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

If \( r = \varphi(p^e) > 1 \), where \( p \) is a prime and \( p^e \mid \pi(p^e) \), then \( p \mid D, \pi(r) = r \), and \( r \) is join irreducible in \( \mathbb{Z} \). Furthermore if \( p \) is an odd prime, then \( \{ \varphi(p) : e > 0, p^e \mid \pi(p^e) \} \) is either the empty set, the singleton \( \{ \varphi(p) \} \), or the infinite set \( \{ \varphi(p) p^{e-1} : e > 0 \} \). Also, the set \( \{ \varphi(2^e) : e > 0, 2^e \mid \pi(2^e) \} \) is either empty, \( \{3, 4, 8, 3\} \), or \( \{3, 4, 8\} \).

Each of the integers \( \varphi(2), \varphi(3), \varphi(4), \) and \( \varphi(8) \) 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


BRIGHAM YOUNG UNIVERSITY

Provo, Utah

Received on 23. 3. 1971 (148)

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 \( K[x_1, \ldots, x_n] \) be the ring of polynomials in \( n \) variables over \( K \).

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

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

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

\[
\sum_{(a_1, \ldots, a_n) \in K^n} \zeta^{b_1 a_1 + \cdots + b_n a_n} = 0.
\]

We shall now prove another criterion for orthogonality by elementary methods. The following lemma will be useful.
By (1) and (2), we have
\[
N(k_1, \ldots, k_n) = \sum_{(a_1, \ldots, a_n) \in \mathbb{K}^n} \prod_{i=1}^n (1 - |f_i(a_1, \ldots, a_n) - k_i|^{q-1})
\]
\[
= (-1)^n \sum_{(a_1, \ldots, a_n) \in \mathbb{K}^n} \prod_{i=1}^n |f_i(a_1, \ldots, a_n) - k_i|^{q-1} - 1
\]
\[
= (-1)^n \sum_{(a_1, \ldots, a_n) \in \mathbb{K}^n} (f_1^{q-1} \cdots f_n^{q-1} + \sum_{a_1, \ldots, a_n \not\equiv k_1, \ldots, k_n \mod q} a_1 \cdots a_n f_1^{q-1} \cdots f_n^{q-1}) = 1.
\]

2. Generators for orthogonal systems. A correspondence between orthogonal systems of polynomials in \(n\) variables over GF(q) and permutation polynomials in one variable over 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 \(K = GF(q^n)\). 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 \(f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]\) with degree in each variable being less than \(q\).

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

We put \(L = GF(q^n)\). We agree to denote elements of \(L\) by Greek letters \(\xi, \eta, \ldots\), and variables ranging over \(L\) by capital letters \(X, Y, \ldots\) The set of reduced permutation polynomials \(F(X)\) over \(L\) forms a group with operation being composition computed \(\mod (X^n - X)\). The set of reduced polynomial vectors \((f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))\) over \(K\), for which \(f_1, \ldots, f_n\) are orthogonal, forms a group with operation being composition and subsequent reduction of each component \(\mod (x^n - x_{q^n} - x_{q^n}^2 - x_{q^n}^3 - \ldots - x^q - x)\), where \((x^n - x_{q^n} - x_{q^n}^2 - x_{q^n}^3 - \ldots - x^q - x)\) is the ideal in \(K[x_1, \ldots, x_n]\) generated by \(x^n - x\), \(1 \leq i \leq n\). By 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 \(\xi_1, \ldots, \xi_n\) be a base of \(L\) over \(K\). If \(F(X)\) is a reduced permutation polynomial over \(L\), we may write
\[
F(\xi) = f_0(\xi_1 + \cdots + a_n \xi_n) = f_1(\xi_1 + \cdots + a_n \xi_n) \xi_1 + \cdots + f_n(\xi_1 + \cdots + a_n \xi_n) \xi_n
\]
with uniquely determined reduced polynomials \(f_i(x_1, \ldots, x_n)\) \(1 \leq i \leq n\) over \(K\). The mapping \(F: F(X) \rightarrow f_1(\xi_1 + \cdots + a_n \xi_n), \ldots, f_n(\xi_1 + \cdots + a_n \xi_n)\) 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 \( \Psi : F(X) \rightarrow (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) \) 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 \( f_i(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \) is a permutation polynomial if and only if there exists a reduced permutation polynomial \( F(X) \in L[X] \) such that \( \Psi[F(X)] = (f_1, f_2, \ldots, f_n) \).

