Pacific Journal of Mathematics

POLYNOMIALS WITH MINIMAL VALUE SETS

WILLIAM H. MILLS

Vol. 14, No. 1 May 1964

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 τ 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.

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 $\mathscr{K}$ of degree $f, f > 0$. Let $\gamma_0, \gamma_1, \cdots, \gamma_r$ denote the distinct values assumed by $F(\tau)$ as τ ranges over $\mathscr{K}$. It follows easily from the fact that a polynomial of degree f has at most f roots, that $r + 1 \geqq q/f$. This is equivalent to $r \geqq [(q-1)/f]$. 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

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

Subtracting the constant γ_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

$$F_i = F - \gamma_i , \qquad 0 \leqq i \leqq r .$$

The polynomials F_i are relatively prime in pairs, and each of them has at least one root in $\mathscr{K}$. Let $\pi_{i1}, \pi_{i2}, \cdots, \pi_{il_i}$ be the distinct roots of F_i that lie in $\mathscr{K}$ and set

$$L_i = \prod_{j=1}^{l_i} (x - \pi_{ij}) , \qquad 0 \leqq i \leqq r .$$

Then $l_i = \deg L_i \geqq 1$, $0 \leqq i \leqq r$, and[1]

$$x^q - x = \prod_{i=0}^{r} L_i . \tag{2}$$

Now set $F_i = L_i U_i$, $0 \leqq i \leqq r$, and

$$G = \prod_{i=0}^{r} U_i . \tag{3}$$

Then the L_i, the U_i and G are polynomials over $\mathscr{K}$, and

$$(x^q - x)G = \prod_{i=0}^{r} F_i . \tag{4}$$

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

$$\deg G = (r+1)f - q \leqq q - 1 + f - q = f - 1 .$$

[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

$$(5) \qquad \deg G < f\,.$$

Set $u_i = \deg U_i$, $0 \leqq i \leqq r$. 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 $-1 \equiv L'L^*$ $(\bmod L)$, where $L^* = L_1L_2\cdots L_r$. Hence $G \equiv -L'L^*G \pmod{LG}$. Since $F = LU$ and $U \mid G$, it follows that $F \mid LG$ and thus

$$G \equiv -L'L^*G \qquad (\bmod F)\,.$$

Now

$$L^*G = U\prod_{i=1}^{r}(L_iU_i) = U\prod_{i=i}^{r}(F-\gamma_i) \equiv -\zeta U \qquad (\bmod F)\,,$$

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

$$(6) \qquad G = \zeta L'U\,.$$

By symmetry it follows that

$$(7) \qquad G = \zeta_i L_i' U_i\,, \qquad 0 \leqq i \leqq r\,,$$

for suitable nonzero elements ζ_i of $\mathscr{K}$.

We next derive another expression for G.

Lemma 1. *There exists a nonzero element θ in $\mathscr{K}$ such that $G = \theta F'$.*

Proof. Since $F' = F_i' = L_i'U_i + L_iU_i'$, it follows from (7) that

$$L_iU_i' = F' - G/\zeta_i\,, \qquad 0 \leqq i \leqq r\,.$$

Therefore $L_0U_0' = LU'$, L_1U_1', and L_2U_2' are linearly dependent. Thus there exist λ, λ_1, and λ_2 in $\mathscr{K}$, not all zero, such that

$$\lambda LU' + \lambda_1L_1U_1' + \lambda_2L_2U_2' = 0\,.$$

Multiplying this relation by UU_1U_2 and noting that $LU = F$, $L_1U_1 = F - \gamma_1$, $L_2U_2 = F - \gamma_2$, we obtain

$$(8) \quad (\lambda U'U_1U_2 + \lambda_1UU_1'U_2 + \lambda_2UU_1U_2')F = \lambda_1\gamma_1UU_1'U_2 + \lambda_2\gamma_2UU_1U_2'\,.$$

Now the degree of the right side of (8) is less than $u + u_1 + u_2$ and

$$u + u_1 + u_2 \leqq \deg G < f = \deg F\,.$$

This is possible only if we have

$$\lambda U' U_1 U_2 + \lambda_1 U U_1' U_2 + \lambda_2 U U_1 U_2' = 0\,. \tag{9}$$

