References

[1] B. J. Birch and D. J. Lewis, *Systems of three quadratic forms*, Acta Arith. 10 (1965), pp. 423–442.

[2] H. Hasse, *Vorlesungen über Zahlentheorie*, Berlin 1950.

[3] D. J. Lewis and S. E. Schuur, *Varieties of small degree over finite fields*, J. Reine Angew. Math. 262/263 (1973), pp. 293–306.

[4] S. E. Schuur, *Systems of quadratic forms over local fields*, Dissertation, University of Michigan, Ann Arbor 1969.

DEPARTMENT OF MATHEMATICS
MICHIGAN STATE UNIVERSITY

Received on 6. 4. 1977
and in revised form on 2. 1. 1978 (933)

ACTA ARITHMETICA
XXXVI (1980)

Equivalence classes of sets of functions over a finite field

by

Gary L. Mullen (Sharon, Penn.)

1. Introduction. In [3] and [6] S. Cavior and the author studied properties of left equivalence of functions over a finite field. In [4] S. Cavior extended the notion of left equivalence to sets of functions. In the present paper we study a further generalization of left equivalence of functions over a finite field.

In Section 2 we develop a notion of left equivalence which generalizes all of the forms of left equivalence studied in [3], [4], and [6]. In particular, we consider left equivalence of sets of functions over a finite field relative to arbitrary groups of permutations. Moreover, we show that many of the results in this general setting can be reduced to the single function case, which was studied in detail in [6].

Let $K = \mathrm{GF}(q)$ denote the finite field of order q and K^r ($r \geqslant 1$) the product of r copies of K. Let $K[x_1, \ldots, x_r] = K[\bar{x}]$ represent the ring of polynomials in r indeterminates over K. By the Lagrange Interpolation Formula ([5], p. 55), each function from K^r into K can be expressed uniquely as a polynomial of degree $< q$. The group of all permutations of K will be represented by Φ so that Φ is isomorphic to S_q. That Ω is an arbitrary subgroup of Φ will be denoted by $\Omega < \Phi$ and $|\Omega|$ will denote the order of Ω.

2. General theory. If $k \geqslant 1$ is a positive integer the k-tuple of functions $(f_1, \ldots, f_k)$ will be denoted by (f_i) so that there are a total of q^{kq^r} distinct k-tuples of functions each containing k functions.

Definition 2.1. Let $\Omega_1, \ldots, \Omega_k < \Phi$. Then (f_i) is *left equivalent* to (g_i) relative to $\Omega_1, \ldots, \Omega_k$ if there exist $\varphi_i \in \Omega_i$ such that $\varphi_i f_i = g_i$ for $i = 1, \ldots, k$.

This is clearly an equivalence relation which, if $k = 1$, reduces to that of the author in [6]. If $k = 1$ and $\Omega_1 = \Phi$, we obtain the left equivalence considered by Cavior in [3]. If $k \geqslant 1$ and $\Omega_i = \Phi$ for $i = 1, \ldots, k$, then Definition 2.1 reduces to that of Cavior in [4].

As an illustration, consider the case where $K = \mathrm{GF}(5)$, $r = 1$, and $k = 2$. Suppose that in cyclic notation $\varphi_1 = (01)$ and $\varphi_2 = (234)$. For

$i = 1, 2$ let $\Omega_i = \langle\varphi_i\rangle$ so that $|\Omega_1 \times \Omega_2| = 6$. If $\lambda_L(\Omega_1, \Omega_2)$ represents the total number of equivalence classes induced by $\Omega_1 \times \Omega_2$ and for $i = 1, 2, 3$, and 6, $c(i)$ denotes the number of equivalence classes of order i, then as will be shown in Section 3, we have

$$c(1) = 7776, \qquad c(3) = 250533,$$
$$c(2) = 46112, \qquad c(6) = 1485671,$$

so that

$$\lambda_L = 1790092.$$

Let $\mu_L\big((f_i), \Omega_1, \ldots, \Omega_k\big)$ represent the number of elements in the class of (f_i) relative to the groups $\Omega_1, \ldots, \Omega_k$. One may easily check that

$$\mu_L\big((f_i), \Omega_1, \ldots, \Omega_k\big) = \prod_{i=1}^{k} \mu_L(f_i, \Omega_i)$$

so that in the general case of a set of k functions, we need only compute the values of $\mu_L(f_i, \Omega_i)$ for $i = 1, \ldots, k$. Formulas for $\mu_L(f_i, \Omega_i)$ are given in [6] in terms of the number of invariant elements of the group Ω_i. Finally, let $\lambda_L(\Omega_1, \ldots, \Omega_k)$ denote the total number of left equivalence classes induced by the groups $\Omega_1, \ldots, \Omega_k$.

