Permutation polynomials in several variables

By HARALD NIEDERREITER in Carbondale (Illinois, U.S.A.)

1. Introduction. In [11] W. NÖBAUER introduced the notion of a permutation polynomial in several variables over a commutative ring with identity, where the polynomial is considered modulo an ideal. We apply this definition to polynomials in several variables with integral coefficients.

Let Z denote the ring of integers and let p be a fixed prime. For a given $n \geqq 1$, we consider lattice points $(a_1, \ldots, a_n)$, $a_i \in Z$, $1 \leqq i \leqq n$. Two lattice points $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$ are said to be congruent modulo p if $a_i \equiv b_i \pmod{p}$ for all $i=1, \ldots, n$. By means of this definition, the set of n-dimensional lattice points is divided into exactly p^n equivalence classes. In the sequel, M_p^n will stand for a complete system of representatives from those equivalence classes. We give the following

Definition 1. A polynomial $f \in Z[x_1, \ldots, x_n]$ is called a permutation polynomial mod p if the congruence $f(x_1, \ldots, x_n) \equiv a \pmod{p}$ has exactly p^{n-1} solutions in M_p^n for each $a=0, 1, \ldots, p-1$.

Remark. The above definition is obviously independent of the choice of M_p^n. The definition coincides with Nöbauer's definition for permutation polynomials over Z modulo the ideal (p) (see [11], p. 342).

For $n=1$, the theory of permutation polynomials is well developed ([1]; [3]; [4]; [5]; [7], ch. 18; [8], ch. 5; [10]; [12]; [13]; [14]). We therefore suppose $n \geqq 2$ from now on. Some results for the case $n=2$ have been obtained by KURBATOV and STARKOV [9]. In this paper, two necessary and sufficient conditions for permutation polynomials mod p are given and all permutation polynomials mod p of degree 1 and degree 2 are characterized. Generalizations to Galois fields shall be discussed elsewhere.

2. Two criteria. First we show the following

Theorem 1. *$f \in Z[x_1, \ldots, x_n]$ is a permutation polynomial* mod p *if and only if each congruence $f(x_1, \ldots, x_n) \equiv a \pmod{p}$, $a=0, 1, \ldots, p-1$, has at least one solution and*

$$\sum_{(a_1, \ldots, a_n) \in M_p^n} [f(a_1, \ldots, a_n)]^{tp^{n-2}} \equiv 0 \pmod{p^{n-1}} \quad \textit{for} \quad t = 1, \ldots, p-1.$$

Proof. Put k_a=number of solutions from M_p^n of $f(x_1, \ldots, x_n) \equiv a \pmod p$, $a=0, 1, \ldots, p-1$. Since $c \equiv d \pmod p$ implies $c^{p^{n-2}} \equiv d^{p^{n-2}} \pmod{p^{n-1}}$, we get

$$\sum_{(a_1,\ldots,a_n)\in M_p^n} [f(a_1, \ldots, a_n)]^{tp^{n-2}} \equiv \sum_{a=0}^{p-1} k_a a^{tp^{n-2}} \pmod{p^{n-1}} \quad \text{for} \quad t = 1, \ldots, p-1.$$

Suppose now that f is a permutation polynomial mod p; then $k_a = p^{n-1}$ for all $a=0, 1, \ldots, p-1$ and we are done.

