TAIWANESE JOURNAL OF MATHEMATICS
Vol. 12, No. 1, pp. 245-253, February 2008
This paper is available online at http://www.tjm.nsysu.edu.tw/

POLYNOMIALS OVER FINITE FIELDS WITH A GIVEN VALUE SET

Jiangmin Pan* and Kar-Ping Shum

Abstract. We study polynomials over finite fields with a given value set. By constructing relations among the coefficients of Lagrange Interpolation Formula of these polynomials, we obtain its new kind of expression. Using this we find some characterizations for the set and the number of such polynomials.

1. Introduction

Definition 1.1. Let F_q be the finite field of $q = p^n$ elements, where p is a prime and n is a positive integer. Let $f \in F_q[x]$, the value set V_f of polynomial f is defined to be the set $\{f(a) : a \in F_q\}$.

It is well known that every function (map) $f : F_q \to F_q$ can be uniquely expressed by a polynomial with degree $\leq q-1$ (since f and g induce the same function on F_q if and only if $f(x) \equiv g(x)(mod\ x^q - x)$). In fact, using well known Lagrange Interpolation Formula, see [5, p. 348], f can be expressed as follows:

$$f(x) = \sum_{a \in F_q} f(a)(1 - (x-a)^{q-1}) \tag{1}$$

Henceforth, it is enough to restrict our attention on polynomials with degree $\leq q-1$.

Throughout the paper, we adopt following definitions and notations.

Definition 1.2. For $0 \leq d \leq q-1$, $1 \leq k \leq q$, we define $M_q(k)$, $N_q(k)$, $M_q(d,k)$, $N_q(d,k)$ as follows:

$$M_q(k) = \{f \in F_q[x] : |V_f| = k\}$$

Received July 13, 2005, accepted July 5, 2006.
Communicated by Shun-Jen Cheng.
2000 *Mathematics Subject Classification*: 13M10, 12Y05.
Key words and phrases: Value set, Minimal value set polynomial, Trace, finite field.
*Supported by the NNSF of China.

$$M_q(d,k) = \{f \in F_q[x] : deg(f) = d \ and \ |V_f| = k\}$$

and

$$N_q(k) = |M_q(k)|, \ N_q(d,k) = |M_q(d,k)|.$$

Definition 1.3. Let $M = \{a_1, \cdots, a_k\}$ be a subset of F_q. We define $M_q(d, M) = M_q(d, \{a_1, \cdots, a_k\})$ as follows:

$$M_q(d,M) = \{f \in F_q[x] : deg(f) = d \ and \ V_f = M\}$$

and $N_q(d,M) = |M_q(d,M)|$.

Proposition 1.4.

$$M_q(k) = \bigcup_{d=0}^{q-1} M_q(d,k), \ M_q(d,k) = \bigcup_{M} M_q(d,M),$$

$$N_q(k) = \sum_{d=0}^{q-1} N_q(d,k), \ N_q(d,k) = \sum_{M} N_q(d,M),$$

where M extends over all k-elements subsets of F_q.

$N_q(d,2) = N_q(d,M)\binom{q}{2}$ *for each 2-elements subset M of F_q.*

Proof. Note that $\varphi : f(x) \to c_1 + (c_2 - c_1) f(x)$ is an one-to-one correspondence between $M_q(d, \{0,1\})$ and $M_q(d, \{c_1, c_2\})$, the second statement follows. The first statement is trivial. ∎

Among the notions defined above, the number $N_q(k)$ is not difficult to determine (see [2, p. 173]). However, the others, in general, are difficult to characterise even in a simple case: F_q is prime and $k = 2$ or 3 (see [1], [4]). Recently, [3] studied the number of polynomials of a given degree over a finite field with value sets of a given cardinality. By observing that the coefficient c_{q-1} of x^{q-1} (we use c_k to denote the coefficient of x^k) of $f(x)$ in (1) $= -\sum_{a \in F_q} f(a)$, the author related these numbers to the solutions of a class of equation over F_q, and, for prime fields, obtained a explicit formula for $N_p(p-1, M)$. In the present paper, we study $M_q(d, M)$ and $N_q(d, M)$ without the restriction $d = q - 1$. In section 2, we give a new expression of polynomials over finite field with a given value set by analyzing the relations among $c_1, c_2, \cdots, c_{q-1}$. In section 3, we obtain a specific characterization of polynomials over F_{2^n} with value set of cardinality 2. Precisely, we give a formula to count the number $N_{2^n}(d,2)$ and determine the explicit form of polynomials in $M_{2^n}(d,2)$ for every d. In section 4, The number of minimal value set polynomials with cardinality p^t is determined. In final section, we obtain a formula to count the number $N_q(q-1,3)$.

