POLYNOMIALS WITH MINIMAL VALUE SETS

WILLIAM H. MILLS
POLYNOMIALS WITH MINIMAL VALUE SETS

W. H. MILLS

Let $\mathbb{F}$ be a finite field of characteristic $p$ that contains exactly $q$ elements. Let $F(x)$ be a polynomial over $\mathbb{F}$ of degree $f$, $f > 0$, and let $r + 1$ denote the number of distinct values $F(\tau)$ as $\tau$ ranges over $\mathbb{F}$. Carlitz, Lewis, Mills, and Straus [1] pointed out that $r \geq [\frac{(q - 1)}{f}]$, and raised the question of determining all polynomials for which $r = [\frac{(q - 1)}{f}]$. 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

(1) \hspace{1cm} r = [\frac{(q - 1)}{f}] \geq 2?

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

$L = \beta + \sum_i \phi_i x^{p^k i}$,

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 $q = p^s$.

1. Preliminaries. Let $\mathbb{F}$ be a finite field with $q$ elements and characteristic $p$. We use Greek letters for elements of $\mathbb{F}$, and small Latin letters, other than $x$, for nonnegative integers. We use capital letters for polynomials in one variable over $\mathbb{F}$. The polynomials denoted by $A, B, C, D, E$ and the integers denoted by $a, b, c, d, e$
vary from proof to proof. The polynomials and integers denoted by other letters, except \( i \) and \( j \), remain the same throughout the paper.

Let \( F = F(x) \) be a polynomial over \( \mathcal{K} \) of degree \( f, f > 0 \). Let \( \gamma_0, \gamma_1, \ldots, \gamma_r \) denote the distinct values assumed by \( F(\tau) \) as \( \tau \) ranges over \( \mathcal{K} \). It follows easily from the fact that a polynomial of degree \( f \) has at most \( f \) roots, that \( r + 1 \geq q/f \). This is equivalent to \( r \geq [(q - 1)/f] \). We intend to study the question raised in [1] of characterizing those polynomials for which \( r = [(q - 1)/f] \). The cases \( r = 0 \) and \( r = 1 \) were fully treated in [1]. Hence we make the assumption that

\[(1) \quad r = [(q - 1)/f] \geq 2.\]

Subtracting the constant \( \gamma_0 \) from \( F \) does not change the value of \( r \). Thus it is sufficient to consider the case \( \gamma_0 = 0 \). In the first two sections of this paper, we assume that

\[ \gamma_0 = 0. \]

Then \( \gamma_i \neq 0 \) for \( i > 0 \). We now set

\[ F_i = F - \gamma_i, \quad 0 \leq i \leq r. \]

The polynomials \( F_i \) are relatively prime in pairs, and each of them has at least one root in \( \mathcal{K} \). Let \( \pi_{i_1}, \pi_{i_2}, \ldots, \pi_{i_r} \) be the distinct roots of \( F_i \) that lie in \( \mathcal{K} \) and set

\[ L_i = \prod_{j=1}^{i} (x - \pi_{i_j}), \quad 0 \leq i \leq r. \]

Then \( l_i = \deg L_i \geq 1, 0 \leq i \leq r \), and\(^1\)

\[(2) \quad x^q - x = \prod_{i=0}^{r} L_i.\]

Now set \( F_i = L_i U_i, 0 \leq i \leq r \), and

\[(3) \quad G = \prod_{i=0}^{r} U_i.\]

Then the \( L_i \), the \( U_i \) and \( G \) are polynomials over \( \mathcal{K} \), and

\[(4) \quad (x^q - x)G = \prod_{i=0}^{r} F_i.\]

Now (4) and (1) give us an upper bound on the degree of \( G \), namely

\[ \deg G = (r+1)f - q \leq q - 1 + f - q = f - 1. \]

\(^1\) The relations (2), (3), (4), (5), (6), and (7) can all be found in [1] under the assumption that the leading coefficient of \( F \) is 1.
Thus we have
\[ \deg G < f. \]

Set \( u_i = \deg U_i, 0 \leq i \leq r \). We already have \( F = F_0 \) by the assumption \( \gamma_0 = 0 \). We set \( L = L_0, U = U_0, l = l_0, \) and \( u = u_0 \).

We now differentiate both sides of (2) and obtain \(-1 \equiv L'L^* \pmod{L} \), where \( L^* = L_1L_2 \cdots L_r \). Hence \( G = -L'L^*G \pmod{LG} \).

Since \( F = LU \) and \( U | G \), it follows that \( F | LG \) and thus
\[ G \equiv -L'L^*G \pmod{F}. \]

Now
\[ L^*G = U \prod_{i=1}^r (L_iU_i) = U \prod_{i=1}^r (F - \gamma_i) = -\zeta U \pmod{F}, \]

where
\[ \zeta = -\prod_{i=1}^r (-\gamma_i) \neq 0. \]

Hence \( G \equiv \zeta L'U \pmod{F} \). Since \( \deg (\zeta L'U) < \deg (LU) = f \) and \( \deg G < f \), we must have
\[ G = \zeta L'U. \]

By symmetry it follows that
\[ G = \zeta_i L_i U_i, \quad 0 \leq i \leq r, \]

for suitable nonzero elements \( \zeta_i \) of \( \mathcal{K} \).

We next derive another expression for \( G \).

