ACTA ARITHMETICA
XXIX (1976)

Equivalence classes of functions over a finite field*

by

GARY L. MULLEN (Sharon, Pa.)

1. Introduction. In [1] Carlitz discussed invariantive properties of polynomials over a finite field. Cavior in [2] and [3] has considered the notion of left equivalence of functions over a finite field K where the underlying group of permutations is taken to be the group Φ of all permutations on K. In this paper we treat the more general case where we allow the permutations to lie in an arbitrary subgroup Ω of Φ.

After developing some general theory of left equivalence in Section 2, we treat the case where Ω is a cyclic group of permutations. Formulas, given in terms of the number of invariant elements of the group Ω, are obtained for the number of equivalence classes of a given order and in particular for the total number of classes induced by the group Ω. As a simple illustration of the type of results which we obtain, let Ω be the cyclic group of order four generated by the permutation $\varphi(x) = x^3+4x^2+2x$ over $K = \mathrm{GF}(5)$. If $\lambda_L(\Omega)$ denotes the number of equivalence classes induced by Ω then $\lambda_L(\Omega) = 782$, and moreover, Ω decomposes $K[x]$ into 1 class of order one, 0 classes of order two, and 781 classes of order four.

In Sections 4 and 5 we develop several results concerning direct sums and prove that if Ω_1 and Ω_2 are conjugate subgroups, then Ω_1 and Ω_2 induce the same number of classes of the same size.

Let $K = \mathrm{GF}(q)$ denote the finite field of order q where $q = p^n$ 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. Two polynomials $f, g \in K[\bar{x}]$ are equal if they are equal as functions. By the Lagrange Interpolation Formula ([4], p. 55), each function f from K^r into K can be expressed as a polynomial of degree $< q$ so that $K[\bar{x}]$ consists of exactly q^{q^r} polynomials. 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.

---

*The results of this paper are contained in the author's doctoral dissertation written under the very helpful direction of Professor Harlan R. Stevens.

2. General theory. We begin with

DEFINITION 2.1. Let $\Omega < \Phi$ and $f, g \in K[\bar{x}]$. Then f is *left equivalent* to g relative to Ω if there exists a $\varphi \in \Omega$ such that $\varphi f = g$.

This relation is obviously an equivalence relation on $K[\bar{x}]$ which reduces to the case considered by Cavior when $\Omega = \Phi$. Let Ωf and $\mu_L(f, \Omega)$ denote the class of f and the number of elements in the class of f relative to Ω while the number of classes induced by Ω will be denoted by $\lambda_L(\Omega)$. One might suspect that for any polynomial f

$$\mu_L(f, \Omega)\,[\Phi: \Omega] = \mu_L(f, \Phi)$$

where $[\Phi: \Omega]$ denotes the index of Ω in Φ. That this is not the case in general is seen from the simple example $f = a$ where $a \in K$.

If $K = \{a_1, \ldots, a_q\}$ and $f \in K[\bar{x}]$ let

$$S_i = \{\bar{\beta} \in K^r \mid f(\bar{\beta}) = a_i\}, \quad i = 1, \ldots, q.$$

Assume that the non-empty S_i's are $S_1, \ldots, S_t$ where t is the order of the range of f. Then $\pi_f = \{S_i \mid i = 1, \ldots, t\}$ is the *partition* of f. We may now prove

THEOREM 2.1. *Let $\Omega < \Phi$ and $f, g \in K[\bar{x}]$. Then f is left equivalent to g relative to Ω if and only if $\pi_f = \pi_g = \{S_i \mid i = 1, \ldots, t\}$ and there exists a $\varphi \in \Omega$ such that $\varphi(\gamma_i) = \delta_i$ where $f(S_i) = \gamma_i$ and $g(S_i) = \delta_i$ for $i = 1, \ldots, t$.*

Proof. Let $\bar{a} \in K^r$ so that $\bar{a} \in S_i$ for some $i = 1, \ldots, t$. Then $g(\bar{a}) = \delta_i = \varphi(\gamma_i) = \varphi(f(\bar{a}))$ which proves the sufficiency. For necessity, if $g = \varphi f$ for some $\varphi \in \Omega$ and $f(\bar{a}) = f(\bar{\beta})$ then $g(\bar{a}) = g(\bar{\beta})$. Similarly since φ is 1-1 if $f(\bar{a}) \neq f(\bar{\beta})$ then $g(\bar{a}) \neq g(\bar{\beta})$ so that $\pi_f = \pi_g$.