2. Expressions of Polynomials over F_q with Given Value Set

Let $q = p^n$, $s = p^t$, where $t \leq n$ is a positive integer. Let $T = \{0, 1, \cdots, q-1\}$. We define a relation "$\sim$" over T as follows:

$0 \sim 0$,
$i \sim j$ iff $i \equiv s^r j (mod\, q-1)$ for some integer $r \geq 0$ when $1 \leq i, j \leq q-1$.

It is not difficult to prove that the relation "$\sim$" is an equivalence relation over T, so it can determine a partition of T. Write

$[i]$: the equivalent class of number i.
$n(i)$: the cardinality of the set $[i]$.
$l(i)$: the largest number of the set $[i]$.
$\bar{k}$: the smallest positive integer of $k\ mod(\ q-1)$.
R : the representative set consisting of the largest integer in each equivalent class of T and $R^* = R \backslash \{0\}$.

The next proposition is obvious.

Proposition 2.1.

(1) $[i] = \{i, \overline{si}, \cdots, \overline{s^{n(i)-1} i}\}$ *for* $1 \leq i \leq q-1$.
(2) $n(i) = min\{j > 0 : s^j i \equiv i (mod\ q-1)\}$. *Particularly,* $n(0) = n(q-1) = 1$.

As a direct consequence of Lemma 2.1, it follows from (1) that

$$c_k = (-1)^q \sum_{a \in F_q} f(a) a^{q-k-1} \quad (k = 1, 2, \cdots, q-1) \tag{2}$$

Theorem 2.2. *Let $f \in F_q[x]$. If $a^s = a$ for each $a \in V_f$, then f can be uniquely expressed in the following form:*

$$f(x) = c_0 + \sum_{i \in R^*} \sum_{j=0}^{n(i)-1} c_i^{s^j} x^{\overline{is^j}} \tag{3}$$

Where c_i satisfying $c_i^{n(i)} = c_i$ for each $i \in R^*$.

Proof. To prove the theorem, by Proposition 2.1, it suffices to prove

$$c_{\overline{is^j}} = c_i^{s^j} \quad \text{for } i = 1, 2, \cdots, q-1.$$

Note that if k, l are positive integers, then x^k and x^l express the same function over F_q if and only if $k \equiv l(mod\ q-1)$. So, for $1 \le i \le q-1$, $a^{(q-i-1)s^j} = a^{q-\overline{is^j}-1}$ for each $a \in F_q$. Then (2) gives

$$\begin{aligned} c_i^{s^j} &= (-1)^{qs^j} \sum_{a \in F_q} f(a)^{s^j} a^{(q-i-1)s^j} \\ &= (-1)^q \sum_{a \in F_q} f(a) a^{q-\overline{is^j}-1} \\ &= c_{\overline{is^j}} \end{aligned}$$

The uniqueness of the expression is obvious. ■

Remark 2.3. In a special case $t \mid n$, i.e., V_f is in the subfield F_s of F_q, $f(x)$ can be expressed in form (3) with $c_i \in F_{p^{n(i)}}$ for all $i \in R^*$.

Corollary 2.4. *Let M be a subset of F_q. If $a^s = a$ for each $a \in M$, then $N_q(d, M) = 0$ if $d \notin R^*$.*

3. Characterization of Polynomials over F_{2^n} with Value Set of Cardinality 2

In this section, we always suppose that $q = 2^n$.

The following Theorem 3.1 and Corollary 3.2 give a specific characterization for polynomials with a value set of cardinality 2 over F_q.

