VALUE SETS OF POLYNOMIALS OVER FINITE FIELDS

DAQING WAN, PETER JAU-SHYONG SHIUE, AND C. S. CHEN

(Communicated by William W. Adams)

Dedicated to the memory of Professor L. Kuipers

Abstract. Let \( \mathbb{F}_q \) be the finite field of \( q \) elements, and let \( V_f \) be the number of values taken by a polynomial \( f(x) \) over \( \mathbb{F}_q \). We establish a lower bound and an upper bound of \( V_f \) in terms of certain invariants of \( f(x) \). These bounds improve and generalize some of the previously known bounds of \( V_f \). In particular, the classical Hermite-Dickson criterion is improved. Our bounds also give a new proof of a recent theorem of Evans, Greene, and Niederreiter. Finally, we give some examples which show that our bounds are sharp.

1. Introduction

Let \( \mathbb{F}_q \) be the finite field of \( q \) elements with characteristic \( p \). If \( f(x) \) is a polynomial over \( \mathbb{F}_q \) of degree smaller than \( q \), a basic question in the theory of finite fields is to estimate the size \( V_f \) of the value set \( \{f(a) | a \in \mathbb{F}_q\} \). Because a polynomial \( f(x) \) cannot assume a given value of more than \( \deg(f) \) times over a field, one has the trivial bound

\[
V_f \leq q - \frac{1}{\deg(f)} + 1.
\]

If the lower bound in (1.1) is attained, \( f(x) \) is called a minimal value set polynomial. The classification of minimal value set polynomials is the subject of several papers; see [1, 4, 5, 8]. The results in these papers assume that \( q \) is large compared to the degree of \( f(x) \). For Dickson polynomials, Chou, Gomez-Calderon, and Mullen [3] obtained an explicit formula for \( V_f \).

If the upper bound in (1.1) is attained, \( f(x) \) is called a permutation polynomial. The classification of permutation polynomials has received considerable attention. See the book of Lidl and Niederreiter [7] and the very recent survey article by Mullen [9]. If \( f(x) \) is not a permutation polynomial, the following upper bound is obtained in [11]:

\[
V_f \leq q - \frac{q - 1}{\deg(f)}. \tag{1.2}
\]
This upper bound coincides with the conjectural upper bound of Mullen [9]. In §§2 and 3 of this paper, we shall give improvements of (1.1) and (1.2). Let \( u_p(f) \) be the smallest positive integer \( k \) such that \( \sum_{x \in \mathbb{F}_q} f(x)^k \neq 0 \). Like the degree of \( f(x) \), \( u_p(f) \) is invariant under linear transformations. Our lower bound depends on the invariant \( u_p(f) \). Our upper bound depends on a similar invariant involving \( p \)-adic liftings, see §3. It is not strange that \( V_f \) is related to \( u_p(f) \). In terms of the invariant \( u_p(f) \), the well-known Hermite-Dickson criterion states that \( f(x) \) is a permutation polynomial if and only if \( u_p(f) = q - 1 \). Our results improve the Hermite-Dickson criterion and give a new proof of a recent theorem of Evans, Greene, and Niederreiter [3]. In §4, we give some examples for which our bounds are sharp.

2. A LOWER BOUND

Let \( f(x) \) be a polynomial over \( \mathbb{F}_q \). Define \( u_p(f) \) to be the smallest positive integer \( k \) such that \( \sum_{x \in \mathbb{F}_q} f(x)^k \neq 0 \). If such \( k \) do not exist, define \( u_p(f) = \infty \). It is easy to check that if \( u_p(f) < \infty \), then \( u_p(f) < q \). One checks that \( u_p(f) \) is invariant under linear transformations. That is, for \( a \in \mathbb{F}_q^* \) and \( b \in \mathbb{F}_q \), we have \( u_p(af + b) = u_p(f(ax + b)) = u_p(f) \). Furthermore, \( u_p(f) \) is invariant under substitutions of permutation polynomials, i.e., \( u_p(f) = u_p(f \circ g) \) for all permutation polynomials \( g(x) \).

