substituting P_G and P_H into (2.2) we have for fixed t and i

$$\frac{r\varphi(t)}{mnb} \frac{\partial^{mn/t}}{\partial z_t^{mn/t}} e^{M(ir,1)(z_1+z_2+\ldots)+M(ir,2)(z_2+z_4+\ldots)+\ldots+M(ir,t)(z_t+z_{2t}+\ldots)+\ldots}\Big|_{z_i=0}$$
$$= \frac{r\varphi(t)}{mnb} \Big[\sum_{u|t} M(ir, u) \Big]^{mn/t}$$

from which (3.3) follows. To obtain (3.4) if we substitute P_G and P_H into (2.3) we obtain a double sum whose general term for fixed i and t is

$$\frac{r\varphi(t)}{mnb} \frac{\partial^{mn/t}}{\partial z_t^{mn/t}} (1+z_1)^{M(ir,1)}(1+2z_2)^{M(ir,2)/2} \ldots (1+tz_t)^{M(ir,t)/t} \ldots \Big|_{z_1=z_2=\ldots=0}$$
$$= \frac{r\varphi(t)}{mnb} \big(M(ir, t)/t\big)_{mn/t}$$

from which (3.4) follows.

THEOREM 3.3. *If G is a cyclic group of order mn and H is cyclic of order $q = p^b$ where $p^z \| mn$ then*

$$\lambda(G, H) = \frac{1}{mnq} \sum_{t|mn} \varphi(t) q^{mn/t} [1 + a(p^i - p^{i-1})] \tag{3.5}$$

where

$$a = \begin{cases} 1 & \text{if} \quad t = kp^i, \\ 0 & \text{if} \quad t \neq kp^i \end{cases}$$

and

$$\lambda'(G, H) = \frac{1}{mnq} \Big[(p^b)_{mn} + \sum_{i=1}^{z} (p^i - p^{i-1})^2 (p^i)^{mn/p^i} (p^{b-i})_{mn/p^i} \Big]. \tag{3.6}$$

Proof. In this case

$$P_H(x_1, \ldots, x_q) = (1/q) \Big[x_1^{p^b} + \sum_{i=1}^{b} (p^i - p^{i-1}) x_{p^i}^{p^{b-i}} \Big]$$

so that upon substituting P_G and P_H into (2.2) we obtain for a general term with t fixed

$$N = \frac{\varphi(t)}{mnq} \frac{\partial^{mn/t}}{\partial z_t^{mn/t}} \Big[e^{p^b(z_1+z_2+\ldots)} + \sum_{i=1}^{b} (p^i - p^{i-1}) e^{p^b(z_{p^i}+z_{2p^i}+\ldots)} \Big]\Big|_{z_1=z_2=\ldots=0}.$$

If $t \neq kp^i$ then

$$N = \frac{\varphi(t)}{mnq} (p^b)^{mn/t}.$$

If $t = kp^i$ for $i = 1, \ldots, z$ then

$$N = \frac{\varphi(t)}{mnq} [(p^b)^{mn/t} + (p^i - p^{i-1})(p^b)^{mn/t}].$$

Summing over all divisors t of mn we obtain (3.5).

To prove (3.6) we have for fixed t dividing mn

$$M = \frac{\varphi(t)}{mnq} \frac{\partial^{mn/t}}{\partial z_t^{mn/t}} \Big[(1+z_1)^{p^b} + \sum_{i=1}^{b} (p^i - p^{i-1})(1 + p^i z_{p^i})^{p^{b-i}} \Big]\Big|_{z_1=z_2=\ldots=0}.$$

If $t = 1$ then $M = (1/mnq)(p^b)_{mn}$ while if $1 < t \neq p^i$ then $M = 0$. If $t = p^i$ for some $i = 1, \ldots, z$ where $p^z \| mn$ then

$$M = (1/mnq)(p^i - p^{i-1})^2 (p^i)^{mn/p^i} (p^{b-i})_{mn/p^i}.$$

Summing over all t dividing mn yields (3.6).

With a slight modification we may prove

COROLLARY 3.4. *If G is a cyclic group of order mn and H is cyclic of order $q = p^b$ where $p \nmid mn$ then*

$$\lambda(G, H) = (1/mnq) \sum_{t|mn} \varphi(t) q^{mn/t} \tag{3.7}$$

and

$$\lambda'(G, H) = (1/mnq)(q)_{mn}. \tag{3.8}$$

4. In this section we show that the results for cyclic groups obtained by the Pólya–deBruijn theory are in agreement with those obtained by the author in Section 4 of [11]. Suppose H is a cyclic group of permutations of F and $\lambda(H)$ is the number of classes induced by H as computed in Corollary 4.2 of [11]. While we do have a more compact formula for the number of classes by using the Pólya–deBruijn theory, we do not obtain information regarding the number of classes of a given order as was obtained in [11] by other techniques. We now prove

THEOREM 4.1. *If $G = \{\mathrm{id}\}$ then $\lambda(G, H) = \lambda(H)$.*

Proof. Suppose $H = \langle \varphi \rangle$ is a cyclic group of permutations of F of order s so that as shown in Corollary 4.2 of [11]

$$\lambda(H) = (1/s) \sum_{t|s} t M(t, m, n) \tag{4.1}$$

where $M(t, m, n) = l(t)^{mn} - \sum M(u, m, n)$ with the sum over all $u | s$, $t | u$, $t \neq u$ and $l(t)$ is the number of fixed points of $\varphi^{s/t}$. Applying Möbius inversion we obtain

$$\lambda(H) = (1/s) \sum_{t|s} t \sum_{a|s/t} \mu(a) l(at)^{mn} \tag{4.2}$$

where $\mu(a)$ is the Möbius function.