The constants λ, λ_1, and λ_2 are not all zero. Without loss of generality we suppose $\lambda_2 \neq 0$. Then (9) gives us $U_2 \mid UU_1U_2'$. Since $U_2 \mid F_2$, U_2 must be relatively prime to both F and F_1. Hence U_2 is relatively prime to UU_1, and $U_2 \mid U_2'$. This implies that $U_2' = 0$. Hence

$$F' = F_2' = L_2'U_2 + L_2U_2' = L_2'U_2 = G/\zeta_2.$$

Thus $G = \zeta_2 F'$, which completes this proof.

Lemma 1 is false for $r \leqq 1$—counter examples can be readily constructed.

LEMMA 2. *For each j, $0 \leqq j \leqq r$, U_j is of the form*

$$U_j = L_j^{w_j} H_j^p\,,$$

where w_j is a nonnegative integer, H_j is a polynomial over $\mathscr{K}$, and $L_j \nmid H_j$.

Proof. By symmetry it is sufficient to prove the lemma for the case $j = 0$. Combining (6) with Lemma 1 we obtain

$$\zeta L' U = G = \theta F' = \theta L' U + \theta L U'\,.$$

Thus

$$\theta L U' = (\zeta - \theta) L' U\,. \tag{10}$$

We set $U = L^w A$, where $L \nmid A$ and $w \geqq 0$. 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 $A = H^p$ for some polynomial H. Then we have $L \nmid H$ and $U = L^w H^p$, which completes this proof.

We now suppose, without loss of generality, that

$$l \leqq l_j\,, \qquad 0 \leqq j \leqq r\,. \tag{11}$$

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

$$\zeta L' U = G = U U_1 U_2 \cdots U_r .$$

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

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

Therefore $L_j \nmid U_j$, 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

$$F = L U = L^v H^p , \tag{12}$$

and

$$F_i = L_i U_i = L_i H_i^p , \qquad 1 \leqq i \leqq r , \tag{13}$$

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

$$\zeta L' = G/U = U_1 U_2 \cdots U_r = (H_1 H_2 \cdots H_r)^p .$$

Thus $L' = S^p$, where $S = \zeta^{-1/p} H_1 H_2 \cdots H_r$. Therefore L is of the form

$$L = x S^p + T^p , \tag{14}$$

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

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

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

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

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

These identities and (12) give us

$$\sum_{j=0}^{r} \rho_j L^{1+vj} H^{pj} = L R(F) = \zeta (x^q - x) L' . \tag{15}$$

Differentiating both sides of (15) and noting that $L'' = 0$ by (14), we get the congruence

$$\rho_0 L' \equiv -\zeta L' \qquad (\text{mod } L) .$$

Since $L' \neq 0$, we obtain

$$\rho_0 = -\zeta . \tag{16}$$

By Lemma 1 we have $F' = G/\theta \neq 0$. Hence $p \nmid v$.

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 ρ_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^dth 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) *$p^d \mid (1 + vj)$. Moreover H is a p^{d-1}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+1}st power and $1 + vr > p^d$. Then the induction hypothesis applies so that $R(x)$ is of the form

$$R(x) = \sum_{i=0}^{c} \omega_i x^{(p^{ki}-1)/v} + \Sigma' \rho_j x^j , \tag{17}$$

where $\omega_i \in \mathscr{K}$, $0 \leqq i \leqq c$, $c = [d/k]$, and the second summation Σ' is over all j such that

$$p^d \mid (1+vj) , \quad p^d < 1 + vj , \quad j \leqq r .$$

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

$$H = A^{p^{d-1}} \quad \text{and} \quad F = L^v A^{p^d}$$

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

$$\Sigma' \rho_j L^{1+vj} A^{jp^d} = \zeta x^q L' + B , \tag{18}$$

where

$$B = -\zeta x L' - \sum_{i=0}^{c} \omega_i L^{p^{ki}} A^{p^d (p^{ki}-1)/v} .$$

The left side of (18) is a p^dth power. Since

$$q \geqq 1 + fr \geqq 1 + vr > p^d$$

and q is a power of p, it follows that $p^{d+1} \mid q$. Hence $\zeta x^q L'$ is a p^{d+1}st power. Therefore B is a p^dth power. Thus we can set

