J. Austral. Math. Soc. (*Series A*) **43** (1987), 171–175

PERMUTATION POLYNOMIALS IN SEVERAL VARIABLES OVER RESIDUE CLASS RINGS

H. K. KAISER and W. NÖBAUER

(Received 21 April 1986)

Communicated by R. Lidl

Abstract

The concept of a permutation polynomial function over a commutative ring with 1 can be generalized to multiplace functions in two different ways, yielding the notion of a k-ary permutation polynomial function ($k > 1$, $k \in \mathbf{N}$) and the notion of a strict k-ary permutation polynomial function respectively. It is shown that in the case of a residue class ring $\mathbf{Z}_m$ of the integers these two notions coincide if and only if m is squarefree.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 13 B 25.

The representation of permutations by polynomials has been thoroughly studied over the past century. Let $\langle R, +, -, 0, \cdot, 1\rangle$ be a commutative ring with identity. Then we call a function $f: R \to R$ a *permutation permutation function* over $\langle R, +, -, 0, \cdot, 1\rangle$ if f is both a permutation of the set R and a polynomial function over $\langle R, +, -, 0, \cdot, 1\rangle$. A polynomial $f(x) \in R[x]$ which induces such an f is called permutation polynomial over $\langle R, +, -, 0, \cdot, 1\rangle$.

A direct generalization of this concept to functions in several variables is not possible, since polynomial functions $f: R^k \to R$, $k > 1$, can never represent a permutation of R^k, since $R^k \neq R$. Hence we have to consider k-tuples $(f_1, \ldots, f_k)$ of functions $f_i: R^k \to R$, $i = 1, \ldots, k$, and we say: a permutation π of $R^k$is represented by $(f_1, f_2, \ldots, f_k)$ if $\pi(r_1, \ldots, r_k) = (f_1(r_1, \ldots, r_k), \ldots, f_k(r_1, \ldots, r_k))$ for all $(r_1, \ldots, r_k) \in R^k$.

This yields the following generalization of a permutation polynomial function to the case of several variables: $f: R^k \to R$ is called *k-place permutation polynomial function* (in short *PPF*) over R, if f is a component in a k-tuple of k-ary

© 1987 Australian Mathematical Society 0263-6115/87 $A2.00 + 0.00

https://doi.org/10.1017/S144678870002930X Published online by Cambridge University Press

functions over R which represent a permutation of R^k and if f is a polynomial function over $\langle R, +, -, 0, \cdot, 1\rangle$. Polynomials $f(x_1, \dots, x_k) \in R[x_1, \dots, x_k]$ which induce such a *PPF* are called *permutation polynomials in k variables* over $\langle R, +, -, 0, \cdot, 1\rangle$. The set of all k-ary *PPF* over $\langle R, +, -, 0, \cdot, 1\rangle$ is denoted by $S_k(R)$. It is easy to see that every k-ary *PPF* f appears as first component in the representation of a suitable permutation of R^k, hence we have: A polynomial function $f: R^k \to R$ is a k-ary *PPF* over $\langle R, +, -, 0, \cdot, 1\rangle$ if and only if there are k-ary functions $f_2, \dots, f_k$ over R such that $(f, f_2, \dots, f_k)$ represents a permutation of R^k.

Another possibility of generalization is the following: A polynomial function $f: R^k \to R$ is called *strict permutation polynomial function* over $\langle R, +, -, 0, \cdot, 1\rangle$ (in short *SPPF*) if there are k-ary polynomial functions $f_2, \dots, f_k$ over $\langle R, +, -, 0, \cdot, 1\rangle$ such that the k-tuple of polynomial functions $(f, f_2, \dots, f_k)$ represents a permutation of R^k. Again we call a polynomial $f(x_1, \dots, x_k) \in R[x_1, \dots, x_k]$ a *strict permutation polynomial* over $\langle R, +, -, 0, \cdot, 1\rangle$ if $f(x_1, x_2, \dots, x_k)$ induces a *SPPF* f. The set of all k-ary *SPPF* over $\langle R, +, -, 0, \cdot, 1\rangle$ will be denoted by $SS_k(R)$. If $P_k(R)$ symbolizes the set of all k-ary polynomial functions $f: R^k \to R$, then $SS_k(R) \subseteq S_k(R) \subseteq P_k(R)$.

