PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 28, Number 2, May 1971

ORTHOGONAL SYSTEMS OF POLYNOMIALS IN FINITE FIELDS

H. NIEDERREITER

ABSTRACT. The notion of an orthogonal system of polynomials in several variables in finite fields is introduced which generalizes a concept of orthogonality by Kurbatov and Starkov. Necessary and sufficient conditions for orthogonality in terms of character sums and permutation polynomials are given. Results of Carlitz on systems of equations in finite fields and earlier results of the author on permutation polynomials in several variables are generalized.

1. **Introduction.** In [4] Kurbatov and Starkov introduced the notion of orthogonality modulo a prime of two polynomials $F(x, y)$ and $G(x, y)$ with integral coefficients. This concept can be extended to systems of polynomials in an arbitrary number of variables over finite fields. Necessary and sufficient conditions are given for a system of polynomials to be orthogonal. In addition, the strong relation to the theory of permutation polynomials in several variables as developed in [5], [6] and to the work of Carlitz [1], [2] on invariant theory of equations in finite fields is revealed.

Let $K=\mathrm{GF}(q)$ be a Galois field, $q=p^s$, p prime, $s\geqq 1$. K^n shall denote the Cartesian product of n copies of K. Unless stated otherwise, all polynomials have coefficients in K. Two polynomials $f(x_1, \cdots, x_n)$, $g(x_1, \cdots, x_n)$ are considered as equal if $f(k_1, \cdots, k_n) = g(k_1, \cdots, k_n)$ for all $(k_1, \cdots, k_n)\in K^n$.

DEFINITION 1. A system of polynomials $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$, $1\leqq m\leqq n$, is said to be *orthogonal* (in K) if the system of equations $f_1(x_1, \cdots, x_n)=k_1, \cdots, f_m(x_1, \cdots, x_n)=k_m$ has exactly q^{n-m} solutions in K^n for each $(k_1, \cdots, k_m)\in K^m$.

Kurbatov and Starkov [4] considered the case $n=m=2$, $K=\mathrm{GF}(p)$. The following definition was given in [5]:

DEFINITION 2. A polynomial $f(x_1, \cdots, x_n)$ is called a *permutation polynomial* (over K) if the equation $f(x_1, \cdots, x_n)=k$ has q^{n-1} solutions in K^n for each $k\in K$.

Using the terminology established in Definition 1, we could as well say that f is a permutation polynomial if f alone forms an orthogonal

Presented to the Society, January 22, 1971 under the title *Systems of polynomial equations in finite fields*; received by the editors July 13, 1970.

AMS 1970 *subject classifications*. Primary 12C05; Secondary 12C25.

Key words and phrases. Orthogonal systems of polynomials, permutation polynomials, equations in finite fields.

system. It follows immediately from Definition 1 that every nonempty subsystem of an orthogonal system of polynomials is again orthogonal. In particular, every polynomial occurring in an orthogonal system is a permutation polynomial. On the other hand, the following theorem shows that every orthogonal system of m polynomials in n variables with $m<n$ can be extended to an orthogonal system containing more polynomials. This was stated implicitly in Carlitz [2, p. 391], but we give a different proof which does not refer to the theory of invariants.

THEOREM 1. *For every orthogonal system* $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$, $1 \leqq m < n$, *and every* r, $1 \leqq r \leqq n-m$, *there exist polynomials* $f_{m+1}(x_1, \cdots, x_n), \cdots, f_{m+r}(x_1, \cdots, x_n)$ *such that* $f_1(x_1, \cdots, x_n), \cdots, f_{m+r}(x_1, \cdots, x_n)$ *form an orthogonal system.*