$$\zeta x^q L' = C^{p^{d+1}} \quad \text{and} \quad B = D^{p^d} .$$

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 $1 + va \geqq 2p^d$. Because of the way a was chosen we have

$$L^{1+va} A^{ap^d} \,\|\, (\zeta x^q L' + B) . \tag{19}$$

Extracting the p^dth roots of both sides of (19) we get

$$L^{(1+va)p^{-d}} A^a \,\|\, (C^p + D).$$

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

$$LA^{a-1} \mid D' . \tag{20}$$

Now

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

Since

$$a > (p^d - 1)/v \geqq (p^{kc} - 1)/v ,$$

we have $(p^{kc} - 1)/v \leqq a - 1$, and

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

Combining this with (20) we get $D' = 0$. Thus D must be a pth 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 pth power. Hence $p \nmid a$, and A itself is a pth power. It follows that H is a p^dth power. Suppose there is a b such that $\rho_b \neq 0$, $1 + vb$ is not a power of p^k, and $p^{d+1} \nmid (1 + vb)$. 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

$$L^{1+vb} A^{bp^d} \,\|\, \{\zeta x^q L' + B - \Sigma'' \rho_j L^{1+vj} A^{jp^d}\} , \tag{21}$$

where Σ'' 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^dth power but not a p^{d+1}st power, and $1 + vr > p^d$. Then $v = 1$ and $p^{d+1} \nmid (1 + r)$.*

Proof. Since L' is a pth power by (14), we have $d \geqq 1$. By Lemma 4 we have

$$R(x) = \sum_{i=0}^{c} \omega_i x^{(p^{ki}-1)/v} + \Sigma^* \rho_j x^j + x^r ,$$

where the ω_i are elements of $\mathscr{K}$, $c = [d/k]$, and the summation Σ^* is over all j such that $p^d \mid (1 + vj)$, $p^d < 1 + vj$, $j < r$. 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 $\zeta \in \mathscr{K}$, it follows that $\zeta L'$ is a p^dth power but not a p^{d+1}st power. Thus we can set

$$H = A^{p^{d-1}} \quad \text{and} \quad \zeta L' = C^{p^d} ,$$

where C is not a pth power. Substitution in (15) gives us

$$L^{1+vr} A^{rp^d} = x^q C^{p^d} + B , \tag{22}$$

where

$$\begin{aligned} B &= -\zeta x L' - LR(F) + LF^r \\ &= -\zeta x L' - \sum_{i=0}^{c} \omega_i L^{p^{ki}} A^{p^d(p^{ki}-1)/v} - \Sigma^* \rho_j L^{1+vj} A^{jp^d} . \end{aligned}$$

Now the left side of (22) is a p^dth power. Moreover

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

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

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

Differentiation now yields

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

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

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

where

$$E = (1 + vr)p^{-d} L'AC + rLA'C - LAC' .$$

Now $A \mid H$ and therefore $LA \mid F$. Moreover

$$C \mid L' = G/(\zeta U) = \zeta^{-1} U_1 U_2 \cdots U_r \mid F_1 F_2 \cdots F_r .$$

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

$$L^{-e+(1+vr)p^{-d}} A^{r-1} \mid (CD' - C'D) , \tag{26}$$

where

$$e = \begin{cases} 0 & \text{if } p^{d+1} \mid (1 + vr) , \\ 1 & \text{if } p^{d+1} \nmid (1 + vr) . \end{cases}$$

Comparing degrees in (26) we obtain

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

Now the leading term of $R(x)$ is x^r and $R(x) \neq x^r$. Set $b = \deg \{R(x) - x^r\}$. Then we have $0 \leqq b < r$ and

$$\begin{aligned} \deg B &\leqq \deg (LF^b) \\ &= (1 + vb)l + bp^d \deg A \leqq (1 + vb)l + (r - 1)p^d \deg A . \end{aligned}$$

