Linearized Polynomials and Permutation Polynomials of Finite Fields

RONALD J. EVANS, JOHN GREENE, & HARALD NIEDERREITER

1. Introduction

Let F_q be the finite field of order $q=p^m$, where $m>0$ and p is prime. A polynomial $f\in F_q[x]$ is called a *permutation polynomial* of F_q if the self-mapping of F_q induced by f is a bijection. We write P_q for the set of all permutation polynomials of F_q. Background information on permutation polynomials can be found in Lidl and Niederreiter [8, Ch. 7] and in the more recent survey article of Lidl and Mullen [7]. We note that $f\in F_q[x]$ and its reduction $\bmod(x^q-x)$ induce the same self-mapping of F_q; hence in the study of mapping properties of f we can always assume $\deg(f)<q$.

For various combinatorial applications, such as complete mappings and latin squares, it is of interest to study polynomials f for which $f(x)+cx\in P_q$ for several values of $c\in F_q$. See for example [1], [2], [3, Ch. 2], [4], [5], [9], [10], [11, Ch. 6], and [13] for such polynomials and their applications. In this connection, there arises the question of characterizing the polynomials f with the property that $f(x)+cx\in P_q$ for "many" values of $c\in F_q$. We prove the following result in this direction.

THEOREM 1. *Let $f\in F_q[x]$ with* $\deg(f)<q$ *be such that*

$$f(x)+cx\in P_q \quad \textit{for at least } [q/2] \textit{ values of } c\in F_q. \tag{1.1}$$

Then the following properties hold.

(1.2) *For every $c\in F_q$ for which $f(x)+cx\notin P_q$, the polynomial $f(x)+cx$ maps F_q into F_q in such a way that each of its values has a multiple of p (distinct) preimages.*
(1.3) *$f(x)+cx\in P_q$ for at least $q-(q-1)/(p-1)$ values of $c\in F_q$.*
(1.4) *$f(x)=ax+g(x^p)$ for some $a\in F_q$ and $g\in F_q[x]$.*

We note that (1.4) proves a conjecture of Stothers [12, p. 170] for all odd primes p. (In the statement of that conjecture, replace the misprints d_p and $(p-3)/2$ by d_q and $(q-3)/2$, respectively.)

Received August 16, 1990.
Michigan Math. J. 39 (1992).

For each q there are examples where (1.3) is "best possible", that is, $f(x)+cx \in P_q$ for exactly $q-(q-1)/(p-1)$ values of $c \in F_q$; see Section 4. For odd q, Theorem 1 is no longer valid if in the hypothesis (1.1) one replaces $[q/2]=(q-1)/2$ by $(q-3)/2$. To see this, note that $x^{(q+1)/2}+cx \in P_q$ for exactly $(q-3)/2$ values of $c \in F_q$ by [10, Thm. 5 and Rem. 1].

For any $g \in P_q$, if $f(x)+cx$ is replaced by $f(x)+cg(x)$ in (1.1), (1.2), and (1.3), then (1.1) still implies (1.2) and (1.3). This follows from Theorem 1 by carrying out the substitution $x=g^*(y)$ in $f(x)+cg(x)$, where g^* is a polynomial representing the inverse of the mapping induced by g (cf. [10, Prop. 1]).

Suppose that (1.2) holds. Then to each $c \in F_q$ for which $f(x)+cx \notin P_q$, there correspond at least $p-1$ distinct nonzero solutions $x \in F_q$ to $f(x)+cx = f(0)$; thus there are at most $(q-1)/(p-1)$ values of such c. This proves that (1.2) implies (1.3). Note also that (1.3) implies (1.1) when p is odd, since $q-(q-1)/(p-1) \geq (q+1)/2$ for $p>2$. By Theorem 1, (1.1) always implies (1.2), and so it follows that (1.1), (1.2), and (1.3) are all equivalent when $p>2$.

