Permutation Polynomials on Matrices*

N. S. James and R. Lidl
Department of Mathematics
University of Tasmania
Hobart, Tasmania 7001, Australia

Submitted by Hans Schneider

ABSTRACT

Families of examples are presented of polynomials over a finite field or a residue class ring of the integers, which, on substitution, permute the $n \times n$ matrices over that field or residue class ring.

INTRODUCTION

Let R denote a finite commutative ring with identity, and let $R_{n\times n}$ denote the ring of $n \times n$ matrices over R. A polynomial $f \in R[x]$ defines, via substitution, a function $f\colon R_{n\times n} \to R_{n\times n}$. The polynomial $f(x)$ is said to represent the function f, and any function f from $R_{n\times n}$ to $R_{n\times n}$ which can be represented by some polynomial $f(x)$ over R is called a (scalar) polynomial function on $R_{n\times n}$. If such a polynomial function f is bijective, then f is called a permutation polynomial function, and any polynomial $f(x)$ which represents f is called a permutation polynomial (abbreviated p.p.) of $R_{n\times n}$.

In the case that $R = \mathbb{F}_q$, the finite field of q elements, scalar polynomial functions and p.p. of $R_{n\times n}$ have been studied by Brawley [1] and Brawley, Carlitz, and Levine [3]. If R is an arbitrary finite commutative ring with identity, Brawley [2] gives a criterion for $f \in R[x]$ to be a p.p. of $R_{n\times n}$. The special case $n = 1$ has been treated extensively in the literature; for $R = \mathbb{F}_q$ the book by Lidl and Niederreiter [10] gives a summary of several results on

*This research was partially supported by Australian Research Grants Scheme, Project F84151831.

52 Vanderbilt Ave., New York, NY 10017 0024-3795/87/$3.50

p.p. of $\mathbb{F}_q$. If $R = \mathbb{Z}_m$ see e.g. Lausch, Müller, Nöbauer [7] and Nöbauer [16] for some examples. Brawley and Schnibben [4] give necessary and sufficient conditions for a polynomial over an arbitrary field F to be a permutation of the $n \times n$ matrices over F. They also consider the case of algebraic extensions of $\mathbb{F}_q$ in this context.

In this paper we give specific examples of classes of polynomials which are p.p. of $R_{n\times n}$, first for $R = \mathbb{F}_q$ and then for $R = \mathbb{Z}_m$. We also settle a problem on p.p. posed by Carlitz [5]. We summarize some of the results in [3]. Let F denote the finite field $\mathbb{F}_q$ of order q, char $F = p$. If $n > 1$, not every function from $F_{n\times n}$ to $F_{n\times n}$ can be represented by a polynomial $f(x) \in F[x]$, but every scalar polynomial function from $F_{n\times n}$ to $F_{n\times n}$ can be represented by a unique polynomial $f \in F[x]$ of degree less than $\delta = q^n + q^{n-1} + \cdots + q$. Let $n > 0$ be an integer, and let $L_n(x) = \prod_{k=1}^{n}(x^{q^k} - x)$. Then L_n is the monic polynomial of least degree δ such that $L_n(A) = 0$ for all $A \in F_{n\times n}$. The number of scalar polynomial functions of $F_{n\times n}$ is q^δ. Brawley [1] determines the number of p.p. functions of $F_{n\times n}$ and in doing so gives a procedure for constructing every p.p. on $F_{n\times n}$. The main result of [3] is

THEOREM 1 (Brawley, Carlitz, Levine). *The polynomial $f \in \mathbb{F}_q[x]$ is a p.p. of $F_{n\times n}$ if and only if*

(i) *$f(x)$ is a p.p. of $\mathbb{F}_q, \mathbb{F}_{q^2}, \ldots, \mathbb{F}_{q^n}$ and*

