ACTA ARITHMETICA
XXXI (1976)

Permutation polynomials in several variables over finite fields

by

GARY L. MULLEN (Sharon, Pa.)

1. Introduction. Various papers have been written concerning permutation polynomials in several variables over a finite field (see e.g. [5], [7]–[10]). This paper is meant as a further contribution to that subject. We first develop several results concerning the number of such permutation polynomials. We then generalize the notions of right and left equivalence discussed by Carlitz and Cavior in [1] and [3] and present some relations between right and left equivalence and permutation polynomials in several variables. The general theory of right and left equivalence will be discussed elsewhere, see for example [6].

Let $K = \mathrm{GF}(q)$ denote the finite field of order q where $q = p^n$ and K^r $(r \geqslant 1)$ represent the product of r copies of K. The ring of polynomials in r variables over K will be denoted by $K[x_1, \ldots, x_r]$. Two polynomials $f, g \in K[x_1, \ldots, x_r]$ are equal if they are equal as functions. It is well known that every function of K^r into K can be represented as a polynomial of degree $< q$ in each variable so that $K[x_1, \ldots, x_r]$ consists of exactly q^{q^r} polynomials.

2. Permutation polynomials. Following Nöbauer in [10] we make the

DEFINITION 1. A polynomial $f \in K[x_1, \ldots, x_r]$ is a *permutation polynomial* (in r variables over K) if the equation $f(x_1, \ldots, x_r) = a$ has q^{r-1} solutions in K^r for each $a \in K$.

By an elementary combinatorial argument, we may prove

LEMMA 1. *The number $N(r, q)$ of permutation polynomials in r variables over* $\mathrm{GF}(q)$ *is given by*

$$N(r, q) = \frac{q^r!}{(q^{r-1}!)^q}.$$

As for the magnitude of the permutation polynomials among the total number q^{q^r} of polynomials over $\mathrm{GF}(q)$ we have

THEOREM 2. *For q fixed*

$$\lim_{r\to\infty}\frac{N(r,q)}{q^{q^r}}=0, \tag{2.1}$$

whereas if r is fixed

$$\lim_{q\to\infty}\frac{N(r,q)}{q^{q^r}}=0. \tag{2.2}$$

Proof. Let $x=q^{r-1}$ from which it follows easily that

$$\frac{(qx)!}{(x!)^q q^{qx}}=\frac{(qx)!}{((qx)(qx-q)(qx-2q)\dots q)^q}\leqslant\left(\frac{qx-1}{qx}\right)\left(\frac{qx-q-1}{qx-q}\right)\dots\left(\frac{q-1}{q}\right).$$

Set

$$L(x)=\left(\frac{qx}{qx-1}\right)\left(\frac{qx-q}{qx-q-1}\right)\dots\left(\frac{q}{q-1}\right)$$

so that it suffices to show $\lim_{x\to\infty}L(x)=\infty$.

Taking logarithms, we obtain

$$\log L(x)=\sum_{n=1}^{x}\log\left(1+\frac{1}{qn-1}\right).$$

We wish to show that

$$\sum_{n=1}^{\infty}\log\left(1+\frac{1}{qn-1}\right)$$

diverges. Thus it is enough to show that for n sufficiently large

$$\log\left(1+\frac{1}{qn-1}\right)-\frac{1}{n\log n}\geqslant 0.$$

Using a Taylor series expansion for $\log\left(1+\frac{1}{qn-1}\right)$, we have

$$\log\left(1+\frac{1}{qn-1}\right)-\frac{1}{n\log n}\geqslant\frac{1}{qn-1}-\frac{1}{2(qn-1)^2}-\frac{1}{n\log n}$$
$$\geqslant\frac{1}{2(qn-1)}-\frac{1}{2(qn-1)^2}\geqslant 0$$

for n sufficiently large which completes the proof of (2.1).