We now show that the Pólya theory yields the same result. If $b_i(\Psi)$ denotes the number of cycles of Ψ of length i, it is clear upon using (2.2) that

$$\lambda(G, H) = (1/s)\frac{\partial^{mn}}{\partial z_1^{mn}}\sum_{\Psi\in H} e^{b_1(\Psi)(z_1+z_2+\cdots)+2b_2(\Psi)(z_2+z_4+\cdots)+\cdots+qb_q(\Psi)(z_q+z_{2q}+\cdots)}\Big|_{z_j=0}$$

$$= (1/s)\sum_{\Psi\in H} b_1(\Psi)^{mn} = (1/s)\sum_{i=1}^{s} b_1(\varphi^i)^{mn}.$$

If φ^i has order k then $b_1(\varphi^i) = l(k)$ where $k|s$ so that

$$\lambda(G, H) = (1/s)\sum_{k|s} v(k)l(k)^{mn}$$

where $v(k)$ is the number of elements of H of order k so that $v(k) = \varphi(k)$ and thus

$$\lambda(G, H) = (1/s)\sum_{k|s}\varphi(k)l(k)^{mn}.$$

It is not difficult to show that in (4.2), for a given divisor k of s, the number of times that $l(k)^{mn}$ occurs is $\sum_{ta=k} t\mu(a) = \varphi(k)$ which completes the proof.

Corresponding to (3.6) of [11] we prove

THEOREM 4.2. *If $G = \{\mathrm{id}\}$ and $H = S_q$ then*

$$\lambda(G, H) = \sum (k_1!k_2!2^{k_2}\ldots k_q!q^{k_q})^{-1}k_1^{mn} \tag{4.3}$$

where the sum is over all nonnegative k_i such that $k_1+2k_2+\ldots+qk_q = q$.

Proof. The proof follows from the Pólya–deBruijn Theorem and the fact that

$$P_H(x_1, \ldots, x_q) = \sum (k_1!k_2!2^{k_2}\ldots k_q!q^{k_q})^{-1}x_1^{k_1}x_2^{k_2}\ldots x_q^{k_q}$$

where the sum is over all $k_1+2k_2+\ldots+qk_q = q$.

Similarly if $H = \{\mathrm{id}\}$ we can determine $\lambda(G, H)$ for any group G by simply evaluating $P_G(q, \ldots, q)$. In this situation Klass in [7] has obtained a formula for E_k, the number of k-element equivalence classes induced by G. In particular

$$E_k = (1/k)\sum_{\{H\leqslant G|[G:H]=k\}}\sum_{K\leqslant G}\mu(H, K)|F_K| \tag{4.4}$$

where $F_K = \{h\in D \mid \sigma(h) = h \text{ for all } \sigma\in K\}$ and $\mu(H, K)$ is the Möbius function defined on the lattice of subgroups of G.

5. Illustrations. As an illustration of the above theory suppose q is a prime so that F reduces to the integers modulo q. If H is a cyclic group of order q then it is not difficult to see that $P_H(x_1, \ldots, x_q) = (1/q)[x_1^q+(q-1)x_q]$ and if $G = \{\mathrm{id}\}$ then $P_G(x_1, \ldots, x_{mn}) = x_1^{mn}$. Thus upon evaluation of (2.2) and (2.3) we have $\lambda(G, H) = q^{mn-1}$ while $\lambda'(G, H) = 0$ if $mn > q$ and $\lambda'(G, H) = (1/q)(q)_{mn}$ if $mn \leqslant q$. For example, if $q = 5$ and $m = n = 2$ then $\lambda(G, H) = 125$ which is in agreement with Corollary 4.2 of [11].

As a second illustration suppose $G = \{\mathrm{id}\}$, $m = n = 2$, $q = 3$ and $H = S_3$. Theorem 4.2 can be applied directly or if (2.2) is used we have $P_H = (1/6)(x_1^3+3x_1x_2+2x_3)$ so that (2.2) becomes

$$(1/6)\frac{\partial^4}{\partial z_1^4} e^{3(z_1+z_2+z_3)}+3e^{z_1+z_2+z_3}e^{2z_2}+2e^{3z_3}\Big|_{z_1=z_2=z_3=0} = (1/6)(3^4+3) = 14$$

which agrees with the example after Corollary 3.4 of [11].

References

[1] L. Carlitz, *Invariantive theory of equations in a finite field*, Trans. Amer. Math. Soc. 75 (1953), pp. 405–427.

[2] — *Invariant theory of systems of equations in a finite field*, J. Analyse Math. 3 (1953/54), pp. 382–413.

[3] S. R. Cavior, *Equivalence classes of functions over a finite field*, Acta Arith. 10 (1964), pp. 119–136.

[4] — *Equivalence classes of sets of polynomials over a finite field*, Journ. Reine Angew. Math. 225 (1967), pp. 191–202.

[5] N. G. deBruijn, *Pólya's theory of counting*; in: *Applied Combinatorial Mathematics* (ed. E. F. Beckenbach), John Wiley and Sons, New York 1964.

[6] J. R. Durbin, *Automorphisms and equivalence of functions over finite fields*, preprint.

[7] M. J. Klass, *A generalization of Burnside's combinatorial lemma*, J. Comb. Theory (A) 20 (1976), pp. 273–278.

[8] G. L. Mullen, *Equivalence classes of functions over a finite field*, Acta Arith. 29 (1976), pp. 353–358.

[9] — *Equivalence classes of polynomials over finite fields*, ibid. 31 (1976), pp. 113–123.

[10] — *Weak equivalence of functions over a finite field*, ibid. 35 (1979), pp. 259–272.

[11] — *Equivalence classes of matrices over finite fields*, Linear Algebra and Appl. 27 (1979), pp. 61–68.

Received on 7.9.1979 (1173)