(ii) *$f'(x)$ does not vanish on $\mathbb{F}_q, \mathbb{F}_{q^2}, \ldots, \mathbb{F}_{q^{[n/2]}}$, where $[n/2]$ is the greatest integer in $n/2$.*

In [3] the following examples of p.p. of $F_{n\times n}$ are given: For $n = 2$, $q = 2$ there are four p.p. of $F_{2\times 2}$, and they are x, $x + 1$, $x^4 + x^2 + x$, $x^4 + x^2 + x + 1$. For $n \geqslant 1$ and $F = \mathbb{F}_q$ the polynomials of the form

$$f(x) = a_0 x + a_1 x^q + \cdots + a_{m-1} x^{q^{m-1}}, \qquad a_i \in F,$$

are p.p. of $F_{n\times n}$ if $a_0 \neq 0$, $m = \operatorname{lcm}\{1, 2, \ldots, n\}$, and the circulant determinant

$$\begin{vmatrix} a_{m-1} & a_{m-2} & \cdots & a_1 & a_0 \\ a_{m-2} & a_{m-3} & \cdots & a_0 & a_{m-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_0 & a_{m-1} & \cdots & a_2 & a_1 \end{vmatrix}$$

is nonzero.

We next give further examples of p.p. of $F_{n\times n}$. Again let $F = \mathbb{F}_q$, char $F = p$.

EXAMPLE 2. We determine all normalized p.p. of $F_{n\times n}$ of degree $\leqslant 5$: A p.p. $f \in F[x]$ is normalized if it is monic, $f(0)=0$, and when the degree m of f is not divisible by p, the coefficient of x^{m-1} is 0. Dickson determined a list of all normalized p.p. of F of degree $\leqslant 5$; see [10, p. 352]. From this list we see by applying Theorem 1 that the following polynomials are p.p. of $F_{n\times n}$, and these are the only normalized p.p. of $F_{n\times n}$ of degree $\leqslant 5$ and $n \geqslant 2$:

$$f(x) = x \qquad \text{for any } q \text{ and } n;$$

$$f(x) = x^4 + a_1x^2 + a_2x,$$

where the only root of $f(x)$ in $\mathbb{F}_q$ is 0, $n=2$, $q \equiv 0 \pmod 2$, $a_2 \neq 0$;

$$f(x) = x^5 + ax,$$

where $a \neq 0$ is not a square in $\mathbb{F}_q$, $n \leqslant 3$, and $q \equiv 0 \pmod 5$.

EXAMPLE 3. First let $F = \mathbb{F}_p$, p an odd prime. We consider $h_k(x) = 1 + x + \cdots + x^k$ and classify those h_k which are p.p. of $F_{2\times 2}$. Matthews [12] showed that h_k is a p.p. of $\mathbb{F}_q$, q a prime or a square of a prime, if and only if $k \equiv 1 \bmod p(q-1)$. Therefore for $n=2$, h_k satisfies part (i) of Theorem 1 if and only if

$$k \equiv 1 \bmod p(p-1) \quad \text{and} \quad k \equiv 1 \bmod p(p^2-1).$$

We show that such h_k also satisfy part (ii). Note that for $x \neq 1$, $h_k(x) = (x^{k+1}-1)/(x-1)$. If h_k is a p.p. of $\mathbb{F}_p$, then $h_k'(a) = 1$ for all $a \neq 1$ in $\mathbb{F}_p$. For $x=1$ we have $h_k'(1) = \frac{1}{2}k(k+1)$, which is 1 if h_k is a p.p. of $\mathbb{F}_p$. In summary, $h_k(x)$ is a p.p. of $F_{2\times 2}$ if and only if $k \equiv 1 \bmod p(p^2-1)$.