PROOF. It suffices to show the theorem for $r=1$. For $(k_1, \cdots, k_m) \in K^m$, put $A_{(k_1, \cdots, k_m)} = \{(x_1, \cdots, x_n) \in K^n \mid f_i(x_1, \cdots, x_n) = k_i, 1 \leqq i \leqq m\}$. By hypothesis, each $A_{(k_1, \cdots, k_m)}$ has q^{n-m} elements. Decompose each $A_{(k_1, \cdots, k_m)}$ in an arbitrary way into q pairwise disjoint subsets $A^{(k)}_{(k_1, \cdots, k_m)}$, $k \in K$, each of them having q^{n-m-1} elements. We construct a mapping $\tau: K^n \to K$ in the following way: a given $(x_1, \cdots, x_n) \in K^n$ lies in a uniquely determined $A^{(k)}_{(k_1, \cdots, k_m)}$; define $\tau(x_1, \cdots, x_n) = k$. By the Lagrange interpolation formula for finite fields as given in Dickson [3], every mapping from K^n into K can be represented by a polynomial. The polynomial $f_{m+1}(x_1, \cdots, x_n)$ representing τ meets all requirements.

2. **Criteria for orthogonality.** A necessary and sufficient condition for orthogonality can be given in terms of characters. We note that the prime field GF(p) of K may be identified with the integers modulo p. The values of the trace function tr($\cdot$) relative to the extension K/GF(p) can then be viewed as integers modulo p. Let ζ denote a fixed primitive pth root of unity. The argument of the following proof is essentially due to Carlitz [1].

THEOREM 2. *The system* $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$, $1 \leqq m \leqq n$, *is orthogonal if and only if for all* $(b_1, \cdots, b_m) \in K^m$ *with* $(b_1, \cdots, b_m) \neq (0, \cdots, 0)$:

$$\sum_{(a_1, \cdots, a_n) \in K^n} \zeta^{\mathrm{tr}[b_1 f_1(a_1, \cdots, a_n) + \cdots + b_m f_m(a_1, \cdots, a_n)]} = 0.$$

PROOF. Let $N(k_1, \cdots, k_m)$ be the number of solutions in K^n of the system $f_1(x_1, \cdots, x_n) = k_1, \cdots, f_m(x_1, \cdots, x_n) = k_m$. We have for all $(b_1, \cdots, b_m) \in K^m$:

$$\sum_{(a_1,\cdots,a_n)\in K^n} \zeta^{\mathrm{tr}[b_1f_1(a_1,\cdots,a_n)+\cdots+b_mf_m(a_1,\cdots,a_n)]}$$

$$= \sum_{(k_1,\cdots,k_m)\in K^m} N(k_1,\cdots,k_m)\zeta^{\mathrm{tr}(b_1k_1+\cdots+b_mk_m)}. \tag{1}$$

If the f_i are orthogonal then $N(k_1,\cdots,k_m)=q^{n-m}$ for all $(k_1,\cdots,k_m)\in K^m$; thus the sum on the right-hand side of (1) is equal to:

$$q^{n-m}\sum_{(k_1,\cdots,k_m)\in K^m} \zeta^{\mathrm{tr}(b_1k_1+\cdots+b_mk_m)}$$

$$= q^{n-m}\Big(\sum_{k_1\in K}\zeta^{\mathrm{tr}(b_1k_1)}\Big)\cdots\Big(\sum_{k_m\in K}\zeta^{\mathrm{tr}(b_mk_m)}\Big)$$

which is zero if at least one b_i is nonzero.

Conversely, if the condition of the theorem is satisfied then we have:

$$N(k_1,\cdots,k_m)$$

$$= \frac{1}{q^m}\sum_{(a_1,\cdots,a_n)\in K^n}\sum_{(b_1,\cdots,b_m)\in K^m} \zeta^{\mathrm{tr}[b_1(f_1(a_1,\cdots,a_n)-k_1)+\cdots+b_m(f_m(a_1,\cdots,a_n)-k_m)]}$$