**Lemma 1.** There exists a nonzero element \( \theta \) in \( \mathcal{K} \) such that \( G = \theta F' \).

**Proof.** Since \( F' = F' = L_i U_i + L_i U_i', \) it follows from (7) that
\[ L_i U_i' = F - G \zeta_i, \quad 0 \leq i \leq r. \]

Therefore \( L_0 U_0' = L U', L_1 U_1', \) and \( L_0 U_0' \) are linearly dependent. Thus there exist \( \lambda, \lambda_1, \) and \( \lambda_2 \) in \( \mathcal{K} \), not all zero, such that
\[ \lambda L U' + \lambda_1 L_1 U_1' + \lambda_2 L_2 U_2' = 0. \]

Multiplying this relation by \( U U_1 U_2 \) and noting that \( LU = F, L_1 U_1 = F - \gamma_1, L_2 U_2 = F - \gamma_2 \), we obtain
\[ (\lambda U' U_1 U_2 + \lambda_1 U U_1' U_2 + \lambda_2 U U_1 U_2') F = \lambda_1 \gamma_1 U U_1' U_2 + \lambda_2 \gamma_2 U U_1 U_2'. \]

Now the degree of the right side of (8) is less than \( u + u_1 + u_2 \) and
This is possible only if we have
\[(9) \quad \lambda U' U_1 U_2 + \lambda \n U_1 U_2 + \lambda_2 U_2 U'_2 = 0.\]
The constants \(\lambda, \lambda_1,\) and \(\lambda_2\) are not all zero. Without loss of generality we suppose \(\lambda_2 \neq 0.\) Then (9) gives us \(U_2 \mid U U_1 U'_2.\) Since \(U_2 \mid F_2,\) \(U_2\) must be relatively prime to both \(F\) and \(F'.\) Hence \(U_2\) is relatively prime to \(U U_1,\) and \(U_2 \mid U'_2.\) This implies that \(U'_2 = 0.\) Hence
\[F' = F'_2 = L' U_2 + L_2 U'_2 = L_2 U_2 = G/\zeta_2.\]
Thus \(G = \zeta_2 F',\) which completes this proof.

Lemma 1 is false for \(r \leq 1—\)counter examples can be readily constructed.

**Lemma 2.** For each \(j, 0 \leq j \leq r,\) \(U_j\) is of the form
\[U_j = L_j w_j H_j,\]
where \(w_j\) is a nonnegative integer, \(H_j\) is a polynomial over \(\mathcal{A},\) and \(L_j \mid H_j.\)

**Proof.** By symmetry it is sufficient to prove the lemma for the case \(j = 0.\) Combining (6) with Lemma 1 we obtain
\[\zeta L' U = G = \theta F' = \theta L' U + \theta U' .\]
Thus
\[(10) \quad \theta U' = (\zeta - \theta)L' U .\]
We set \(U = L^w A,\) where \(L \nmid A\) and \(w \geq 0.\) Then substitution in (10) gives us
\[\theta w L^w L' A + \theta L^{w+1} A' = (\zeta - \theta) L L^w A.\]
This reduces to
\[\theta L A' = (\zeta - \theta - w \theta) L' A.\]
Thus \(L \mid (\zeta - \theta - w \theta) L' A.\) Since \(L\) is the product of distinct linear factors, it follows that \(L\) and \(L'\) are relatively prime. Since \(L \nmid A,\) this implies that \(\zeta - \theta - w \theta = 0.\) Therefore \(\theta L A' = 0.\) It follows that \(A' = 0.\) Hence \(A = H^w\) for some polynomial \(H.\) Then we have \(L \nmid H\) and \(U = L^w H^w,\) which completes this proof.

We now suppose, without loss of generality, that
\[(11) \quad l \leq l_j, \quad 0 \leq j \leq r.\]
**Lemma 3.** Under the assumption (11), the constants $w_j$ of Lemma 2 satisfy

$$w_1 = w_2 = \cdots = w_r = 0.$$ 

**Proof.** Combining (3) and (6) we obtain

$$\zeta L'U = G = UU_1U_2\cdots U_r.$$ 

Now suppose $1 \leq j \leq r$. Then $U_j \mid L'$, and hence

$$u_j \leq \deg L' < l \leq l_j.$$ 

Therefore $L_j \not\mid U_j$, so that we have $w_j = 0$. This completes the proof.

Set $H = H_0$ and $v = w_0 + 1$. Then from Lemmas 2 and 3 we obtain

(12) \[ F = LU = L^vH^v, \]

and

(13) \[ F_i = L_iU_i = L_iH_i^v, \quad 1 \leq i \leq r, \]

where $L \mid H$, $L_i \mid H_i$. Moreover

$$\zeta L' = G \mid U = U_1U_2\cdots U_r = (H_1H_2\cdots H_r)^v.$$ 

Thus $L' = S^v$, where $S = \zeta^{-1}H_1H_2\cdots H_r$. Therefore $L$ is of the form

(14) \[ L = xS^v + T^v, \]

where $T$, as well as $S$, is a polynomial over $\mathbb{K}$.

2. The polynomial $R(x)$. Set

$$R(x) = \prod_{i=1}^r (x - \gamma_i) = \sum_{j=0}^r \rho_j x^j,$$

where $\rho_j \in \mathbb{K}$, $0 \leq j \leq r$, $\rho_r = 1$. From (4) and (6) we obtain

$$LUR(F) = FR(F) = \prod_{i=0}^r F_i = (x^q - x)G = \zeta(x^q - x)L'U.$$ 

These identities and (12) give us

(15) \[ \sum_{j=0}^r \rho_j L^{i+j}H^{pj} = LR(F) = \zeta(x^q - x)L'. \]

Differentiating both sides of (15) and noting that $L'' = 0$ by (14), we get the congruence
\[ \rho \sigma L' \equiv -\zeta L' \pmod{L}. \]

Since \( L' \neq 0 \), we obtain

\[ (16) \quad \rho \sigma = -\zeta . \]

By Lemma 1 we have \( F'' = G\theta \not\equiv 0 \). Hence \( p \not| v \).