Next we give examples of p.p. $h_k(x)$ of $F_{n\times n}$ for $F = \mathbb{F}_q$, q an odd prime power, and $n \geqslant 1$. Matthews [12] proved that $h_k(x)$ is a p.p. of F_q if $k \equiv 1 \bmod p(q-1)$, where p is $\operatorname{char}\mathbb{F}_q$. Therefore $h_k(x)$ satisfies part (i) of Theorem 1 if

$$k \equiv 1 \bmod p \operatorname*{lcm}_{1 \leqslant i \leqslant n} \{q^i - 1\}. \tag{1}$$

To verify part (ii) of Theorem 1 for the p.p. $h_k(x)$ we note that $h_k'(x) = \{kx^{k+1} - (k+1)x^k + 1\}/(x-1)^2$ for $x \neq 1$. Then $h_k'(a) \neq 0$ for all k satisfying (1), and $a \neq 1$ in $\mathbb{F}_{q^i}$. For $x=1$ we have $h_k'(1) = \frac{1}{2}k(k+1)$, which also is nonzero over $\mathbb{F}_{q^i}$ whenever k satisfies (1). Hence $h_k(x)$ is a p.p. of $F_{n\times n}$ if (1) is satisfied. In the case $q=2$ one can verify directly that k has to satisfy the additional condition $k\equiv 1 \pmod 4$.

THE CARLITZ POLYNOMIALS

We next consider the interesting family of polynomials of the form $x^{m+1}+ax$ with m a divisor of $q-1$. Carlitz [5] stated that, for q sufficiently large, permutation polynomials of $\mathbb{F}_q$ of the form $x^{(q+k-1)/k}+ax$, $q\equiv 1 \bmod k$, $k\geqslant 2$, exist. Polynomials of the form $x^{(q+1)/2}+ax$, q odd, have been studied in [5], [6], and more recently Niederreiter and Robinson [15] gave necessary and sufficient conditions for such binomials to be permutation polynomials of $\mathbb{F}_q$. It can be verified that the family of polynomial functions of the form $ax^{(q+1)/2}+bx$ is closed under composition; see [14], [15]. This property makes these polynomials particularly attractive for applications, since the inverse of a p.p. of $\mathbb{F}_q$ of this form is again of this form.

There are few examples of families of p.p. which are closed under composition. In order to see if these polynomials can serve as examples of p.p. of $F_{n\times n}$, we use Theorem 1 and have to verify first that the polynomials are p.p. of $\mathbb{F}_{q^i}$. For $q\equiv 1 \bmod 2$ Carlitz [5, 6] showed that the polynomial $f(x)=x^{(q+1)/2}+ax$, $a=(c^2+1)(c^2-1)^{-1}$, $c^2\neq \pm 1$ or 0 in $\mathbb{F}_q$, is a p.p. of $\mathbb{F}_q$ provided $q\geqslant 7$, but is not a permutation polynomial for any $\mathbb{F}_{q^r}$, $r>1$. Therefore the polynomial $f(x)$ cannot be a p.p. of $F_{n\times n}$ for $n>1$. Carlitz [5] posed a similar question for $q\equiv 1 \bmod 3$, and $g(x)=x^{(q+2)/3}+ax$ as an open problem. More generally, we can show

THEOREM 4. *The polynomial* $f(x)=x^{(q+k-1)/k}+ax$, $a\in\mathbb{F}_q$, $a\neq 0$, *is not a p.p. of any* $\mathbb{F}_{q^r}$, $r>1$, *where* $q\equiv 1 \bmod k$, $q=p^e$, $k^2-2k=up+v$ *for integers* u *and* v *with* $0\leqslant v\leqslant p-k$.