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 \( X^{a^{n-1}} - a^2 X, X + a \) (\( a \in L, a \neq 0 \)) form a generating system for the group of reduced permutation polynomials in one variable over \( L = GF(q^2) \).

Proof. The symmetric group \( S_n \) 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

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

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

By Theorem 2 and Theorem 3, the orthogonal systems \( \Psi(X^{a^{n-1}}), \Psi(-a^2 X), \Psi(X + a) \) generate the group of reduced orthogonal systems over \( K \). To determine the image of \( X^{a^{n-1}} \) under \( \Psi \), we compute \((x_1 x_2 + \ldots + x_n x_n)^{a^{n-1}}\) by the binomial theorem, express the power products of the \( x_i \) by linear combinations of the \( x_i \), reduce the coefficients of the \( x_i \) \( \text{mod } a \), \( x_i^2 - x_i \), and thus get

\[
\Psi(X^{a^{n-1}}) = \left( p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n) \right),
\]

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

\[
-(a x_1 + \ldots + x_n) x_1 \equiv \begin{cases} r_1(x_1, \ldots, x_n) x_1 + \ldots + r_n(x_1, \ldots, x_n) x_n, & \text{if } \Psi(X^{a^{n-1}}), \\
\end{cases}
\]

Combining the above results, we get the following set of generators for the group of reduced orthogonal systems over \( K \): \( (p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)) \) and the systems \( (r_1(x_1, \ldots, x_n), \ldots, r_n(x_1, \ldots, x_n)) \) and \( (x_1, x_1 + x_n) \) for \( (a_1, \ldots, a_n) \in K^n \) with \( (a_1, \ldots, a_n) \neq (0, \ldots, 0) \). 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 \( K = GF(q), q \) 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

\[
p_1(x, y) = \sum_{i=0}^{q-1} \left( \frac{q^i}{q^2} \right) d^{q^i-1} a^{q^i-3} y^{q^i},
\]

\[
p_2(x, y) = \sum_{i=0}^{q-1} \left( \frac{q^i}{q^2} \right) d^{q^i-1} a^{q^i-3} y^{q^i+1},
\]

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

(iii) \((x + a, y + b) + (a, b) \neq (0, 0) \).

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

\[
(x \xi + y)^{q-2} = \sum_{j=0}^{q-2} \left( \frac{q^2}{q} \right) \xi^{q^2-1-j} x^{q^2-2-j} y^j = p_1(x, y) x + p_2(x, y),
\]

and

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

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

Remark. If \( q = 3 \) (mod 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 these polynomials is separable over \( K \), there exist irreducible polynomials of this type.

3. Sums of polynomials as permutation polynomials. We start with the polynomial \( h(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) + g(x_{m+1}, \ldots, x_n), 1 \leq m < n, K = GF(q) \). It is easy to see that if one of \( f \) or \( g \) is a permutation polynomial over \( K \), then \( h \) is one ([1], 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 \( h(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) + g(x_{m+1}, \ldots, x_n), 1 \leq m < n, \) is a permutation polynomial over \( K = GF(q), q \) 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 permu-
On orthogonal systems and permutation polynomials

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

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

\[
M(0) = M(1) = \ldots = M(q-1) = q^{n-m-1}.
\]

Assume \( D = 0 \). We use the fact that \( D \) is also the resultant of the two polynomials \( F(x) = x^n - 1 \) and \( G(x) = N(0)x^{n-1} + N(1)x^{n-2} + \ldots + N(q-1) \) 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 \( q \)-cyclotomic polynomial, and \( G(1) = q^{n-1} \neq 0 \). Therefore \( \Phi_q(x) \) divides \( G(x) \), and so \( G(x) = N(0)\Phi_q(x) \). Equating coefficients yields \( N(a) = N(0) = q^{n-1} \) for all \( a \in \mathbb{K} \), a contradiction to \( f \) not being a permutation polynomial over \( \mathbb{K} \).