DEFINITION 2.2. Let $\Omega < \Phi$ and $f \in K[\bar{x}]$. A permutation $\varphi \in \Omega$ is a *left automorphism* of f relative to Ω if $\varphi f = f$.

Let $A_L(f, \Omega)$ and $\nu_L(f, \Omega)$ denote the group and number of left automorphisms of f relative to Ω. It is easily seen that if $\Omega < \Phi$ then

$$A_L(f, \Omega) < A_L(f, \Phi) \quad \text{and} \quad A_L(f, \Omega) = A_L(f, \Phi) \cap \Omega.$$

Moreover if $A_L(f, \Omega)$ is normal in Ω then Ωf is a group under the operation $(\psi f)(\varphi f) = \psi(\varphi f)$. If $\varphi f = g$ for some $\varphi \in \Omega$ then

$$A_L(g, \Omega) = \varphi A_L(f, \Omega)\varphi^{-1} \quad \text{so that} \quad \nu_L(g, \Omega) = \nu_L(f, \Omega).$$

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

The following theorem, whose proof is immediate, generalizes the corresponding result of Cavior [2].

THEOREM 2.2. *Let $f \in K[\bar{x}]$. Then for any group Ω*

$$\mu_L(f, \Omega)\nu_L(f, \Omega) = |\Omega|.$$

If $f \in K[\bar{x}]$ let R_f denote the range of f and $|R_f|$ the number of distinct elements in R_f. We have

LEMMA 2.3. *A permutation φ is a left automorphism of a polynomial f if and only if $\varphi(a) = a$ for all $a \in R_f$.*

If φ is a permutation of K, let

$$F_\varphi = \{a \in K \mid \varphi(a) = a\}$$

denote the set of invariant elements of φ. More generally, 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 is crucial in what follows.

THEOREM 2.4. *Suppose Ω has l invariant elements. Then the number of polynomials for which each permutation in Ω is a left automorphism is l^{q^r}.*

Proof. By Lemma 2.3, $\varphi \in \Omega$ is a left automorphism of a polynomial f if and only if $\varphi(a) = a$ for all $a \in R_f$. Thus a permutation $\varphi \in \Omega$ will be a left automorphism of those f for which $R_f \subseteq F_\Omega$. Since there are l distinct elements in F_Ω, there are l^{q^r} functions which map K^r into F_Ω which completes the proof.

3. Cyclic groups. In this section we suppose that Ω is a cyclic group of permutations of order n. Let $H(t)$ denote the unique subgroup of Ω of order t for each t which divides n. Let $F_{H(t)}$ represent the invariant elements of $H(t)$ and $l(t)$ their number respectively. Finally suppose $N(t)$ denotes the number of polynomials f such that $A_L(f, \Omega) = H(t)$.

By Theorem 2.4 for fixed t, $l(t)^{q^r}$ is the number of polynomials f such that $H(t) < A_L(f, \Omega)$. The number of polynomials f such that $H(t) \lneqq A_L(f, \Omega)$ is given by $\sum N(u)$ where the sum is over all u such that $u \mid n$, $t \mid u$, and $t \neq u$. Thus we have proven

THEOREM 3.1. *For each divisor t of n*

$$N(t) = l(t)^{q^r} - \sum N(u)$$

where the sum is over all u for which $u \mid n$, $t \mid u$, and $t \neq u$.

COROLLARY 3.2. *For each divisor t of n there are $tN(t)/n$ classes of order n/t and*

$$\lambda_L(\Omega) = \frac{1}{n}\sum_{t \mid n} tN(t).$$

COROLLARY 3.3. *Let $f \in K[\bar{x}]$. Then $\nu_L(f, \Omega) = t$, or equivalently $\mu_L(f, \Omega) = n/t$, if and only if $H(t)$ is the largest subgroup of Ω for which $R_f \subseteq F_{H(t)}$.*

Note. By the largest subgroup of Ω for which $R_f \subseteq F_{H(t)}$ we mean that if $H(t) < K$ and $R_f \subseteq F_K$ then $H(t) = K$.