If $K = \{\alpha_1, \ldots, \alpha_q\}$ and $f \in K[\bar{x}]$ let $S_j = \{\beta \in K^r \mid f(\bar{\beta}) = \alpha_j\}$ for $j = 1, \ldots, q$. Assume that the non-empty S_j's are $S_1, \ldots, S_t$ where t is the order of the range of f. Then $\pi_f = \{S_j \mid j = 1, \ldots, t\}$ is the *partition* of f.

THEOREM 2.1. *Let $\Omega_1, \ldots, \Omega_k < \Phi$. Then (f_i) is left equivalent to (g_i) relative to $\Omega_1, \ldots, \Omega_k$ if and only if $\pi_{f_i} = \pi_{g_i} = \{S_j^i \mid j = 1, \ldots, t_i\}$ and fhere exist $\varphi_i \in \Omega_i$ such that $\varphi_i(\gamma_j^i) = \delta_j^i$ where $f_i(S_j^i) = \gamma_j^i$ and $g_i(S_j^i) = \delta_j^i$ tor $j = 1, \ldots, t_i$.*

Proof. Fix i and let $\bar{\alpha} \in K^r$ so that $\bar{\alpha} \in S_j^i$ for some $j = 1, \ldots, t_i$. Hence $g_i(\bar{\alpha}) = \delta_j^i = \varphi_i(\gamma_j^i) = \varphi_i\big(f_i(\bar{\alpha})\big)$ which proves the sufficiency. For necessity, suppose $\varphi_i f_i = g_i$ for some $\varphi_i \in \Omega_i$. If $f_i(\bar{\alpha}) = f_i(\bar{\beta})$ then $g_i(\bar{\alpha}) = g_i(\bar{\beta})$. Similarly since φ_i is 1-1, if $f_i(\bar{\alpha}) \neq f_i(\bar{\beta})$ then $g_i(\bar{\alpha}) \neq g_i(\bar{\beta})$ so that $\pi_{f_i} = \pi_{g_i}$. This completes the proof.

DEFINITION 2.2. Let $\Omega_1, \ldots, \Omega_k < \Phi$. Then the k-tuple $(\varphi_1, \ldots, \varphi_k)$ is a *left automorphism* of (f_i) relative to $\Omega_1, \ldots, \Omega_k$ if $\varphi_i f_i = f_i$ for $i = 1, \ldots, k$.

Let $A_L\big((f_i), \Omega_1, \ldots, \Omega_k\big)$ and $\nu_L\big((f_i), \Omega_1, \ldots, \Omega_k\big)$ denote the group and number of left automorphisms of the set (f_i) relative to the groups $\Omega_1, \ldots, \Omega_k$. Then we have

$$A_L\big((f_i), \Omega_1, \ldots, \Omega_k\big) = A_L(f_1, \Omega_1) \times \ldots \times A_L(f_k, \Omega_k)$$

so that

$$\nu_L\big((f_i), \Omega_1, \ldots, \Omega_k\big) = \prod_{i=1}^{k} \nu_L(f_i, \Omega_i).$$

Thus the general case can again be reduced to that of the one variable case studied in [6]. Moreover, if $(\varphi_1, \ldots, \varphi_k)(f_i) = (g_i)$ then

$$A_L\big((g_i), \Omega_1, \ldots, \Omega_k\big) = (\varphi_1, \ldots, \varphi_k) A_L\big((f_i), \Omega_1, \ldots, \Omega_k\big)(\varphi_1, \ldots, \varphi_k)^{-1}$$

so that

$$\prod_{i=1}^{k} \nu_L(g_i, \Omega_i) = \prod_{i=1}^{k} \nu_L(f_i, \Omega_i).$$

Thus the number of left automorphisms depends only upon the class and not on the particular sets of functions in the class.

The following theorem, whose proof we omit, generalizes the corresponding results of [3], [4], and [6].

THEOREM 2.2. *If $\Omega_1, \ldots, \Omega_k < \Phi$ then for any set (f_i)*

$$\prod_{i=1}^{k} [\mu_L(f_i, \Omega_i)\nu_L(f_i, \Omega_i)] = \prod_{i=1}^{k} |\Omega_i|. \tag{2.1}$$

If φ is a permutation let $F_\varphi = \{\alpha \in K \mid \varphi(\alpha) = \alpha\}$ denote the set of invariant elements of φ. If Ω is a group of permutations, define the invariant set F_Ω of the group Ω by $F_\Omega = \bigcap_{\varphi \in \Omega} F_\varphi$. The following theorem generalizes Theorem 2.4 of [6].