Suppose on the other hand that $f(x)=x^3$ and $q=2^k$ with $k \equiv 3 \pmod 6$. Then $f(x)+cx \in P_q$ for exactly one value of $c \in F_q$, namely $c=0$, while $f(x)+x=1$ has three distinct solutions in F_q. Thus (1.3) does not always imply (1.2) when $p=2$. Moreover, (1.2) does not always imply (1.1) when $p=2$; see Theorem 3.

As will be shown below, the following conjecture is stronger than Theorem 1.

CONJECTURE 2. *Let $f \in F_q[x]$ be such that $f(x)+cx \in P_q$ for at least $[q/2]$ values of $c \in F_q$. Then*

(1.5) $\qquad f(x)-f(0)$ *is a linearized p-polynomial over F_q.*

Here, as in [8, Def. 3.49], a polynomial over F_q is said to be a *linearized p-polynomial* over F_q if each of its terms has degree equal to a power of p.

Conjecture 2 is stronger than Theorem 1 in the sense that (1.5) implies the properties (1.2), (1.3), and (1.4). To verify this, we need only show that (1.5) implies (1.2). Suppose that $f(x)-f(0)$ is a linearized p-polynomial and that $f(x)+cx \notin P_q$ for some $c \in F_q$. The polynomial $f(x)+cx-f(0)$ induces a linear transformation of the F_p-vector space F_q into itself whose kernel K is a subspace of cardinality p^t for some $t>0$. For each value $b \in F_q$ of this transformation, there is a unique coset of K consisting of the preimages of b. Thus b has p^t preimages and (1.2) follows.

Suppose that Conjecture 2 is true. Then since (1.5) implies (1.2), it would follow that (1.1), (1.2), (1.3), and (1.5) are all equivalent when $p>2$.

In order to state the next theorem, we need the following notation. For an integer x, let $L(x)$ denote the least nonnegative residue of $x \pmod{q-1}$. For indeterminate y, positive integer n, and $f \in F_q[x]$, define $s_n = s_{n,f} \in F_q[y]$ by

$$s_n(y) = \sum_{b \in F_q} (f(b)+by)^n. \tag{1.6}$$

THEOREM 3. *Let $f(x)=x^e$ with $0<e<q$. If p is odd, the following five properties are equivalent.*

(1.7) *$f(x)+cx\in P_q$ for at least $[q/2]$ values of $c\in F_q$.*
(1.8) *$f(x)$ is a linearized p-polynomial; that is, e is a power of p.*
(1.9) *For every $c\in F_q$ for which $f(x)+cx\notin P_q$, the polynomial $f(x)+cx$ maps F_q into F_q in such a way that each of its values has a multiple of p preimages.*
(1.10) *$s_n(y)=0$ for each n, $1\le n\le q-2$.*
(1.11) *For each integer k with $1\le k\le q-2$, some p-adic digit of $L(k-ke)$ is less than the corresponding p-adic digit of k.*

If $p=2$, then (1.7)$\Rightarrow$(1.8)$\Rightarrow$(1.9)$\Leftrightarrow$(1.10)$\Leftrightarrow$(1.11), *but neither* (1.7) *nor* (1.9) *is necessarily equivalent to* (1.8).

Theorem 3 verifies Conjecture 2 in the case that $f(x)$ is a monomial. Theorem 1 verifies Conjecture 2 in the case $q=p$. (See also [12, Thm. 2].)

Theorems 1 and 3 will be proved in Sections 2 and 3, respectively. In Section 4, we discuss bounds on the number of $c\in F_q$ for which $f(x)+cx\in P_q$.