Definition 3.1. Let $\Omega_1, \Omega_2 < \Phi$. Suppose that Ω_1 and Ω_2 decompose $K[\bar{x}]$ into the equivalence classes $A_1, \ldots, A_{t_1}$ and $B_1, \ldots, B_{t_2}$ respectively. Then Ω_1 and Ω_2 induce *equivalent* decompositions of $K[\bar{x}]$ 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 Ω_1 and Ω_2 are cyclic groups of order n. Then Ω_1 and Ω_2 induce equivalent left decompositions of $K[\bar{x}]$ if and only if for each divisor t of n, $H_1(t)$ and $H_2(t)$ have the same number of invariant elements where $H_j(t)$ $(j = 1, 2)$ denotes the unique subgroups of Ω_1 and Ω_2 of order t.*

Proof. Follows from Theorem 3.1 and Corollary 3.2.

Corollary 3.5. *Let $\Omega_1, \Omega_2 < \Phi$ such that $|\Omega_1| = |\Omega_2| = p$ a prime. Then Ω_1 and Ω_2 induce equivalent left decompositions of $K[\bar{x}]$ if and only if Ω_1 and Ω_2 have the same number of invariant elements.*

As Corollary 3.5 shows, if Ω_1 and Ω_2 are isomorphic, they need not induce equivalent left decompositions of $K[\bar{x}]$. For example, if $2p \leqslant q$ then there exist groups Ω_1 and Ω_2 of order p which are clearly isomorphic, but which have different numbers of invariant elements and thus induce inequivalent left decompositions of $K[\bar{x}]$.

4. Direct sums. Suppose that $\Omega = H_1 \oplus \ldots \oplus H_n$ where each H_i is generated by φ_i for $i = 1, \ldots, n$. Let

$$K_i = \{a \in K \mid \varphi_i(a) \neq a\}, \quad i = 1, \ldots, n. \tag{4.1}$$

Theorem 4.1. *Let $f \in K[\bar{x}]$ and $\Omega = H_1 \oplus \ldots \oplus H_n$. If the K_i's defined in (4.1) are pairwise disjoint then*

$$A_L(f, \Omega) = A_L(f, H_1) \oplus \ldots \oplus A_L(f, H_n).$$

Proof. Let $\psi \in A_L(f, \Omega)$ so that $\psi = \psi_1 \ldots \psi_n$ where $\psi_i \in H_i$. We wish to show that $\psi_i f = f$ for $i = 1, \ldots, n$. Let $\bar{a} \in K^r$ be arbitrary.

Case 1: Suppose $f(\bar{a}) \in K \setminus \bigcup_{i=1}^{n} K_i$. Then $\psi_i(f(\bar{a})) = f(\bar{a})$ for $i = 1, \ldots, n$.

Case 2: Suppose $f(\bar{a}) \in K_i$ for some $i = 1, \ldots, n$. Fix $1 \leqslant j \leqslant n$ and consider ψ_j. If $i \neq j$ then $\psi_j(f(\bar{a})) = f(\bar{a})$ so suppose that $i = j$ and let $\psi_i(f(\bar{a})) = \gamma$ for some $\gamma \in K$. Then we have

$$f(\bar{a}) = \psi_1 \ldots \psi_n(f(\bar{a})) = \psi_1 \ldots \psi_i(f(\bar{a})) = \psi_1 \ldots \psi_{i-1}(\gamma).$$

Clearly $f(\bar{a}) \in \sigma$ where σ is a cycle of φ_i and moreover $\sigma \subseteq K_i$ for the same i. But $\gamma = \psi_i(f(\bar{a})) = \varphi_i^{l_i}(f(\bar{a})) \in \sigma$ for some positive integer l_i which implies that $\gamma \in K_i$. Since the K_i's are pairwise disjoint we have

$$f(\bar{a}) = \psi_1 \ldots \psi_{i-1}(\gamma) = \gamma.$$

Hence $\psi_i f = f$ for $i = 1, \ldots, n$ which, along with the fact that $A_L(f, H_i) < H_i$, completes the proof.

