

**4. Properties of the fixed points.** In conclusion we mention without proof some properties of the fixed points of  $\pi^2$ .

If  $r = \varrho(p^e) > 1$ , where  $p$  is a prime and  $p^e | \pi(p^e)$ , then  $p | D$ ,  $\pi(r) = r$ , and  $r$  is join irreducible in  $\mathcal{R}$ . Furthermore if  $p$  is an odd prime, then  $\{\varrho(p^e) : e > 0, p^e | \pi(p^e)\}$  is either the empty set, the singleton  $\{\varrho(p)\}$ , or the infinite set  $\{\varrho(p)p^{e-1} : e > 0\}$ . Also, the set  $\{\varrho(2^e) : e > 0, 2^e | \pi(2^e)\}$  is either empty,  $\{2\}$ ,  $\{4\}$ ,  $\{2, 4\}$ , or  $\{2^e : e > 0\}$ .

Each of the integers  $\varrho(2)$ ,  $\varrho(3)$ ,  $\varrho(4)$ , and  $\varrho(8)$  divide 24. Finally, if there is a join irreducible fixed point of  $\pi^2$  that is not a fixed point of  $\pi$ , then there is precisely one pair of such elements. In this case, this pair is either  $\{2, 3\}$ ,  $\{4, 3\}$ ,  $\{8, 3\}$ , or  $\{8, 6\}$ .

#### References

- [1] R. H. Crowell, *Graphs of linear transformations over finite fields*, J. Soc. Indust. Appl. Math. 10 (1962), pp. 103-112.
- [2] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, New York 1952.
- [3] J. D. Fulton and W. L. Morris, *On arithmetical functions related to the Fibonacci numbers*, Acta Arith. 16 (1969), pp. 105-110.
- [4] M. Hall, *An isomorphism between linear recurring sequences and algebraic rings*, Trans. Amer. Math. Soc. 44 (1938), pp. 196-218.
- [5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Fourth Edition, London 1960.
- [6] D. W. Robinson, *The Fibonacci matrix modulo m*, Fib. Q. 1 (1963), pp. 29-36.
- [7] — *Solution to problem 5216*, Amer. Math. Monthly 72 (1965), pp. 680-681.
- [8] M. Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. 33 (1931), pp. 153-165.
- [9] — *The arithmetical theory of linear recurring series*, Trans. Amer. Math. Soc. 35 (1933), pp. 600-628.

BRIGHAM YOUNG UNIVERSITY  
Provo, Utah

Received on 23. 3. 1971

(148)

## On orthogonal systems and permutation polynomials in several variables

by

R. LIDL (Wien) and H. NIEDERREITER (Carbondale, Ill.)

**1. Introduction.** A polynomial  $f(x)$  with coefficients in the Galois field  $K = \text{GF}(q)$  with  $q$  elements,  $q = p^e$ ,  $p$  prime,  $e \geq 1$ , determines a mapping  $f: x \rightarrow f(x)$  of  $K$  into  $K$ . This mapping is a bijection if and only if the equation  $f(x) = a$  has a solution in  $K$  for every  $a \in K$ . In this case, the polynomial  $f(x)$  is called a *permutation polynomial* over  $K$ . Such polynomials have been studied extensively ([3], [4], [11]). Various papers have also been devoted to extending the notion of a permutation polynomial to polynomials in several variables ([1], [2], [6], [7], [9], [10]). The present paper is meant as a further contribution to this subject matter.

For  $n \geq 1$ , let  $K^n$  denote the cartesian product of  $n$  copies of  $K$ , and let  $K[x_1, \dots, x_n]$  be the ring of polynomials in  $n$  variables over  $K$ .

**DEFINITION 1** (Nöbauer [10]). A polynomial  $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$  is called a *permutation polynomial* (in  $n$  variables over  $K$ ) if the equation  $f(x_1, \dots, x_n) = a$  has  $q^{n-1}$  solutions in  $K^n$  for each  $a \in K$ .

**DEFINITION 2** (Niederreiter [8]). A system of polynomials  $f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n)$  from  $K[x_1, \dots, x_n]$  is said to be *orthogonal* (in  $K$ ) if the system of equations  $f_i(x_1, \dots, x_n) = k_i$ ,  $1 \leq i \leq n$ , has exactly one solution in  $K^n$  for each  $(k_1, \dots, k_n) \in K^n$ .