2. Proof of Theorem 1

The theorem is trivial for $q=2$, so we can assume $q\ge 3$. Replacing $f(x)$ by $f(x)-f(0)$, we can also assume that $f(0)=0$. With $s_n(y)$ defined by (1.6), we have $\deg(s_n)\le n-1$ for $1\le n\le q-2$. If $c\in F_q$ is such that $f(x)+cx\in P_q$, then

$$s_n(c)=\sum_{b\in F_q}(f(b)+bc)^n=\sum_{b\in F_q}b^n=0\quad\text{for } 1\le n\le q-2.$$

Hence if $f(x)+cx\in P_q$ for at least $[q/2]$ values of $c\in F_q$, then

(2.1) $$s_n=0\quad\text{for } 1\le n\le [q/2].$$

Define $a_j\in F_q[y]$, $0\le j\le q$, by the polynomial identity

(2.2) $$\prod_{b\in F_q}(z-f(b)-by)=\sum_{j=0}^{q}a_j(y)z^{q-j}$$

in the indeterminates y and z, so that in particular $a_0=1$ and $a_q=0$. For $1\le j\le q-1$, the coefficient of y^j in $a_j(y)$ equals the coefficient of z^{q-j} in

$$\prod_{b\in F_q}(z-b)=z^q-z.$$

Therefore $\deg(a_j)\le j-1$ for $1\le j\le q-2$. If $c\in F_q$ is such that $f(x)+cx\in P_q$, then the substitution $y=c$ in (2.2) yields $a_j(c)=0$ for $1\le j\le q-2$. Hence if $f(x)+cx\in P_q$ for at least $[q/2]$ values of $c\in F_q$, then

(2.3) $$a_j=0\quad\text{for } 1\le j\le [q/2].$$

By the Newton identities [8, Thm. 1.75] we have for arbitrary $c\in F_q$:

(2.4) $$\sum_{j=0}^{t-1}a_j(c)s_{t-j}(c)=-ta_t(c)\quad\text{for } t=1,2,\dots,q;$$

(2.5) $$\sum_{j=0}^{q} a_j(c)s_{q+k-j}(c)=0 \quad \text{for } k=1,2,\ldots.$$

By (2.1), (2.3), (2.4), and (2.5), we get for arbitrary $c\in F_q$:

(2.6) $$s_t(c)=-ta_t(c) \quad \text{for } t=1,2,\ldots,q;$$

(2.7) $$-s_{1+k}(c)=-s_{q+k}(c)=\sum_{j=[q/2]+1}^{q-1} a_j(c)s_{q+k-j}(c) \quad \text{for } k=1,2,\ldots.$$

Now fix $c\in F_q$. Assume first that

(2.8) $$a_j(c)=0 \quad \text{for } 1\le j\le q-2.$$

Then, by (2.6),

(2.9) $$s_n(c)=0 \quad \text{for } 1\le n\le q-2,$$

and by (2.7) with $k=q-2$ we obtain $-s_{q-1}(c)=a_{q-1}(c)s_{q-1}(c)$; hence

(2.10) $$a_{q-1}(c)=-1 \quad \text{or} \quad s_{q-1}(c)=0.$$

Next, assume that (2.8) fails to hold, so by (2.3) we have

(2.11) $$a_r(c)\ne 0 \quad \text{for some } r \text{ with } [q/2]+1\le r\le q-2,\ r \text{ minimal}.$$

Then we prove by induction that

(2.12) $$s_n(c)=0 \quad \text{for all } n\ge 1.$$

By (2.1) and the fact that $q-r\le[q/2]$, we have $s_n(c)=0$ for $1\le n\le q-r$. Assume that $s_n(c)=0$ for $1\le n\le N$ with some $N\ge q-r$. Then by (2.7) with $k=N-q+r+1$ and the minimality of r, we get

$$0=-s_{N-q+r+2}(c)=\sum_{j=r}^{q-1} a_j(c)s_{N+r+1-j}(c)=a_r(c)s_{N+1}(c);$$

thus $s_{N+1}(c)=0$ by (2.11), and the induction is complete.

We have now proved, in view of (2.6), (2.8), (2.9), (2.10), and (2.12), that for each fixed $c\in F_q$ we have either

(2.13) $$s_n(c)=0 \quad \text{for } 1\le n\le q-1$$

or

(2.14) $$a_n(c)=s_n(c)=0 \quad \text{for } 1\le n\le q-2 \quad \text{and} \quad a_{q-1}(c)=s_{q-1}(c)=-1.$$

In particular,

(2.15) $$s_n=0 \quad \text{for } 1\le n\le q-2.$$

If (2.14) holds for c, then the right-hand side of (2.2) with $y=c$ is z^q-z, so $f(x)+cx\in P_q$. If (2.13) holds for c, then by (2.6), the right-hand side of (2.2) with $y=c$ is a polynomial in z^p and thus equals a pth power of a polynomial in $F_q[z]$. This proves (1.2).