Let \( k \) be the smallest positive integer such that \( v \mid (p^k - 1) \). The main objective of this section is to show that \( 1 + vj \) is a power of \( p^k \) for every nonzero coefficient \( \rho_j \) of \( R(x) \).

In the proof of the following lemma the notation \( A \| B \) means that \( A \mid B \) and \((A, B/A) = 1\).

**Lemma 4.** Let \( d \) be a nonnegative integer such that \( L' \) is a \( p^d \)th power and \( 1 + vr > p^{d-1} \). If \( j \) is an integer such that \( \rho_j \neq 0 \), then either (i) \( 1 + vj \) is a power of \( p^k \), or (ii) \( p^a \mid (1 + vj) \). Moreover \( H \) is a \( p^d \)st power.

**Proof by induction on \( d \).** The desired result is trivial for \( d = 0 \). We suppose that it is true for an integer \( d \) and show that this implies that it is true for \( d + 1 \). Thus we assume that \( L' \) is a \( p^d \)st power and \( 1 + vr > p^d \). Then the induction hypothesis applies so that \( R(x) \) is of the form

\[ (17) \quad R(x) = \sum_{i=0}^{c} \omega_i x^{(p^k-1)/r} + \sum' \rho_j x^j , \]

where \( \omega_i \in \mathbb{K} \), \( 0 \leq i \leq c \), \( c = \lfloor d/k \rfloor \), and the second summation \( \sum' \) is over all \( j \) such that

\[ p^a \mid (1 + vj) , \quad p^a < 1 + vj , \quad j \leq r . \]

Moreover \( H \) is a \( p^{d-1} \)st power. Thus

\[ H = A^{p^d} \quad \text{and} \quad F = L^* A^{p^d} \]

for some polynomial \( A \) over \( \mathbb{K} \). Substitution in (15) gives us

\[ (18) \quad \sum' \rho_j L^{1+vj} A^{p^d} = \zeta x^r L' + B , \]

where

\[ B = -\zeta x L' - \sum_{i=0}^{c} \omega_i L^{p^i} A^{p^d((p^k-1)/r)} . \]

The left side of (18) is a \( p^d \)th power. Since

\[ q \geq 1 + fr \geq 1 + vr > p^d \]

and \( q \) is a power of \( p \), it follows that \( p^{d+1} \mid q \). Hence \( \zeta x^r L' \) is a \( p^{d+1} \)st power. Therefore \( B \) is a \( p^d \)th power. Thus we can set
$\zeta x^q L' = C^{pd+1}$ and $B = D^d$.

Since $1 + vr > p^d$ and $\rho_r \neq 0$, it follows that the left side of (18) does not vanish identically. Let the term corresponding to $j = a$ be the nonzero term of lowest degree in the left side of (18). Thus $a$ is the least integer such that $\rho_a \neq 0$ and $1 + va > p^d$. Then $p^d \mid (1 + va)$, and hence $1 + va \geq 2p^d$. Because of the way $a$ was chosen we have

$$L^{1+va}A^{apd} \parallel (\zeta x^qL' + B).$$

Extracting the $p^d$th roots of both sides of (19) we get

$$L^{1+va}A^{apd} \parallel (C^p + D).$$

Since $1 + va \geq 2p^d$ this gives us $L^2A^a \mid (C^p + D)$. By differentiation we obtain

$$LA^{a-1} \mid D'.$$

Now

$$\deg D' < p^{-d} \deg B \leq p^{-d} \deg \{L^{p^d}A^{pd(p^{d-1})/v}\} \leq \deg \{LA^{(p^{d-1})/v}\}.$$

Since

$$a > (p^d - 1)/v \geq (p^k - 1)/v,$$

we have $(p^k - 1)/v \leq a - 1$, and

$$\deg D' < \deg (LA^{a-1}).$$

Combining this with (20) we get $D' = 0$. Thus $D$ must be a $p$th power, and $B$ a $p^{d+1}$st power. Thus the right side of (19) is a $p^{d+1}$st power. Hence the left side of (19) is also a $p^{d+1}$st power. Now $L \nmid H$. Since $L$ is the product of distinct linear factors we have $L \nmid A$, $p^{d+1} \mid (1 + va)$, and $A^a$ is a $p$th power. Hence $p \nmid a$, and $A$ itself is a $p$th power. It follows that $H$ is a $p^d$th power. Suppose there is a $b$ such that $\rho_b \neq 0$, $1 + vb$ is not a power of $p^k$, and $p^{d+1} \mid (1 + vb)$. Without loss of generality suppose that $b$ is the smallest integer with these properties. By (17) we have $1 + vb > p^d$, and by (18) we have

$$L^{1+vb}A^{bpd} \parallel \{\zeta x^qL' + B - \Sigma''\rho_jL^{1+sj}A^{jpd}\},$$

where $\Sigma''$ is over those $j$ such that $j < b$, $p^{d+1} \mid (1 + vj)$. The right side of (21) is a $p^{d+1}$st power. Hence the left side of (21) is also a $p^{d+1}$st power. Therefore $p^{d+1} \mid (1 + vb)$, a contradiction. It follows that for every $j$ such that $\rho_j \neq 0$, either $1 + vj$ is a power of $p^k$ or $p^{d+1} \mid (1 + vj)$. This establishes the desired result for $d + 1$, and
completes this proof.