Simple criteria for orthogonality in terms of character sums can be given ([8], Theorem 2). Let  $\zeta$  denote a fixed primitive  $p$ th root of unity over the rationals, and let  $\text{tr}(\cdot)$  be the trace function relative to the extension  $K/\text{GF}(p)$ . Then the system  $f_1, \dots, f_n$  is orthogonal if and only if, for all  $(b_1, \dots, b_n) \in K^n$  with  $(b_1, \dots, b_n) \neq (0, \dots, 0)$ , we have

$$\sum_{(a_1, \dots, a_n) \in K^n} \zeta^{\text{tr}[b_1 f_1(a_1, \dots, a_n) + \dots + b_n f_n(a_1, \dots, a_n)]} = 0.$$

We shall now prove another criterion for orthogonality by elementary methods. The following lemma will be useful.

LEMMA 1. Let  $a_0, a_1, \dots, a_{q-1}$  be  $q$  elements of  $K$ . Then the following two conditions are equivalent:

- (i)  $a_0, a_1, \dots, a_{q-1}$  are distinct;
- (ii)  $\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{for } 0 \leq t \leq q-2, \\ -1 & \text{for } t = q-1. \end{cases}$

Proof. For fixed  $i$  with  $0 \leq i \leq q-1$ , consider the polynomial

$$f_i(x) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j.$$

We have  $f_i(a_i) = 1$  and  $f_i(c) = 0$  for all  $c \neq a_i$ . Therefore the polynomial

$$f(x) = \sum_{i=0}^{q-1} f_i(x) = - \sum_{j=0}^{q-1} \left( \sum_{i=0}^{q-1} a_i^{q-1-j} \right) x^j$$

maps each element of  $K$  into 1 if and only if  $\{a_0, a_1, \dots, a_{q-1}\} = K$ . Since the degree of  $f$  is less than  $q$ , the polynomial  $f(x)$  maps each element of  $K$  into 1 if and only if  $f(x) = 1$ . The proof is complete.

THEOREM 1. The system  $f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n)$  from  $K[x_1, \dots, x_n]$  is orthogonal if and only if the following two conditions are satisfied:

- (1)  $\sum_{(a_1, \dots, a_n) \in K^n} [f_1(a_1, \dots, a_n)]^{t_1} \dots [f_n(a_1, \dots, a_n)]^{t_n} = 0$   
for  $0 \leq t_i \leq q-1$  and not all  $t_i = q-1$ ;
- (2)  $\sum_{(a_1, \dots, a_n) \in K^n} [f_1(a_1, \dots, a_n)]^{q-1} \dots [f_n(a_1, \dots, a_n)]^{q-1} = (-1)^n.$

Proof. If  $f_1, \dots, f_n$  is an orthogonal system, then

$$\begin{aligned} \sum_{(a_1, \dots, a_n) \in K^n} [f_1(a_1, \dots, a_n)]^{t_1} \dots [f_n(a_1, \dots, a_n)]^{t_n} \\ = \sum_{(b_1, \dots, b_n) \in K^n} b_1^{t_1} \dots b_n^{t_n} = \left( \sum_{b_1 \in K} b_1^{t_1} \right) \dots \left( \sum_{b_n \in K} b_n^{t_n} \right) \end{aligned}$$

and the necessity of (1) and (2) follows from Lemma 1.

For  $(k_1, \dots, k_n) \in K^n$ , let  $N(k_1, \dots, k_n)$  denote the number of solutions in  $K^n$  of the system of equations

$$f_i(x_1, \dots, x_n) = k_i \quad \text{for } 1 \leq i \leq n.$$

It suffices to show that  $N(k_1, \dots, k_n) \neq 0$  for all  $(k_1, \dots, k_n) \in K^n$ . We shall show that  $N(k_1, \dots, k_n)$ , regarded as an integer mod  $p$ , is nonzero.