**Theorem 2.1.** If \( u_p(f) < \infty \), then \( V_f \geq u_p(f) + 1 \).

**Proof.** Let \( N_a \) be the number of solutions of the equation \( f(x) = a \) over \( \mathbb{F}_q \). Then

\[
N_a = \sum_{x \in \mathbb{F}_q} (1 - (f(x) - a)^{(q-1)}) = -\sum_{x \in \mathbb{F}_q} (f(x) - a)^{q-1} \\
\quad \equiv -\sum_{k=1}^{q-1} \left( \sum_{x \in \mathbb{F}_q} \binom{q-1}{k} f(x)^k \right) (-a)^{q-1-k} \pmod{p}.
\]

Since \( \binom{q-1}{k} \neq 0 \pmod{p} \) for \( 1 \leq k \leq q-1 \), by the definition of \( u_p(f) \) we conclude that the polynomial \( N_a \) (as a polynomial of \( a \)) has degree \( q - 1 - u_p(f) \). Since \( N_a = 0 \) for all \( a \) not in the value set of \( f(x) \), it follows that there are at least \( q - V_f \) elements \( a \in \mathbb{F}_q \) such that \( N_a \equiv 0 \pmod{p} \). Thus, \( q - 1 - u_p(f) \geq q - V_f \). This proves that \( V_f \geq u_p(f) + 1 \).

**Remark 2.2.** If \( f(x) \) is a permutation polynomial, then the Hermite-Dickson criterion shows that \( u_p(f) = q - 1 \). Thus, Theorem 2.1 is sharp for permutation polynomials. If \( f(x) \) is the monomial \( x^d \), then one checks that \( u_p(f) = (q-1)/(d, q-1) \) and \( V_f = (q-1)/(d, q-1) + 1 \). Thus, Theorem 2.1 is also sharp for monomials. This shows that Theorem 2.1 is sharp for polynomials of all degrees. For more sharp examples, see §4. If \( V_f = 1 \), \( f \) must be a constant. If \( V_f = 2 \), Theorem 2.1 shows that \( u_p(f) = 1 \). This implies that \( \deg(f) = q - 1 \).

**Remark 2.3.** Equation (2.1) shows that if \( u_p(f) = \infty \), then \( N_a \) is divisible by \( p \) for all \( a \in \mathbb{F}_q \). This shows that if \( \deg(f) < p \), then \( u_p(f) < \infty \). In particular, \( u_p(f) \) is always finite for the prime field \( \mathbb{F}_p \) and Theorem 2.1 can be applied unconditionally to the prime field \( \mathbb{F}_p \). Polynomials with \( u_p(f) = \infty \)
have also appeared in the recent paper [3] by Evans, Greene, and Niederreiter. In fact, we shall show in the next section that our bound can be used to give a new proof of their main theorem. We note that if \( f(x) \equiv s \circ g \circ h(x) \pmod{(x^q - x)} \), where \( h(x) \) is a permutation polynomial, \( g(x) = \sum_i a_i x^{p^i} \) is a \( p \)-linearized nonpermutation polynomial and \( s(x) \) is any polynomial, then \( u_p(f) = \infty \).

**Corollary 2.4.** Let \( \deg(f) = d \) and \( u_p(f) < \infty \). Then

\[
V_f \geq \begin{cases} 
\frac{(q-1)}{d} + 1 & \text{if } d \mid q - 1, \\
\frac{(q-1)}{d} + 2 & \text{if } d \nmid q - 1. 
\end{cases}
\]

**Proof.** Let \( f(x) = a_dx^d + \cdots + a_0 \in F_q(x) \). One checks that \( u_p(f) = \lfloor (q-1)/d \rfloor \) if \( d \mid q - 1 \). Otherwise, \( u_p(f) \geq \lfloor (q-1)/d \rfloor + 1 \). The corollary follows.

**Corollary 2.5.** Let \( 3 \leq d < p \). Assume that \( d \) does not divide \( q - 1 \). Then

\[
(2.2) \quad V_f > \left\lfloor \frac{q-1}{d} \right\rfloor + \frac{2(q-1)}{d^2}.
\]

**Proof.** Assume that (2.2) is not true. Since \( 3 \leq d < p \), the theorem of Gomez-Calderon [4] shows that \( V_f = \lfloor (q-1)/d \rfloor + 1 \). Since \( d \) does not divide \( q - 1 \) and \( u_p(f) < \infty \) \((d < p)\), Corollary 2.5 shows that \( V_f > \lfloor (q-1)/d \rfloor + 1 \). This is a contradiction. The corollary is proved.