We noted in Section 1 that (1.2) implies (1.3), so it remains to prove (1.4). By (2.15),

$$\sum_{b\in F_q}\sum_{k=0}^{n}\binom{n}{k}(by)^{n-k}f(b)^k=0 \quad \text{for } 1\le n\le q-2;$$

equivalently,

$$\sum_{b\in F_q} b^{n-k}f(b)^k=0 \quad \text{if } 1\le k\le n\le q-2 \text{ and } p\nmid\binom{n}{k}. \tag{2.16}$$

Taking $k=1$ in (2.16), we get

$$\sum_{b\in F_q} b^{n-1}f(b)=0 \quad \text{if } 1\le n\le q-2 \text{ and } p\nmid n.$$

Thus $f(x)$ has no monomial of degree $q-n$ whenever $1\le n\le q-2$ and $p\nmid n$. This proves (1.4). □

3. Proof of Theorem 3

The following three lemmas will be used for the proof of Theorem 3. Throughout this section we may assume that $q>2$, as the results are trivial for $q=2$.

LEMMA 4. *For any $f\in F_q[x]$ with $\deg(f)<q$,* (1.9) *and* (1.10) *are equivalent.*

Proof. By the definition of $s_n(y)$ in (1.6), we see that (1.9) implies (1.10). Conversely, suppose that (1.10) holds. Then by the Newton identities (2.4),

$$s_t(c)=-ta_t(c) \quad \text{for } t=1,2,\dots,q, \text{ all } c\in F_q. \tag{3.1}$$

By the Newton identities (2.5), we see that for all $c\in F_q$,

$$a_j(c)s_{q-1}(c)=0 \quad \text{for } j=1,2,\dots,q-2, \tag{3.2}$$

and

$$a_{q-1}(c)s_{q-1}(c)+s_{q-1}(c)=0. \tag{3.3}$$

It follows from (3.1), (3.2), and (3.3) that for each fixed $c\in F_q$, either (2.13) or (2.14) holds. Finally, (1.9) holds by the argument used to prove (1.2) following (2.15). □

LEMMA 5. *Suppose that $f(x)=x^e$ with $0<e<q$. Then* (1.10) *and* (1.11) *are equivalent.*

Proof. In view of (2.16), we see that (1.10) holds if and only if

$$\sum_{b\in F_q} b^{n-k+ke}=0 \quad \text{whenever } 1\le k\le n\le q-2 \text{ and } p\nmid\binom{n}{k}.$$

Thus (1.10) holds if and only if

$$n \not\equiv k - ke \pmod{q-1} \quad \text{whenever } 1 \le k \le n \le q-2 \text{ and } p \nmid \binom{n}{k}.$$

Thus (1.10) fails to hold if and only if

$$p \nmid \binom{n}{k} \quad \text{with } n = L(k-ke), \text{ for some } k, 1 \le k \le q-2.$$

If we write the p-adic expansions of n, k as

$$n = \sum_{i \ge 0} n_i p^i, \qquad k = \sum_{i \ge 0} k_i p^i,$$

then [11, p. 19]

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1} \cdots \pmod{p},$$

so $p \nmid \binom{n}{k}$ if and only if $n_i \ge k_i$ for each i. Therefore (1.10) fails to hold if and only if there exists k, $1 \le k \le q-2$, such that $n_i \ge k_i$ for each i, with $n = L(k-ke)$. This proves the equivalence of (1.10) and (1.11). □

LEMMA 6. *Suppose that $0 < e < q$ and that $x^e + cx \in P_q$ for at least $[q/2]$ values of $c \in F_q$. Then e is a power of p.*

Proof. Define

$$V = \{c \in F_q : x^e + cx \in P_q\}, \qquad W = \{c \in F_q : x^e + cx \notin P_q\}.$$

If $c \in W$, each value of $x^e + cx$ has a multiple of p preimages, since (1.2) holds by Theorem 1. Therefore $0 \notin W$, so $x^e \in P_q$. Thus $(e, q-1) = 1$. We may now assume that $q > 3$; otherwise the result is clear.