By (1) and (2), we have

$$\begin{aligned} N(k_1, \dots, k_n) &= \sum_{(a_1, \dots, a_n) \in K^n} \prod_{i=1}^n [1 - (f_i(a_1, \dots, a_n) - k_i)^{q-1}] \\ &= (-1)^n \sum_{(a_1, \dots, a_n) \in K^n} \prod_{i=1}^n [(f_i(a_1, \dots, a_n) - k_i)^{q-1} - 1] \\ &= (-1)^n \sum_{(a_1, \dots, a_n) \in K^n} \left( f_1^{q-1} \dots f_n^{q-1} + \sum_{\substack{t_1, \dots, t_n=0 \\ \text{not all } t_i=q-1}}^{q-1} a_{1, \dots, t_n} f_1^{t_1} \dots f_n^{t_n} \right) = 1. \end{aligned}$$

**2. Generators for orthogonal systems.** A correspondence between orthogonal systems of polynomials in  $n$  variables over  $\text{GF}(q)$  and permutation polynomials in one variable over  $\text{GF}(q^n)$  has been established by several authors in different ways ([1], [3], [8]). We want to use this correspondence to determine a generating system for all orthogonal systems in  $n$  variables over  $K = \text{GF}(\bar{q})$ . Since we are now only interested in polynomial mappings, and since  $a^q = a$  for every  $a \in K$ , we may confine our attention to polynomials  $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$  with degree in each variable being less than  $q$ .

DEFINITION 3. The polynomial  $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$  is called *reduced* if the degree of  $f$  in each variable is less than  $q$ . The polynomial vector  $(f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$  is called *reduced* if each of its components is reduced.

We put  $L = \text{GF}(q^n)$ . We agree to denote elements of  $L$  by Greek letters  $\xi, \eta, \dots$ , and variables ranging over  $L$  by capital letters  $X, Y, \dots$ . The set of reduced permutation polynomials  $F(X)$  over  $L$  forms a group with operation being composition computed mod  $(X^q - X)$ . The set of reduced polynomial vectors  $(f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$  over  $K$ , for which  $f_1, \dots, f_n$  are orthogonal, forms a group with operation being composition and subsequent reduction of each component mod  $(\bar{\omega}_1^q - x_1, \dots, \bar{\omega}_n^q - x_n)$ , where  $(\bar{\omega}_1^q - x_1, \dots, \bar{\omega}_n^q - x_n)$  is the ideal in  $K[x_1, \dots, x_n]$  generated by  $\bar{\omega}_i^q - x_i, 1 \leq i \leq n$ . By an abuse of language, we shall call this group the group of reduced orthogonal systems over  $K$ . There is a natural isomorphism from the former group onto the latter which we are going to describe now. Let  $\xi_1, \dots, \xi_n$  be a base of  $L$  over  $K$ . If  $F(X)$  is a reduced permutation polynomial over  $L$ , we may write

$$F(\xi) = F(a_1 \xi_1 + \dots + a_n \xi_n) = f_1(a_1, \dots, a_n) \xi_1 + \dots + f_n(a_1, \dots, a_n) \xi_n$$

with uniquely determined reduced polynomials  $f_i(x_1, \dots, x_n), 1 \leq i \leq n$ , over  $K$ . The mapping  $\Psi: F(X) \rightarrow (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$  is compatible with the above mentioned group operations. The following theorem is an immediate consequence of [8], corollary of Theorem 7.

**THEOREM 2.** *The mapping  $\Psi: F(X) \rightarrow (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$  is an isomorphism of the group of reduced permutation polynomials over  $L$  onto the group of reduced orthogonal systems over  $K$ .*

**COROLLARY.** *The reduced polynomial  $f_i(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$  is a permutation polynomial if and only if there exists a reduced permutation polynomial  $F(X) \in L[X]$  such that  $\Psi(F(X)) = (f_1, f_2, \dots, f_n)$ .*

*Proof.* This follows from Theorem 2 and [8], Theorem 1.

Theorem 2 enables us to find a generating system for the group of reduced orthogonal systems in  $K$ . By virtue of the above corollary, we have then simultaneously found a system which generates all permutation polynomials in  $n$  variables over  $K$ . The following result for permutation polynomials in one variable is mainly due to Carlitz [4]. For the remainder of this section, we suppose  $n \geq 2$ .

