Finite Fields Appl. **1** (1995) 437–439

WHEN ARE WEAK PERMUTATION POLYNOMIALS STRONG?

Sophie Frisch

Abstract. For a commutative finite ring with identity R, the two definitions of *permutation polynomial in several indeterminates over* R coincide if and only if R is a direct sum of finite fields.

Amer. Math. Soc. 1991 Mathematics Subject Classification: 11T06, 13M10; Secondary: 13B25.

All rings considered are commutative and finite, and ring always means ring with identity. A polynomial $f \in R[x]$ is said to be a *permutation polynomial* (abbreviated PP) if the function it defines on R through substitution, $r \mapsto f(r)$, is a permutation. This notion has been generalized to polynomials in several indeterminates in two different ways. We will characterize the rings for which the two coincide. (For quotient rings of the integers this has been done by Kaiser and Nöbauer [1].)

We write the cartesian product of n copies of a set S as $S^{<n>}$, to avoid confusion with the power S^n, if S happens to be an ideal. An m-tuple of polynomials $(f_0, f_1, \ldots, f_{m-1})$ in n indeterminates over R induces a function $(r_0, \ldots, r_{n-1}) \mapsto (f_0(r_0, \ldots, r_{n-1}), \ldots, f_{m-1}(r_0, \ldots, r_{n-1}))$, which we denote by the same name, $(f_0, f_1, \ldots, f_{m-1})\colon R^{<n>} \to R^{<m>}$.

Definition. Let f be a polynomial in n indeterminates with coefficients in R. f is a *strong* PP if there exist polynomials $f_1, \ldots, f_{n-1}$ in n indeterminates over R, such that the function $(f, f_1, \ldots, f_{n-1})\colon R^{<n>} \to R^{<n>}$ is a permutation.

f is a *weak* PP if for every r in R the cardinality of the inverse image of r under $f\colon R^{<n>} \to R$ is $|R|^{n-1}$.

Clearly, strong PP implies weak PP. It is easy to see that f is a weak PP if and only if there exist functions $g_i\colon R^{<n>} \to R$ (not necessarily representable by polynomials), such that $(f, g_1, \ldots, g_{n-1})$ permutes $R^{<n>}$ (cf. [2, p120]).

If F is a finite field, it is well known that every function $\gamma\colon F^{<n>} \to F$ is represented by a polynomial with coefficients in F, namely by $g(x_1, \ldots, x_n) =$

$\sum_{(c_1,..,c_n)\in F^{<n>}} \gamma(c_1,\ldots,c_n) \prod_{i=1}^{n}\bigl(1-(x_i-c_i)^{|F|-1}\bigr)$; therefore every weak PP over a finite field is a strong PP [3, p369].

Lemma 1. *Let $n \in \mathbb{N}$. A finite direct sum of finite commutative rings has the property "every weak PP over R in n indeterminates is strong" if and only if every summand has it.*

Proof. If $R = R_1 \times \ldots \times R_k$, there is a natural isomorphism of $R[X]$ (X a set of indeterminates) to $R_1[X] \times \ldots \times R_k[X]$, sending f to $[f^{(1)},\ldots,f^{(k)}]$, where $f^{(i)}$ results from f by projection of the coefficients onto R_i. Since addition and multiplication (and therefore evaluation of polynomials) in a direct sum of rings are defined componentwise, we may identify a vector $\bar{r} \in R^{<n>}$ with the k-tuple of its components $[\bar{r}^{(1)},\ldots,\bar{r}^{(k)}]$, $\bar{r}^{(i)} \in R_i^{<n>}$, and $f \in R[x_1,\ldots,x_n]$ with $[f^{(1)},\ldots,f^{(k)}]$, and the function $f\colon R^{<n>} \to R$ will correspond to the k-tuple of functions $f^{(i)}\colon R_i^{<n>} \to R_i$ acting independently on the components of $R^{<n>}$: $f(\bar{r}) = [f^{(1)}(\bar{r}^{(1)}),\ldots,f^{(k)}(\bar{r}^{(k)})]$. Therefore f is a weak [strong] PP over R if and only if each $f^{(i)}$ is a weak [strong] PP over R_i. Indeed, if f is a weak PP, then $\left|f^{-1}(\{r_1\} \times R_2 \times \ldots \times R_k)\right| = |R|^{n-1}\,|R_2|\ldots|R_k|$. On the other hand $f^{-1}(\{r_1\} \times R_2 \times \ldots \times R_k) = {f^{(1)}}^{-1}(r_1) \times R_2^{<n>} \times \ldots \times R_k^{<n>}$, so $\left|{f^{(1)}}^{-1}(r_1)\right| = |R_1|^{n-1}$. The remaining implications are even more straightforward. The statement of the Lemma now follows. (Note that every weak PP over R_i, $f^{(i)} \in R_i[x_1,\ldots,x_n]$, can be completed to a system $[f^{(1)},\ldots,f^{(k)}]$ of weak PPs on the components of R by setting $f^{(j)} = x_1$, $i \neq j$.) □

For a commutative ring R, $\mathrm{Rad}(R)$ denotes the intersection of all maximal ideals in R.