Corollary 4.2. *Under the hypothesis of Theorem 4.1*

$$\nu_L(f, \Omega) = \prod_{i=1}^{n} \nu_L(f, H_i) \quad \textit{and} \quad \mu_L(f, \Omega) = \prod_{i=1}^{n} \mu_L(f, H_i).$$

5. Conjugate subgroups. In this section we show that conjugate subgroups of Φ induce equivalent left decompositions of $K[\bar{x}]$. We first develop several very general results concerning an arbitrary group of permutations. Let $\Omega < \Phi$ be of order n. Suppose Ω has subgroups $H_1, \ldots, H_\nu$ of orders $d_1, \ldots, d_\nu$. Finally, suppose that N_i represents the number of polynomials f such that $A_L(f, \Omega) = H_i$.

Theorem 5.1. *For each $i = 1, \ldots, \nu$*

$$N_i = l_i^{q^r} - \sum_j N_j \tag{5.1}$$

where the sum is over all j such that $H_i \subsetneqq H_j$.

Proof. By Theorem 2.4, the number of polynomials f such that H_i leaves f fixed is given by $l_i^{q^r}$. From this we subtract the number of polynomials f such that the containment is proper. The number of such f is given by the sum in (5.1).

Corollary 5.2. *Let d be a divisor of n. Then there are*

$$\frac{d}{n} \sum_i N_i$$

classes of order n/d and

$$\lambda_L(\Omega) = \frac{1}{n} \sum_{d \mid n} d \sum_i N_i$$

where the sums are over all i such that $|H_i| = d$.

We may now prove

Theorem 5.3. *If Ω_1 and Ω_2 are conjugate subgroups of Φ then Ω_1 and Ω_2 induce equivalent left decompositions of $K[\bar{x}]$.*

Proof. It is easy to show that if two groups are conjugate they have the same number of invariant elements. Since the subgroups of Ω_2 are conjugate to the corresponding subgroups of Ω_1, the subgroups of Ω_2 have the same number of invariant elements as the corresponding subgroups of Ω_1. We may now apply Theorem 5.1 and Corollary 5.2 to complete the proof.

Corollary 5.4. *If Ω_1 and Ω_2 are p-Sylow subgroups of Φ then Ω_1 and Ω_2 induce equivalent left decompositions of $K[\bar{x}]$.*

References

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

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

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

[4] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, New York 1958.

THE PENNSYLVANIA STATE UNIVERSITY
Sharon, Pennsylvania, U.S.A.

Received on 17. 5. 1974
and in revised form on 30. 9. 1974 (575)

ACTA ARITHMETICA
XXIX (1976)

Some results on the distribution of values of additive functions on the set of pairs of positive integers, II

by

G. Jogesh Babu (Urbana, Ill.)

1. Introduction. H. DeLange [1] in 1969 defined a density for sets of pairs $[m, n]$ of positive integers and determined it for some sets defined by arithmetical properties. In this paper we give necessary and sufficient conditions for a real-valued additive arithmetic function f on the set of pairs of positive integers to have a distribution (mod 1) and generalize a result obtained in [5] to additive functions defined on the set of pairs of positive integers.

2. Notations and definitions. Throughout this paper the letters p, q with or without suffixes denote always prime numbers. The letters $m, n, r, s, \ldots$ with or without suffixes denote positive integers and t, k denote non-negative integers. If A is a set of pairs of positive integers then $N(A)$ denotes the cardinality of the pairs in A. Let E be a set of pairs $[m, n]$ of positive integers. If

$$(1/xy)\,N\{[m, n]\in E\colon\ m \leqslant x \text{ and } n \leqslant y\}$$

tends to a limit a as x and y tend to infinity independently, then we say that the set E possesses density a, see [1].

Let Z_2 denote the set of pairs of positive integers.

Definition. A real-valued function on Z_2 is said to be *additive* if

$$f(m_1 m_2, n_1 n_2) = f(m_1, n_1) + f(m_2, n_2)$$

whenever $(m_1 n_1, m_2 n_2) = 1$.

Definition. A real-valued additive function f on Z_2 is said to have *distribution* (mod 1) if there is a nondecreasing, right continuous function F on the real line such that $F(c) = 0$ if $c < 0$, $F(c) = 1$ if $c > 1$ and for all continuity points $a, b \in (0, 1)$ of F and $a < b$, the density of

$$[[m, n]\colon\ a < \{f(m, n)\} < b]$$

exists and equals $F(b) - F(a)$, where $\{z\}$ denotes the fractional part of z.

We put $\|x\| = \min(\{x\}, 1 - \{x\})$ and $e(t) = \exp(2\pi i t)$.