**THEOREM 3.** *The permutation polynomials  $X^{q^n-2}$ ,  $-a^2X$ , and  $X+a$  ( $a \in L, a \neq 0$ ) form a generating system for the group of reduced permutation polynomials in one variable over  $L = \text{GF}(q^n)$ .*

*Proof.* The symmetric group  $S_{q^n}$  is generated by all transpositions  $(0a), a \in L, a \neq 0$ . It is easy to show that the transposition  $(0a)$  is represented by the transposition polynomial

$$G(X) = (-a^2) \left( \left( (X-a)^{q^n-2} + \frac{1}{a} \right)^{q^n-2} - a \right)^{q^n-2}.$$

Thus  $G(X)$  is a finite composition of the polynomials listed in Theorem 3.

By Theorem 2 and Theorem 3, the orthogonal systems  $\Psi(X^{q^n-2})$ ,  $\Psi(-a^2X)$ , and  $\Psi(X+a)$  generate the group of reduced orthogonal systems over  $K$ . To determine the image of  $X^{q^n-2}$  under  $\Psi$ , we compute  $(x_1\xi_1 + \dots + x_n\xi_n)^{q^n-2}$  by the binomial theorem, express the power products of the  $\xi_i$  by linear combinations of the  $\xi_i$ , reduce the coefficients of the  $\xi_i \pmod{(x_1^q - x_1, \dots, x_n^q - x_n)}$ , and thus get

$$\Psi(X^{q^n-2}) = (p_1(x_1, \dots, x_n), \dots, p_n(x_1, \dots, x_n)),$$

where the  $p_i, 1 \leq i \leq n$ , form an orthogonal system in  $K$ . The image of  $-a^2X$  is an orthogonal system  $r_1, \dots, r_n$  in  $K$  consisting of linear polynomials, which can be effectively determined from the identity

$$\begin{aligned} -(a_1\xi_1 + \dots + a_n\xi_n)^2(x_1\xi_1 + \dots + x_n\xi_n) \\ = r_1(x_1, \dots, x_n)\xi_1 + \dots + r_n(x_1, \dots, x_n)\xi_n. \end{aligned}$$

Combining the above results, we get the following set of generators for the group of reduced orthogonal systems over  $K$ :  $(p_1(x_1, \dots, x_n), \dots, p_n(x_1, \dots, x_n))$ , and the systems  $(r_1(x_1, \dots, x_n), \dots, r_n(x_1, \dots, x_n))$  and  $(x_1+a_1, \dots, x_n+a_n)$  for all  $(a_1, \dots, a_n) \in K^n$  with  $(a_1, \dots, a_n) \neq (0, \dots, 0)$ . Let us now look at a special case, namely  $n = 2$  and  $q$  odd.

**THEOREM 4.** *The following orthogonal systems of polynomials in two variables over  $K = \text{GF}(q), q$  odd, form a generating system for all orthogonal systems of polynomials in two variables over  $K$  (and thus for all permutation polynomials in two variables over  $K$ ). The element  $d$  is a fixed nonsquare in  $K$ .*

(i) *The reduced form of*

$$\begin{aligned} p_1(x, y) &= \sum_{i=0}^{\frac{q^2-3}{2}} \binom{q^2-2}{2i} d^{\frac{q^2-3-2i}{2}} x^{q^2-2-2i} y^{2i}, \\ p_2(x, y) &= \sum_{i=0}^{\frac{q^2-3}{2}} \binom{q^2-2}{2i+1} d^{\frac{q^2-3-2i}{2}} x^{q^2-3-2i} y^{2i+1}; \end{aligned}$$

(ii)  $r_1(x, y) = (-a^2d - b^2)x - 2aby, r_2(x, y) = -2abdx + (-a^2d - b^2)y$  with  $a, b \in K$  and  $(a, b) \neq (0, 0)$ .

(iii)  $(x+a, y+b)$  with  $a, b \in K$  and  $(a, b) \neq (0, 0)$ .

*Proof.* The polynomial  $\varphi(x) = x^2 - d$  is irreducible over  $K$ . Let  $\varphi(\xi) = 0$ ; then 1 and  $\xi$  form a base of  $L = \text{GF}(q^2)$  over  $K$ . We have

$$(x\xi + y)^{q^2-2} = \sum_{j=0}^{q^2-2} \binom{q^2-2}{j} \xi^{q^2-2-j} x^{q^2-2-j} y^j = p_1(x, y)\xi + p_2(x, y),$$

and

$$-(a\xi + b)^2(x\xi + y) = -(a^2d + 2ab\xi + b^2)(x\xi + y) = r_1(x, y)\xi + r_2(x, y),$$

and the result follows from the general discussion preceding Theorem 4.