Both generalizations have been investigated in a series of papers (see H. Lausch and W. Nöbauer [1] and bibliography thereto appended). Especially for permutation polynomials over finite fields a number of results are known (see R. Lidl and H. Niederreiter [2]). In the case of finite fields the two notions of *PPF* and *SPPF* coincide, since every k-ary function over $GF(q)$ ($k \in \mathbb{N}$, arbitrary) with values in $GF(q)$ can be represented by a polynomial function over $GF(q)$. In [3] W. Nöbauer raised the problem for which finite commutative rings this coincidence holds. In this paper we solve the problem for all residue class rings $\mathbb{Z}_m$ of the integers.

First we recall some properties of permutation polynomial functions and permutation polynomials over $\langle R, +, -, 0, \cdot, 1\rangle$. Permutation polynomial functions over finite rings can be characterized as follows:

THEOREM. *Let $\langle R, +, -, 0, \cdot, 1\rangle$ be a finite commutative ring with identity. A polynomial function $f \in P_k(R)$ is a k-ary PPF if and only if for every $r \in R$ the set of all solutions in R of the equation $f(x_1, \dots, x_k) = r$ has the cardinality $|R|^{k-1}$.*

For a proof see H. Lausch and W. Nöbauer ([1], Chapter 3, Proposition 12.21.).

LEMMA 1. (i) *If $f(x_1, x_2, \dots, x_k) \in R[x_1, x_2, \dots, x_k]$ is a k-ary permutation polynomial over $\langle R, +, -, 0, \cdot, 1\rangle$, then $f(x_1, x_2, \dots, x_k)$ is an n-ary permutation polynomial over $\langle R, +, -, 0, \cdot, 1\rangle$ for every $n > k$.*

https://doi.org/10.1017/S144678870002930X Published online by Cambridge University Press

(ii) *If* $f(x_1,\dots,x_k)\in R[x_1,x_2,\dots,x_k]$ *then we denote by* $\bar f(x_1,\dots,x_k)$ *the polynomial which is obtained by removing the constant term from* f. *Then the following holds: The k-tuple* $(f_1(x_1,\dots,x_k),\dots,f_k(x_1,\dots,x_k))$ *of k-ary polynomials over* $\langle R,+,-,0,\cdot,1\rangle$ *induces a permutation of* R^k *if and only if* $(\bar f_1(x_1,\dots,x_k), \bar f_2(x_1,\dots,x_k),\dots,\bar f_k(x_1,\dots,x_k))$ *does so as well.*

PROOF. (i) follows easily from the preceding theorem and (ii) is evident.

Now we turn to the problem of finding all $\mathbb{Z}_m$ for which every $f\in\mathbb{Z}_m$ is a *PPF* if and only if f is a *SPPF*. Let $m=p_1^{e_1}\cdot p_2^{e_2}\cdot\ \dots\ \cdot p_n^{e_n}$ be the prime factorization of m. Then $\mathbb{Z}_m$ is isomorphic to the product of the residue class rings $\mathbb{Z}_{p_i^{e_i}}$, $i=1,\dots,n$. The following theorem is taken from H. Lausch and W. Nöbauer [1] (Chapter 3, Proposition 12.43).

THEOREM. *If* $\mathbf{V}$ *is the variety of commutative rings with identity and* $R=A\times B$ *in* $\mathbf{V}$ *then there is a bijective mapping of* $SS_k(R)$ *onto* $SS_k(A)\times SS_k(B)$ *which is, if R is finite, the restriction of a bijective mapping from* $S_k(R)$ *onto* $S_k(A)\times S_k(B)$.