$$= \frac{1}{q^m}\sum_{(b_1,\cdots,b_m)\in K^m} \zeta^{\mathrm{tr}(-b_1k_1-\cdots-b_mk_m)} \cdot \sum_{(a_1,\cdots,a_n)\in K^n} \zeta^{\mathrm{tr}[b_1f_1(a_1,\cdots,a_n)+\cdots+b_mf_m(a_1,\cdots,a_n)]}$$

$$= \frac{1}{q^m}q^n = q^{n-m}.$$

COROLLARY. *The system* $f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n)$, $1\leqq m\leqq n$, *is orthogonal if and only if for all* $(b_1,\cdots,b_m)\in K^m$ *with* $(b_1,\cdots,b_m)\neq(0,\cdots,0)$ *the polynomial* $b_1f_1(x_1,\cdots,x_n)+\cdots+b_mf_m(x_1,\cdots,x_n)$ *is a permutation polynomial over* K.

PROOF. This follows easily from a criterion for permutation polynomials given in [5] which corresponds to the case $m=1$ in Theorem 2.

THEOREM 3. *The system* $f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n)$, $1\leqq m\leqq n$, *is orthogonal if and only if* $g(f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n))$ *is a permutation polynomial in* n *variables for all permutation polynomials* $g(y_1,\cdots,y_m)$ *in* m *variables.*

PROOF. Since $g(y_1,\cdots,y_m)=b_1y_1+\cdots+b_my_m$ is a permutation polynomial as soon as at least one coefficient is $\neq 0$, the condition is sufficient by the corollary to Theorem 2. On the other hand, let the f_i

form an orthogonal system and let $g(y_1, \cdots, y_m)$ be a permutation polynomial. For a $k \in K$, consider the equation

$$g(f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)) = k.$$

We get all solutions in K^n by first solving

$$g(y_1, \cdots, y_m) = k \tag{2}$$

and then, for each solution $(a_1, \cdots, a_m)$ of (2), solving the system

$$f_i(x_1, \cdots, x_n) = a_i, \qquad 1 \leqq i \leqq m. \tag{3}$$

Since (2) has exactly q^{m-1} solutions in K^m and each system of the form (3) has exactly q^{n-m} solutions in K^n, the original equation has exactly q^{n-1} solutions in K^n, i.e. $g(f_1, \cdots, f_m)$ is a permutation polynomial.

In the light of the corollary to Theorem 2, one might attempt to introduce a notion of orthogonality for systems of more than n polynomials in the following way: $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$, $m > n$, are orthogonal if for all $(b_1, \cdots, b_m) \in K^m$ with $(b_1, \cdots, b_m) \neq (0, \cdots, 0)$ the polynomial $b_1 f_1(x_1, \cdots, x_n) + \cdots + b_m f_m(x_1, \cdots, x_n)$ is a permutation polynomial. Unfortunately, no system of more than n polynomials satisfies this condition. This follows from

THEOREM 4. *For every system $f_1(x_1, \cdots, x_n), \cdots, f_{n+1}(x_1, \cdots, x_n)$ of polynomials there exist coefficients $b_1, \cdots, b_{n+1} \in K$ not all zero such that $b_1 f_1(x_1, \cdots, x_n) + \cdots + b_{n+1} f_{n+1}(x_1, \cdots, x_n)$ is not a permutation polynomial.*

PROOF. Suppose $f_1(x_1, \cdots, x_n), \cdots, f_{n+1}(x_1, \cdots, x_n)$ are polynomials such that $b_1 f_1(x_1, \cdots, x_n) + \cdots + b_{n+1} f_{n+1}(x_1, \cdots, x_n)$ is a permutation polynomial for all $(b_1, \cdots, b_{n+1}) \in K^{n+1}$ with $(b_1, \cdots, b_{n+1}) \neq (0, \cdots, 0)$. Then, in particular, the $f_1(x_1, \cdots, x_n)$ $\cdots, f_n(x_1, \cdots, x_n)$ form an orthogonal system. Hence the transformation $y_i = f_i(x_1, \cdots, x_n)$, $1 \leqq i \leqq n$, is one-to-one from K^n onto K^n. The inverse of this mapping can be represented by polynomials, say $x_i = g_i(y_1, \cdots, y_n)$, $1 \leqq i \leqq n$. Since the property of being a permutation polynomial in n variables is invariant under one-to-one transformations from K^n onto K^n, the polynomial