Conversely, suppose that the condition of the theorem is satisfied. Then

$$\sum_{a=0}^{p-1} k_a a^{tp^{n-2}} \equiv 0 \pmod{p^{n-1}} \quad \text{for all} \quad t = 1, \ldots, p-1.$$

Since the above congruence also holds for $t=0$ (with $0^0=1$), we get a system of homogeneous linear equations in $k_0, \ldots, k_{p-1}$ over the residue class ring modulo p^{n-1} with determinant D being a Vandermonde determinant. Thus

$$D = \prod_{0 \leq i < j \leq p-1} (j^{p^{n-2}} - i^{p^{n-2}}).$$

Since $i^{p^{n-2}} \equiv j^{p^{n-2}} \pmod p$ would imply $i \equiv j \pmod p$, we have $D \not\equiv 0 \pmod p$, i.e. D is not a zero divisor in the residue class ring modulo p^{n-1}. Therefore $k_a \equiv 0 \pmod{p^{n-1}}$ for $a=0, 1, \ldots, p-1$. By hypothesis, $k_a \geqq 1$ for all $a=0, 1, \ldots, p-1$ and so $k_a \geqq p^{n-1}$ for all $a = 0, 1, \ldots, p-1$. From $\sum_{a=0}^{p-1} k_a = p^n$ it follows that $k_a = p^{n-1}$ for all $a = 0, 1, \ldots, p-1$.

Theorem 2. *$f \in Z[x_1, \ldots, x_n]$ is a permutation polynomial* mod p *if and only if*

$$\sum_{(a_1,\ldots,a_n)\in M_p^n} e^{2\pi i \frac{m}{p} f(a_1,\ldots,a_n)} = 0 \quad \textit{for all} \quad m = 1, \ldots, p-1.$$

Proof. Again putting k_a=number of solutions from M_p^n of $f(x_1, \ldots, x_n) \equiv \equiv a \pmod p$, $a=0, 1, \ldots, p-1$, we have

$$\sum_{(a_1,\ldots,a_n)\in M_p^n} e^{2\pi i \frac{m}{p} f(a_1,\ldots,a_n)} = \sum_{a=0}^{p-1} k_a e^{2\pi i \frac{m}{p} a} \quad \text{for} \quad m = 1, \ldots, p-1.$$

So if $k_a = p^{n-1}$ for all $a=0, 1, \ldots, p-1$, then the necessity of the condition follows easily.

Conversely, suppose that $\sum_{a=0}^{p-1} k_a e^{2\pi i \frac{m}{p} a} = 0$ for all $m=1, \ldots, p-1$. This gives rise to the following system of linear equations for $k_0, k_1, \ldots, k_{p-1}$:

$$k_0 + k_1 + \cdots + k_{p-1} = p^n,$$

$$\sum_{a=0}^{p-1} k_a e^{2\pi i \frac{m}{p} a} = 0 \qquad (m = 1, \ldots, p-1).$$

The determinant Δ of this system is a Vandermonde determinant, hence

$$\Delta = \prod_{0 \leqq r < s \leqq p-1} \left(e^{2\pi i \frac{s}{p}} - e^{2\pi i \frac{r}{p}}\right) \neq 0.$$

So there is a unique solution to the system, and this solution is $k_0 = k_1 = \dots = k_{p-1} = p^{n-1}$.

Remark. Theorem 2 clearly holds for $n=1$ as well. Actually, Theorem 2 is contained in a general result of CARLITZ [2, Theorem 4. 6.] but we have included the foregoing proof because of its simplicity.

3. Some auxiliary results.

Lemma 1 (NÖBAUER [11]). *If* $f \in Z[x_1, \dots, x_n]$ *can be written in the form* $f(x_1, \dots, x_n) = g(x_1, \dots, x_k) + h(x_{k+1}, \dots, x_n)$, $1 \leqq k < n$, *where* $h \in Z[x_{k+1}, \dots, x_n]$ *is a permutation polynomial* mod p *and* $g \in Z[x_1, \dots, x_k]$, *then* f *is a permutation polynomial* mod p.

Lemma 2. *Let* $f \in Z[x_1, \dots, x_n]$ *be a permutation polynomial* mod p. *If* $x_i = a_{i1}y_1 + a_{i2}y_2 + \dots + a_{in}y_n + b_i$ $(a_{ij} \in Z,\ b_i \in Z,\ 1 \leqq i \leqq n,\ 1 \leqq j \leqq n)$ *is a linear substitution with* $\det(a_{ij}) \not\equiv 0 \pmod{p}$, *then the resulting polynomial* $g(y_1, \dots, y_n)$ *is again a permutation polynomial* mod p.