This theorem reduces our study to $\mathbb{Z}_{p^e}$, p prime, $e\in\mathbb{N}$, $e>1$ (since for finite fields $\mathbb{Z}_p$—as mentioned above—every *PPF* is *SPPF*). First we consider the case $k=2$:

We show that in this case there are *PPF* over $\mathbb{Z}_{p^e}$ which are not *SPPF*. φ denotes Euler's phi-function.

LEMMA 2. *The binary function* $f:\mathbb{Z}_{p^e}^2\to\mathbb{Z}_{p^e}$, *p prime*, $e>1$, *defined by* $f(x,y)=px+y^{\varphi(p^e)+1}\bmod p^e$ *is a PPF.*

PROOF. If we multiply every $x\in\mathbb{Z}_{p^e}$ by p, we obtain (mod p^e) every non negative multiple of p which is smaller than p^e exactly p times. If $(y,p^e)=1$ then

$$y^{\varphi(p^e)+1}=y^{p^e-p^{e-1}+1}\equiv y \mod p^e$$

by the theorem of Fermat-Euler. If $(y,p^e)>1$ then

$$y^{\varphi(p^e)+1}=y^{p^e-p^{e-1}+1}\equiv 0 \mod p^e$$

since we have $p^e-p^{e-1}+1>p^e-p^{e-1}\geqslant 2p^{e-1}-p^{e-1}=p^{e-1}\geqslant (1+1)^{e-1}=\sum_{i=0}^{e-1}\binom{e-1}{i}\geqslant e$. Let $a\in\mathbb{Z}_{p^e}$ be a fixed element and $a\equiv t \bmod p$, $t\in\{0,\dots,p-1\}$. Then we obtain by $f(x,a)$ every element of $\mathbb{Z}_{p^e}$ which is congruent $t \bmod p$ exactly p times, if x runs through the whole of $\mathbb{Z}_{p^e}$. Since the

https://doi.org/10.1017/S144678870002930X Published online by Cambridge University Press

congruence $y^{\varphi(p^e)+1} \equiv i \bmod p$ $(i = 0, 1, \ldots, p-1)$ has p^{e-1} incongruent solutions mod p^e, we have: The equation $f(x, y) = u$ possesses $p \cdot p^{e-1} = p^e$ solutions in $\mathbb{Z}_{p^e}$ for every $u \in \mathbb{Z}_{p^e}$. Hence f is a binary *PPF* over $\mathbb{Z}_{p^e}$.

LEMMA 3. *$f\colon \mathbb{Z}_{p^e}^2 \to \mathbb{Z}_{p^e}$, defined by $f(x, y) = px + y^{\varphi(p^e)+1}$ for all $(x, y) \in \mathbb{Z}_{p^e}^2$ is not SPPF.*

PROOF. We denote $f^{-1}(0) \subseteq \mathbb{Z}_{p^e}^2$ by ${}_fN_0$. For the function f defined in Lemma 2 we have

$${}_fN_0 = \{0, p^{e-1}, 2p^{e-1}, \ldots, (p-1)p^{e-1}\} \times \{0, p, 2p, \ldots, (p^{e-1}-1)p\}.$$

Since $|{}_fN_0| = p^e$, a necessary condition for f to be a binary *SPPF* is the existence of a polynomial function $g\colon \mathbb{Z}_{p^e}^2 \to \mathbb{Z}_{p^e}$ such that g restricted to ${}_fN_0$ is a mapping onto $\mathbb{Z}_{p^e}$. But such a g does not exist, since for any polynomial $g(x, y)$ with constant term c, we have $g(\xi, \eta) \equiv c \bmod p$ for all $(\xi, \eta) \in {}_fN_0$.

To settle the general case let $k > 2$ be a fixed integer. Then $f\colon \mathbb{Z}_{p^e}^k \to \mathbb{Z}_{p^e}$, defined by $f(x_1, \ldots, x_k) := px_1 + x_2^{\varphi(p^e)+1}$ for all $(x_1, \ldots, x_k) \in \mathbb{Z}_{p^e}^k$, is by Lemma 2 and Lemma 1, (i) a k-ary *PPF* over $\mathbb{Z}_{p^e}$ and ${}_fN_0 = \{0, p^{e-1}, 2p^{e-1}, \ldots, (p-1)p^{e-1}\} \times \{0, p, 2p, \ldots, (p^{e-1}-1)p\} \times \mathbb{Z}_{p^e}^{k-2}$.