Substitution in (27) gives us, after simplification,

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

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

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

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

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

Since $\rho_b \neq 0$, this gives us $p^d \mid (1 + vb)$. Since $p^d \mid (1 + vr)$, it follows that $p^d \mid v(r - b)$ and $p \nmid v$. Hence $v(r - b) = p^d$ and $v = 1$. Finally since $e = 1$ we have

$$p^{d+1} \nmid (1 + vr) = 1 + r ,$$

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^dth power. By Lemma 5 we have $v = 1$ and $p^{d+1} \nmid (1 + r)$.

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

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

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

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

by (4), so that

$$\Sigma^+ \rho_j F^{j+1} = x^q G + B , \tag{28}$$

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

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

Then, extracting the p^dth roots of both sides of (28), we get

$$\sum_{j=1}^{a} \xi_j F^j = x^{qp^{-d}} C + D , \tag{29}$$

where $a = (r+1)p^{-d} \geqq 2$, the ξ_j are in $\mathscr{K}$, $\xi_a = 1$, and $\deg D \leqq f/p$. Now $p \nmid a$ since $p^{d+1} \nmid (r+1)$. We set $\bar{F} = F + \xi_{a-1}/a$. Then (29) becomes

$$\sum_{j=0}^{a} \eta_j \bar{F}^j = x^{qp^{-d}} C + D , \tag{30}$$

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

$$\sum_{j=1}^{a} j\eta_j \bar{F}^{j-1} \bar{F}' = x^{qp^{-d}} C' + D' . \tag{31}$$

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

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

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

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

where

$$\deg E < (a-2)f + \deg C .$$

Now

$$\deg C = p^{-d} \deg G < p^{-d} f \leqq f/p$$

by (5). Hence $\deg E < (a-1)f$, and

$$\deg (C'D - CD') < \deg (CD) < 2f/p \leqq (a-1)f\ .$$

Therefore

$$\deg (C'D - CD' - E) < (a-1)f = \deg \bar{F}^{a-1}\ ,$$

and (32) yields

$$C'\bar{F} = aC\bar{F}'\ .$$

Now $\bar{F}' = F' = \theta^{-1}G \neq 0$ by Lemma 1. Therefore $aC\bar{F}' \neq 0$. Hence $C' \neq 0$ and thus $C \nmid C'$. It follows that $(\bar{F}, C) \neq 1$. Since

$$C^{p^d} = G = \prod_{i=0}^{r} U_i$$

we have $(\bar{F}, U_b) \neq 1$ for some $b, 0 \leqq b \leqq r$. Hence $(\bar{F}, F_b) \neq 1$. Since $\bar{F} - F_b \in \mathscr{K}$, we must have $\bar{F} = F_b$. Therefore

$$C'F_b = aCF_b'\ .$$

Since $v = 1$, we have $F_b = L_b H_b^p$, whether or not $b = 0$. Hence

$$C'L_b H_b^p = aCL_b' H_b^p\ ,$$

and $C'L_b = aCL_b'$. Now L_b is relatively prime to L_b'. Therefore $L_b \mid C$. Since $v = 1$ we have

$$C^{p^d} = G = \prod_{i=0}^{r} U_i = \prod_{i=0}^{r} H_i^p\ .$$

It follows that $L_b \mid H_0 H_1 \cdots H_r$. On the other hand $L_b \nmid H_b$, while for $i \neq b$ we have $(L_b, H_i) = 1$. Therefore $L_b \nmid H_0 H_1 \cdots H_r$, 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 $\mathscr{K}$ be a finite field of characteristic p that contains exactly q elements. Let $F(x)$ be a polynomial over $\mathscr{K}$ of degree $f, f > 0$. Let $\gamma_0, \gamma_1, \cdots, \gamma_r$ be the distinct values $F(\tau)$ as τ ranges over $\mathscr{K}$, and let l_i denote the number of distinct roots in $\mathscr{K}$ of the polynomial $F(x) - \gamma_i$. Let the γ_i be arranged in such a way that $l_0 \leqq l_i$, $1 \leqq i \leqq r$. Set $L = \Pi(x - \pi)$, where the product is over the distinct roots π of $F(x) - \gamma_0$ that lie in $\mathscr{K}$. Suppose that*