THEOREM 2.3. *Suppose Ω_i has l_i invariant elements for $i = 1, \ldots, k$. Then the number of k-tuples (f_i) of functions for which each permutation in $\Omega_1 \times \ldots \times \Omega_k$ is a left automorphism is $\prod_{i=1}^{k} l_i^{q^r}$.*

Proof. The k-tuple $(\varphi_1, \ldots, \varphi_k)$ is a left automorphism of (f_i) if and only if for each $i = 1, \ldots, k$ $\varphi_i(\alpha) = \alpha$ for all $\alpha \in R_{f_i}$. For each $i = 1, \ldots, k$ there are $l_i^{q^r}$ distinct functions which map K^r into F_{Ω_i}. Hence there are $l_1^{q^r} \ldots l_k^{q^r}$ distinct k-tuples for which $(\varphi_1, \ldots, \varphi_k)$ leaves $(f_1, \ldots, f_k)$ fixed from which the result follows.

3. Cyclic groups.

In this section we develop several results in the case where the groups of permutations are cyclic. Suppose that for $i = 1, \ldots, k$ Ω_i is a cyclic group of permutations of order n_i where the n_i's are pairwise relatively prime. Let $H(t_i)$ denote the subgroup of Ω_i of order t_i where $t_i \mid n_i$. Let $F_{H(t_i)}$ and $l(t_i)$ denote the set and number of invariant elements of $H(t_i)$. Finally let $N(t_1 \ldots t_k)$ represent the number of k-tuples $(f_1, \ldots, f_k)$ such that $A_L(f_1, \Omega_1) \times \ldots \times A_L(f_k, \Omega_k) = H(t_1) \times \ldots \times H(t_k)$.

THEOREM 3.1. *For* $t_i | n_i$, $i = 1, \ldots, k$

$$N(t_1 \ldots t_k) = \prod_{i=1}^{k} N(t_i) \tag{3.1}$$

where

$$N(t_i) = \sum_{a | \frac{n_i}{t_i}} \mu(a) [l(at_i)]^{q^r} \tag{3.2}$$

and $\mu(a)$ *is the Möbius function.*

Proof. Since the n_i's are pairwise relatively prime, for each $t_i | n_i$, $i = 1, \ldots, k$ there is a unique divisor of $n_1 \ldots n_k$ of the form $t_1 \ldots t_k$ from which (3.1) follows.

For each $i = 1, \ldots, k$, $[l(t_i)]^{q^r}$ is the number of functions f_i such that $H(t_i) < A_L(f_i, \Omega_i)$. The number of f_i for which the containment is proper is given by $\sum N(u_i)$ where the sum is over all u_i such that $u_i | n_i$, $t_i | u_i$, and $t_i \neq u_i$. Hence for each $i = 1, \ldots, k$

$$N(t_i) = [l(t_i)]^{q^r} - \sum_{\substack{u_i | n_i \\ t_i | u_i \\ t_i \neq u_i}} N(u_i). \tag{3.3}$$

For simplicity of notation, fix i and let $n = n_i$, $t = t_i$ and $u = u_i$. We now show that (3.3) can be written in the form (3.2) which will complete the proof.

Fix n and let $n = st$. Let $N(t) = f(s)$ and $l(t) = \lambda(s)$ so that (3.3) becomes

$$f(s) = [\lambda(s)]^{q^r} - \sum_{\substack{v | s \\ v > 1}} f(v). \tag{3.4}$$

Since s is an arbitrary division of n, the Möbius inversion formula applies so that

$$f(s) = \sum_{ab = s} \mu(a) [\lambda(b)]^{q^r} \tag{3.5}$$

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

$$N(t) = \sum_{a | \frac{n}{t}} \mu(a) [l(at)]^{q^r} \tag{3.6}$$

which completes the proof.

COROLLARY 3.2. *For* $t_i | n_i$, $i = 1, \ldots, k$ *there are*

$$\prod_{i=1}^{k} \frac{t_i N(t_i)}{n_i} \tag{3.7}$$

left equivalence classes of order $\prod_{i=1}^{k} n_i / t_i$ *and*

$$\lambda_L(\Omega_1, \ldots, \Omega_k) = \prod_{i=1}^{k} \lambda_L(\Omega_i) \tag{3.8}$$

where

$$\lambda_L(\Omega_i) = \sum_{t_i | n_i} \frac{t_i N(t_i)}{n_i} \tag{3.9}$$

and $N(t_i)$ *is given by* (3.2).

Proof. From (2.1) and the fact that for each $i = 1, \ldots, k$, $N(t_i)$ represents the number of functions f_i such that $A_L(f_i, \Omega_i) = H(t_i)$, we see that the number of classes of order $\prod_{i=1}^{k} n_i / t_i$ is given by (3.7). Clearly for each $i = 1, \ldots, k$

$$\lambda_L(\Omega_i) = \sum_{t_i | n_i} \frac{t_i N(t_i)}{n_i}$$

so that

$$\lambda_L(\Omega_1, \ldots, \Omega_k) = \sum_{t_1 | n_1} \cdots \sum_{t_k | n_k} \prod_{i=1}^{k} \frac{t_i N(t_i)}{n_i}$$

which can be rearranged to

$$= \prod_{i=1}^{k} \sum_{t_i | n_i} \frac{t_i N(t_i)}{n_i} = \prod_{i=1}^{k} \lambda_L(\Omega_i).$$

Hence, from (3.8), we see that the problem of determining the total number of left equivalence classes of sets of functions has been reduced to that of the single function case. We further note that if $k = 1$, then Theorem 3.1 and Corollary 3.2 reduce to Theorem 3.1 and Corollary 3.2 of [6].