$$f(y_1, \cdots, y_n) = f_{n+1}(g_1(y_1, \cdots, y_n), \cdots, g_n(y_1, \cdots, y_n))$$

has the property that $f(y_1, \cdots, y_n) + b_1 y_1 + \cdots + b_n y_n$ is a permutation polynomial for all $(b_1, \cdots, b_n) \in K^n$. By using the corollary to Theorem 2 and the fact that a nonzero multiple

of a permutation polynomial is still a permutation polynomial, it follows that the system of polynomials $f(y_1, \cdots, y_n) + (f(0, 0, \cdots, 0) - f(1, 0, \cdots, 0))y_1, y_2, \cdots, y_n$ is orthogonal. Thus each system

$$\begin{aligned} f(y_1, \cdots, y_n) + (f(0, 0, \cdots, 0) - f(1, 0, \cdots, 0))y_1 &= k_1, \\ y_2 &= k_2, \\ &\vdots \\ y_n &= k_n, \\ (k_1, \cdots, k_n) &\in K^n, \end{aligned}$$

has exactly one solution. In particular, putting $k_2 = \cdots = k_n = 0$, we get that the equation

$$g(y_1) = f(y_1, 0, \cdots, 0) + (f(0, 0, \cdots, 0) - f(1, 0, \cdots, 0))y_1 = k_1$$

has exactly one solution for each $k_1 \in K$. This is a contradiction to $g(0) = g(1) = f(0, 0, \cdots, 0)$.

3. **Further properties.** We introduce the following notion: a *coset* of a system of polynomials $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$, $1 \leqq m \leqq n$, is a nonempty subset of K^n which is mapped by the system into a single element of K^m. We can then give a necessary and sufficient condition for permutation polynomials with prescribed cosets.

THEOREM 5. *Let the system* $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$, $1 \leqq m \leqq n$, *be orthogonal. Then the following two conditions for a polynomial* $g(x_1, \cdots, x_n)$ *are equivalent*:

(i) $g(x_1, \cdots, x_n)$ *is a permutation polynomial with all cosets of the system of* f_i *being cosets of* g *as well.*

(ii) $g(x_1, \cdots, x_n)$ *can be expressed in the form*

$$g(x_1, \cdots, x_n) = h(f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n))$$

with h *being a permutation polynomial in* m *variables.*

PROOF. Suppose (ii) holds. Then, by Theorem 3, g is a permutation polynomial and, clearly, every coset of the system of f_i is a coset of g. To show the converse, we define a mapping τ from K^m into K in the following way: for a given $(y_1, \cdots, y_m) \in K^m$ there exists $(x_1, \cdots, x_n) \in K^n$ such that $f_i(x_1, \cdots, x_n) = y_i$, $1 \leqq i \leqq m$; put $\tau(y_1, \cdots, y_m) = g(x_1, \cdots, x_n)$. τ is well defined for if $(z_1, \cdots, z_n) \in K^n$ is another n-tuple with $f_i(z_1, \cdots, z_n) = y_i$, $1 \leqq i \leqq m$, then $\{(x_1, \cdots, x_n), (z_1, \cdots, z_n)\}$ is a coset of the system of f_i and thus $\tau(y_1, \cdots, y_m) = g(z_1, \cdots, z_n) = g(x_1, \cdots, x_n)$. τ can be

represented by a polynomial $h(y_1, \cdots, y_m)$. Then $g(x_1, \cdots, x_n) = h(f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n))$ and h is a permutation polynomial.

