On Value Sets of Polynomials over a Finite Field

Wayne Aitken*

Department of Mathematics, California State University, San Marcos, California 92096
E-mail: waitken@mailhost1.csusm.edu

Communicated by Gerhard Turnwald

Received October 7, 1997; revised April 20, 1998

We study value sets of polynomials over a finite field, and value sets associated to pairs of such polynomials. For example, we show that the value sets (counting multiplicities) of two polynomials of degree at most \( d \) are identical or have at most \( q - (q - 1)/d \) values in common where \( q \) is the number of elements in the finite field. This generalizes a theorem of D. Wan concerning the size of a single value set. We generalize our result to pairs of value sets obtained by restricting the domain to certain subsets of the field. These results are preceded by results concerning symmetric expressions (of low degree) of the value set of a polynomial. K. S. Williams, D. Wan, and others have considered such expressions in the context of symmetric polynomials, but we consider (multivariable) polynomials invariant under certain important subgroups of the full symmetry group.

1. NOTATION AND HISTORICAL INTRODUCTION

This paper will use the following notation:

- Let \( \mathbb{F}_q \) be a finite field of characteristic \( p \) with \( q \) elements.
- Fix, once and for all, an ordering of \( \mathbb{F}_q \),

\[
\mathbb{F}_q = \{a_1, a_2, \ldots, a_q\}.
\]

- Given elements \( r_1, \ldots, r_n \) in a ring \( R \), let \( \sigma_k(r_1, \ldots, r_n) \in R \) denote the \( k \)th elementary symmetric expression of \( r_1, \ldots, r_n \), i.e.,

\[
\sigma_k(r_1, \ldots, r_n) \overset{\text{def}}{=} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} r_{i_1}r_{i_2}\cdots r_{i_k}.
\]

* Partially supported by NSA Grant MDA904-94-H-2054.
**Definition.** A polynomial \( f \in \mathbb{F}_q[x] \) is said to be a *permutation polynomial* if the function \( c \mapsto f(c) \) is surjective on \( \mathbb{F}_q \) (and hence bijective).

**Definition.** A polynomial \( F \) in \( \mathbb{F}_q[x,y] \) is said to be an *absolutely irreducible* if \( F \) is irreducible in \( \overline{\mathbb{F}}_q[x,y] \) where \( \overline{\mathbb{F}}_q \) is the algebraic closure of \( \mathbb{F}_q \).

**Definition.** A polynomial \( f \) in \( \mathbb{F}_q[x] \) is said to be an *exceptional polynomial* over \( \mathbb{F}_q \) if \( f(x) - f(y) \) has no absolutely irreducible factor in \( \mathbb{F}_q[x,y] \) except \( x - y \) (or constant multiples of \( x - y \)).

One of the most fundamental results in the theory of permutation polynomials is the following theorem of Cohen:

*Let \( f \) be a polynomial in \( \mathbb{F}_q[x] \). If \( f \) is exceptional over \( \mathbb{F}_q \) then it is a permutation polynomial over \( \mathbb{F}_q \).*

This theorem was originally conjectured by Davenport and Lewis [DL] in 1963, and proved by Cohen [C] in 1970 who used techniques from algebraic number theory. In 1993, D. Wan [Wa] gave a simpler proof in which he proved the following two theorems and showed how the above theorem follows from them.

**Theorem 1.** Let \( f \in \mathbb{F}_q[x] \) be a polynomial of positive degree \( d \). Then

\[
\sigma_k(f(a_1), \ldots, f(a_q)) = 0
\]

for \( 0 < k < (q-1)/d \).

**Theorem 2.** Let \( f \in \mathbb{F}_q[x] \) be a polynomial of positive degree \( d \). If \( f \) is not a permutation polynomial then the number of elements in the image \( f(\mathbb{F}_q) \) is less than or equal to \( q - \frac{2^{\frac{d}{2}}}{d} \).

