228. *Permutation Polynomials in Several Variables over Finite Fields*

By Harald NIEDERREITER
Department of Mathematics, Southern Illinois University,
Carbondale, Ill., U. S. A.

(Comm. by Kinjirô KUNUGI, M. J. A., Nov. 12, 1970)

Let $K=GF(q)$ be a Galois field with q elements, $q=p^s, p$ prime, $s\geq 1$. Let K^n denote the Cartesian product of n copies of K. The following definition is basic for our further investigation:

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

For $n=1$, this coincides with the well-known notion of a permutation polynomial in one variable ([3], ch. 5; [1]; [6]). We shall characterize the permutation polynomials of degree at most two such that they can be determined effectively. For rather obvious reasons, the cases $p\neq 2$ and $p=2$ have to be distinguished.

The prime field $GF(p)$ of K can be identified with the residue class field $Z/(p)$. We shall freely use this identification in the sequel. In particular, the trace tr (a) of an element $a\in K$ relative to the extension $K/GF(p)$ can be viewed as an integer modulo p. Throughout this paper, ξ will always stand for a fixed primitive p-th root of unity. The following criterion is crucial:

Theorem 1. *$f\in K[x_1,\cdots,x_n]$ is a permutation polynomial if and only if*

$$\sum_{(a_1,\cdots,a_n)\in K^n}\xi^{\mathrm{tr}(bf(a_1,\cdots,a_n))}=0 \qquad \textit{for all non-zero } b\in K.$$

Proof. We have

$$\sum_{(a_1,\cdots,a_n)\in K^n}\xi^{\mathrm{tr}(bf(a_1,\cdots,a_n))}=\sum_{a\in K}N(a)\xi^{\mathrm{tr}(ba)} \qquad \text{for all } b\in K$$

where $N(a)$ is the number of solutions in K^n of $f(a_1,\cdots,a_n)=a$. If f is a permutation polynomial, then $N(a)=q^{n-1}$ for all $a\in K$ and so for all non-zero $b\in K$:

$$\sum_{(a_1,\cdots,a_n)\in K^n}\xi^{\mathrm{tr}(bf(a_1,\cdots,a_n))}=q^{n-1}\sum_{a\in K}\xi^{\mathrm{tr}(ba)}=q^{n-1}\sum_{c\in K}\xi^{\mathrm{tr}(c)}=0.$$

Conversely, suppose that the condition of the theorem is satisfied. Then for all $a\in K$:

$$N(a)=\frac{1}{q}\sum_{(a_1,\cdots,a_n)\in K^n}\sum_{b\in K}\xi^{\mathrm{tr}[b(f(a_1,\cdots,a_n)-a)]}$$

$$=\frac{1}{q}\sum_{(a_1,\cdots,a_n)\in K^n}\sum_{b\in K}\xi^{\mathrm{tr}(bf(a_1,\cdots,a_n))}\xi^{\mathrm{tr}(-ab)}$$

$$=\frac{1}{q}\sum_{b\in K}\xi^{\operatorname{tr}(-ab)}\sum_{(a_1,\cdots,a_n)\in K^n}\xi^{\operatorname{tr}(bf(a_1,\cdots,a_n))}=\frac{1}{q}q^n=q^{n-1}.$$

Lemma 1. *Suppose $f\in K[x_1,\cdots,x_n]$ is of the form $f(x_1,\cdots,x_n)=g(x_1,\cdots,x_m)+h(x_{m+1},\cdots,x_n)$, $1\leq m<n$, where $h\in K[x_{m+1},\cdots,x_n]$ is a permutation polynomial and $g\in K[x_1,\cdots,x_m]$. Then f is a permutation polynomial.*