**Lemma 5.** Suppose there exists an integer $d$ such that $L'$ is a $p^d$th power but not a $p^{d+1}$st power, and $1 + vr > p^d$. Then $v = 1$ and $p^{d+1} \not| (1 + r)$.

**Proof.** Since $L'$ is a $p$th power by (14), we have $d \geq 1$. By Lemma 4 we have

$$R(x) = \sum_{i=0}^{e} \omega_i x^{(p^d-1)\nu} + \sum^* \rho_i x^i + w^r,$$

where the $\omega_i$ are elements of $\mathcal{H}$, $c = [d/k]$, and the summation $\sum^*$ is over all $j$ such that $p^d \mid (1 + vr)$, $p^d < 1 + vj$, $j < r$. Moreover since $1 + vr > p^d$ and $\rho_r \neq 0$, we have $p^d \mid (1 + vr)$. Furthermore $H$ is a $p^{d-1}$st power. Since $\zeta \in \mathcal{H}$, it follows that $\zeta L'$ is a $p^d$th power but not a $p^{d+1}$st power. Thus we can set

$$H = A^{p^{d-1}}$$

and $\zeta L' = C^d$,

where $C$ is not a $p$th power. Substitution in (15) gives us

(22) $$L^{1+vr}A^{pd} = x^dC^d + B,$$

where

$$B = -\zeta xL' - LR(F) + LF^r$$

$$= -\zeta xL' - \sum_{i=0}^{e} \omega_i L^{ik} A^{pd(p^d-1)/a} - \sum^* \rho_i L^{1+vr} A^{pd}.$$

Now the left side of (22) is a $p^d$th power. Moreover

$$q \geq 1 + fr \geq 1 + vr > p^d,$$

so that $p^{d+1} \mid q$. Therefore $B$ is a $p^d$th power, say $B = D^{p^d}$. Extracting the $p^d$th roots of both sides of (22) we obtain

(23) $$L^{(1+vr)p^{-d}} A^{1-1} = x^{p^{-d}}C + D.$$

Differentiation now yields

(24) $$L^{-1+(1+vr)p^{-d}} A^{r-1}((1 + vr)p^{-d} L'A + rLA') = x^{p^{-d}}C' + D'.$$

since $p^{d+1} \mid q$. Multiplying (24) by $C$, (23) by $C'$, and subtracting, we get

(25) $$L^{-1+(1+vr)p^{-d}} A^{r-1} E = CD' - C'D,$$

where

$$E = (1 + vr)p^{-d} L'AC + rLA'C - LAC'.$$
Now $A | H$ and therefore $LA | F$. Moreover

$$C | L' = G/\langle \zeta U \rangle = \zeta^{-1}U_1U_2 \cdots U_r | F_1F_2 \cdots F_r.$$ 

Hence $C$ is relatively prime to $LA$. Since $C$ is not a $p$th power we have $C' \neq 0$. Hence $C \not| LA'C'$. It follows that $E \neq 0$. From (25) we obtain $CD' \neq C'D$ and

$$(26) \quad L^{-\frac{e}{d+1}r-1} (CD' - C'D),$$

where

$$e = \begin{cases} 
0 & \text{if } p^{d+1} | (1 + vr), \\
1 & \text{if } p^{d+1} \not| (1 + vr). 
\end{cases}$$

Comparing degrees in (26) we obtain

$$(27) \quad (1 + vr - ep^d)l + p^d(r - 1) \deg A < p^d \deg (CD) = \deg (L'B).$$

Now the leading term of $R(x)$ is $x^r$ and $R(x) \not= x^r$. Set $b = \deg \{R(x) - x^r\}$. Then we have $0 \leq b < r$ and

$$\deg B \leq \deg (LF^b) = (1 + vb)l + bp^d \deg A \leq (1 + vb)l + (r - 1)p^d \deg A.$$ 

Substitution in (27) gives us, after simplification,

$$v(r - b)l < ep^d l + \deg L' < (ep^d + 1)l.$$ 

Hence $v(r - b) \leq ep^d$. Therefore $e \neq 0$. Hence $e = 1$ and

$$v(r - b) \leq p^d.$$ 

Since $p^d | (1 + vr)$ and $1 + vr > p^d$, we have $1 + vr \geq 2p^d$ and

$$1 + vb = 1 + vr - v(r - b) \geq p^d.$$ 

Since $\rho_b \neq 0$, this gives us $p^d | (1 + vb)$. Since $p^d | (1 + vr)$, it follows that $p^d | v(r - b)$ and $p \not| v$. Hence $v(r - b) = p^d$ and $v = 1$. Finally since $e = 1$ we have

$$p^{d+1} \not| (1 + vr) = 1 + r,$$

which completes this proof.

**Lemma 6.** If $d$ is an integer such that $p^d < 1 + vr$, then $L'$ is a $p^{d+1}$st power.

**Proof.** Suppose the result is false. Then $L'$ is not a $p^{d+1}$st power and $p^d < 1 + vr$. Without loss of generality we suppose that $L'$ is a $p^d$th power. By Lemma 5 we have $v = 1$ and $p^{d+1} \not| (1 + r)$. 