Theorem 2 was first conjectured by Mullen [Mu] in the case where \( q \) is odd and \( d \) is even. Wan’s proofs of Theorems 1 and 2 build on ideas of Williams [Wi], but circumvent the difficulties of Williams’ approach by employing a p-adic lifting theorem. Later, G. Turnwald [Tu] gave elementary proofs of Theorems 1 and 2.

This paper gives generalizations of Theorems 1 and 2. Theorem 1 will be extended in Theorem 3 below to expressions more general than those symmetric under the full symmetry group on \( q \) elements (and in the process gives a new elementary proof of Theorem 1, substantially different than that in [Tu]). Theorem 2 will be generalized to pairs of polynomials and to images of certain subsets of \( \mathbb{F}_q \).

(A good introduction to permutation polynomials and exceptional polynomials is [LN], while [Mu] is a good source for more recent results. Note that the above definition of exceptional is that given in [Wa], but other authors often impose the additional condition that \( x - y \) divides \( f(x) - f(y) \).)
to exactly first order. However, Cohen’s Theorem as stated above is valid for either definition.)

2. SYMMETRY PROPERTIES OF VALUE SETS

Given \( \varphi \) a permutation of \( \{1, 2, \ldots, q\} \) and \( F \in \mathbb{F}_q[x_1, x_2, \ldots, x_q] \), define \( \varphi F \) to be the element of \( \mathbb{F}_q[x_1, x_2, \ldots, x_q] \) given by the equation

\[
\varphi F(x_1, x_2, \ldots, x_q) \overset{\text{def}}{=} F(x_{\varphi(1)}, x_{\varphi(2)}, \ldots, x_{\varphi(q)}).
\]

Note that this defines an (\( \mathbb{F}_q \)-algebra) action of the permutation group (on \( q \) elements) on \( \mathbb{F}_q[x_1, x_2, \ldots, x_q] \). This action restricts to an action on homogeneous polynomials of a given degree.

Let \( b \in \mathbb{F}_q^* \), and let \( \varphi_b \) be the unique permutation of \( \{1, 2, \ldots, q\} \) with the property that \( ba_i = a_{\varphi_b(i)} \). Given \( b \in \mathbb{F}_q^* \) and \( F \in \mathbb{F}_q[x_1, x_2, \ldots, x_q] \), define \( bF \) to be \( \varphi_b F \). Note that this defines an (\( \mathbb{F}_q \)-algebra) action of \( \mathbb{F}_q^* \) on \( \mathbb{F}_q[x_1, x_2, \ldots, x_q] \). This action restricts to an action on homogeneous polynomials of a given degree.

**Theorem 3.** Suppose \( F \in \mathbb{F}_q[x_1, x_2, \ldots, x_q] \) is a polynomial of degree \( D \), and \( G \) is a subgroup of \( \mathbb{F}_q^* \) of order \( g \) which fixes \( F \) (i.e., \( bF = F \) for all \( b \in G \)). If \( f \in \mathbb{F}_q[x] \) is a polynomial of degree \( d \) and if \( dD < g \), then

\[
F(f(a_1), f(a_2), \ldots, f(a_q)) = F(f(0), f(0), \ldots, f(0)).
\]

**Proof.** Let \( h \in \mathbb{F}_q[t] \) be defined as

\[
h(t) \overset{\text{def}}{=} F(f(a_1t), \ldots, f(a_qt)).
\]

Note that \( h \) has degree less than \( g \). Note also that if \( b \in G \), then

\[
h(b) = F(f(a_1b), \ldots, f(a_qb)) = F(f(a_{\varphi_b(1)}), \ldots, f(a_{\varphi_b(q)})) = bF(f(a_1), \ldots, f(a_q)) = h(1).
\]

Thus \( h(t) - h(1) \) has at least \( g \) zeros, but its degree is less than \( g \). Thus \( h(t) - h(1) = 0 \). In particular, \( h(1) = h(0) \). The results follows.