Proof. This follows easily from Theorem 1, since

$$\sum_{(a_1,\cdots,a_n)\in K^n}\xi^{\operatorname{tr}(bf(a_1,\cdots,a_n))}=\sum_{(a_1,\cdots,a_n)\in K^n}\xi^{\operatorname{tr}(bg(a_1,\cdots,a_m))}\xi^{\operatorname{tr}(bh(a_{m+1},\cdots,a_n))}$$
$$=\Big(\sum_{(a_1,\cdots,a_m)\in K^m}\xi^{\operatorname{tr}(bg(a_1,\cdots,a_m))}\Big)\Big(\sum_{(a_{m+1},\cdots,a_n)\in K^{n-m}}\xi^{\operatorname{tr}(bh(a_{m+1},\cdots,a_n))}\Big)=0$$

for all non-zero $b\in K$.

In the proof of Theorems 2 and 3 we shall frequently refer to the following lemma which is an immediate consequence of the definition of a permutation polynomial.

Lemma 2. *The property of being a permutation polynomial is invariant under nonsingular linear transformations of the variables, i.e. transformations of the form $x_i=\sum_{j=1}^{n}a_{ij}y_j+b_i, a_{ij}\in K, b_i\in K, 1\leq i\leq n$, $\det(a_{ij})\neq 0$.*

This suggests the following definition:

Definition 2. *Two polynomials $f,g\in K[x_1,\cdots,x_n]$ are said to be equivalent if they can be transformed into each other by nonsingular linear transformations of the variables.*

Using this definition, the first case of our main result can now be expressed as follows:

Theorem 2. *For $p\neq 2$, a polynomial $f\in K[x_1,\cdots,x_n]$ of degree at most two is a permutation polynomial if and only if f is equivalent to a polynomial of the form $g(x_1,\cdots,x_{n-1})+x_n$, $g(x_1,\cdots,x_{n-1})\in K[x_1,\cdots,x_{n-1}]$.*

Proof. The sufficiency of the condition follows from Lemma 1 and Lemma 2, since x_n is a permutation polynomial.

Conversely, any linear polynomial is certainly equivalent to a polynomial of the above form. A quardratic permutation polynomial $f\in K[x_1,\cdots,x_n]$, as any quadratic polynomial over K, is equivalent to a polynomial of the form $e_1x_1^2+\cdots+e_kx_k^2+b_1x_1+\cdots+b_nx_n+c$, $1\leq k\leq n$, $e_i\neq 0$ for $1\leq i\leq k$, which is in turn equivalent to $e_1x_1^2+\cdots+e_kx_k^2+b_{k+1}x_{k+1}+\cdots+b_nx_n+d$. We are done if we can show that there exists a j, $k+1\leq j\leq n$, such that $b_j\neq 0$. Assume the contrary. Then, by Lemma 2, the polynomial $e_1x_1^2+\cdots+e_kx_k^2+d$ is a permutation polynomial over K. On the other hand, we have for all $b\in K, b\neq 0$:

$$\sum_{(a_1,\cdots,a_n)\in K^n}\xi^{\operatorname{tr}[b(e_1a_1^2+\cdots+e_ka_k^2+d)]}=q^{n-k}\xi^{\operatorname{tr}(bd)}\Big(\sum_{a_1\in K}\xi^{\operatorname{tr}(be_1a_1^2)}\Big)\cdots \tag{1}$$
$$\cdots\Big(\sum_{a_k\in K}\xi^{\operatorname{tr}(be_ka_k^2)}\Big)=q^{n-k}\xi^{\operatorname{tr}(bd)}\tau_1\cdots\tau_k$$

with $\tau_i=\sum_{a_i\in K}\xi^{\mathrm{tr}(be_ia_i^2)}, 1\leq i\leq k$.

