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 $a\in K$:

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