Let $c \in F_q$. Observe that $c \in W$ if and only if $x^{e-1} = -c$ has nonzero solutions $x \in F_q$. Thus $c \in W$ if and only if $-c$ is a nonzero dth power in F_q, where $d = (e-1, q-1)$. Thus $\mathrm{card}(W) = (q-1)/d$, so $d > 1$ by the hypothesis of Lemma 6. By definition of W, we see that $c \in W$ if and only if $x^e + cx = 1 + c$ has solutions $x \ne 1$ in F_q. Thus $c \in W$ if and only if $(x^e - 1)/(x-1) = -c$ has solutions $x \ne 1$ in F_q. In particular $(u^e - 1)/(u-1)$ is a dth power in F_q for all $u \ne 1$ in F_q.

Let B be a multiplicative character on F_q (with $B(0) = 0$) and suppose that the order of B divides d. Then

$$\sum_{0 \ne u \in F_q} B(1-u^e)\bar{B}(1-u) = q-2, \tag{3.4}$$

where $\bar{B}$ denotes the inverse of B. For arbitrary multiplicative characters M, N on F_q, define the Gauss sum $G(M)$ and the Jacobi sum $J(M,N)$ by

$$G(M) = \sum_{u \in F_q} M(u)\zeta^{T(u)}, \qquad J(M,N) = \sum_{u \in F_q} M(u)N(1-u),$$

where $\zeta = \exp(2\pi i/p)$ and $T: F_q \to F_p$ is the trace map. For $y \in F_q$, it is easily proved that

$$(q-1)N(1-y) = \sum_M J(N,M)\bar{M}(y), \quad y \ne 0, \tag{3.5}$$

where the sum is over all $q-1$ characters M on F_q. (Formula (3.5) is a finite field analog of the binomial theorem.) By (3.4) and (3.5),

$$\sum_u \sum_M J(B,M)\bar{M}^e(u)\bar{B}(1-u) = (q-1)(q-2),$$

so

$$\sum_M J(B,M)J(\bar{B},\bar{M}^e) = (q-1)(q-2). \tag{3.6}$$

If each summand on the left-hand side of (3.6) is replaced by its absolute value, then the resulting sum equals $(q-1)(q-2)$; see [8, Thm. 5.22]. Hence $J(B,M) = J(B,M^e)$ for all M and for all B of order dividing d. Consequently, for all such M and B,

$$\frac{G(MB)}{G(M)} = \frac{G(M^eB)}{G(M^e)}; \tag{3.7}$$

see [8, Thm. 5.21]. In (3.7), take the product over all d characters B of order dividing d. It then follows from the Davenport–Hasse product formula [8, Cor. 5.29] that for all M,

$$G^d(M)/G(M^d) \sim G^d(M^e)/G(M^{ed}), \tag{3.8}$$

where the symbol $\sim$ denotes that the two sides of (3.8) have the same prime ideal factorization in the cyclotomic field $\mathbf{Q}(\exp(2\pi i/p(q-1)))$. For integer x, let $s(x)$ denote the sum of the p-adic digits of $L(x)$, where as before $L(x)$ denotes the least nonnegative integer congruent to $x (\bmod\, q-1)$. By (3.8) and Stickelberger's theorem [6, p. 212, Thm. 3], $ds(t) - s(td) = ds(et) - s(etd)$ for all integers t. In particular, for $t = d^n$,

$$ds(d^n) - s(d^{n+1}) = ds(ed^n) - s(ed^{n+1}) \quad \text{for } n = 0, 1, 2, \ldots .$$