Therefore $k = 1$ and $p^a < 1 + r$. It follows from Lemma 4 that $R(x)$ is of the form

$$R(x) = \sum_{i=0}^{\xi-1} \omega_i x^{\xi^i-1} + \sum^+ \rho_j x^j,$$

where the summation $\sum^+$ is over all $j$ such that $p^d | (1 + j)$, $j \leq r$. Moreover $H$ is a $p^{d-1}$st power and $p^d | (1 + r)$. Now

$$FR(F) = \prod_{i=0}^{\xi} (F - \gamma_i) = \prod_{i=0}^{\xi} F_i = (x^a - x)G$$

by (4), so that

(28) \[ \sum^+ \rho_j F_i^{j+1} = x^a G + B, \]

where $deg B \leq p^d - f$. The left side of (28) is a $p^a$th power. Moreover $q \geq 1 + f \geq 1 + r > p^d$, so that $x^a$ is a $p^{d+1}$st power. Since $G = \zeta L'U$ and $U = L^{-1}H^p = H^p$, it follows that $G$ is a $p^a$th power. Hence $B$ is also a $p^a$th power. We set

$$G = C^{p^a} \quad \text{and} \quad B = D^{p^a}.$$ 

Then, extracting the $p^a$th roots of both sides of (28), we get

(29) \[ \sum_{j=1}^{p^a} \xi_j F_j = x^{p^a - d} C + D, \]

where $a = (r + 1)p^{-a} \geq 2$, the $\xi_j$ are in $\mathbb{N}$, $\xi_a = 1$, and $deg D \leq f/p$. Now $p \nmid a$ since $p^{a+1} \nmid (r + 1)$. We set $\bar{F} = F + \xi_{a-1}a$. Then (29) becomes

(30) \[ \sum_{j=0}^{a} \eta_j \bar{F}_j^{j+1} = x^{p^a - d} C + D, \]

where the $\eta_j$ are in $\mathbb{N}$, $\eta_a = 1$, and $\eta_{a-1} = 0$. Differentiating (30) we obtain

(31) \[ \sum_{j=1}^{a} \eta_j \bar{F}_j^{j-1} \bar{F}' = x^{p^a - d} C' + D'. \]

Eliminating $x^{p^a - d}$ from (30) and (31) we get

$$\eta_0 C' + \sum_{j=1}^{a} \eta_j \bar{F}_j^{j-1} (C' \bar{F} - jC\bar{F}') = C'D - CD'. \]

Since $\eta_{a-1} = 0$, it follows that

(32) \[ \bar{F}^{a-1}(C' \bar{F} - aC\bar{F}') = C'D - CD' - E, \]

where

$$deg E < (a - 2)f + \deg C.$$
Now
\[ \deg C = p^{-a} \deg G < p^{-a}f \leq f/p \]
by (5). Hence \( \deg E < (a - 1)f \), and
\[ \deg (C'D - CD') < \deg (CD) < 2f/p \leq (a - 1)f . \]
Therefore
\[ \deg (C'D - CD' - E) < (a - 1)f = \deg F'^{a-1} , \]
and (32) yields
\[ C'F = aCF' . \]
Now \( F' = F'' = \theta^{-G} \neq 0 \) by Lemma 1. Therefore \( aCF' \neq 0 \). Hence \( C' \neq 0 \) and thus \( C \nmid C' \). It follows that \( (\bar{F}, C) \neq 1 \). Since
\[ C'^d = G = \prod U_i \]
we have \( (\bar{F}, U_b) \neq 1 \) for some \( b, 0 \leq b \leq r \). Hence \( (\bar{F}, F_b) \neq 1 \). Since \( \bar{F} - F_b \in \mathcal{K} \), we must have \( \bar{F} = F_b \). Therefore
\[ C'F_b = aCF'_b . \]
Since \( v = 1 \), we have \( F_b = L_bH_b^\gamma \), whether or not \( b = 0 \). Hence
\[ C'L_bH_b^\gamma = aCL_bH_b^\gamma , \]
and \( C'L_b = aCL_b^\gamma \). Now \( L_b \) is relatively prime to \( L_b \). Therefore \( L_b \mid C \). Since \( v = 1 \) we have
\[ C'^d = G = \prod U_i = \prod H_i^\gamma . \]
It follows that \( L_b \mid H_bH_1 \cdots H_r \). On the other hand \( L_b \nmid H_b \), while for \( i \neq b \) we have \( (L_b, H_i) = 1 \). Therefore \( L_b \nmid H_bH_1 \cdots H_r \), a contradiction. This completes the proof of this lemma.

We are now in a position to prove the most general theorem of this paper. We drop the assumption \( \gamma_0 = 0 \).

**Theorem 1.** Let \( \mathcal{K} \) be a finite field of characteristic \( p \) that contains exactly \( q \) elements. Let \( F(x) \) be a polynomial over \( \mathcal{K} \) of degree \( f, f > 0 \). Let \( \gamma_0, \gamma_1, \ldots, \gamma_r \) be the distinct values \( F(\tau) \) as \( \tau \) ranges over \( \mathcal{K} \), and let \( l_i \) denote the number of distinct roots in \( \mathcal{K} \) of the polynomial \( F(x) - \gamma_i \). Let the \( \gamma_i \) be arranged in such a way that \( l_0 \leq l_i, 1 \leq i \leq r \). Set \( L = II(x - \pi) \), where the product is over the distinct roots \( \pi \) of \( F(x) - \gamma_0 \) that lie in \( \mathcal{K} \). Suppose that
\[ r = \lceil (q - 1)/f \rceil \geq 2. \] Then there exist positive integers \( v, k, m; \) a polynomial \( N \) over \( \mathcal{K}; \) and \( \omega_0, \omega_1, \ldots, \omega_m \) in \( \mathcal{K} \) such that \( L \nmid N, v \mid (p^k - 1), 1 + vr = p^m, L' \) is a \( p^m \)th power, \( \omega_0 \neq 0, \omega_m = 1, \)

\[ F(x) = L^sN^{p^m} + \gamma_0, \]