**Remark.** If  $q \equiv 3 \pmod{4}$ , then we may take  $d = -1$ . If  $q$  is even, an explicit result similar to Theorem 4 can be given. Instead of working with  $x^2 - d$ , we have to use an irreducible polynomial over  $K$  of the form  $x^2 + x + c$  with  $c \in K$ . Since each of those polynomials is separable over  $K$ , there exist irreducible polynomials of this type.

**3. Sums of polynomials as permutation polynomials.** We shall first consider polynomials of the form  $h(x_1, \dots, x_n) = f(x_1, \dots, x_m) + g(x_{m+1}, \dots, x_n), 1 \leq m < n$ , over  $K = \text{GF}(q)$ . It is easy to see that if one of  $f$  or  $g$  is a permutation polynomial over  $K$ , then  $h$  is one ([7], Lemma 1, [10]). We ask now for conditions under which the converse of this statement holds true. In a sense to be specified below, it will turn out that the converse holds if and only if  $q$  is prime.

**THEOREM 5.** *The polynomial  $h(x_1, \dots, x_n) = f(x_1, \dots, x_m) + g(x_{m+1}, \dots, x_n), 1 \leq m < n$ , is a permutation polynomial over  $K = \text{GF}(q), q$  prime, iff at least one of  $f$  and  $g$  is a permutation polynomial.*

*Proof.* Suppose  $h$  is a permutation polynomial and  $f$  is not a permutation polynomial over  $K$ . We want to show that necessarily  $g$  is a permutation polynomial over  $K$ .



tation polynomial over  $K$ . For  $a \in K$ , let  $N(a)$  be the number of solutions of  $f(x_1, \dots, x_m) = a$  in  $K^m$ , and let  $M(a)$  be the number of solutions of  $g(x_{m+1}, \dots, x_n) = a$  in  $K^{n-m}$ . The number of solutions of  $h(x_1, \dots, x_n) = a$  in  $K^n$  is equal to  $q^{n-1}$  for each  $a \in K$ . On the other hand, the number of solutions of the last equation can also be expressed as  $\sum_{a_1+a_2=a} N(a_1) M(a_2)$ .

Thus we arrive at a system of linear equations for  $M(0), M(1), \dots, M(q-1)$ , the determinant of which is the cyclic determinant  $D = \det(a_{ij})$  with  $a_{ij} = N(i+j-2), 1 \leq i \leq q, 1 \leq j \leq q$ , where  $i+j-2$  is taken mod  $q$ . If we can show  $D \neq 0$ , then the system has a unique solution, namely

$$M(0) = M(1) = \dots = M(q-1) = q^{n-m-1}.$$

Assume  $D = 0$ . We use the fact that  $D$  is also the resultant of the two polynomials  $F(x) = x^q - 1, G(x) = N(0)x^{q-1} + N(1)x^{q-2} + \dots + N(q-1)$  over the rationals. Thus  $F(x)$  and  $G(x)$  have a common root in some extension field of the rationals. But  $F(x) = (x-1)\Phi_q(x)$ , where  $\Phi_q(x)$  is the irreducible  $q$ th cyclotomic polynomial, and  $G(1) = q^m \neq 0$ . Therefore  $\Phi_q(x)$  divides  $G(x)$ , and so  $G(x) = N(0)\Phi_q(x)$ . Equating coefficients yields  $N(a) = N(0) = q^{m-1}$  for all  $a \in K$ , a contradiction to  $f$  not being a permutation polynomial over  $K$ .