### 3. An Upper Bound

To describe the upper bound, we need \( p \)-adic liftings. Let \( Q_p \) be the field of \( p \)-adic rational numbers. Let \( K \) be the unique unramified extension of \( Q_p \) with residue field \( F_q \). Let \( T \) be the set of Teichmüller liftings of \( F_q \) in \( K \). \( T \) is the set of all \( b \in K \) satisfying \( bq = b \). Let \( F(x) \) be a lifting of \( f(x) \) to \( K(x) \). Define \( U_q(f) \) to be the smallest positive integer \( k \) such that

\[
(3.1) \quad \sum_{x \in T} F(x)^k \not\equiv 0 \pmod{pk}.
\]

One checks that \( U_q(f) \) is independent of the choice of the lifting \( F(x) \). Furthermore, \( U_q(f) \) is invariant under linear transformations, in fact, invariant under substitutions of permutation polynomials. Unlike \( u_p(f) \), \( U_q(f) \) is always finite as we shall show in the proof of Theorem 3.1. If \( f(x) \) is a permutation polynomial, then \( u_p(f) = U_q(f) = q - 1 \).

**Theorem 3.1.** Assume that \( f \in F_q(x) \) is not a permutation polynomial. Then

\[
(3.2) \quad V_f \leq q - U_q(f).
\]

In order to prove Theorem 3.1, we need to use the following lemma from [11].

**Lemma 3.2.** Let \( T = \{t_1, \ldots, t_q\} \) with \( t_q = 0 \). Let \( w \) be an integer satisfying \( 1 \leq w \leq q - 1 \). Given \( p \)-adic integers \( b_1, \ldots, b_w, a_{w+1}, \ldots, a_q \) in \( K \), there are uniquely determined \( p \)-adic integers \( a_1, \ldots, a_w \) in \( K \) such that

\[
(3.3) \quad \sum_{i=1}^q (t_i + pa_i)^k = pk b_k, \quad 1 \leq k \leq w.
\]
Proof of Theorem 3.1. Let \( w = q - V_f \). Since \( f(x) \) is not a permutation polynomial, we have \( w \geq 1 \). Let \( F(x) \) be a lifting of \( f(x) \) to \( K[x] \). By the definition of \( w \), we can reorder the sequence \( \{F(t_i)\} \) as \( \{c_i\} \) such that \( c_{w+1}, \ldots, c_q \) are the representatives of the residue classes modulo \( p \) of the sequence \( \{F(t_i)\} \). By assuming \( f(0) = 0 \), we may assume that \( c_q \) is divisible by \( p \).

We claim that \( w \geq U_q(f) \), i.e., \( V_f \leq q - U_q(f) \). This implies that \( U_q(f) \) is always finite. If the claim is not true, i.e., \( w \leq U_q(f) - 1 \), we derive a contradiction as follows: For all \( 1 \leq k \leq w \), the definition of \( U_q(f) \) shows that

\[
\sum_{i=1}^{q} c_i^k = \sum_{i=1}^{k} F^k(t_i) = pkb_k,
\]

where the \( b_k \) are \( p \)-adic integers. By Lemma 3.2, there are \( p \)-adic integers \( a_1, \ldots, a_w \) such that

\[
\sum_{i=1}^{w} a_i^k + \sum_{i=w+1}^{q} c_i^k = pkb_k, \quad 1 \leq k \leq w.
\]

Furthermore, none of the \( a_i \) is congruent to any \( c_j \). Thus, we have

\[
\sum_{i=1}^{w} a_i^k = \sum_{i=1}^{w} a_i^k + \sum_{i=w+1}^{q} c_i^k - pkb_k
\]

\[
= \left( \sum_{i=1}^{w} a_i^k + \sum_{i=w+1}^{q} c_i^k - pkb_k \right) + \sum_{i=1}^{w} c_i^k
\]

\[
= \sum_{i=1}^{w} c_i^k, \quad 1 \leq k \leq w.
\]

From this equation and Newton’s formula about symmetric polynomials, we deduce that the two polynomials \( \prod_{i=1}^{w} (x - a_i) \) and \( \prod_{i=1}^{w} (x - c_i) \) have the same coefficients (note that we are in characteristic zero). Thus, their roots \( \{a_i\} \) and \( \{c_i\} \) are the same. This contradicts the fact that none of the \( a_i \) is congruent to any \( c_j \). Thus, the claim is true and the theorem is proved.

Remark. One checks that

\[
u_p(f) \geq U_q(f) \geq \left\lceil \frac{q-1}{\deg(f)} \right\rceil.
\]

Thus, Theorem 2.1 and Theorem 3.1 improve (1.1) and (1.2). The second inequality in (3.7) is an equality if and only if \( \deg(f) \) divides \( q-1 \). This and Theorem 3.1 show that the bound (1.2) is not sharp if \( \deg(f) \) does not divide \( q-1 \).