(33)

\[ \prod_{i=1}^{r} (x - \gamma_i + \gamma_0) = \sum_{\xi=0}^{m} \omega_{\xi}x^{(p^k - 1)/\xi}, \]

and

(34)

\[ \sum_{\xi=0}^{m} \omega_{\xi}L^{\xi kf}N^{\xi k m(p^k - 1)/\xi} = -\omega_0(x^q - x)L'. \]

Proof. Without loss of generality we can suppose that \( \gamma_0 = 0, \) so that our previous discussion applies. Let \( d \) be the integer such that

\[ p^d \geq 1 + vr > p^{d-1}. \]

It follows from Lemma 6 that \( L' \) is a \( p^d \)th power. We now apply Lemma 4 to conclude that either \( 1 + vr \) is a power of \( p^k \) or \( p^k \mid (1 + vr). \) In either case we must have \( p^d = 1 + vr. \) Since \( k \) is the smallest positive integer such that \( v \mid (p^k - 1), \) it follows that \( k \mid d. \) We put \( m = d/k. \) Then \( L' \) is a \( p^m \)th power and \( 1 + vr = p^m. \) Applying Lemma 4 again we find that \( R(x) \) is of the form

\[ R(x) = \sum_{i=0}^{m} \omega_{i}x^{(p^k - 1)/\xi}, \]

so that (33) holds. Moreover \( H \) is a \( p^{d-1} \)st power by Lemma 4, and therefore \( H^p \) is a \( p^{m} \)th power. Thus there is a polynomial \( N \) over \( \mathcal{K} \) such that

\[ F = L^sH^p = L^sN^{p^m}. \]

Furthermore since \( L \nmid H, \) it follows that \( L \nmid N. \) Using (16) we obtain \( \omega_0 = \rho_0 = -\zeta \neq 0. \) It follows at once from (33) that \( \omega_m = 1. \) Finally we substitute in (15) to obtain (34). This completes the proof of the theorem.

In the next two sections we apply Theorem 1 to a number of special cases.

3. A special case. There are two general types of polynomials known for which (1) holds [1, § 5]. For every polynomial of the first type both \( L' \) and \( N \) are constants. Thus this case is of special interest. Here we have the following result:
**Lemma 7.** Suppose that $L'$ and $N$ are both constants. Then $q$ is a power of $p^k$, and $F$ is of the form

$$F = \alpha L^\gamma + \gamma, \quad L = \beta + \sum_{j=0}^{d} \varphi_j x^{pk^j},$$

where $L$ factors into distinct linear factors over $\mathcal{K}$ and $\nu \mid (p^k - 1)$.

**Proof.** Since $N$ is a constant it follows from Theorem 1 that $F = \alpha L^\gamma + \gamma$, where $\alpha \in \mathcal{K}$ and $\gamma = \gamma_0 \in \mathcal{K}$. Suppose that $L$ is not of the form given in (35). Then, since $L'$ is a constant, we can write

$$L = \beta + \sum_{j=0}^{c} \varphi_j x^{pk^j} + \sum_{j=a}^{l/p} \delta_j x^{p^j}$$

where $a$ and $c$ are integers such that

$$p^{k(c+1)} > pa > p^k, \quad l \geq pa,$$

and $\delta_a \neq 0$. Moreover $L' = \varphi_0 \neq 0$. Now (34) becomes

$$\sum_{i=0}^{m} \chi_i L^{pk^i} = -\omega_0 \varphi_0 (x^q - x),$$

where the $\chi_i$ are in $\mathcal{K}$, $\chi_0 = \omega_0 \neq 0$, and $\chi_m \neq 0$. Substituting (36) in (37) we get

$$\psi + \sum_{j=0}^{c} \psi_j x^{pk^j} + \chi_0 \delta_a x^{pa} + \sum_{j=pa+1}^{l/p} \sigma_j x^{p^j} = -\omega_0 \varphi_0 (x^q - x),$$

for suitable $\psi$, $\psi_j$, $\sigma_j$ in $\mathcal{K}$. Since $\chi_0 \delta_a \neq 0$, this implies that either $pa = 1$ or $pa = q$. Comparing degrees we obtain

$$q = lp^{km} > l \geq pa.$$

Clearly $pa \neq 1$. This contradiction implies that $L$ is of the desired form, which completes this proof.