Theorem 3.1.

$$M_q(2) = \Big\{ a + b \sum_{i \in R^*} \sum_{j=0}^{n(i)-1} c_i^{2^j} x^{\overline{i2^j}} : a \in F_q, b \in F_q^*, c_i \in F_{2^{n(i)}} \text{ not all zero} \Big\} \tag{4}$$

Proof. By Proposition 1.4, each polynomial $f(x) \in M_q(2)$ has the form:

$$f(x) = a + bg(x)$$

where $g(x) \in F_q[x]$ with the value set $V_g = \{0, 1\}$. Theorem 2.3 now implies that the set in left-hand side of (4) is contained in the set in right-hand side.

Conversely, for every $i \in R^*$, since $c_i^{2^{n(i)}} = c_i$ and $\overline{i2^{n(i)}} = i$, one can check that $\sum_{i \in R^*} \sum_{j=0}^{n(i)-1} c_i^{2^j} x^{\overline{i2^j}}$ (denoted by $h(x)$) satisfies

$$h(x)^2 \equiv h(x)(mod\ x^q - x)$$

So $V_h \subseteq \{0, 1\}$. Our proof is then finished by noting that these polynomials have degrees $\in \{1, 2, \cdots, q-1\}$. ■

Corollary 3.2. *Write* $R^* = \{l(i_1), l(i_2), \cdots, l(i_r)\}$ *with* $l(i_j)$ *ordered such that* $l(i_1) < l(i_2) < \cdots < l(i_r)$, *where* $r =| R^* |$. *Then*

$$N_q(d,2) = \begin{cases} 2^{1+\sum_{j=1}^{k-1} n(i_j)}(2^{n(i_k)} - 1)\binom{q}{2} & \textit{when } d = l(i_k) \\ 0 & \textit{other case} \end{cases}$$

The "even" property of degrees of polynomials in $M_q(2)$ is revealed as follows.

Theorem 3.3. *Let* $f \in F_q[x]$ *and* $|V_f| = 2$. *Then* $deg(f)$ *is always an even integer* $\geq 2^{n-1}$ *except* $deg(f) = q-1$.

Proof. The inequality is trivial. If $deg(f) \neq q-1$, by Corollary 2.4, it is suffices to prove that $l(i)$ are even for all $i \neq q-1$, equivalently, following claim:

Claim: If $\overline{2^{r+1}i}$ is odd, then $\overline{2^r i} > \overline{2^{r+1}i}$.

Suppose $\overline{2^{r+1}i} = 2k+1 < q-1$, then $\overline{2^r i} > 2^{n-1}$. Otherwise, $\overline{2^{r+1}i} = 2\overline{2^r i}$ is even, a contradiction. So $\overline{2^r i} - \overline{2^{r+1}i} = \overline{2^r i} - (2\overline{2^r i} - (q-1)) = q - 1 - \overline{2^r i} > 0$. ■

Corollary 3.4. $M_q(2^{n-1}, 2) = \{a + bTr_{F_q/F_2}(cx) : a \in F_q, b, c \in F_q^*\}$, *and* $N_q(2^{n-1}, 2) = (2^{n+1} - 2)\binom{q}{2}$.

Proof. It is easy to see that $l(1) = 2^{n-1}$, $n(1) = n$, $l(i) > l(1)$ for $1 < i \leq q-1$ and each polynomial $f \in M_q(2^{n-1}, 2)$ can be expressed as follows:

$$f(x) = a + b(cx + c^2x^2 + \cdots + c^{2^{n-1}}x^{2^{n-1}}) = a + bTr_{F_q/F_2}(cx)$$

where $a \in F_q$, b, $c \in F_q^*$. The second result is then obvious. ■

Corollary 3.5. $N_q(q-1, 2) = 2^{q-1}\binom{q}{2}$.

