ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 23, Number 1, Winter 1993

SPECIAL VALUE SET POLYNOMIALS OVER FINITE FIELDS

JAVIER GOMEZ-CALDERON

ABSTRACT. Let F_q denote the finite field of order q where q is a prime power. In this paper we prove that if m and n are two integers dividing $q-1$, $2 \le m$, $2 \le n$ and $d = mn < \sqrt[4]{q}$, then

$$\frac{2q}{2m+2n-1} \le |\{(x^m+b)^n : x \in F_q\}| \le \min\{(q-1)/m, (q-1)/n\} + 1$$

for all $0 \ne b$ in F_q.

1. Introduction. Let F_q denote the finite field of order q where q is a prime power. If $f(x)$ is a polynomial of degree d over F_q, let $V_f = \{f(x) : x \in F_q\}$ denote the image or value set of $f(x)$ and let $|V_f|$ denote the cardinality of V_f. It is clear that if f is of degree d,

$$[(q-1)/d] + 1 \le |V_f| \tag{1}$$

where $[x]$ denotes the greatest integer $\le x$. Hence,

$$[(q-1)/d] + 1 \le |V_f| \le q. \tag{2}$$

A permutation polynomial over F_q has a value set of maximal possible cardinality so that if $f(x)$ permutes F_q, then $|V_f| = q$. Many papers have been written concerning permutation polynomials over finite fields, with an excellent survey being given in Lidl and Niederreiter [**6**, Chapter 7] and Lidl and Mullen [**5**].

At the other extreme, a polynomial for which equality is achieved in (1) is called a minimal value set polynomial. Minimal value set polynomials over finite fields have been studied in Carlitz, Lewis, Miller and Straus [**1**] and Mills [**7**]. Recently, in [**4**], Gomez-Calderon and

Received by the editors on June 30, 1990, and in revised form on January 20, 1991.

Madden considered polynomials with small but not minimal sets. They gave a complete list of polynomials of degree $d < \sqrt[4]{q}$ which have a value set of size less than $2q/d$, twice the minimum possible. If $d > 15$ then $f(x)$ is one of the following polynomial forms:

(a) $f(x) = (x+a)^d + b$, where $d \mid (q-1)$

(b) $f(x) = ((x+a)^{d/2} + b)^2 + c$, where $d \mid (q^2-1)$

(c) $f(x) = ((x+a)^2 + b)^{d/2} + c$, where $d \mid (q^2-1)$

or

(d) $f(x) = g_d(x+b, a) + c$, where $d \mid (q^2-1)$ and $g_d(x,a)$ denotes the Dickson polynomial of degree d defined by

$$g_d(x,a) = \sum_{t=0}^{[d/2]} \frac{d}{d-t} \binom{d-t}{t} (-a)^t x^{d-2t}.$$

The cardinality of the value set of the power polynomial x^d over F_q depends only upon $(d, q-1)$, the greatest common divisor of d and $q-1$. To be more specific,

$$|V_{x^d}| = (q-1)/(d, q-1) + 1. \tag{3}$$

Thus, if $d|(q-1)$, we have a minimal value set polynomial, while if $(d, q-1) = 1$, we have a set with maximal possible cardinality q.

Now the value set of the Dickson polynomial $g_d(x,a)$ has also been studied in Chou, Gomez-Calderon and Mullen [**2**]. There, the authors have shown that

$$|V_{g_d(x,a)}| = \frac{q-1}{2(d, q-1)} + \frac{q+1}{2(d, q+1)} + \alpha$$

where α, as a function of d, q and a, takes the values 0, 1, and 1/2.

In the present paper we consider the cardinality of the value set of the polynomials $(x^m + b)^n$ generalizing those given in (b) and (c). We show that if $d = mn$ divides $q-1$, $2 \le m$, $2 \le n$, $d < \sqrt[4]{q}$ and $0 \ne b \in F_q$, then

$$\begin{aligned} \frac{2q}{2m+2n-1} &\le |\{(x^m+b)^n : x \in F_q\}| \\ &\le \min\{(q-1)/m, (q-1)/n\} + 1. \end{aligned}$$

The improvement of the trivial lower bound,

$$\frac{q-1}{mn}+1 \le |\{(x^m+b)^n : x \in F_q\}|,$$

is an expected result according to [**3, 7**]. In [**3**], it is shown that if $f(x)$ denotes a polynomial of degree d, $3 \le d < p$, $q = p^n$, and

$$|V_f| < [(q-1)/d] + (2(q-1)/d^2) - 1,$$

then

$$|V_f| = [(q-1)/d] + 1.$$

Hence, by [**7**],

$$f(x) = (x-a)^d + b,$$

and d divides $q-1$.