The converse of Lemma 7 is already known [1]: *If $q$ is a power of $p^k$, and if $F$ is of the form (35), then the polynomial $F$ satisfies the equality $r = [(q - 1)/f]$. This was proved in [1] as follows: Let $\tau$ be a root of $L$. Replacing $x$ by $x + \tau$ we can assume that $\beta = 0$. Let $l = \deg L$ as before, and set $L(x) = L$. Because of the form of $L$ the values assumed by $L(\tau)$ as $\tau$ ranges over $\mathcal{K}$ form a vector space over the subfield $GF(p^k)$. Since we have assumed that $L$ factors into distinct linear factors over $\mathcal{K}$, it follows that $L$ has exactly $l$ distinct roots in $\mathcal{K}$. Therefore this vector space contains exactly $q/l$ distinct elements. Then since $F = \alpha L^\gamma + \gamma$, where $\nu \mid (p^k - 1)$, it follows that the number of values assumed by $F(\tau)$ as*
\[ \tau \text{ ranges over } \mathbb{K} \text{ is exactly} \]
\[ 1 + (-1 + q/\ell)v = 1 + (q - \ell)/f = 1 + [(q - 1)/f] \]
Hence \( r = [(q - 1)/f] \).

Thus we have a complete characterization of those polynomials for which \( r = [(q - 1)/f] \geq 2 \), subject to the condition that \( L' \) and \( N \) are both constants. One significance of this result can be seen from the following lemma:

**Lemma 8.** If \( f \leq \sqrt{q} \), and \( r = [(q - 1)/f] \geq 2 \), then \( L' \) and \( N \) are both constants.

**Proof.** Theorem 1 applies so that we have \( 1 + rv = p^{m^k} \), and \( f = vl + p^{m^k} \deg N \). Moreover \( f^2 \leq q \) and \( r = [(q - 1)/f] \) so that

\[ f \leq q/f \leq r + 1 = 1 + (p^{m^k} - 1)/v \leq p^{m^k} \]

Thus \( p^{m^k} \deg N < f \leq p^{m^k} \), \( \deg N = 0 \), and \( N \) is a constant. Furthermore \( L' \) is a \( p^{m^k} \)th power by Theorem 1 and \( \deg L' < l \leq f \leq p^{m^k} \). Hence \( L' \) is also a constant, and the proof of this lemma is complete.

The above results give us a complete characterization of those polynomials \( F' \) for which \( r = [(q - 1)/f] \geq 2 \) and \( 0 < f \leq \sqrt{q} \). Now suppose that \( r = [(q - 1)/f] < 2 \) and \( 0 < f \leq \sqrt{q} \). Then

\[ 2 > (q - 1)/f \geq (f^2 - 1)/f \]
\[ f^2 - 2f - 1 < 0 \], and thus \( f = 1 \) or \( f = 2 \). Now \( q \) is a prime power and \( f^2 \leq q < 2f + 1 \). Hence we have either (i) \( f = 1 \) and \( q = 2 \), or (ii) \( f = 2 \) and \( q = 4 \). If \( f = 1 \), then \( F' \) is clearly of the form (35) with \( v = k = 1 \) and \( d = 0 \). If \( f = 2 \) and \( q = 4 \), then \( r = 1 \), and since \( F_0 \) and \( F_1 \) together have 4 distinct roots in \( \mathbb{K} \), it follows that \( F_0 \) has two distinct roots in \( \mathbb{K} \), so that \( F' \) is still of the form (35), this time with \( p = 2 \) and \( v = k = d = 1 \). Thus we see that the condition \( r \geq 2 \) can be dropped here. Combining all these results we obtain one of our major results:

**Theorem 2.** Let \( F(x) \) be a polynomial over the finite field \( \mathbb{K} \) of characteristic \( p \) and let \( q \) denote the number of elements of \( \mathbb{K} \). Let \( r + 1 \) denote the number of distinct values assumed by \( F(\tau) \) as \( \tau \) ranges over \( \mathbb{K} \), and let \( f \) be the degree of \( F(x) \). Suppose that \( 0 < f \leq \sqrt{q} \). Then

\[ r = [(q - 1)/f] \]

if and only if \( F \) is of the form
where $L$ is a polynomial that factors into distinct linear factors over $\mathbb{F}$ and that has the form

$$L = \beta + \sum_{i=0}^{d} \varphi_i w^{k_i} .$$

and where $v$ and $k$ are integers such that $v \mid (p^k - 1)$, $q$ is a power of $p^k$, and $\alpha$, $\beta$, $\gamma$, and the $\varphi_i$ are elements of $\mathbb{F}$.

4. The cases $q = p$ and $q = p^2$. The results of §1 enable us to treat the case $q = p$ quickly.

Suppose $q = p$ and $r = [(q - 1)/f^2]$. If $\gamma = 0$, then the results of §1 apply, so that

$$F = L^p H^p, \quad L = xS^p + T^p$$

by (12) and (14). Since

$$\deg F = f \leq \frac{1}{2}(q - 1) = \frac{1}{2}(p - 1) < p ,$$

the polynomials $H$, $S$, and $T$ are all constants. Thus $F$ is of the form $\alpha(x + \beta)^p$ and $v = f$. It is easily shown that $v \mid (q - 1)$ here. Dropping the assumption $\gamma = 0$, we see that if $q = p$ and $r = [(q - 1)/f^2] \geq 2$, then $f \mid (q - 1)$ and $F$ is of the form

$$F = \alpha(x + \beta)^f + \gamma .$$

We note that in this case $L'$ and $N$ must both be constants, so that we could have obtained this result from Lemma 7.