Therefore, for all integers $n \geq 0$,

$$s(d^n)/d^n - s(d^{n+1})/d^{n+1} = s(ed^n)/d^n - s(ed^{n+1})/d^{n+1}.$$

Summing from $n = 0$ to $n = \infty$, we get $s(1) = s(e)$. Thus e is a power of p. $\square$

REMARK. Suppose that a pair of integers d, e satisfies $d > 1$, $d \mid (e-1)$, and $(e, q-1) = 1$. For $\theta = \exp(2\pi i/(q-1))$, define $\sigma \in \mathrm{Gal}(\mathbf{Q}(\theta)/\mathbf{Q})$ by $\sigma(\theta) = \theta^e$. Fix a character N on F_q of order $q-1$. The proof of Lemma 6 shows that if σ fixes $J(B, N^{d^n})$ for each B of order dividing d and each $n = 0, 1, 2, \ldots$, then e is a power of p. Thus the set of such $J(B, N^{d^n})$ generates the decomposition field in $\mathbf{Q}(\theta)$ for the prime p.

Proof of Theorem 3. Lemmas 4 and 5 show that (1.9), (1.10), and (1.11) are equivalent. Lemma 6 shows that (1.7) implies (1.8). It was shown in Section 1 that (1.5) ⇒ (1.2) ⇒ (1.3). Thus (1.8) implies (1.9) and, for odd p, (1.9) implies (1.7).

It remains to show that neither (1.7) nor (1.9) need be equivalent to (1.8) in the case $p = 2$. First suppose that $q = 8$, $e = 6$. For each integer k, $1 \leq k \leq 6$, some binary digit of $L(2k)$ is less than the corresponding binary digit of k. Thus (1.11) holds, so (1.9) holds. Therefore (1.9) is not equivalent to (1.8), since $e=6$ is not a power of 2. Finally, suppose that $q=4$, $e=2$. Then (1.8) holds. However, $x^2+cx\in P_q$ for exactly one value of $c\in F_q$, namely $c=0$, so that (1.7) fails to hold. □

4. The Number of c for which $f(x)+cx\in P_q$

We begin by discussing general upper bounds for the cardinality of the set $V(f)=\{c\in F_q: f(x)+cx\in P_q\}$. If $\deg(f)\le 1$, then $\operatorname{card}(V(f))=q-1$. Thus, in the sequel let $1<\deg(f)<q$ and suppose without loss of generality that $f(0)=0$. Define $U(f)=\{-f(b)/b: 0\ne b\in F_q\}$. If $c=-f(b)/b$ for some nonzero $b\in F_q$, then $f(x)+cx$ maps both 0 and b to 0, so $c\notin V(f)$. Thus $\operatorname{card}(V(f))\le q-\operatorname{card}(U(f))$. Since each element of $U(f)$ has at most $\deg(f)-1$ nonzero preimages under the map $-f(x)/x$,

$$\operatorname{card}(U(f))\ge\left\lceil\frac{q-1}{\deg(f)-1}\right\rceil.$$

Thus

$$\operatorname{card}(V(f))\le q-\left\lceil\frac{q-1}{\deg(f)-1}\right\rceil. \tag{4.1}$$

In the case $q=p>2$, Theorem 1 yields another upper bound, namely

$$\operatorname{card}(V(f))\le (q-3)/2 \quad \text{if } q=p>2. \tag{4.2}$$

Still another upper bound has been given by Chou [1, Thm. 2.3.3]:

$$\operatorname{card}(V(f))\le q-1-\deg(f). \tag{4.3}$$

A generalization of (4.3) for prime q has been given by Stothers [12, Thm. 1].

Note that $x^p+cx\notin P_q$ if and only if $x^p+cx=0$ has a nonzero solution $x\in F_q$. Thus $\operatorname{card}(V(f))=q-(q-1)/(p-1)$ when $f(x)=x^p$. This example shows that we can have equality in (4.1) for every q.