**Theorem 6.** In \( \mathbb{K} = \text{GF}(q) \), \( q \) not prime, there exist polynomials \( f(x_1, \ldots, x_n) \) and \( g(x_{a+1}, \ldots, x_n) \) 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 \( a_1, \ldots, a_r \) 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 6. By the Lagrange interpolation formula for finite fields as given in Dickson [5], there exists a polynomial \( g(x_{a+1}, \ldots, x_n) \) over \( \mathbb{K} \) 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 \( b \in \mathbb{K} \).

By the same interpolation formula, there exists a polynomial \( f(x_1, \ldots, x_n) \) over \( \mathbb{K} \) such that

\[
N(0) = N(1) = \ldots = N(p-1) = \frac{1}{p} q^{n-m} \quad \text{and} \quad N(c) = 0
\]

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

\[
f(x_1, \ldots, x_n) + g(x_{a+1}, \ldots, x_n) = a + \alpha, \quad \text{in } \mathbb{K}^n
\]

will be equal to

\[
\left( \frac{1}{p} q^{n-m} \right) \left( \frac{1}{r} q^{n-m} \right) = \frac{q^{n-m}}{p r}.\]

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

Let us now look at polynomials of the form

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

All polynomials considered have coefficients in \( \mathbb{K} = \text{GF}(q) \). 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 8.** Suppose \( f(x_1, \ldots, x_n) \) has \( k \) zeros in \( \mathbb{K}^{n-1} \) with \( q^k \), let \( g(x_1, \ldots, x_{n-1}) \) be arbitrary, and let \( p(x_1, \ldots, x_n) \) be a polynomial such that \( p(b_1, \ldots, b_{n-1}, x_n) \) is a permutation polynomial in \( x_n \) for all \( b_1, \ldots, b_{n-1} \in \mathbb{K} \).

Then

\[
h(x_1, \ldots, x_n) = p(x_1, \ldots, x_n) f(x_1, \ldots, x_{n-1}) + g(x_1, \ldots, x_{n-1})
\]

is not a permutation polynomial over \( \mathbb{K} \).

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

\[
g(x_1, \ldots, x_{n-1}) = b \in \mathbb{K}.
\]

(3)

\[
f(x_1, \ldots, x_{n-1}) = 0.
\]

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

\[
h(x_1, \ldots, x_n) = b
\]

has more than \( q^{n-1} \) solutions in \( \mathbb{K}^n \). If \( (c_1, \ldots, c_{n-1}, c_n) \in \mathbb{K}^{n-1} \) is a solution of (3), then \( h(c_1, \ldots, c_{n-1}, c_n) = b \) independent of \( c_n \), thus we get a contribution of at least \( q \left[ \frac{k}{q} \right] + 1 \) solutions of (4) from all those \( (c_1, \ldots, c_{n-1}) \) together. Furthermore, there exist \( q^{n-1} - k \) vectors \( (b_1, \ldots, b_{n-1}) \in \mathbb{K}^{n-1} \) for which \( f(b_1, \ldots, b_{n-1}) = 0 \). For such a vector, \( h(b_1, \ldots, b_{n-1}, x_n) \) is a permutation polynomial in \( x_n \) thus there exists exactly one solution in \( x_n \) of the equation \( h(b_1, \ldots, b_{n-1}, x_n) = b \). We thereby get \( q^{n-1} - k \) more solutions of (4). Hence, the total number of solutions of (4) is at least \( q \left[ \frac{k}{q} \right] + 1 \) + \( q^{n-1} - k \), which is greater than \( q^{n-1} \).
Remark. The simplest way to satisfy the condition on $p(x_1, \ldots, x_n)$ in Theorem 7 is to take a permutation polynomial in the single variable $x_n$.

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

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

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

$$h(x_1, \ldots, x_n) = b$$

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

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

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

References