Proof. For $f(x)$ to be a p.p. of $\mathbb{F}_{q^r}$, Hermite's criterion (see [10, p. 349]) requires that for each integer t with $1\leqslant t\leqslant q^r-2$ and $t\not\equiv 0 \bmod p$, the reduction of $f(x)^t \bmod x^{q^r}-x$ have degree $\leqslant q^r-2$. We note that

$$f(x)^t=\sum_{i=0}^{t}\binom{t}{i}x^{\{(q+k-1)/k\}t-\{(q-1)/k\}i}a^i.$$

If $t=k(q^{r-1}-1)$, then after reduction the only term with exponent q^r-1

of x is the one where

$$i = k\frac{(q+k-1)(q^{r-1}-1)-(q^r-1)}{q-1}.$$

Let $n = n_0 + n_1 p + n_2 p^2 + \cdots$ and $s = s_0 + s_1 p + s_2 p^2 + \cdots$ for $0 \leqslant n_j < p$, $0 \leqslant s_j < p$. Then by Lucas's theorem

$$\binom{n}{s} \equiv \binom{n_0}{s_0}\binom{n_1}{s_1}\binom{n_2}{s_2}\cdots \mod p.$$

We have

$$\binom{n_j}{s_j} \not\equiv 0 \mod p \quad \text{if and only if} \quad n_j \geqslant s_j.$$

Now

$$\begin{aligned} t &= k(q^{r-1}-1) = (k-1)p^{e(r-1)} + p^{e(r-1)} - k \\ &= (k-1)p^{e(r-1)} + (p-1)p^{e(r-1)-1} + \cdots + (p-1)p + (p-k). \end{aligned}$$

Also

$$i = k(k-1)q^{r-2} + k(k-1)q^{r-3} + \cdots + k(k-1)q + k(k-1) - k.$$

Since $t \geqslant i$, the leading digit of t must be greater than or equal to the corresponding digit of i. All other digits of t, with the exception of the p^0 digit, are $p-1$ and hence greater than or equal to the corresponding digit of i. The p^0 digit of t is $p-k$, which is greater than or equal to the p^0 digit of $i = tv$, where $k^2 - 2k = up + v$. Therefore

$$\binom{t}{i} \not\equiv 0 \mod p$$

and hence $\deg f(x)^t = q^r - 1$. So $f(x)$ cannot be a p.p. of $\mathbb{F}_{q^r}$. This always holds in the case that $p \geqslant k^2 - k$, since $v \leqslant k^2 - 2k$. ∎

As a special case we consider $k = 3$, $r = 2$.

COROLLARY 5*. *The polynomial* $f(x) = x^{(q+2)/3} + ax,\ a \neq 0$, *over* $\mathbb{F}_q$, $q = p^e \equiv 1 \bmod 3,\ p > 5$, *is not a permutation polynomial of* $\mathbb{F}_{q^2}$.

Proof. According to the proof of Theorem 2 we evaluate

$$\binom{t}{i} = \binom{3(q-1)}{3} = \frac{(3q-3)(3q-4)(3q-5)}{3 \times 2} \not\equiv 0 \bmod p$$

for $p = \operatorname{char} \mathbb{F}_q$. ■

One can also verify that for $q = p^e \equiv 1 \pmod 4$, $p = 7$ or $p > 11$, the polynomial $f(x) = x^{(q+3)/4} + ax,\ a \neq 0$, over $\mathbb{F}_q$ is not a permutation polynomial of $\mathbb{F}_{q^2}$. This is the special case $k = 4$ of Theorem 4.

We note that Nöbauer [16] proved that the polynomials of the form $f(x) = x^{(p+1)/2} + ax$ are p.p. of $\mathbb{Z}/(p^e)$ for all integers $e \geqslant 1$ and primes $p \geqslant 7$ if $a = (c+1)(c-1)^{-1}$, c a quadratic residue mod p and c incongruent to $1, -1, -3, -3^{-1}$ mod p. If $p \equiv 1 \bmod 3$ is sufficiently large, then one can always choose an a such that $x^{(p+2)/3} + ax$ is a p.p. of $\mathbb{Z}/(p^e)$, $e \geqslant 1$.

The following result of Niederreiter and Robinson is relevant to Theorem 4. We use the notation of Theorem 4 and let $m = (q + k - 1)/k$ and $q \equiv 1 \bmod k$.