Proof. This simply follows from the fact that a linear substitution of the above form transforms a given M_p^n into another M_p^n.

Definition 2. Let Z_p denote the residue class ring $Z/(p)$. For $f \in Z[x_1, \dots, x_n]$, let $\bar{f}$ be the image of f under the canonical homomorphism from $Z[x_1, \dots, x_n]$ into $Z_p[x_1, \dots, x_n]$. Two polynomials $f, g \in Z[x_1, \dots, x_n]$ are said to be equivalent mod p if there exists a linear substitution T of the form mentioned in Lemma 2 such that $\overline{Tf} = \bar{g}$.

Equivalence mod p is easily seen to be an equivalence relation in $Z[x_1, \dots, x_n]$.

Lemma 3. *Let* f *be equivalent* mod p *to* g; $f, g \in Z[x_1, \dots, x_n]$. *Then* f *is a permutation polynomial* mod p *if and only if* g *is one.*

Proof. This follows from Lemma 2 and Definition 2.

4. Linear polynomials.

Theorem 3. $f(x_1, \dots, x_n) = b_1x_1 + \dots + b_nx_n + b \in Z[x_1, \dots, x_n]$ *is a permutation polynomial* mod p *if and only if* g.c.d. $(b_1, \dots, b_n, p) = 1$.

Proof. If g.c.d. $(b_1, \dots, b_n, p)=p$, then $f(a_1, \dots, a_n) \equiv b \pmod p$ for all lattice points and so f is not a permutation polynomial mod p. If g.c.d. $(b_1, \dots, b_n, p)=1$, then WLOG g.c.d. $(b_n, p)=1$. But then $b_n x_n$ is a permutation polynomial mod p and so we can infer from Lemma 1 that f itself is one.

5. Quadratic polynomials, case $p \neq 2$.

Theorem 4. *Let $f \in Z[x_1, \dots, x_n]$ be a polynomial of degree 2. Then f is a permutation polynomial* mod p *if and only if f is equivalent* mod p *to a polynomial of the form $g(x_1, \dots, x_n) = h(x_1, \dots, x_{n-1}) + b_n x_n$ with $h \in Z[x_1, \dots, x_{n-1}]$,* g.c.d. $(b_n, p)=1$.

Proof. The sufficiency of the condition follows from Lemma 1 and Lemma 3 and the fact that $b_n x_n$ is a permutation polynomial mod p.

Conversely, suppose that f is a permutation polynomial mod p. Since Z_p is a field of characteristic $p \neq 2$, f is equivalent mod p to a polynomial of the form $r(x_1, \dots, x_n) = u_1 x_1^2 + \dots + u_k x_k^2 + d_{k+1} x_{k+1} + \dots + d_n x_n + d$, $0 \leqq k \leqq n$, g.c.d. $(u_i, p)=1$ for $1 \leqq i \leqq k$. If $k<n$ and g.c.d. $(d_j, p)=1$ for at least one j, $k+1 \leqq j \leqq n$, then we are done. Otherwise, f is equivalent mod p to $s(x_1, \dots, x_n) = u_1 x_1^2 + \dots + u_k x_k^2 + d$, $0<k \leqq n$. By Lemma 3, s is a permutation polynomial mod p. On the other hand, we have for $m = 1, \dots, p-1$:

$$\sum_{(a_1,\dots,a_n)\in M_p^n} e^{2\pi i \frac{m}{p} s(a_1,\dots,a_n)} = p^{n-k} e^{2\pi i \frac{m}{p} d} \left(\sum_{a_1=0}^{p-1} e^{2\pi i \frac{m}{p} u_1 a_1^2} \right) \cdots \left(\sum_{a_k=0}^{p-1} e^{2\pi i \frac{m}{p} u_k a_k^2} \right) =$$

$$= p^{n-k} e^{2\pi i \frac{m}{p} d} \sigma_1 \dots \sigma_k \quad \text{with} \quad \sigma_j = \sum_{a_j=0}^{p-1} e^{2\pi i \frac{m}{p} u_j a_j^2}, \qquad 1 \leqq j \leqq k.$$