If $f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n)$ are orthogonal then the cosets of this system are exactly the one-element subsets of K^n. Thus the condition on the cosets of g in (i) is automatically satisfied and we get the

COROLLARY. *Let $f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n)$ be an orthogonal system. Then $g(x_1, \cdots, x_n)$ is a permutation polynomial if and only if $g(x_1, \cdots, x_n) = h(f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n))$ with a permutation polynomial $h(y_1, \cdots, y_n)$.*

We have seen in the proof of Theorem 1 that there is quite a variety of possibilities of completing an orthogonal system $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$, $1 \leqq m < n$, to an orthogonal system $f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n)$. Nevertheless, we can find polynomial relations between the polynomials occurring in different completions.

THEOREM 6. *Let $f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n)$ be an orthogonal system. Then the system $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$, $g_{m+1}(x_1, \cdots, x_n), \cdots, g_n(x_1, \cdots, x_n)$, $1 \leqq m < n$, is orthogonal if and only if all $g_j(x_1, \cdots, x_n)$, $m+1 \leqq j \leqq n$, are of the form*

$$g_j(x_1, \cdots, x_n) = \sum_{(k_1, \cdots, k_m) \in K^m} p^{(j)}_{(k_1, \cdots, k_m)}(f_{m+1}(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n)) \cdot \prod_{i=1}^{m} [1 - (f_i(x_1, \cdots, x_n) - k_i)^{q-1}]$$

with polynomials $p^{(j)}_{(k_1, \cdots, k_m)}$ in $n-m$ variables such that $p^{(m+1)}_{(k_1, \cdots, k_m)}$, $\cdots$, $p^{(n)}_{(k_1, \cdots, k_m)}$ form an orthogonal system for each $(k_1, \cdots, k_m) \in K^m$.

PROOF. Let $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n), g_{m+1}(x_1, \cdots, x_n)$, $\cdots, g_n(x_1, \cdots, x_n)$ be an orthogonal system. For $(k_1, \cdots, k_m) \in K^m$, put $A_{(k_1, \cdots, k_m)} = \{(x_1, \cdots, x_n) \in K^n \mid f_i(x_1, \cdots, x_n) = k_i,\ 1 \leqq i \leqq m\}$. If $(x_1, \cdots, x_n)$ runs through $A_{(k_1, \cdots, k_m)}$, then both $(g_{m+1}(x_1, \cdots, x_n), \cdots, g_n(x_1, \cdots, x_n))$ and $(f_{m+1}(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n))$ attain each vector value of K^{n-m} exactly once. Thus

$$(g_{m+1}(x_1, \cdots, x_n), \cdots, g_n(x_1, \cdots, x_n)) = \tau_{(k_1, \cdots, k_m)}(f_{m+1}(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n))$$

for all $(x_1, \cdots, x_n) \in A_{(k_1, \cdots, k_m)}$, where $\tau_{(k_1, \cdots, k_m)}$ is a permutation of

K^{n-m}. Let $\tau^{(j)}_{(k_1,\cdots,k_m)}$, $m+1\leqq j\leqq n$, be the coordinate functions of $\tau_{(k_1,\cdots,k_m)}$. Each $\tau^{(j)}_{(k_1,\cdots,k_m)}$ can be represented by a polynomial $p^{(j)}_{(k_1,\cdots,k_m)}(y_{m+1},\cdots,y_n)$ and the desired property of those polynomials follows from the fact that τ is a permutation. We have for $(x_1,\cdots,x_n)\in A_{(k_1,\cdots,k_m)}$:

$$g_j(x_1,\cdots,x_n)=p^{(j)}_{(k_1,\cdots,k_m)}(f_{m+1}(x_1,\cdots,x_n),\cdots,f_n(x_1,\cdots,x_n)).$$