THEOREM 6 (Niederreiter and Robinson [15, Theorem 9]). *If* $m \geqslant 2$ *is not a power of the characteristic of* $\mathbb{F}_q$ *and* $q \geqslant (m^2 - 4m + 6)^2$, *then* $x^m + ax \in \mathbb{F}_q[x]$ *is not a p.p. of* $\mathbb{F}_q$ *for any* $a \neq 0$.

We see from this result that $x^m + ax \in \mathbb{F}_q[x]$ with $a \neq 0$ is not a p.p. of the extension field $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$ if $q^r \geqslant (m^2 - 4m + 6)^2$.

THE DICKSON POLYNOMIALS $g_k(x, a)$

The Dickson polynomial $g_k(x, a)$ of degree k over $\mathbb{F}_q$ is defined by

$$g_k(x, a) = \sum_{i=0}^{[k/2]} \frac{k}{k-i} \binom{k-i}{i} (-a)^i x^{k-2i},$$

where a is an element in $\mathbb{F}_q$. If u is an element of an extension of F_q and

*This has been shown independently by Daqing Wan for arbitrary prime p.

$u + a/u = x$, then we have

$$g_k\left(u+\frac{a}{u}, a\right) = u^k + \left(\frac{a}{u}\right)^k \tag{2}$$

by using Waring's formula; see [10]. It can be shown that the polynomials $g_k(x, a)$ are closed under composition if and only if $a = 1$, -1, or 0. If $a = 0$ then $g_k(x, a) = x^k$. If $a = 1$, then the Dickson polynomials $g_k(x, 1)$ are closely related to the classical Chebyshev polynomials of the first kind, $T_k(x)$, since $g_k(x, 1) = 2T_k(x/2)$. In recent years considerable attention has been given to the theory and applications of Dickson polynomials $g_k(x, a)$; for example, see [7], [8], [10], [11], [13], [17]. Brawley and Schnibben [4] studied Dickson polynomials in the wider context of establishing which Dickson polynomials give permutations on $n \times n$ matrices over arbitrary algebraic extensions of $\mathbb{F}_q$ (finite or infinite). We specialize their more general result for our purposes and state

THEOREM 7 (Brawley and Schnibben). *Let a be a nonzero element of $\mathbb{F}_q$; let $n > 1$ be an integer and $F = \mathbb{F}_q$. Then the Dickson polynomial $g_k(x, a)$ is a p.p. of $F_{n\times n}$ if and only if*

$$\left(k, q \operatorname*{lcm}_{1 \leqslant i \leqslant n} \{q^{2i} - 1\}\right) = 1. \tag{3}$$

Brawley [2] extended the investigations of permutations of the $n \times n$ matrices over $\mathbb{F}_q$ to permutations of the $n \times n$ matrices over a finite commutative ring R with identity. Each such R is a direct sum $R = L_1 + \cdots + L_t$ of local rings L_i. A local ring L is a finite commutative ring with identity which has a unique ideal M. Let the nilpotency be at least 2, and let $\mathbb{F}_p$ be the residue field. A polynomial $f(x) \in R[x]$ is a permutation of $R_{n\times n}$ if and only if each $f_i(x)$ is a permutation of $(L_i)_{n\times n}$ where $f_i(x) \in L_i[x]$ and $f(x) = f_1(x) + \cdots + f_t(x)$. The main result of [2] says that $f(x) \in L[x]$ is a p.p. of $L_{n\times n}$ if and only if

$$\bar{f}(x) \text{ is a p.p. of } \mathbb{F}_{p^i}, \qquad i = 1, 2, \dots, n; \tag{4.i}$$

$$\bar{f}'(x) = 0 \text{ has no roots in } \mathbb{F}_{p^i}, \qquad i = 1, 2, \dots, n. \tag{4.ii}$$