Proof. For each polynomial $f \in \bigcup_{d<q-1} M_q(d, \{0, 1\})$, by Theorem 3.1, $x^{q-1} + f(x) \in M_q(q-1, \{0, 1\})$, and each polynomial in $M_q(q-1, \{0, 1\})$ can be obtained in this way, so $N_q(q-1, \{0, 1\}) = \sum_{d<q-1} N_q(d, \{0, 1\})$. Therefore, $N_q(q-1, 2) = \sum_{d<q-1} N_q(d, 2)$. The result now follows by $N_q(2) = 2^q\binom{q}{2}$. ■

Corollary 3.6. *If* $q-1$ *is a (Mersenne) prime, with notations as in Theorem 3.2, we have*

$$M_q(2) = \Big\{a + b\Big(c_{q-1}x^{q-1} + Tr_{F_q/F_2}(c_{i_1}x^{i_1} + c_{i_2}x^{i_2} + \cdots + c_{i_{r-1}}x^{i_{r-1}})\Big)\Big\}$$

where $a \in F_q, b \in F_q^*$, $c_{i_1}, \cdots, c_{i_{r-1}} \in F_q$, $c_{q-1} \in F_2$ *and* c_i *not all zero.*

Proof. First, $n(q-1) = 1$. For $1 \le i \le q-2$, we have $n(i) = n$, the result now follows by Theorem 3.1 and the additivity of traces. ∎

4. Minimal Value Set Polynomials with Given Cardinality over Finite Fields

If $f \in F_q[x]$ has degree d, since every polynomial cannot have zeroes more than its degree in any field, it is easy to see that

$$\lfloor \frac{q-1}{d} \rfloor + 1 \le |V_f| \le q \tag{5}$$

(We use $\lfloor k \rfloor$ to denote the integer part of k). Polynomials achieving the lower bound are said to be $minimal\ value\ set\ polynomials$, and polynomials achieving the upper bound q (i.e., $V_f = F_q$) are known as $permutation\ polynomials$ (see [5, Chapter 7]).

Let $q = p^n$, $s = p^t$, where t is a positive divisor of n. Set $\lambda = \lfloor \frac{q-1}{s-1} \rfloor$. Then it is easy to see that $f(x) \in M_q(s)$ is a minimal value set polynomial if and only if $p^{n-t} \le deg(f) \le \lambda$.

The following theorem give the expression of minimal value set polynomials with cardinality s over F_q.

Theorem 4.2. *Set* $S = \{p^{n-t}, p^{n-t}+1, \cdots, \lambda\}$. *Then the set of all minimal value set polynomials with the value set* F_s *is as follows:*

$$\left\{ c_0 + \sum_{i \in R^* \bigcap S} \sum_{j=0}^{n(i)-1} c_i^{s^j} x^{\overline{is^j}} : c_0 \in F_s, c_i \in F_{s^{n(i)}} \text{ not all zero} \right\}.$$

Proof. Similar to the proof of Theorem 3.1. ∎

Corollary 4.2. *Write* $R^* \bigcap S = \{l(i_1), l(i_2), \cdots, l(i_m)\}$ *with* $l(i_1) < l(i_2) < \cdots < l(i_m)$. *Then for* $p^{n-t} \le d \le \lambda$, *we have*

$$N_q(d, F_s) = \begin{cases} s^{1+\sum_{j=1}^{k-1} n(i_j)}(s^{n(i_k)} - 1) & \textit{when } d = l(i_k) \\ 0 & \textit{other case} \end{cases}$$

Example Let $q = 5^3$. Determine all minimal value set polynomials with the value set F_5 over F_q.

First, it is easy to compute that $S = \{25, 26, 27, 28, 29, 30, 31\}$, $R^* \bigcap S = \{25, 30, 31\}$, $n(25) = n(30) = 3$ and $n(31) = 1$. Then Theorem 4.1 and Corollary 4.2 shows that the set of all minimal value set polynomials with the value set F_5 is $M_q(25, F_5) \bigcup M_q(30, F_5) \bigcup M_q(31, F_5)$ and

$$\begin{aligned} M_q(25, F_5) &= \{c_0 + Tr_{F_q/F_5}(c_1 x) : c_0 \in F_5, c_1 \in F_q^*\}, N_q(25, F_5) = 620. \\ M_q(30, F_5) &= \{c_0 + Tr_{F_q/F_5}(c_1 x + c_2 x^6) \\ &\qquad : c_0 \in F_5, c_1 \in F_q, c_2 \in F_q^*\}, N_q(30, F_5) = 77500. \\ M_q(31, F_5) &= \{c_0 + Tr_{F_q/F_5}(c_1 x + c_2 x^6) + c_3 x^{31}) \\ &\qquad : c_0 \in F_5, c_1, c_2 \in F_q, c_3 \in F_5^*\}, N_q(31, F_5) = 312500. \end{aligned}$$

Remark 4.3. Informally speaking, minimal value set polynomials over prime fields (i.e., $q = p$) are few (see [2], [4], [6]). However in case $q = p^n > p$, minimal value set polynomials over F_q are rich.