Lemma 2. *Let R be a commutative finite ring with* $\mathrm{Rad}(R) \neq (0)$*. If* $\mathrm{Rad}(R)$ *is generated as an ideal by n elements, then there exists a weak PP over R in $n+1$ indeterminates that is not strong.*

Proof. Suppose $(0) \neq \mathrm{Rad}(R) = Q$ and let $h(y) = y\bigl(\prod_{p\in Q}(y-p)\bigr)^{c}$, with c a multiple of $[R:M]-1$ for every maximal ideal M of R; then $h(p) = 0$ for all $p \in Q$ and $h(r) \equiv r \bmod Q$ for all $r \in R$. If $Q = q_1R + \ldots + q_nR$, let $g(x_1,\ldots,x_n) = q_1x_1 + \ldots + q_nx_n$. Then $g(R^{<n>}) = Q$ and for every $p \in Q$ $\left|g^{-1}(p)\right| = |\ker(g)| = |R|^{n} / |Q|$. Set $f(x_1,\ldots,x_n,y) = g(x_1,\ldots,x_n) + h(y)$; we show that f is a weak but not a strong PP.

First note that $f(r_1,\dots,r_n,s) \equiv s \bmod Q$ for all $r_1,\dots,r_n,\ s \in R$. We have $\left|f^{-1}(r)\right| = |R|^n$ for every $r \in R$, because there are $|Q|$ choices for s in $r+Q$ and for each such s there are $|R|^n / |Q|$ choices for $(r_1,\dots,r_n)$ such that $g(r_1,\dots,r_n) = r - h(s)$; so f is a weak PP. Suppose f is a strong PP, i.e. there exist $f_1,\dots,f_n \in R[x_1,\dots,x_n,y]$, such that $(f,f_1,\dots,f_n)$ permutes $R^{<n+1>}$. W.l.o.g. we assume the constant terms of $f_1,\dots,f_n$ to be 0 (adding a constant does not affect bijectivity). Then $\left|(f,f_1,\dots,f_n)^{-1}(\{0\}\times Q^{<n>})\right| = |Q|^n$. In contradiction to this there exists a set $S \subseteq (f,f_1,\dots,f_n)^{-1}(\{0\}\times Q^{<n>})$ with $|S| > |Q|^n$, namely $S = f^{-1}(0) \cap Q^{<n+1>}$. By hypothesis $Q \neq (0)$, but (being the radical) Q is nilpotent, so $Q^2 \neq Q$. Let $\tilde{g}$ be g restricted to arguments in Q, then $\tilde{g}(Q^{<n>}) \subseteq Q^2$, so $|\tilde{g}(Q^{<n>})| < |Q|$ and $|\ker(\tilde{g})| = |Q|^n / |\tilde{g}(Q^{<n>})| > |Q|^{n-1}$. Therefore $\left|f^{-1}(0) \cap Q^{<n+1>}\right| = |\ker(\tilde{g})| \cdot |Q| > |Q|^n$. □

Theorem. *If R is a commutative finite ring, then every weak PP over R is a strong PP if and only if R is a direct sum of finite fields.*

Proof. By Lemma 1 and the remark preceding it, every weak PP over a finite direct sum of finite fields is strong. Conversely, if R is a finite commutative ring such that every weak PP over R is strong, then Lemma 2 implies $\mathrm{Rad}(R) = (0)$. But for a commutative finite ring R "$\mathrm{Rad}(R) = (0)$" and "R is a direct sum of finite fields" are equivalent: This is an easy consequence of the fact that every commutative finite ring is a direct sum of local rings; cf. [4, p95]. □

REFERENCES

1. H. K. Kaiser and W. Nöbauer, Permutation polynomials in several variables over residue class rings. *J. Austral. Math. Soc. (Ser. A)* **43** (1987), 171–175.

2. H. Lausch and W. Nöbauer, "Algebra of Polynomials,"

   North-Holland, Amsterdam, 1973.

3. R. Lidl and H. Niederreiter, "Finite Fields," Addison-Wesley,

   Reading, MA, 1983.

4. B. R. McDonald, "Finite Rings with Identity," Dekker, New York, 1974.

INSTITUT FÜR MATHEMATIK (C), TECHNISCHE UNIVERSITÄT GRAZ,
KOPERNIKUSGASSE 24, A-8010 GRAZ, AUSTRIA
e-mail: frisch@blah.tu-graz.ac.at