Here $f(x) \in L[x]$ maps to $\bar{f}(x)$ under the natural homomorphism $L \to \mathbb{F}_p$. In the special case $R = \mathbb{Z}_m$ we can show that some Dickson polynomials over R

are p.p. of $R_{n\times n}$. We note that if $m = p_1^{e_1} \cdots p_t^{e_t}$ is the prime factor decomposition of m, then

$$\mathbb{Z}_m = \mathbb{Z}_{p_1^{e_1}} + \cdots + \mathbb{Z}_{p_t^{e_t}}.$$

If $e > 1$, then the maximal ideal m of $\mathbb{Z}_{p^e}$ is (p) and $\mathbb{Z}_{p^e}/(p) = \mathbb{F}_p$. From Theorem 7 we know that $g_k(x,a)$, considered as a polynomial over $\mathbb{F}_p$, satisfies the conditions (4) if and only if the condition (3) holds with q a prime. Thus we have a set of new examples of p.p. on matrices over $\mathbb{Z}_m$.

THEOREM 8. *The Dickson polynomial $g_k(x,a) \in \mathbb{Z}_m[x]$, $a \neq 0$, is a p.p. of $R_{n\times n}$ for $R = \mathbb{Z}_m$ if and only if* (3) *holds for each prime q which divides m.*

THE DICKSON POLYNOMIALS $f_k(x,a)$

The polynomials $g_k(x,a)$ of the previous section are also referred to as Dickson polynomials of the first kind. In this final section we give some examples of permutations of $F_{n\times n}$ induced by Dickson polynomials of the second kind. We also state an open problem for those polynomials.

The Dickson polynomials of the second kind over $\mathbb{F}_q$ are denoted by $f_k(x,a)$ and defined as

$$f_k(x,a) = \sum_{i=0}^{[k/2]} \binom{k-i}{i} (-a)^i x^{k-2i}.$$

For $u \neq \pm 1$ and $x = u + a/u$ we can define $f_k(x,a)$ by the functional equation

$$f_k(x,a) = \frac{u^{k+1} - (a/u)^{k+1}}{u - a/u}$$

and

$$f_k(2\sqrt{a}, a) = (k+1)(\sqrt{a})^k, \qquad f_k(-2\sqrt{a}, a) = (-1)^k (k+1)(\sqrt{a})^k.$$

The polynomials $f_k(x,1)$ are closely related with the classical Chebyshev polynomials of the second kind. We note that $f_k(x,a)$ satisfies the recurrence relation

$$f_k(x,a) = xf_{k-1}(x,a) - af_{k-2}(x,a) \quad \text{with} \quad f_0(x,a) = 1 \quad \text{and} \quad f_1(x,a) = x.$$

Matthews [12] showed that the polynomial $f_k(x,1)$ is a p.p. of $\mathbb{F}_q$, q odd, if k satisfies the system of congruences

$$\begin{aligned} k+1 &\equiv \pm 2 \bmod p, \\ k+1 &\equiv \pm 2 \bmod \tfrac{1}{2}(q-1), \\ k+1 &\equiv \pm 2 \bmod \tfrac{1}{2}(q+1). \end{aligned} \tag{5}$$

See also Lidl [9].

In extensive computer experiments we established the existence of several examples of polynomials f_k which give permutations of $n \times n$ matrices over $\mathbb{F}_q$ for $n = 2$ and $n = 3$. We list a few numerical values. First we note that $f_1(x,a) = x$, so for $k = 1$ we obtain the identity map of $F_{n\times n}$. Let $a = 1$, and let $f_k(x,1)$ be abbreviated by f_k.

Example 9 (Dickson permutations f_k).

(i) Let $p = 3$ and $n = 2$. Then f_{21} is a p.p. of $F_{2\times 2}$ for $F = \mathbb{F}_3$. $k = 21$ is the smallest possible $k > 1$ for which f_k is a p.p. of $F_{2\times 2}$. This can be verified by using Theorem 1 in conjunction with (5).