We note that Theorem 1 follows from Theorem 3 since each elementary symmetric polynomial \( \sigma_k(x_1, \ldots, x_q) \) is invariant under the action of \( \mathbb{F}_q^* \), and
since, for $0 < k < q - 1$, 

$$\sigma_k(f(0), \ldots, f(0)) = \left( \frac{q}{k} \right) f(0)^k = 0 \cdot f(0)^k = 0.$$ 

We illustrate Theorem 3 with a couple of examples:

**EXAMPLE 2.1.** Consider the field $\mathbb{F}_{11}$ where the elements of $\mathbb{F}_{11}$ are ordered as follows: 1, 2, 3, ..., 9, 10, 0. Consider the polynomial

$$F = x_1x_2 + x_1x_6 + x_2x_4 + x_3x_6 + x_4x_7 + x_4x_8 + x_5x_8 + x_5x_{10} + x_7x_9 + x_9x_{10} + x_{11}^2.$$ 

Note that $F$ is invariant under the action of $\mathbb{F}_{11}^*$ (one only needs to check invariance under the generator $2 \in \mathbb{F}_{11}^*$). Note also that since $F$ has 11 terms, $F(c, c, \ldots, c) = 0$ for any $c \in \mathbb{F}_{11}$. Thus Theorem 3 implies that

$$F(f(1), f(2), \ldots, f(10), f(0)) = 0$$

for any polynomial $f \in \mathbb{F}_{11}[T]$ of degree up to 4.

**EXAMPLE 2.2.** Consider the field $\mathbb{F}_{17}$ where the elements of $\mathbb{F}_{17}$ are ordered as follows: 1, 2, 3, ..., 15, 16, 0. Consider the polynomial

$$F = x_3^2x_7 + x_5^2x_6 + x_6^2x_{14} + x_7^2x_5 + x_8^2x_{12} + x_9^2x_3 + x_{10}^2x_{11} + x_{11}^2x_{14} + x_{14}x_{10}.$$ 

Note that $F$ is invariant under the action of $(\mathbb{F}_{17}^*)^2$, the group of squares (one only needs to check invariance under generator $2 \in (\mathbb{F}_{17}^*)^2$). Note also that $F(c, c, \ldots, c) = 8c^3$ for any $c \in \mathbb{F}_{17}$. Thus Theorem 3 implies that

$$F(f(1), f(2), \ldots, f(16), f(0)) = 8f(0)^3$$

for any quadratic or linear polynomial $f \in \mathbb{F}_{17}[T]$.

3. **VALUE POLYNOMIALS**

Let $f \in \mathbb{F}_q[x]$ be a polynomial. The value polynomial associated to $f$, written $\Phi_f$, is defined as

$$\Phi_f(T) \overset{\text{def}}{=} \prod_{i=1}^{q} (T - f(a_i))$$
(see [Tu] for a similar definition). Note that $\Phi_f$ is an element of $\mathbb{F}_q[T]$ of degree $q$.

More generally, if $S$ is a subset of $\mathbb{F}_q$ then $\Phi_{f,S} \in \mathbb{F}_q[T]$, the value polynomial associated to $f$ and $S$, is defined by the formula

$$\Phi_{f,S}(T) \overset{\text{def}}{=} \prod_{s \in S} (T - f(s)).$$

**Lemma 3.1.** Suppose $f \in \mathbb{F}_q[x]$ has positive degree $d$. Then $\Phi_f(T) - T^q$ has degree at most $q - (q - 1)/d$ (or is the zero polynomial).