2. Theorem and proof. We will need the following two lemmas.

Lemma 1. *Let $f(x)$ be a monic polynomial over F_q of degree d less and prime to q. Let N denote the number of linear factors of $f^*(x,y) = f(x) - f(y)$ over $F_q[x,y]$. Then any irreducible factor of $f^*(x,y)$ of degree less than N factors into linear factors over $\overline{F}_q[x,y]$, where $\overline{F}_q$ denotes the algebraic closure of F_q.*

Proof. Let $x - a_1y - b_1,\ x - a_2y - b_2, \dots, x - a_Ny - b_N$ denote the linear factors of $f^*(x,y)$. Thus,

$$f(x) - f(y) \equiv 0 \bmod (x - a_iy - b_i)$$

for $i = 1, 2, \dots, N$.

At the level of polynomials of one variable, this means that

$$f(a_iy + b_i) = f(y)$$

for $i = 1, 2, \dots, N$. Hence,

$$f(a_ia_jy + a_ib_j + b_i) = f(a_jy + b_j) = f(y)$$

for all i and j, $1 \leq i,\, j \leq N$. Therefore, the set of constants a_i form a cyclic multiplicative group of order N. Hence, $f^*(x,y)$ has a factor of the form

$$x - cy + e$$

where the multiplicative order of c is N. Thus,

$$f^*(x,y) = (x - cy - e)H_1(x,y)$$

for some polynomial $H_1(x,y)$ in $F_q[x,y]$.

Substituting $cy + e$ for y once, we obtain

$$f^*(x, cy+e) = (x - c^2y - ce - e)H_1(x, cy+e).$$

If $N > 1$, we also have

$$f^*(x, cy+e) = (x + e/(c-1) - c^2(y + e/(c-1)))H_2(x,y).$$

Repeating this substitution, we have

$$\begin{aligned} f^*(x, cy+e) &= \left(x - c^i y - \sum_{j=0}^{i-1} c^j e\right) H_i(x,y) \\ &= (x + e/(c-1) - c^i(y + e/(c-1)))H_i(x,y) \end{aligned}$$

for $i = 1, 2, \ldots, N$.

Therefore,

$$(x+e/(c-1))^N - (y+e/(c-1))^N = \prod_{i=1}^{N}((x+e/(c-1)) - c^i(y+e/(c-1)))$$

divides $f^*(x,y)$. Hence, by a change of variables, we assume without loss of generality that

$$f^*(x,y) = (x^N - y^N)\prod_{i=1}^{S} f_i(x,y) \tag{4}$$

where $f_i(x,y)$ are irreducible polynomials.

Now, each of the nonlinear factors $f_i(x,y)$ can be written uniquely as a sum of homogeneous polynomials

$$f_i(x,y) = \sum_{j=0}^{n_i} h_{ij}(x,y)$$

where $h_{ij}(x,y)$ denotes a homogeneous polynomial of degree j. Considering only the terms of highest degree in (4), we see

$$x^d - y^d = (x^N - y^N) \prod_{i=1}^{S} h_{in_i}(x,y).$$

Thus, the polynomials $h_{in_i}(x,y)$ are relatively prime in pairs, and they divide $x^d - y^d$. Let w be a primitive N-th root of unity, and suppose that there is a factor $f_i(x,y)$ with degree $n_i < N$. If we substitute x and y in (4) with $w^e x$ and $w^e y$ respectively, we obtain

$$\begin{aligned} f(x) - f(y) &= f(w^e x) - f(w^e y) \\ &= (x^N - y^N) \prod_{i=1}^{S} f_i(w^e x, w^e y). \end{aligned}$$

Thus, for any fixed e,

$$w^{-en_i} f_i(w^e x, w^e y) = f_{i'}(x,y)$$

for an appropriate i'. We have already seen that the terms of highest order are relatively prime in pairs; so i' must be i. We obtain

$$h_{in_i}(x,y) + \sum_{j=1}^{n_i} w^{-je} h_{in_i - j}(x,y) = f_i(x,y) = \sum_{j=0}^{n_i} h_{ij}(x,y)$$

for all e, consequently

$$f_i(x,y) = h_{in_i}(x,y).$$

So, $f_i(x,y)$ divides $x^d - y^d$. Accounting for our change of variables completes the proof of the lemma. $\square$

Lemma 2. *Let $f(x)$ be a monic polynomial over F_q of degree $d < q$. Let $\#f^*(x,y)$ be the number of solutions (x,y) in $F_q \times F_q$ of the equation $f^*(x,y) = 0$. Assume*

$$\#f^*(x,y) \leq cq$$

for some constant c, $1 < c < d$. Then

$$q/c \leq |V_f|.$$

Proof. Let R_i denote the number of images $f(x)$ that occur exactly i times as x ranges over F_q, not counting multiplicities. Then we have

$$\sum_{i=1}^{d} iR_i = q, \qquad |V_f| = \sum_{i=1}^{d} R_i, \quad \text{and} \quad \#f^*(x,y) = \sum_{i=1}^{d} i^2 R_i.$$