5. Formula for $N_q(q-1, 3)$

Definition 5.1. Let $f \in F_q[x]$ and $V_f = \{v_1, v_2, v_3\}$. Set $m_i = |f^{-1}(v_i)| = |\{a \in F_q : f(a) = v_i\}|$ for $i = 1, 2, 3$. We call $M_f = (m_1, m_2, m_3)$ the $multiplicity\ vector$ of polynomial f.

Definition 5.2. Let $S = (m_1, m_2, m_3)$ be the multiplicity vector of a polynomial in $F_q[x]$. We define $N_q(d, S)$ as follows:

$$N_q(d, S) = |\{f \in F_q[x] : deg(f) = d \ and \ M_f = S\}|$$

Note that $m_1 + m_2 + m_3 = q$ and $N_q(d, 3) = \sum_S N_q(d, S)$, where the summation extends over all possible multiplicity vector S.

Theorem 5.3. *Let $q \geq 3$ and $S = (m_1, m_2, m_3)$ as in the above. Set $N = \frac{q!q(q-1)(q-3)}{m_1!m_2!m_3!}$. We have*

(1) *If there exists m_i such that $p \mid m_i$, then $N_q(q-1, S) = 0$.*

(2) *If $p \nmid m_i$ for $i = 1, 2, 3$, then*

$$N_q(q-1, S) = \begin{cases} N & m_1, m_2, m_3 \text{ are different} \\ \frac{1}{6}N & m_1 = m_2 = m_3 \\ \frac{1}{2}N & \text{other case} \end{cases}$$

Proof. Suppose $f \in M_q(3)$ such that $M_f = (m_1, m_2, m_3)$ and $V_f = \{v_1, v_2, v_3\}$.

By (2), the coefficient of x^{q-1} in $f(x)$ is $c_{q-1} = -\sum_{i=1}^{3} m_i v_i$. So $f \in M_q(q-1, S)$ if and only if $m_1 v_1 + m_2 v_2 + m_3 v_3 \neq 0$.

Consider the equation

$$m_1 x_1 + m_2 x_2 + m_3 x_3 = 0 \tag{6}$$

over F_q with restriction $x_i \neq x_j$ if $i \neq j$.

Case 1. If there exists one m_i, for example m_1, such that $p \mid m_1$.

Since $m_1 + m_2 + m_3 = q$, the equation (6) shows $p \mid m_2$ and $x_2 \neq x_3$, in turn, $p \mid m_3$. Therefore, $c_{q-1} = 0$. This proves (1) in the theorem.

Case 2. If $p \nmid m_i$ for $i = 1, 2, 3$.

For any given $x_2, x_3 \in F_q$ with $x_2 \neq x_3$, there exists an unique $x_1 \in F_q$ satisfying (6) and x_1 not equals x_2 or x_3, so the number of solutions in F_q of the equation (6) is $q(q-1)$. Our proof is then finished by Theorem 2.2 in [3]. ∎

Acknowledgment

The authors are grateful to the referee for the helpful suggestions.

References

1. A. Biró, On polynomials over prime fields taking only two values on the multiplicative group, *Finite Fields Appl.* **6** (2000), 302-308.

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

3. P. Das, The number of polynomials of a finite field with value sets of a given cardinality, *Finite fields Appl., 9* (2003), 168-174.

4. J. Gomez-Calderon, Polynomials with small value set over finite fields, *J. Number Theory*, **28** (1988), 167-188.

5. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, Addision-Wesley, Reading, MA, 1983.

6. W. H. Mills, Polynomials with minimal value sets, *Amer. Math. Soc.*, **4** (1963), 225-241.

Jiangmin Pan
Department of Mathematics,
Yunnan University,
Kunming 650091,
P. R. China
E-mail: jmpan@ynu.edu.cn

Kar-ping Shum
Department of Mathematics,
The Chinese University of Hong Kong,
Hong Kong
E-mail: kpshum@math.cnhk.edu.hk