If mu_j is a quadratic residue modulo p, then $\sigma_j = \sum_{a=0}^{p-1} e^{2\pi i \frac{a^2}{p}}$ and thus $|\sigma_j| = \sqrt{p}$ ([6], ch. 2). If mu_j is a quadratic nonresidue modulo p, then $\sigma_j + \sum_{a=0}^{p-1} e^{2\pi i \frac{a^2}{p}} = 2 \sum_{b=0}^{p-1} e^{2\pi i \frac{b}{p}} = 0$ and thus $|\sigma_j| = \sqrt{p}$. In any case we have $\sigma_j \neq 0$ for all $j=1, \dots, k$ and this contradiction to Theorem 2 completes the proof.

From a close inspection of the preceding proof we are led to a simple and systematic method for detecting quadratic permutation polynomials which is based on coefficient matrices. To fix this idea, we give the following definitions:

Definition 3. Let A be a matrix whose elements are rational numbers of the form a/b with $p \nmid b$. Then $\text{rank}_p\, A$ is the rank of A, considered as a matrix over Z_p.

Definition 4. Let $f(x_1, \ldots, x_n) = \sum_{1 \leqq i \leqq j \leqq n} a_{ij} x_i x_j + \sum_{r=1}^{n} c_r x_r + c$ be a quadratic polynomial from $Z[x_1, \ldots, x_n]$. Then

$$A(f) = \begin{pmatrix} a_{11} & \frac{1}{2}a_{12} & \cdots & \frac{1}{2}a_{1n} \\ \frac{1}{2}a_{12} & a_{22} & \cdots & \frac{1}{2}a_{2n} \\ \vdots & \vdots & & \vdots \\ \frac{1}{2}a_{1n} & \frac{1}{2}a_{2n} & \cdots & a_{nn} \end{pmatrix}, \qquad A'(f) = \left(A(f) \left| \begin{matrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{matrix} \right. \right).$$

Let us note that the k in the proof of the preceding theorem is nothing else than $\operatorname{rank}_p A(f)$. Furthermore, f will be equivalent mod p to a polynomial of the form given in Theorem 4 if and only if the last column of the augmented matrix $A'(f)$, considered as a vector over Z_p, is linearly independent of the preceding column vectors. Therefore:

Theorem 5. *A quadratic polynomial* $f \in Z[x_1, \ldots, x_n]$ *is a permutation polynomial* mod p *if and only if* $\operatorname{rank}_p A'(f) > \operatorname{rank}_p A(f)$.

6. Quadratic polynomials, case $p=2$. Since $a^2 \equiv a \pmod 2$ for integers a, we can replace terms x_i^2 by x_i whenever they occur. Having this convention in mind, we can prove the following

Theorem 6. *A polynomial* $f \in Z[x_1, \ldots, x_n]$ *of degree* 2 *is a permutation polynomial* mod 2 *if and only if* f *is equivalent* mod 2 *to a polynomial of the form* $g(x_1, \ldots, x_n) = h(x_1, \ldots, x_{n-1}) + x_n$, $h \in Z[x_1, \ldots, x_{n-1}]$.