Let us now consider the case $q = p^2$. Comparing the degrees of the two sides of (34) we obtain

$$p^{mk} + r p^{mk} \deg N = q + \deg L' \leq q + l - 1 = p^2 + l - 1 .$$

Therefore

$$p^l + p \deg N \leq p^2 + l - 1 .$$

Thus $p^l \leq p^2 + l - 1$ or $l \leq p + 1$. Since $L'$ is a $p$th power, it follows that $l \equiv 0$ or $1 \pmod{p}$. Therefore $l = 1$, $p$, or $p + 1$. If $l = p$ or $p + 1$, the inequality (38) gives us

$$p \deg N \leq p^2 - l(p - 1) - 1 \leq p - 1 ,$$

deg $N = 0$ and $N$ is a constant. If $l = 1$, then $L$ is of the form $x + \beta$, $L' = 1$, and (34) gives us
\[
N|(-\omega_0x^q + w_0x - \omega_0L) = -\omega_0(x^q + \beta) = -\omega_0L^q.
\]

Thus in case \(l = 1\), we see that \(N\) is a constant times a power of \(L\). Since \(L \nmid N\), this implies that \(N\) is a constant. Thus \(N\) is a constant in all three cases.

If \(L'\) is also a constant then Lemma 7 applies, and \(F\) is of the form (35) with either (i) \(l = 1, d = 0, \) and \(v \mid (p^2 - 1)\), or (ii) \(l = p, k = d = 1, \) and \(v \mid (p - 1)\).

Now suppose that \(L'\) is not a constant. Since \(L'\) is a \(p^m\)th power by Theorem 1, we must have \(l = p + 1\) and \(m = k = 1\). Since \(N\) is a constant we have \(F = \alpha L + \gamma\), where \(\alpha \in \mathbb{K}\) and \(\gamma = \gamma_0 \in \mathbb{K}\). Moreover \(L\) is of the form \(L = xS + T^p\) by (14).

Since \(L\) has leading coefficient 1, \(S\) is of the form \(S = x + \varphi\). Moreover \(T\) is of the form \(T = \mu x + \nu\). Now (34) becomes

\[
\omega_0L + \chi L^p = -\omega_0(x^q - x)S^p,
\]

where \(\chi \in \mathbb{K}\). Comparing leading coefficients we see that \(\chi = -\omega_0\). Therefore

\[
L^p = (x^q - x)S^p + L = x^{p}S^p + T^p.
\]

Extracting \(p\)th roots we obtain \(L = x^{p}S + T\). Thus

\[
xS^p + T^p = x^pS + T,
\]
or

(39) \[x^{p+1} + \mu^px^p + \varphi^px + \nu^p = x^{p+1} + \varphi x^p + \mu x + \nu.\]

Comparing the coefficients of \(x\) in (39) we obtain \(\mu = \varphi^p\). Therefore

\[
L = x^pS + T = x^{p+1} + \varphi^pS + \varphi^pS + \nu = (x + \varphi)^{p+1} + \beta,
\]

where \(\beta = \nu - \varphi^{p+1}\). Comparing the constant terms of (39) we get \(\nu^p = \nu\). Therefore \(\nu \in GF(p)\), the prime field of \(\mathbb{K}\). Now \(\varphi^{p+1} \in GF(p)\). Hence \(\beta \in GF(p)\). Since \(L\) has distinct roots we have \(\beta \neq 0\). Now if \(v = 1\), then \(F = \alpha L + \gamma\), and \(F - \gamma - \alpha \beta\) has exactly one distinct root in \(\mathbb{K}\), contradicting (11). Thus \(v \geq 2\). We have shown that if \(q = p^2, \ r = [(q - 1)/f] \geq 2\) and \(L'\) is not constant, then \(F\) is of the form \(\alpha L^r + \gamma\), where \(L\) is of the form

\[
L = (x + \varphi)^{p+1} + \beta,
\]

where \(\beta \in GF(p), \ \beta \neq 0, \ \nu \mid (p - 1), \ v \geq 2\).

Conversely if \(q = p^2\) and \(F\) has this form, then \(L(\tau) \in GF(p)\) for all \(\tau \in \mathbb{K}\), and thus \(F\) assumes at most

\[
1 + (p - 1)/v = 1 + (q - 1)/f = 1 + [(q - 1)/f].
\]
distinct values. Since we always have $r \geq [(q - 1)/f]$, this implies that $r = [(q - 1)/f]$.

We have completed the discussion of the case $q = p^2$. We sum up our results for this case in our final theorem:

**Theorem 3.** Let $\mathbb{K}$ be a field of characteristic $p$ that contains exactly $p^2$ elements. Let $F(x)$ be a polynomial over $\mathbb{K}$ of degree $f$, $f > 0$. Let $F(\tau)$ assume exactly $r + 1$ distinct values as $\tau$ ranges over $\mathbb{K}$. If $r = [(p^2 - 1)/f] \geq 2$, then $F(x)$ has one of the following three forms:

(i) $F(x) = \alpha(x + \beta)^r + \gamma$, where $v|(p^2 - 1)$, $\alpha \neq 0$,

(ii) $F(x) = \alpha(x^p + \varphi x + \beta)^r + \gamma$, where $x^p + \varphi x + \beta$ has $p$ distinct roots in $\mathbb{K}$, $v|(p - 1)$, $\alpha \neq 0$,

(iii) $F(x) = \alpha((x + \varphi)^{r+1} + \beta)^r + \gamma$, where $\beta \in GF(p)$, $\beta \neq 0$, $v \geq 2$, $v|(p - 1)$, and $\alpha \neq 0$.

Conversely if $F(x)$ has one of these three forms, then $r = [(q - 1)/f]$.

For $q > p^2$, the question of the characterization of all polynomials $F$ for which (1) holds, remains open. The most general types of polynomials known for which (1) holds are described in [1, §5]. At present it seems unlikely that there are any more.

**Reference**


**Yale University**