Corollary 3.3. Assume that \( u_p(f) + U_q(f) > q - 1 \). Then either \( u_p(f) = \infty \) or \( f(x) \) is a permutation polynomial over \( F_q \).

Proof. Assume that \( u_p(f) \neq \infty \). If \( f(x) \) is not a permutation polynomial, Theorem 2.1 and Theorem 3.1 would imply that \( 1 + u_p(f) \leq V_f \leq q - U_q(f) \). Thus, \( u_p(f) + U_q(f) \leq q - 1 \). This contradicts our assumption.

In view of (3.7) and Corollary 3.3, we have
Corollary 3.4. A polynomial $f(x)$ over $\mathbb{F}_q$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $q - 1 - \left[\frac{(q-1)}{\deg(f)}\right] < u_p(f) < \infty$.

If $q = p$, then $u_p(f) = U_q(f)$ is always finite. Corollary 3.3 implies that

Corollary 3.5 (Roger). Let $q = p$. A polynomial $f(x)$ over $\mathbb{F}_q$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $u_p(f) > \frac{(p - 1)}{2}$.

Remark. The Hermite-Dickson criterion says that $f(x)$ is a permutation polynomial if and only if $u_p(f) = q - 1$. In the case $q = p$, this criterion was improved by Roger [10] as stated in Corollary 3.5. The theorem of Rogers was rediscovered by Kurbatov and Starkov [6]. Corollary 3.3 improves both the Hermite-Dickson criterion and the Rogers Theorem.

Corollary 3.6. Let $f(x) = g^2(x)$, where $g(x)$ is a permutation polynomial. Assume that $q$ is odd. Then $1 + u_p(f) = V_f = q - U_q(f)$. In particular, both Theorem 2.1 and Theorem 3.1 are sharp in this case.

Proof. It is trivial if $g(x) = x$. In the general case, since $V_f$, $u_p(f)$, and $U_q(f)$ are all invariant under substitutions of permutation polynomials, we are reduced to the case $g(x) = x$.

Corollary 3.7 (Evans, Greene, and Niederreiter [3]). Let $f(x) \in \mathbb{F}_q[x]$ with $\deg(f) < q$ be such that $f(x) + cx$ is a permutation polynomial for at least $\lfloor q/2 \rfloor$ values of $c \in \mathbb{F}_q$. Then the following properties hold.

(i) For every $c \in \mathbb{F}_q$ for which $f(x) + cx$ is not a permutation polynomial, $f(x) + cx$ maps $\mathbb{F}_q$ into $\mathbb{F}_q$ in such a way that each of its values has a multiple of $p$ distinct preimages, i.e., $u_p(f(x) + cx) = \infty$.

(ii) $f(x) + cx$ is a permutation polynomial for at least $q - (q - 1)/(p - 1)$ values of $c \in \mathbb{F}_q$.

(iii) $f(x) = ax + g(x^p)$ for some $a \in \mathbb{F}_q$ and $g(x) \in \mathbb{F}_q[x]$.

Proof. If $c \in \mathbb{F}_q$ is such that $f(x) + cx$ is a permutation polynomial, then we have $u_p(f(x) + cx) = U_q(f(x) + cx) = q - 1$. If now $f(x) + cx$ is a permutation polynomial for at least $\lfloor q/2 \rfloor$ values of $c \in \mathbb{F}_q$, then for $0 < k < q - 1$, the congruence equation $\sum_{x \in T}(F(x) + cx)^k \equiv 0 \pmod{pk}$ in $c$ of degree at most $(k - 1)$ has at least $\lfloor q/2 \rfloor$ solutions $c \in T$. This implies that the $p$-adic integral polynomial $\sum_{x \in T}(F(x) + cx)^k$ in $c$ of degree at most $(k - 1)$ is identically congruent to zero modulo $pk$ for all $k \leq \lfloor q/2 \rfloor$. Thus, $U_q(f(x) + cx) \geq \lfloor q/2 \rfloor + 1$ for all $c \in \mathbb{F}_q$, and $u_p(f(x) + cx) \geq \lfloor q/2 \rfloor + 1$ for all $c \in \mathbb{F}_q$. Corollary 3.3 shows that for each $c \in \mathbb{F}_q$, either $u_p(f(x) + cx) = \infty$ or $f(x) + cx$ is a permutation polynomial. This proves (i) and shows that for all $c \in \mathbb{F}_q$,

$$s_n(c) = \sum_{a \in \mathbb{F}_q} \left((f(a) + ca)^n\right) = 0, \quad 1 \leq n \leq q - 2.$$  