Let Q denote the set of non-zero squares in K and N the set of non-squares in K. If $be_i\in Q$, then

$$\tau_i=1+2\sum_{a\in Q}\xi^{\mathrm{tr}(a)}=(\sum_{a\in Q}\xi^{\mathrm{tr}(a)}-\sum_{a\in N}\xi^{\mathrm{tr}(a)})+(1+\sum_{a\in Q}\xi^{\mathrm{tr}(a)}+\sum_{a\in N}\xi^{\mathrm{tr}(a)})$$
$$=(\sum_{a\in Q}\xi^{\mathrm{tr}(a)}-\sum_{a\in N}\xi^{\mathrm{tr}(a)})+\sum_{a\in K}\xi^{\mathrm{tr}(a)}=\sum_{a\in Q}\xi^{\mathrm{tr}(a)}-\sum_{a\in N}\xi^{\mathrm{tr}(a)}$$

which is a Gaussian sum associated with K. Thus, as shown in [2], $|\tau_i|=\sqrt{q}$. On the other hand, if $be_i\in N$, then

$$\tau_i=1+2\sum_{a\in N}\xi^{\mathrm{tr}(a)}=2(1+\sum_{a\in N}\xi^{\mathrm{tr}(a)}+\sum_{a\in Q}\xi^{\mathrm{tr}(a)})-(1+2\sum_{a\in Q}\xi^{\mathrm{tr}(a)})$$
$$=2\sum_{a\in K}\xi^{\mathrm{tr}(a)}-(1+2\sum_{a\in Q}\xi^{\mathrm{tr}(a)})=-(1+2\sum_{a\in Q}\xi^{\mathrm{tr}(a)})$$

and therefore $|\tau_i|=\sqrt{q}$. In any case, the left-hand side of (1) turns out to $be\neq 0$. This contradiction to Theorem 1 completes the proof.

It follows easily from the preceding proof that the rank of the matrix A associated with the quadratic form occurring in f and the rank of the augmented matrix $A'(=A+$coefficients of the linear terms) are sufficiently strong invariants for deciding whether f is a permutation polynomial or not. More explicitly, f is a permutation polynomial if and only if rank $A'>$rank A.

Theorem 3. *For $p=2$, a polynomial $f\in K[x_1,\cdots,x_n]$ of degree at most two is a permutation polynomial if and only if f is equivalent to either $g(x_1,\cdots,x_{n-1})+x_n$ or $g(x_1,\cdots,x_{n-1})+x_n^2$, $g(x_1,\cdots,x_{n-1})\in K[x_1,\cdots,x_{n-1}]$.*

Proof. *Sufficiency.* Since both x_n and x_n^2 are permutation polynomials, then so f is one by Lemma 1 and Lemma 2.

Necessity. Any linear permutation polynomial is equivalent to a polynomial of the form $g(x_1,\cdots,x_{n-1})+x_n$. Let f be a quadratic permutation polynomial over K, $f=Q(x_1,\cdots,x_n)+L(x_1,\cdots,x_n)$, Q a quadratic form and L a linear polynomial over K. As shown in [4], [5], any quadratic form over K is equivalent to a polynomial of the form $x_1x_2+x_3x_4+\cdots+x_{m-1}x_m+\sum_{i=1}^n e_i^2x_i^2$, $0\leq m\leq n$. Thus f is equivalent to $x_1x_2+x_3x_4+\cdots+x_{m-1}x_m+\sum_{i=1}^n e_i^2x_i^2+\sum_{i=1}^n d_ix_i+d$. We substitute $x_i=y_i+d_i$, $1\leq i\leq m$, $x_i=y_i$, $m+1\leq i\leq n$, and get f equivalent to $H=y_1y_2+y_3y_4+\cdots+y_{m-1}y_m+\sum_{i=1}^n e_i^2y_i^2+\sum_{i=m+1}^n d_iy_i+e$. Put $h=d_{m+1}y_{m+1}+\cdots+d_ny_n+e_{m+1}^2y_{m+1}^2+\cdots+e_n^2y_n^2$. By Lemma 2, H is a permutation polynomial. From this it follows that h is a permutation polynomial. For otherwise there would exist a non-zero $b\in K$ such that:

$$\sum_{(a_{m+1},\cdots,a_n)\in K^{n-m}}\xi^{\mathrm{tr}(bh(a_{m+1},\cdots,a_n))}\neq 0. \tag{2}$$