**THEOREM 6.** *In  $K = \text{GF}(q)$ ,  $q$  not prime, there exist polynomials  $f(x_1, \dots, x_m)$  and  $g(x_{m+1}, \dots, x_n)$  such that  $f+g$ , but neither  $f$  nor  $g$ , are permutation polynomials.*

*Proof.* We have  $q = p^e$  with  $p$  prime and  $e > 1$ . For a moment, we consider  $\text{GF}(p)$  and  $\text{GF}(q)$  as additive abelian groups. The quotient group  $\text{GF}(q)/\text{GF}(p)$  has order  $r = p^{e-1}$ . We construct a system  $a_1, \dots, a_r$  of elements in  $\text{GF}(q)$  by choosing a representative from each coset. Let the counting functions  $M$  and  $N$  have the same meaning as in the proof of Theorem 5. By the Lagrange interpolation formula for finite fields as given in Dickson [5], there exists a polynomial  $g(x_{m+1}, \dots, x_n)$  over  $K$  such that  $M(a_j) = \frac{1}{r} q^{n-m}$  for  $1 \leq j \leq r$  and  $M(b) = 0$  for all other elements

$b \in K$ . By the same interpolation formula, there exists a polynomial  $f(x_1, \dots, x_m)$  over  $K$  such that

$$N(0) = N(1) = \dots = N(p-1) = \frac{1}{p} q^m \quad \text{and} \quad N(c) = 0$$

for all other elements  $c \in K$ . Neither  $f$  nor  $g$  is a permutation polynomial. But  $f+g$  is a permutation polynomial over  $K$ . Since every  $k \in K$  has a unique representation of the form  $k = a + a_j$  with  $a \in \text{GF}(p)$  and  $1 \leq j \leq r$ , the total number of solutions of the equation

$$f(x_1, \dots, x_m) + g(x_{m+1}, \dots, x_n) = k = a + a_j \quad \text{in } K^n$$

will be equal to

$$\left(\frac{1}{p} q^m\right) \left(\frac{1}{r} q^{n-m}\right), \quad \text{or} \quad q^{n-1}.$$

We used the fact that  $f$  only takes values in  $\text{GF}(p)$  and  $g$  only takes values in the system  $a_1, \dots, a_r$ .

Let us now look at polynomials of the form

$$h(x_1, \dots, x_n) = p(x_1, \dots, x_n)f(x_1, \dots, x_{n-1}) + g(x_1, \dots, x_{n-1}) \quad \text{with } n \geq 2.$$

All polynomials considered have coefficients in  $K = \text{GF}(q)$ . We are interested in conditions on  $p$  and  $f$  which guarantee that  $h$  is not a permutation polynomial for any  $g$ . In a sense, the subsequent result is best possible (see Theorem 8).

**THEOREM 7.** *Suppose  $f(x_1, \dots, x_{n-1})$  has  $k$  zeros in  $K^{n-1}$  with  $q \nmid k$ , let  $g(x_1, \dots, x_{n-1})$  be arbitrary, and let  $p(x_1, \dots, x_n)$  be a polynomial such that  $p(b_1, \dots, b_{n-1}, x_n)$  is a permutation polynomial in  $x_n$  for all  $b_1, \dots, b_{n-1} \in K$ . Then*

$$h(x_1, \dots, x_n) = p(x_1, \dots, x_n)f(x_1, \dots, x_{n-1}) + g(x_1, \dots, x_{n-1})$$

*is not a permutation polynomial over  $K$ .*

*Proof.* We consider systems of equations of the form

$$(3) \quad \begin{aligned} g(x_1, \dots, x_{n-1}) &= b \in K, \\ f(x_1, \dots, x_{n-1}) &= 0. \end{aligned}$$

There exists  $b \in K$  such that the above system has at least  $\left\lceil \frac{k}{q} \right\rceil + 1$  simultaneous solutions in  $K^{n-1}$ . For otherwise, the number of zeros of  $f$  would be at most  $q \left\lfloor \frac{k}{q} \right\rfloor$ , or less than  $k$ , a contradiction. For such a  $b \in K$ , we show that the equation