Proof. The sufficiency of the condition follows from Lemma 1 and Lemma 3. Conversely, suppose that f is a permutation polynomial mod 2 whose degree modulo 2 is two (otherwise Theorem 3 yields the desired result). By possibly renaming the variables, we get modulo 2:

$$f(x_1, \ldots, x_n) = x_1(x_{i_1} + x_{i_2} + \cdots + x_{i_d} + b) + f_1(x_2, \ldots, x_n)$$

with $2 \leqq i_1 < i_2 < \cdots < i_d \leqq n$. Thus f is equivalent mod 2 to $x_1 x_2 + r(x_2, \ldots, x_n)$. Consider $r(x_2, \ldots, x_n)$ modulo 2. Let M be the least integer such that a term of the form $x_M x_j$, $M < j$, occurs in r, or $M = n+1$ if r is linear. If r contains a linear term x_i with $3 \leqq i < M$, then we are done. Otherwise, f is equivalent mod 2 to $x_1 x_2 + cx_2 + s(x_M, \ldots, x_n)$. If $M=2$, then we apply the above reduction process to s and we get f equivalent mod 2 to $x_1 x_2 + x_2 x_3 + t(x_3, \ldots, x_n)$ which, in turn, is equivalent mod 2 to $x_1 x_2 + t(x_3, \ldots, x_n)$. Since this is also true for $M > 2$, we obtain by repeated application of the reduction process: f is either equivalent mod 2 to the desired form or, after possibly renaming the variables, to a polynomial of the form $q(x_1, \dots, x_n) = x_1 x_2 + x_3 x_4 + \dots + x_{2k-1} x_{2k}$.

We complete the proof by showing that q cannot be a permutation polynomial mod 2. In fact, using Theorem 2 with $m=1$, we have:

$$\sum_{(a_1,\dots,a_n)\in M_2^n} e^{\pi i q(a_1,\dots,a_n)} = 2^{n-2k}\left(\sum_{a_1=0}^{1}\sum_{a_2=0}^{1}(-1)^{a_1 a_2}\right)\dots\left(\sum_{a_{2k-1}=0}^{1}\sum_{a_{2k}=0}^{1}(-1)^{a_{2k-1}a_{2k}}\right) \neq 0.$$

References

[1] L. Carlitz, Permutations in a finite field, *Proc. Amer. Math. Soc.*, **4** (1953), 538.

[2] L. Carlitz, Invariantive theory of equations in a finite field, *Trans. Amer. Math. Soc.*, **75** (1953), 405—427.

[3] L. Carlitz, Some theorems on permutation polynomials, *Bull. Amer. Math. Soc.*, **68** (1962), 120—122.

[4] L. Carlitz, Permutations in finite fields, *Acta Sci. Math.*, **24** (1963), 196—203.

[5] L. Carlitz and C. Wells, The number of solutions of a special system of equations in a finite field, *Acta Arithmetica*, **12** (1966), 77—84.

[6] H. Davenport, *Multiplicative Number Theory* (Chicago, 1967).

[7] L. E. Dickson, *History of the Theory of Numbers*. Vol. 3 (Washington, 1923).

[8] L. E. Dickson, *Linear Groups* (Leipzig, 1901).

[9] V. A. Kurbatov and N. G. Starkov, The analytic representation of permutations (Russian), *Sverdlovsk. Gos. Ped. Inst. Učen. Zap.*, **31** (1965), 151—158.

[10] W. Nöbauer, Über Gruppen von Restklassen nach Restpolynomidealen, *Sitzungsber. Österr. Akad. Wiss.*, Abt. IIa, **162** (1953), 207—233.

[11] W. Nöbauer, Zur Theorie der Polynomtransformationen und Permutationspolynome, *Math. Ann.*, **157** (1964), 332—342.

[12] W. Nöbauer, Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen, *Monatsh. Math.*, **69** (1965), 230—238.

[13] L. Rédei, Über eindeutig umkehrbare Polynome in endlichen Körpern, *Acta Sci. Math.*, **11** (1946), 85—92.

[14] C. Wells, Groups of permutation polynomials, *Monatsh. Math.*, **71** (1967), 248—262.

SOUTHERN ILLINOIS UNIVERSITY

(Received June 2, 1970)