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 $\mathrm{mod}(x^q - x)$ 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*

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

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).