Hence

$$\begin{aligned} &g_j(x_1,\cdots,x_n)\\ &\quad=\sum_{(k_1,\cdots,k_m)\in K^m} c_{A_{(k_1,\cdots,k_m)}}(x_1,\cdots,x_n)\\ &\qquad\cdot p^{(j)}_{(k_1,\cdots,k_m)}(f_{m+1}(x_1,\cdots,x_n),\cdots,f_n(x_1,\cdots,x_n)) \end{aligned}\tag{4}$$

with c denoting a characteristic function. But

$$c_{A_{(k_1,\cdots,k_m)}}(x_1,\cdots,x_m)=\prod_{i=1}^{m}[1-(f_i(x_1,\cdots,x_n)-k_i)^{q-1}]$$

and one part of the proof is complete. On the other hand, if all g_j, $m+1\leqq j\leqq n$, are of the form (4) then it is easily seen that the system $f_1,\cdots,f_m,g_{m+1},\cdots,g_n$ is orthogonal.

Kurbatov and Starkov [4] established a one-to-one correspondence between orthogonal systems $F(x,y)$, $G(x,y)$ in GF(p) and permutation polynomials in one variable over GF(p^2). We generalize this to the following

THEOREM 7. *If $n=mr$ with an integer r, then there is a one-to-one correspondence between orthogonal systems $f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n)$ in $K=\mathrm{GF}(q)$ and permutation polynomials in r variables over $L=\mathrm{GF}(q^m)$.*

PROOF. Let $\omega_1,\cdots,\omega_m$ be a base of L over K. If $\alpha_1,\cdots,\alpha_r$ are r variables in L, then we can write $\alpha_i=x_{(i-1)m+1}\omega_1+x_{(i-1)m+2}\omega_2+\cdots+x_{im}\omega_m$, $1\leqq i\leqq r$, $x_j\in K$, $1\leqq j\leqq n$. Suppose $f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n)$ is an orthogonal system in K; then $P(\alpha_1,\cdots,\alpha_r)=f_1(x_1,\cdots,x_n)\omega_1+\cdots+f_m(x_1,\cdots,x_n)\omega_m$ defines a permutation polynomial over L since the equation $P(\alpha_1,\cdots,\alpha_r)=\alpha=k_1\omega_1+\cdots+k_m\omega_m$, $k_t\in K$, has $q^{n-m}=(q^m)^{r-1}$ solutions for each $\alpha\in L$. On the other hand, if $P(\alpha_1,\cdots,\alpha_r)$ is a permutation polynomial over L, then the coordinate functions $f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n)$ with respect to the base $\omega_1,\cdots,\omega_m$ are uniquely determined and form an orthogonal system in K.

The preceding theorem also generalizes another known result. For in the case $m=n$, we get a simple corollary the content of which is already contained in Carlitz [1, p. 409], but is stated there in a different fashion.

COROLLARY. *There is a one-to-one correspondence between orthogonal systems* $f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n)$ *in* $K=\mathrm{GF}(q)$ *and permutation polynomials in one variable over* $L=\mathrm{GF}(q^n)$.

In particular, there are exactly $q^n!$ different orthogonal systems $f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n)$ in K. More generally, it follows from results of Carlitz [2, p. 390] that the number of different orthogonal systems $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$ in K is $q^n!/(q^{n-m}!)q^m$.

REFERENCES

1. L. Carlitz, *Invariantive theory of equations in a finite field*, Trans. Amer. Math. Soc. **75** (1953), 405–427. MR **15**, 291.

2. ———, *Invariant theory of systems of equations in a finite field*, J. Analyse Math. **3** (1953/54), 382–413. MR **16**, 116.

3. L. E. Dickson, *General theory of modular invariants*, Trans. Amer. Math. Soc. **10** (1909), 123–158.

4. V. A. Kurbatov and N. G. Starkov, *The analytic representation of permutations*, Sverdlovsk. Gos. Ped. Inst. Učen. Zap. **31** (1965), 151–158. (Russian) MR **35** #6652.

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

6. H. Niederreiter, *Permutation polynomials in several variables*, Acta. Sci. Math. (Szeged) (to appear).

SOUTHERN ILLINOIS UNIVERSITY, CARBONDALE, ILLINOIS 62901