Regarding (2.2) it is easily seen using the multinomial expansion of

$$(1+\dots+1)^{q^r-1}=q^{q^r-1}$$

that

$$\frac{q^r!}{(q^{r-1}!)^q}=q\cdot\frac{(q^r-1)!}{(q^{r-1}!)^{q-1}(q^{r-1}-1)!}<q$$

from which (2.2) follows.

3. Right equivalence. Let Φ denote the group of all permutations of K^r so that Φ is isomorphic to the symmetric group S_{q^r}. If Ω is a subgroup of Φ, it will be denoted by $\Omega<\Phi$. Moreover $|\Omega|$ will represent the order of Ω and $[\Phi:\Omega]$ the index of Ω in Φ.

DEFINITION 2. Let $\Omega<\Phi$ and $f,g\in K[x_1,\dots,x_r]$. Then f is *right equivalent* to g relative to Ω if there exists a $\varphi\in\Omega$ such that $f\varphi=g$.

This relation is easily seen to be an equivalence relation on $K[x_1,\dots,x_r]$ which reduces to that of Carlitz [1] when $\Omega=\Phi$. Let $\nu_R(f,\Omega)$ denote the number of $\varphi\in\Omega$ such that $f\varphi=f$.

Define $N_f(a)$ to be the number of solutions in K^r of the equation $f=a$. Carlitz ([1], Theorem 4.2) has shown that f is right equivalent to g relative to Φ if and only if $N_f(a)=N_g(a)$ for all $a\in K$. We may now prove several characterizations of permutation polynomials in terms of right equivalence.

THEOREM 3. *Let $f\in K[x_1,\dots,x_r]$. Then f is a permutation polynomial if and only if f is right equivalent to x_1 relative to Φ.*

Proof. Let $g=x_1$ in Carlitz's result.

THEOREM 4. *Let $f\in K[x_1,\dots,x_r]$. Then f is a permutation polynomial if and only if $\nu_R(f,\Phi)=(q^{r-1}!)^q$.*

Proof. We make use of the following result of Carlitz ([1], Theorem 4.4)

$$\nu_R(f,\Phi)=\prod_{a\in K}(N_f(a))!. \tag{3.1}$$

The necessity is clear. For sufficiency suppose

$$(p^n!)^q=a_1!\,a_2!\dots a_q!. \tag{3.2}$$

Assume that all of the a_i's are different from p^n. Clearly the number of terms on the left of (3.2) is qp^n and a simple argument shows that the number of terms on the right of (3.2) is $\leqslant qp^n-1$.

The power of p dividing the left is

$$q\sum_{i=1}^{\infty}\left[\frac{p^n}{p^i}\right]=q\left(\frac{p^n-1}{p-1}\right).$$

The power of p dividing the right of (3.2) is

$$\sum_{j=1}^{q}\sum_{i=1}^{\infty}\left[\frac{a_j}{p^i}\right]\leqslant\sum_{i=1}^{\infty}\left[\frac{qp^n-1}{p^i}\right]=\left[\frac{qp^n-p}{p}\right]+\left[\frac{qp^n-p^2}{p^2}\right]+\dots<q\left(\frac{p^n-1}{p-1}\right),$$

a contradiction. Thus some $a_i=p^n$ so that by induction on the number of factors $a_j=p^n$ for $j=1,\dots,q$ which completes the proof.

COROLLARY 5. *Suppose $r = 1$ and $\Omega < \Phi$. Then the group of permutation polynomials on K is decomposed by Ω into $[\Phi : \Omega]$ right equivalence classes each containing $|\Omega|$ elements.*

Proof. If f is a permutation polynomial and f is right equivalent to g relative to Ω then g is a permutation polynomial so that the class of f consists entirely of permutation polynomials. Moreover, $N_f(a) = 1$ for all $a \in K$ so that by (3.1) $\nu_R(f, \Phi) = 1$ which implies that $\nu_R(f, \Omega) = 1$. The class of f relative to Ω must contain $|\Omega|$ distinct permutation polynomials for if $f\varphi_1 = f\varphi_2$ for some $\varphi_1, \varphi_2 \in \Omega$ then $f\varphi_1\varphi_2^{-1} = f$. But since $\nu_R(f, \Omega) = 1$, we have $\varphi_1 = \varphi_2$ from which the result follows since there are a total of $q!$ permutation polynomials.