(ii) Let $p = 5$ and $n = 2$. Then f_{417} is a p.p. of $F_{2\times 2}$ for $F = \mathbb{F}_5$. Here $k = 417$ is not the smallest possible $k > 1$ for which f_k is a p.p. of $F_{2\times 2}$. We can use (5) and Theorem 1 to verify that f_{417} is a p.p. Computer experiments showed that f_{57} is a p.p. of $F_{2\times 2}$, but $k = 57$ does not satisfy the conditions (5).

(iii) Let $p = 3$ and $n = 3$. Then f_{361} is a p.p. of $F_{3\times 3}$, as can be verified by applying Theorem 1 and (5). Here $k = 361$ is not the smallest possible $k > 1$ with this property. We found experimentally that f_{177} is a p.p. of $F_{3\times 3}$, but $k = 177$ does not satisfy (5).

From these examples it is clear that some f_k are p.p. of $F_{n\times n}$. It is an open problem to classify all of them. In the first instance one would need necessary and sufficient conditions for $f_k(x,a)$ to be a p.p. of $\mathbb{F}_q$. In the case of prime fields computer experiments suggest the following.

Conjecture. The conditions (5) are necessary and sufficient for f_k to be a p.p. of $\mathbb{F}_p$, p an odd prime.

REFERENCES

1 J. V. Brawley, The number of polynomial functions which permute the matrices over a finite field, *J. Combin. Theory* 21:147–154 (1976).
2 J. Brawley, Polynomials over a ring which permute the matrices over that ring, *J. Algebra* 38:93–99 (1976).
3 J. V. Brawley, L. Carlitz, and J. Levine, Scalar polynomial functions on the $n \times n$ matrices over a finite field, *Linear Algebra Appl.* 10:199–217 (1975).
4 J. Brawley and G. E. Schnibben, Polynomials which permute the matrices over a field, *Linear Algebra Appl.*, 86:145–160 (1987).
5 L. Carlitz, Some theorems on permutation polynomials, *Bull. Amer. Math. Soc.* 68:120–122 (1962).
6 L. Carlitz, Permutations in finite fields, *Acta Sci. Math. (Szeged)* 24:196–203 (1963).
7 H. Lausch, W. B. Müller, and W. Nöbauer, Über die Struktur einer durch Dicksonpolynome dargestellten Permutationsgruppe des Restklassenringes modulo n, *J. Reine Angew. Math.* 261:88–99 (1973).
8 H. Lausch and W. Nöbauer, *Algebra of Polynomials*, North Holland, Amsterdam, 1973.
9 R. Lidl, On cryptosystems based on polynomials and finite fields, in *Advances in Cryptology* (T. Beth, N. Cot, and I. Ingemarsson, Eds.), Lecture Notes in Comput. Sci., vol. 209, Springer, Berlin, 1985, pp. 10–15.
10 R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Vol. 20. Addison-Wesley, Reading, Mass., 1983.
11 R. Lidl and W. B. Müller, Permutation polynomials in RSA-cryptosystems, in *Advances in Cryptology*, Plenum, New York, 1984, pp. 293–301.
12 R. W. Matthews, Permutation Polynomials in One and Several Variables, Ph.D. Thesis, Univ. of Tasmania, Hobart, 1982.
13 W. B. Müller and W. Nöbauer, Some remarks on public key cryptosystems, *Studia Sci. Math. Hungar.* 16:71–76 (1981).
14 G. L. Mullen and H. Niederreiter, The structure of a group of permutation polynomials, *J. Austral. Math. Soc. Ser. A* 38:164–170 (1985).
15 H. Niederreiter and K. H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* 33:197–212 (1982).
16 W. Nöbauer, Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen, *Monatsh. Math.* 69:230–238 (1965).
17 R. Nöbauer, Über die Fixpunkte von durch Dicksonpolynome dargestellten Permutationen, *Acta Arith.* 45:91–99 (1985).

Received 9 December 1986; revised 22 December 1986