Using the same b, we consider

$$
\begin{aligned}
(3)\qquad & \sum_{(a_1,\cdots,a_n)\in K^n} \xi^{\operatorname{tr}(bH(a_1,\cdots,a_n))} \\
&= \Big(\sum_{(a_1,\cdots,a_m)\in K^m} \xi^{\operatorname{tr}[b(a_1a_2+\cdots+a_{m-1}a_m+e_1^2a_1^2+\cdots+e_m^2a_m^2+e)]} \Big) \\
&\quad \times \Big(\sum_{(a_{m+1},\cdots,a_n)\in K^{n-m}} \xi^{\operatorname{tr}(bh(a_{m+1},\cdots,a_n))} \Big) \\
&= \xi^{\operatorname{tr}(be)} \Big(\sum_{(a_1,a_2)\in K^2} \xi^{\operatorname{tr}[b(a_1a_2+e_1^2a_1^2+e_2^2a_2^2)]} \Big) \\
&\quad \cdots \Big(\sum_{(a_{m-1},a_m)\in K^2} \xi^{\operatorname{tr}[b(a_{m-1}a_m+e_{m-1}^2a_{m-1}^2+e_m^2a_m^2)]} \Big) \\
&\quad \times \Big(\sum_{(a_{m+1},\cdots,a_n)\in K^{n-m}} \xi^{\operatorname{tr}(bh(a_{m+1},\cdots,a_n))} \Big).
\end{aligned}
$$

For an i with $1 \leq i \leq m-1$, let us consider

$$\sum_{(a_i,a_{i+1})\in K^2} \xi^{\operatorname{tr}[b(a_ia_{i+1}+e_i^2a_i^2+e_{i+1}^2a_{i+1}^2)]}.$$

From $\operatorname{tr}(a)=a+a^2+a^4+\cdots+a^{2^{s-1}}$ and $a^{2^s}=a$ for all $a\in K$ we can infer that $\operatorname{tr}(a^2)=a^2+a^4+a^8+\cdots+a^{2^s}=a+a^2+a^4+\cdots+a^{2^{s-1}}=\operatorname{tr}(a)$ for all $a\in K$. Furthermore, there exists a non-zero $c\in K$ such that $b=c^2$. Thus

$$
\begin{aligned}
\operatorname{tr}[b(a_ia_{i+1}+e_i^2a_i^2+e_{i+1}^2a_{i+1}^2)] &= \operatorname{tr}(ba_ia_{i+1})+\operatorname{tr}(c^2e_i^2a_i^2)+\operatorname{tr}(c^2e_{i+1}^2a_{i+1}^2) \\
&= \operatorname{tr}(ba_ia_{i+1})+\operatorname{tr}(ce_ia_i)+\operatorname{tr}(ce_{i+1}a_{i+1}) \\
&= \operatorname{tr}(ba_ia_{i+1}+ce_ia_i+ce_{i+1}a_{i+1}) \\
&= \operatorname{tr}[(a_i+c^{-1}e_{i+1})(ba_{i+1}+ce_i)+e_ie_{i+1}].
\end{aligned}
$$

Therefore

$$
\begin{aligned}
(4)\qquad & \sum_{(a_i,a_{i+1})\in K^2} \xi^{\operatorname{tr}[b(a_ia_{i+1}+e_i^2a_i^2+e_{i+1}^2a_{i+1}^2)]} \\
&= \sum_{(a_i,a_{i+1})\in K^2} \xi^{\operatorname{tr}[(a_i+c^{-1}e_{i+1})(ba_{i+1}+ce_i)+e_ie_{i+1}]} \\
&= \xi^{\operatorname{tr}(e_ie_{i+1})} \sum_{a_i\in K} \sum_{a_{i+1}\in K} \xi^{\operatorname{tr}[(a_i+c^{-1}e_{i+1})(ba_{i+1}+ce_i)]} \\
&= q\xi^{\operatorname{tr}(e_ie_{i+1})} \neq 0.
\end{aligned}
$$

It follows from (2), (3), (4) that $\sum_{(a_1,\cdots,a_n)\in K^n} \xi^{\operatorname{tr}(bH(a_1,\cdots,a_n))} \neq 0$, a contradiction. Hence h is a permutation polynomial. Implicitly we have also shown that $m<n$.