COROLLARY 6. *Suppose $r = 1$ and $\Omega_1, \Omega_2 < \Phi$. If $|\Omega_1| = |\Omega_2|$ then Ω_1 and Ω_2 decompose the group of permutation polynomials on K into the same number of right equivalence classes of the same size.*

4. Left equivalence. Let Ψ denote the group of all permutations on K so that Ψ is isomorphic to S_q.

DEFINITION 3. Let $\Omega < \Psi$ and $f, g \in K[x_1, \ldots, x_r]$. 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 $K[x_1, \ldots, x_r]$ which generalizes the case considered by Cavior in [3]. Let $\nu_L(f, \Omega)$ denote the number of $\varphi \in \Omega$ such that $\varphi f = f$.

LEMMA 7. *Let $\Omega < \Psi$ and $f \in K[x_1, \ldots, x_r]$ be a permutation polynomial. Then $\nu_L(f, \Omega) = 1$ and if g is left equivalent to f relative to Ω then g is a permutation polynomial.*

Proof. Using a result of Cavior ([4], Theorem 4.4 with $k = 1$) we have

$$\nu_L(f, \Psi) = (q-t)!$$

where t is the order of the range of f. The first part of the lemma is now clear. Since f is a permutation polynomial, it alone forms an orthogonal system, see [9]. The second part of the lemma follows if we apply Theorem 3 of [9] with $m = 1$.

THEOREM 8. *Let $\Omega < \Psi$. Then the set of permutation polynomials in r variables over K is decomposed by Ω into $q^r!/\left((q^{r-1}!)^q|\Omega|\right)$ left equivalence classes each containing $|\Omega|$ elements.*

Proof. By Lemma 7, if f is a permutation polynomial then the class of f consists entirely of permutation polynomials. Suppose Ω decomposes the set of permutation polynomials into m left equivalence classes $\Omega f_1, \ldots, \Omega f_m$. Since each f_i is a permutation polynomial, by Lemma 7 $\nu_L(f_i, \Omega) = 1$ so that each class contains precisely $|\Omega|$ permutation polynomials. The result now follows upon applying Lemma 1.

COROLLARY 9. *Suppose $r = 1$ and $\Omega < \Psi$. Then the group of permutation polynomials on K is decomposed by Ω into $[\Psi : \Omega]$ left equivalence classes each containing $|\Omega|$ elements.*

COROLLARY 10. *Suppose $r = 1$ and $\Omega_1, \Omega_2 < \Psi$. If $|\Omega_1| = |\Omega_2|$ then Ω_1 and Ω_2 decompose the group of permutation polynomials on K into the same number of left equivalence classes of the same size.*

We observe from Corollaries 5 and 9 that if $r = 1$ and Ω is any group of permutations on K, then Ω decomposes the group of permutation polynomials on K into the same number of right and left equivalence classes of the same size.

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] V. A. Kurbatov and N. G. Starkov, *The analytic representation of permutations* (Russian), Sverdlovsk. Gos. Ped. Inst. Učen. Zap. 31 (1965), pp. 151–158.

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

[7] H. Niederreiter, *Permutation polynomials in several variables over finite fields*, Proc. Japan Acad. 46 (1970), pp. 1001–1005.

[8] — *Permutation polynomials in several variables*, Acta Sci. Math. (Szeged) 33 (1972), pp. 53–58.

[9] — *Orthogonal systems of polynomials in finite fields*, Proc. Amer. Math. Soc. 28 (2) (1971), pp. 415–422.

[10] W. Nöbauer, *Zur Theorie der Polynomtransformationen und Permutationspolynome*, Math. Ann. 157 (1964), pp. 332–342.

Received on 29. 10. 1974 (633)