COROLLARY 3.3. *If* (f_i) *is a set of functions then* $\nu_L((f_i), \Omega_i) = \prod_{i=1}^{k} t_i$, *or equivalently,* $\mu_L((f_i), \Omega_i) = \prod_{i=1}^{k} n_i / t_i$ *if and only if* $H(t_1) \times \ldots \times H(t_k)$ *is the largest subgroup of* $\Omega_1 \times \ldots \times \Omega_k$ *for which* $R_{f_i} \subseteq F_{H(t_1) \times \ldots \times H(t_k)}$.

DEFINITION 3.1. Let $\Omega_1, \ldots, \Omega_k$, $\Omega'_1, \ldots, \Omega'_k < \Phi$. Suppose that $\Omega = \Omega_1 \times \ldots \times \Omega_k$ and $\Omega' = \Omega'_1 \times \ldots \times \Omega'_k$ decompose $(K[\bar{x}])^k$ into the equivalence classes $A_1, \ldots, A_{t_1}$ and $B_1, \ldots, B_{t_2}$ respectively. Then Ω and Ω' induce *equivalent* decompositions of $(K[\bar{x}])^k$ if $\{|A_i|\}$ is a permutation of $\{|B_i|\}$ where $|A|$ denotes the order of the set A. Otherwise, the decompositions are *inequivalent*.

THEOREM 3.4. *Suppose $\Omega = \Omega_1 \times \ldots \times \Omega_k$ and $\Omega' = \Omega_1' \times \ldots \times \Omega_k'$ where Ω_i and Ω_i' are cyclic groups of permutations of order n_i where the n_i's are pairwise relatively prime. Then Ω and Ω' induce equivalent left decompositions of $(K[\bar{x}])^k$ if and only if for each $t_1 \ldots t_k \mid n_1 \ldots n_k$, $H(t_i)$ and $H'(t_i)$ $(i = 1, \ldots, k)$ have the same number of invariant elements where $H(t_i)$ and $H'(t_i)$ are the subgroups of Ω_i and Ω_i' of order t_i.*

Proof. Follows from Theorem 3.1 and Corollary 3.2.

We now illustrate the above theory in the case where $K = GF(5)$, $r = 1$, and $k = 2$. Suppose that in cyclic notation $\varphi_1 = (01)$, $\varphi_2 = (234)$, and $\Omega_i = \langle \varphi_i \rangle$ for $i = 1, 2$ so that $|\Omega_1 \times \Omega_2| = 6$. For $i = 1, 2, 3$, and 6 let $c(i)$ denote the number of equivalence classes of order i induced by $\Omega_1 \times \Omega_2$. Let $l(i)$ represent the number of invariant elements of $\langle \varphi_i^{n_i/t_i} \rangle = H(t_i)$ for $i = 1, 2$ so that $l(1) = 5$, $l(2) = 3$, and $l(3) = 2$. If $N(t_1 t_2)$ represents the number of pairs (f_1, f_2) such that $A_L(f_1, \Omega_1) \times A_L(f_2, \Omega_2) = H(t_1) \times H(t_2)$ then by Theorem 3.1 we see that

$$N(2\cdot 3) = N(2)N(3) = 243\cdot 32 = 7776,$$
$$N(1\cdot 3) = N(1)N(3) = 2882\cdot 32 = 92224,$$
$$N(2\cdot 1) = N(2)N(1) = 243\cdot 1093 = 751599,$$
$$N(1\cdot 1) = N(1)N(1) = 2882\cdot 3093 = 8914026$$

so that by (3.7)

$$c(1) = 7776, \qquad c(3) = 250533,$$
$$c(2) = 46112, \qquad c(6) = 1485671,$$

and thus $\lambda_L(\Omega_1, \Omega_2) = 1790092$. Using (3.8) we also note that

$$\lambda_L(\Omega_1, \Omega_2) = \lambda_L(\Omega_1)\lambda_L(\Omega_2) = 1684\cdot 1063 = 1790092.$$

Acknowledgment. The author wishes to thank the referee for his helpful suggestions which improved the quality of this paper.

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 (1954), pp. 382–413.

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

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

[5] L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Dover Publications, Inc., New York 1958.

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

Received on 7. 5. 1977
and in revised form on 6. 1. 1978 (937)