LEMMA 4. *The function f defined above is not a SPPF over $\mathbb{Z}_{p^e}$.*

PROOF. Let us assume in the contrary that f is *SPPF*. Then there are $\varphi_2, \ldots, \varphi_k \in P_k(\mathbb{Z}_{p^e})$ such that $(f, \varphi_2, \ldots, \varphi_k)$ represents a permutation of $\mathbb{Z}_{p^e}^k$ and all φ_i, $i = 2, \ldots, k$ are assumed to be without constant term. If we restrict f, $\varphi_2, \ldots, \varphi_k$ to ${}_fN_0$ then $(f, \varphi_2, \ldots, \varphi_k)$ has to represent all k-tuples over $\mathbb{Z}_{p^e}$ with first component 0. Thus $(\varphi_2, \ldots, \varphi_k)$ has to represent each element of $\mathbb{Z}_{p^e}^{k-1}$ if $(x_1, x_2, \ldots, x_k)$ runs over ${}_fN_0$. Hence $(\varphi_2, \ldots, \varphi_k)$, if considered mod p, represents all the elements of $\mathbb{Z}_p^{k-1}$, if $(x_1, x_2, \ldots, x_k)$ runs over ${}_fN_0$.

Each polynomial φ_i can be written as $g_i(x_3, x_4, \ldots, x_k) + h_i(x_1, x_2, \ldots, x_k)$, where every term of $h_i(x_1, x_2, \ldots, x_k)$ has a factor x_1 or x_2. Since $x_1 \equiv x_2 \equiv 0 \bmod p$ for all $(x_1, x_2, \ldots, x_k) \in {}_fN_0$, we obtain $\varphi_i(x_1, x_2, \ldots, x_k) \equiv g_i(x_3, x_4, \ldots, x_k) \bmod p$ for every $(x_1, x_2, \ldots, x_k) \in {}_fN_0$. Hence $(\varphi_2, \ldots, \varphi_k)$ has at most $|\mathbb{Z}_{p^e}|^{k-2}$ distinct values mod p if $(x_1, x_2, \ldots, x_k)$ runs over ${}_fN_0$, a contradiction. Hence f is not a k-ary *SPPF* over $\mathbb{Z}_{p^e}$.

This yields the following

THEOREM. *Let R be a finite commutative ring with identity which is isomorphic to a direct product $\mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}}$ (p_i, $i = 1, \ldots, n$, not necessarily distinct primes, $e_i \in \mathbb{Z}$, $e_i \geqslant 1$, for $i = 1, \ldots, n$). Then every k-ary PPF is SPPF ($k > 1$, $k \in \mathbb{N}$ arbitrary) if and only if all $e_i = 1$.*

https://doi.org/10.1017/S144678870002930X Published online by Cambridge University Press

COROLLARY. *Let $\mathbf{Z}_m$ be a residue class ring of the integers. Then every k-ary PPF is SPPF if and only if m is squarefree.*

References

[1] H. Lausch and W. Nöbauer, *Algebra of polynomials* (North-Holland, Amsterdam, 1973).
[2] R Lidl and H. Niederreiter, *Finite fields* (Addison-Wesley, Reading, Massachusetts, 1983).
[3] W. Nöbauer, 'Darstellung von Permutationen durch Polynome und rationale Funktionen', *Berichte des Math. Forschungsinst. Oberwolfach* **5** (1971), 89–100.

Institut für Algebra und Diskrete Mathematik
Technische Universität Wien
Wiedner Hauptstraße 8–10
A-1040 Vienna, Austria

https://doi.org/10.1017/S144678870002930X Published online by Cambridge University Press