Further, we can apply Cauchy-Schwartz inequality to obtain

$$\begin{aligned} q^2 &= \left(\sum_{i=1}^{d} iR_i \right)^2 \\ &= \left(\sum_{i=1}^{d} (i\sqrt{R_i})(\sqrt{R_i}) \right)^2 \\ &\leq \left(\sum_{i=1}^{d} i^2 R_i \right) \left(\sum_{i=1}^{d} R_i \right) \\ &\leq \#(f^*(x,y))|V_f|. \end{aligned}$$

Therefore,

$$|V_f| \geq q^2/\#f^*(x,y) \geq q^2/cq = q/c. \qquad \square$$

We are ready for the main result.

Theorem 3. *Let F_q be the finite field with q elements. Let m and n be two integers dividing $q-1$, $2 \leq m$, $2 \leq n$, and $d = mn < \sqrt[4]{q}$. Then*

$$\frac{2q}{2m+2n-1} \leq |V_{(x^m+b)^n}| \leq \min\{(q-1)/m, (q-1)/n\} + 1 \tag{5}$$

for all $b \in F_q^*$.

Proof. Set $f(x) = (x^m + b)^n$, $b \in F_q^*$. Then

$$\begin{aligned} f^*(x,y) &= f(x) - f(y) \\ &= (x^m + b)^n - (y^m + b)^n \\ &= \prod_{j=0}^{m-1} (x - w_m^j y) \prod_{i=1}^{n-1} (x^m - w_n^i y^m + b - w_n^i b) \end{aligned}$$

where w_r denotes a primitive root of unity of order r. Now, by Lemma 1, the factors

$$H_i(x,y) = x^m - w_n^i y^m + b - w_n^i b$$

are either: absolutely irreducible or a product of linear factors. Assume that one of the factors $H_i(x,y)$, say

$$H(x,y) = x^m - Ay^m + B, \qquad B \neq 0,$$

is a product of distinct linear factors. Thus,

$$\begin{aligned} x^m - Ay^m + B &= \prod_{i=1}^{m} (x - a_i y - c_i), \\ x^m - Ay^m &= \prod_{i=1}^{m} (x - a_i y) \end{aligned} \tag{6}$$

and

$$B = \prod_{i=1}^{m} (-c_i).$$

Therefore, taking $x = a_1 y$ in (6), we obtain

$$B = (-c_1) \prod_{i=2}^{m} ((a_1 - a_i)y - c_i).$$

Hence, $c_1 = 0$ and, consequently, $B = 0$, a contradiction. Therefore, all the factors $H_i(x,y)$ are absolutely irreducible.

Now, as shown in [**6**, p. 330–333], we have

$$|\#H_i(x,y) - q| \leq (m-1)(m-2)\sqrt{q} + m^2.$$

Hence,

$$|\#f(x,y) - m(q-1) + 1) - (n-1)q| \leq (n-1)(m-1)(m-2)\sqrt{q} + m^2(n-1)$$

or

$$|\#f(x,y) - q(m+n-1) + m - 1| \leq (n-1)(m-1)(m-2)\sqrt{q} + m^2(n-1).$$

Combining with $d = mn < \sqrt[4]{q}$, we obtain

$$\#f(x,y) \leq q(m+n-1/2).$$

Hence, by Lemma 2, we have

$$\frac{2q}{2m+2n-1} \leq |V_{(x^m+b)^n}|.$$

Since the second inequality in (5) is a trivial result from (3), the proof of the theorem has been completed. □

Acknowledgment. The author thanks the referee for his suggestions that improved the final version of the paper.

REFERENCES

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.

2. W.S. Chou, J. Gomez-Calderon and G.L. Mullen, *Value sets of Dickson polynomials over finite fields*, J. Number Theory **30** (1988), 334–344.

3. J. Gomez-Calderon, *A note on polynomials with minimal value set over finite fields*, Mathematika **35** (1988), 144–148.

4. J. Gomez-Calderon and D.J. Madden, *Polynomials with small value sets over finite fields*, J. Number Theory **28** (1988), 167–188.

5. 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.

6. R. Lidl and Niederreiter, *Finite fields*, Encyclopedia Math. Appl., Vol. 20, Addison-Wesley, Reading, MA, 1983 (now distributed by Cambridge Univ. Press).

7. W.H. Mills, *Polynomials with minimal value sets*, Pacific J. Math. **14** (1964), 225–241.

Department of Mathematics, New Kensington Campus, Pennsylvania State University, New Kensington, Pennsylvania 15068