Thus, $s_n(y)$ is identically zero. As in [3], (iii) follows easily by comparing the coefficients of $y^{n-1}$ in $s_n(y)$, where $n$ is not divisible by $p$. Also as in [3], (ii) follows easily from (i), because to each $c \in \mathbb{F}_q$ for which $f(x) + cx$ is not a permutation polynomial there correspond at least $p - 1$ distinct nonzero solutions $x \in \mathbb{F}_q$ to $f(x) + cx = f(0)$. Thus, there are at most $(q - 1)/(p - 1)$ values of such $c$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
4. More sharp examples

In this section, we consider polynomials of the form \( x^rf(x^{(q-1)/d}) \), where \( d \) is a positive integer dividing \( q - 1 \) and \( r \) is relatively prime to \( (q - 1) \). The question of when such a polynomial is a permutation polynomial was treated in [12]. The size of the value set for this type of polynomials can be determined in a similar way. We show that our bounds are sharp for some of the polynomials of this type.

If \( d = 1 \), we get monomials \( x^r \) which are permutation polynomials since \( r \) is relatively prime to \( q - 1 \). Thus, Theorem 2.1 is sharp.

If \( d = 2 \), then we get polynomials of the form \( g_a(x) = x^r(x^{(q-1)/2} + a) \), where \( a \in F_q \) (excluding the trivial case \( a = 0 \)). From the work in [12], we know that \( g_a(x) \) is a permutation polynomial if and only if \( a^2 \neq 1 \) and \((a^2 - 1) \) is a quadratic residue of \( F_q \). If \( g_a(x) \) is a permutation polynomial, then Theorem 2.1 is sharp. If \( g_a(x) \) is not a permutation polynomial, then one checks that the value set \( V(g_a(x)) = (q + 1)/2 \). Let \( \psi \) be the multiplicative quadratic character of \( F_q \). Then

\[
\sum_{x \in F_q} g_a(x)^k = \sum_{\psi(x) = 1} x^{rk}(a + 1)^k + \sum_{\psi(x) = -1} x^{rk}(a - 1)^k.
\]

**Table I.** \( f(x) = x^7 + ax \)

<table>
<thead>
<tr>
<th>( q )</th>
<th>( a )</th>
<th>( \frac{q-1}{\deg(f)} + 1 )</th>
<th>( 1 + u_p(f) )</th>
<th>( V_f )</th>
<th>( q - U_q(f) )</th>
<th>( q - \frac{q-1}{\deg(f)} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>1</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>2</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>3</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>4</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>6</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>7</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>8</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>9</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>10</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>11</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>12</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>13</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>14</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>15</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>18</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
</tbody>
</table>
From this equation and the assumption that $a^2 = 1$ or $a^2 - 1$ is a quadratic nonresidue, we compute that $u_p(g_a(x)) = (q - 1)/2$. In a similar way, we show that $U_q(g_a(x)) = (q - 1)/2$. Thus, both Theorem 2.1 and Theorem 3.1 are sharp if $a^2 = 1$ or $a^2 - 1$ is a quadratic nonresidue.

For a general $d$, the method in [12] can be used to prove that the cardinality of the value set of $g_{r,d} = x^{r}f(x^{(q-1)/d})$ is of the form $1 + i(q - 1)/d$ for some integer $i$ with $1 \leq i \leq d$. If $i = d$, then we get permutation polynomials. Thus, Theorem 2.1 is sharp. If $i = d - 1$, then the value set has cardinality $q - (q - 1)/d$ and it can be proved that $u_p(g_{r,d}) = U_q(g_{r,d}) = (q - 1)/d$. Thus, Theorem 3.1 is sharp in this case. If $i = 1$, then the value set has cardinality $q - (q - 1)/d$ and it can be proved that $u_p(g_{r,d}) = U_q(g_{r,d}) = (q - 1)/d$. Thus, Theorem 2.1 is sharp in this case.

Table I compares the various bounds and the value set of the polynomials of the form $f_a(x) = x^7 + ax = x(x^{(19-1)/3} + a)$. In the above notation, $q = 19$, $r = 1$, and $d = 3$. We note that $f_a(x)$ is a permutation polynomial if $a = 0, 5, 16, \text{ and } 17$.

**Acknowledgment**

We would like to thank Ronald Evans for several helpful comments.

**References**