$r = [(q-1)/f] \geqq 2$. *Then there exist positive integers* v, k, m; *a polynomial* N *over* $\mathscr{K}$; *and* $\omega_0, \omega_1, \cdots, \omega_m$ *in* $\mathscr{K}$ *such that* $L \nmid N$, $v \mid (p^k - 1)$, $1 + vr = p^{mk}$, L' *is a* p^{mk}th *power*, $\omega_0 \neq 0$, $\omega_m = 1$,

$$F(x) = L^v N^{p^{mk}} + \gamma_0 \ ,$$

$$\prod_{i=1}^{r} (x - \gamma_i + \gamma_0) = \sum_{i=0}^{m} \omega_i x^{(p^{ki}-1)/v} \ , \tag{33}$$

and

$$\sum_{i=0}^{m} \omega_i L^{p^{ki}} N^{p^{km}(p^{ki}-1)/v} = -\omega_0 (x^q - x) L' \ . \tag{34}$$

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

$$p^d \geqq 1 + vr > p^{d-1} \ .$$

It follows from Lemma 6 that L' is a p^dth power. We now apply Lemma 4 to conclude that either $1 + vr$ is a power of p^k or $p^d \mid (1 + vr)$. 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^{mk}th power and $1 + vr = p^{mk}$. Applying Lemma 4 again we find that $R(x)$ is of the form

$$R(x) = \sum_{i=0}^{m} \omega_i x^{(p^{ki}-1)/v} \ ,$$

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

$$F = L^v H^p = L^v N^{p^{mk}} \ .$$

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*

$$F = \alpha L^v + \gamma,\ L = \beta + \sum_{j=0}^{d} \varphi_j x^{p^{kj}}, \tag{35}$$

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

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

$$L = \beta + \sum_{j=0}^{c} \varphi_j x^{p^{kj}} + \sum_{j=a}^{l/p} \delta_j x^{pj} \tag{36}$$

where a and c are integers such that

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

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

$$\sum_{i=0}^{m} \chi_i L^{p^{ki}} = -\omega_0 \varphi_0 (x^q - x), \tag{37}$$

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

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

for suitable ψ, ψ_j, σ_j in $\mathscr{K}$. Since $\chi_0 \delta_a \neq 0$, this implies that either $pa = 1$ or $pa = q$. Comparing degrees we obtain

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

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 π be a root of L. Replacing x by $x + \pi$ 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 τ ranges over $\mathscr{K}$ form a vector space over the subfield $GF(p^k)$. Since we have assumed that L factors into distinct linear factors over $\mathscr{K}$, it follows that L has exactly l distinct roots in $\mathscr{K}$. Therefore this vector space contains exactly q/l distinct elements. Then since $F = \alpha L^v + \gamma$, where $v \mid (p^k - 1)$, it follows that the number of values assumed by $F(\tau)$ as

τ ranges over $\mathscr{K}$ is exactly

$$1 + (-1 + q/l)/v = 1 + (q - l)/f = 1 + [(q - 1)/f] .$$

Hence $r = [(q - 1)/f]$.

Thus we have a complete characterization of those polynomials for which $r = [(q - 1)/f] \geqq 2$, 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 $f \leqq \sqrt{q}$, and $r = [(q - 1)/f] \geqq 2$, then L' and N are both constants.*