$$(4) \quad h(x_1, \dots, x_n) = b$$

has more than  $q^{n-1}$  solutions in  $K^n$ . If  $(e_1, \dots, e_{n-1}) \in K^{n-1}$  is a solution of (3), then  $h(e_1, \dots, e_{n-1}, x_n) = b$  independent of  $x_n$ , thus we get a contribution of at least  $q \left( \left\lceil \frac{k}{q} \right\rceil + 1 \right)$  solutions of (4) from all those  $(e_1, \dots, e_{n-1})$  together. Furthermore, there exist  $q^{n-1} - k$  vectors  $(b_1, \dots, b_{n-1}) \in K^{n-1}$  for which  $f(b_1, \dots, b_{n-1}) \neq 0$ . For such a vector,  $h(b_1, \dots, b_{n-1}, x_n)$  is a permutation polynomial in  $x_n$ , thus there exists exactly one solution in  $x_n$  of the equation  $h(b_1, \dots, b_{n-1}, x_n) = b$ . We thereby get  $q^{n-1} - k$  more solutions of (4). Hence, the total number of solutions of (4) is at least  $q \left( \left\lceil \frac{k}{q} \right\rceil + 1 \right) + q^{n-1} - k$ , which is greater than  $q^{n-1}$ .

Remark. The simplest way to satisfy the condition on  $p(x_1, \dots, x_n)$  in Theorem 7 is to take a permutation polynomial in the single variable  $x_n$ .

THEOREM 8. Suppose  $f(x_1, \dots, x_{n-1})$  has  $k$  zeros in  $K^{n-1}$  with  $q|k$ , and take  $p(x_1, \dots, x_n)$  as in Theorem 7. Then there exists  $g(x_1, \dots, x_{n-1})$  such that

$$h(x_1, \dots, x_n) = p(x_1, \dots, x_n)f(x_1, \dots, x_{n-1}) + g(x_1, \dots, x_{n-1})$$

is a permutation polynomial over  $K$ .

Proof. Let  $k = qm$ . We choose  $g$  in such a way that  $g$ , restricted to the set of zeros of  $f$ , attains each element of  $K$  equally often, hence  $m$  times, as a value. This choice of  $g$  is possible by virtue of the Lagrange interpolation formula for finite fields ([5]). We shall show that the corresponding  $h$  is a permutation polynomial. To this end, consider the equation

$$(5) \quad h(x_1, \dots, x_n) = b$$

for given  $b \in K$ . If  $(c_1, \dots, c_{n-1}) \in K^{n-1}$  is a zero of  $f$ , then

$$h(c_1, \dots, c_{n-1}, x_n) = g(c_1, \dots, c_{n-1})$$

independent of  $x_n$ . By the construction of  $g$ , we get in this way  $qm = k$  solutions of (5). If  $f(b_1, \dots, b_{n-1}) \neq 0$ , then we conclude as in the proof of Theorem 7 that all those  $(b_1, \dots, b_{n-1}) \in K^{n-1}$  together yield  $q^{n-1} - k$  more solutions of (5). In toto, we have then exactly  $q^{n-1}$  solutions of (5), and the proof is complete.

#### 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] — *Permutations in finite fields*, Acta Sci. Math. (Szeged) 24 (1963), pp. 196-203.
- [4] — *Permutations in a finite field*, Proc. Amer. Math. Soc. 4 (1953), p. 538.
- [5] L. E. Dickson, *General theory of modular invariants*, Trans. Amer. Math. Soc. 10 (1909), pp. 123-158.
- [6] V. A. Kurbatov and N. G. Starkov, *The analytic representation of permutations* (Russian), Sverdlovsk. Gos. Ped. Inst. Učen. Zap. 31 (1965), pp. 151-158.
- [7] H. Niederreiter, *Permutation polynomials in several variables over finite fields*, Proc. Japan Acad. 46 (1970), pp. 1001-1005.
- [8] — *Orthogonal systems of polynomials in finite fields*, Proc. Amer. Math. Soc. 28(1971), pp. 415-422.
- [9] — *Permutation polynomials in several variables*, Acta Sci. Math. (Szeged), 33(1972), pp. 53-58.

- [10] W. Nöbauer, *Zur Theorie der Polynomtransformationen und Permutationspolynome*, Math. Ann. 157 (1964), pp. 332-342.
- [11] C. Wells, *Generators for groups of permutation polynomials over finite fields*, Acta Sci. Math. (Szeged), 29 (1968), pp. 167-176.
- [12] R. Lidl, *Über Permutationspolynome in mehreren Unbestimmten*, Monatsh. Math. 75 (1971), pp. 432-440.

TECHNISCELE HOCHSCHULE WIEN  
Wien, Austria  
SOUTHERN ILLINOIS UNIVERSITY  
Carbondale, Illinois

Received on 1. 9. 1971

(214)