If p is odd, $x^{(q+1)/2}+cx\in P_q$ for exactly $(q-3)/2$ values of $c\in F_q$ by [10, Thm. 5 and Rem. 1]. This example shows that we may have equality in both (4.2) and (4.3) for all odd q. If q is a square and $e=\sqrt{q}$, then $x^e+cx\in P_q$ for exactly $q-1-e$ values of $c\in P_q$. This provides further examples where equality holds in (4.3).

Sometimes $\operatorname{card}(V(f))$ is quite small. If $f(x)=x^2$, for example, then $\operatorname{card}(V(f))=0$ for all odd q and $\operatorname{card}(V(f))=1$ for even q. Using deep methods, Cohen [2] has proved that if $f\in P_q$, $n=\deg(f)>1$, and $q=p>(n^2-3n+4)^2$, then $\operatorname{card}(V(f))=1$. For a related result involving monomials $f(x)$, see [10, Thm. 9].

Finally, we remark that if $\operatorname{card}(V(f))\ge[q/2]$ (as in Theorem 1), then $\operatorname{card}(V(f))\equiv -1 \pmod{p}$. To see this, suppose that $\operatorname{card}(V(f))\ge[q/2]$. Then (1.2) holds by Theorem 1, so for $c\in F_q$,

$$\sum_{0\neq x\in F_q}(f(x)+cx)^{q-1}=\begin{cases}0 & \text{if } c\notin V(f),\\ q-1 & \text{if } c\in V(f).\end{cases}$$

Thus

$$\begin{aligned}-\operatorname{card}(V(f)) &= \sum_{c\in F_q}\sum_{0\neq x\in F_q}(f(x)+cx)^{q-1}\\ &= \sum_{0\neq x\in F_q}\sum_{c\in F_q}(f(x)+cx)^{q-1}=\sum_{0\neq x\in F_q}(q-1)\equiv 1(\operatorname{mod} p).\end{aligned}$$

References

1. W.-S. Chou, *Permutation polynomials on finite fields and combinatorial applications,* Ph.D. thesis, Penn. State Univ., 1990.
2. S. D. Cohen, *Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials,* Canad. Math. Bull. 33 (1990), 230–234.
3. J. Denes and A. D. Keedwell, *Latin squares,* Ann. Discrete Math., 46, North-Holland, Amsterdam, 1991.
4. A. B. Evans, *Generating orthomorphisms of* $GF(q)^+$, Discrete Math. 63 (1987), 21–26.
5. ———, *Orthomorphisms of* $GF(q)^+$, Ars Combin. 27 (1989), 121–131.
6. K. Ireland and M. Rosen, *A classical introduction to modern number theory,* Springer, New York, 1982.
7. R. Lidl and G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field?* Amer. Math. Monthly 95 (1988), 243–246.
8. R. Lidl and H. Niederreiter, *Finite fields,* Addison-Wesley, Reading, MA, 1983.
9. G. L. Mullen and H. Niederreiter, *Dickson polynomials over finite fields and complete mappings,* Canad. Math. Bull. 30 (1987), 19–27.
10. H. Niederreiter and K. H. Robinson, *Complete mappings of finite fields,* J. Austral. Math. Soc. Ser. A 33 (1982), 197–212.
11. L. Rédei, *Lacunary polynomials over finite fields,* North-Holland, Amsterdam, 1973.
12. W. W. Stothers, *On permutation polynomials whose difference is linear,* Glasgow Math. J. 32 (1990), 165–171.
13. D. Q. Wan, *On a problem of Niederreiter and Robinson about finite fields,* J. Austral. Math. Soc. Ser. A 41 (1986), 336–338.

Ronald J. Evans
Department of Mathematics
University of California, San Diego
La Jolla, CA 92093-0112

John Greene
Department of Mathematics
University of Minnesota, Duluth
Duluth, MN 55812

Harald Niederreiter
Institute for Information Processing
Austrian Academy of Sciences
Sonnenfelsgasse 19
A-1010 Vienna
Austria