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

$$f \leqq q/f \leqq r + 1 = 1 + (p^{mk} - 1)/v \leqq p^{mk} .$$

Thus $p^{mk} \deg N < f \leqq p^{mk}$, $\deg N = 0$, and N is a constant. Furthermore L' is a p^{mk}th power by Theorem 1 and $\deg L' < l \leqq f \leqq p^{mk}$. 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 $r = [(q - 1)/f] \geqq 2$ and $0 < f \leqq \sqrt{q}$. Now suppose that $r = [(q - 1)/f] < 2$ and $0 < f \leqq \sqrt{q}$. Then

$$2 > (q - 1)/f \geqq (f^2 - 1)/f ,$$

$f^2 - 2f - 1 < 0$, and thus $f = 1$ or $f = 2$. Now q is a prime power and $f^2 \leqq q < 2f + 1$. 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 $\mathscr{K}$, it follows that F_0 has two distinct roots in $\mathscr{K}$, 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 $r \geqq 2$ 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 $\mathscr{K}$ of characteristic p and let q denote the number of elements of $\mathscr{K}$. Let $r + 1$ denote the number of distinct values assumed by $F(\tau)$ as τ ranges over $\mathscr{K}$, and let f be the degree of $F(x)$. Suppose that $0 < f \leqq \sqrt{q}$. Then*

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

if and only if F is of the form

$$F = \alpha L^v + \gamma ,$$

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

$$L = \beta + \sum_{i=0}^{d} \varphi_i x^{p^{ki}} .$$

and where v and k are integers such that $v \mid (p^k - 1)$, q is a power of p^k, and α, β, γ, and the φ_i are elements of $\mathscr{K}$.

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 $r = [(q-1)/f] \geqq 2$. If $\gamma_0 = 0$, then the results of § 1 apply, so that

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

by (12) and (14). Since

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

the polynomials H, S, and T are all constants. Thus F is of the form $\alpha(x+\beta)^v$ and $v = f$. It is easily shown that $v \mid (q-1)$ here. Dropping the assumption $\gamma_0 = 0$, we see that if $q = p$ and $r = [(q-1)/f] \geqq 2$, 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

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

Therefore

$$pl + p \deg N \leqq p^2 + l - 1 . \tag{38}$$

Thus $pl \leqq p^2 + l - 1$ or $l \leqq p + 1$. Since L' is a pth 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

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

$\deg N = 0$ and N is a constant. If $l = 1$, then L is of the form $x + \beta$, $L' = 1$, and (34) gives us

$$N \mid (-\omega_0 x^q + w_0 x - \omega_0 L) = -\omega_0(x^q + \beta) = -\omega_0 L^q .$$

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^{mk}th power by Theorem 1, we must have $l = p + 1$ and $m = k = 1$. Since N is a constant we have $F = \alpha L^v + \gamma$, where $\alpha \in \mathscr{K}$ and $\gamma = \gamma_0 \in \mathscr{K}$. Moreover L is of the form $L = xS^p + T^p$ 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

$$\omega_0 L + \chi L^p = -\omega_0(x^q - x)S^p ,$$

where $\chi \in \mathscr{K}$. Comparing leading coefficients we see that $\chi = -\omega_0$. Therefore

$$L^p = (x^q - x)S^p + L = x^{p^2}S^p + T^p .$$

Extracting pth roots we obtain $L = x^p S + T$. Thus

$$xS^p + T^p = x^p S + T ,$$

or

$$x^{p+1} + \mu^p x^p + \varphi^p x + \nu^p = x^{p+1} + \varphi x^p + \mu x + \nu . \tag{39}$$

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

$$L = x^p S + T = x^{p+1} + \varphi x^p + \varphi^p x + \nu = (x + \varphi)^{p+1} + \beta ,$$

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 $\mathscr{K}$. 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 $\mathscr{K}$, contradicting (11). Thus $v \geqq 2$. We have shown that if $q = p^2$, $r = [(q - 1)/f] \geqq 2$ and L' is not constant, then F is of the form $\alpha L^v + \gamma$, where L is of the form

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

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

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

$$1 + (p - 1)/v = 1 + (q - 1)/f = 1 + [(q - 1)/f]$$

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

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

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

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

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

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

1. L. Carlitz, D. J. Lewis, W. H. Mills and E. G. Straus, *Polynomials over finite fields with minimal value sets*, Mathematika **8** (1961), 121-130.

YALE UNIVERSITY

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 14, No. 1 May, 1964