Let us look at h now. Taking into account only the terms with non-zero coefficients and renaming the y_i, d_i and $e_i, m+1\leq i\leq n$, we have $h=d_{m+1}x_{m+1}+\cdots+d_rx_r+e_{m+1}^2x_{m+1}^2+\cdots+e_r^2x_r^2$ with either $d_i\neq 0$ or $e_i\neq 0$ for each $i, m+1\leq i\leq r$. If there exists an $i, m+1\leq i\leq r$, such that either $d_i=0, e_i\neq 0$, or $d_i\neq 0, e_i=0$, then the proof is complete. In the remaining case we have for all $i, m+1\leq i\leq r$, that both $d_i\neq 0$ and $e_i\neq 0$. We shall show that h being a permutation polynomial implies that the vectors $(d_{m+1},\cdots,d_r)$ and $(e_{m+1},\cdots,e_r)$ are linearly independent over K.

For otherwise there exists a non-zero $c\in K$ such that $d_i=ce_i, m+1\leq i\leq r$, hence $h=c(e_{m+1}x_{m+1}+\cdots+e_rx_r)+(e_{m+1}x_{m+1}+\cdots+e_rx_r)^2$. It follows that h is equivalent to $p(x)=cx+x^2$. But this is not a permutation polynomial since $p(0)=p(c)=0$.

The linear independence of $(d_{m+1},\cdots,d_r)$ and $(e_{m+1},\cdots,e_r)$ implies that there exist i, j with $m+1 \leq i < j \leq r$, such that $\begin{vmatrix} d_i & d_j \\ e_i & e_j \end{vmatrix} \neq 0$. Then the substitution $y_i = d_{m+1}x_{m+1} + \cdots + d_r x_r$, $y_j = e_{m+1}x_{m+1} + \cdots + e_r x_r$, $y_t = x_t$, $t \neq i, j$, $m+1 \leq t \leq r$, is nonsingular. This substitution transforms h into $y_i + y_j^2$ and thus H (and, by transitivity, f itself) is equivalent to a polynomial of the desired form.

We have seen in the course of the proof that the problem of deciding whether f is a permutation polynomial or not boils down to the question of finding the canonical form of the quadratic form contained in f. There exist invariants which allow to answer this just from the coefficients of the form ([5]).

It seems to be difficult to characterize permutation polynomials of degree at least three in the above fashion. Definitely, the results obtained here do not carry over to that case. As a counterexample, note that $x^3 + y^3$ is a permutation polynomial over $GF(5)$ but is not equivalent to a polynomial of the form $g(x) + y$.

References

[1] L. Carlitz: Permutations in finite fields. Acta Sci. Math. Szeged, **24**, 196–203 (1963).

[2] H. Davenport: On primitive roots in finite fields. Quart. J. Math., **8**, 308–312 (1937).

[3] L. E. Dickson: Linear Groups. Teubner, Leipzig (1901).

[4] ——: Determination of the structure of all linear homogenous groups in a Galois field which are defined by a quadratic invariant. Amer. J. Math., **21**, 193–256 (1899).

[5] ——: Invariantive reduction of quadratic forms in the $GF[2^n]$. Amer. J. Math., **30**, 263–281 (1908).

[6] C. Wells: Groups of permutation polynomials. Monatsh. Math., **71**, 248–262 (1967).