# POLYNOMIALS WITH MINIMAL VALUE SETS

W. H. MILLS

Let $\mathscr{K}$ be a finite field of characteristic $p$ that contains exactly $q$ elements. Let $F(x)$ be a polynomial over $\mathscr{K}$ of degree $f, f > 0$, and let $r + 1$ denote the number of distinct values $F(\tau)$ as $\tau$ ranges over $\mathscr{K}$. Carlitz, Lewis, Mills, and Straus [1] pointed out that $r \geqq [(q-1)/f]$, and raised the question of determining all polynomials for which $r = [(q-1)/f]$. The cases $r = 0$ and $r = 1$ are special cases that do not fit into the general pattern. These are treated in [1], and do not concern us here. Thus we arrive at the statement of our main problem: For what polynomials $F(x)$ do we have

$$r = [(q-1)/f] \geqq 2? \tag{I}$$

Carlitz, Lewis, Mills, and Straus [1] determined all polynomials with $f < 2p + 2$ for which (I) holds. In the present paper this result is extended—all polynomials with $f \leqq \sqrt{q}$ for which (I) holds are determined. These are polynomials of the form

$$F(x) = \alpha L^v + \gamma ,$$

where $L$ is a polynomial that factors into distinct linear factors over $\mathscr{K}$ and that has the form

$$L = \beta + \sum_i \varphi_i x^{p^{ki}} ,$$

and where $v$ and $k$ are integers such that $v \mid (p^k - 1)$ and $q$ is a power of $p^k$. Regardless of the size of $f$ our present methods give a great deal of information about $F(x)$. Furthermore many of the proofs of [1] can be shortened and simplified by using the results of § 1 of the present paper.

The results of [1] provide a complete answer for the case $q = p$. In the present paper the problem is completely solved for the case $q = p^2$.

**1. Preliminaries.** Let $\mathscr{K}$ be a finite field with $q$ elements and characteristic $p$. We use Greek letters for elements of $\mathscr{K}$, and small Latin letters, other than $x$, for nonnegative integers. We use capital letters for polynomials in one variable over $\mathscr{K}$. The polynomials denoted by $A, B, C, D, E$ and the integers denoted by $a, b, c, d, e$

Received May 1, 1963. Presented to the American Mathematical Society March 4, 1963. This work was partially supported by the National Science Foundation under NSF Grant 18916.