**Proof.** This is a direct consequence of Wan’s theorem (Theorem 1) or its generalization (Theorem 3). We merely note that

$$\Phi_f(T) - T^q = \sum_{k=1}^{q} (-1)^k \sigma_k(f(a_1), \ldots, f(a_q)) T^{q-k},$$

and $\sigma_k(f(a_1), \ldots, f(a_q)) = 0$ for $k < (q - 1)/d$. So the largest possible value of the degree is $q - (q - 1)/d$. ■

**Lemma 3.2.** Suppose $f \in \mathbb{F}_q[x]$ has positive degree $d$ and $f(0) = 0$. Suppose also that $S$ is a subset of $\mathbb{F}_q$ with $n$ elements, and $G$ is a subgroup of $\mathbb{F}_q^*$ of order $g$ that acts on $S$. Then $\Phi_{f,S}(T) - T^n$ has degree at most $n - g/d$ (or is the zero polynomial).

**Proof.** Let $a_{i_1}, \ldots, a_{i_n}$ be the elements of $S$. Then

$$\Phi_{f,S}(T) - T^n = \sum_{k=1}^{n} (-1)^k \sigma_k(f(a_{i_1}), \ldots, f(a_{i_n})) T^{n-k}.$$

Let $F_k(x_1, \ldots, x_n) \overset{\text{def}}{=} \sigma_k(x_{i_1}, \ldots, x_{i_n})$. Clearly $F_k$ is invariant under $G$. By Theorem 3, if $k < q/d$ then

$$\sigma_k(f(a_{i_1}), \ldots, f(a_{i_n})) = F_k(f(a_1), \ldots, f(a_q)) = F_k(f(0), \ldots, f(0)).$$

However,

$$F_k(f(0), \ldots, f(0)) = \sigma_k(0, \ldots, 0) = 0$$

for $k > 0$. Thus the $T^{n-k}$ term of $\Phi_{f,S}(T) - T^n$ is zero for $0 < k < g/d$. ■
4. VALUE SETS OF PAIRS OF POLYNOMIALS

We define a set with multiplicities of size $n$ or a multiset of size $n$ to be an unordered $n$-tuple. (More formally, it is an equivalence class of finite sequences of length $n$ where two sequences are equivalent if and only if one is a permutation of the other). All the standard set-theoretical constructions are defined for sets with multiplicities in the natural way: unions, subsets, intersections, etc.

Let $S$ be a subset of $\mathbb{F}_q$, and let $f \in \mathbb{F}_q[x]$ be a polynomial. We define $f[S]$ to be the set with multiplicities defined by the values $f(s)$ as $s$ varies in $S$. More precisely, if $S = \{s_1, s_2, \ldots, s_n\}$, then $f[S]$ is the equivalence class of the finite sequence $(f(s_1), f(s_2), \ldots, f(s_n))$ under the above mentioned equivalence relation. Note $f[S]$ can be contrasted with $f(S)$ which is the set of values without counting multiplicities.

**Theorem 4.** Suppose $f_1, f_2 \in \mathbb{F}_q[x]$ are two non-constant polynomials of degree at most $d$. Then the size of the intersection of $f_1[\mathbb{F}_q]$ and $f_2[\mathbb{F}_q]$ (i.e., counting multiplicities) is either $q$ or is at most $q - (q - 1)/d$.

**Proof.** By Lemma 3.1, the polynomial $\Phi_{f_1} - \Phi_{f_2}$ has degree at most $q - (q - 1)/d$ or is the zero polynomial. However, each term of the intersection supplies a root of this polynomial. The result follows.

We note that Theorem 2 follows from the above result: just take $f_2 = x$.

**Theorem 5.** Suppose $f_1, f_2 \in \mathbb{F}_q[x]$ are two nonconstant polynomials of degree at most $d$ such that $f_1(0) = f_2(0)$. Suppose also that $G$ is a subgroup of $\mathbb{F}_q^*$ with $g$ elements, and $S_1$ and $S_2$ are subsets of $\mathbb{F}_q$ both of size $n$ and both invariant under multiplication by elements of $G$. Then the size of the intersection of $f_1[S_1]$ and $f_2[S_2]$ (i.e., counting multiplicities) is either $n$ or is at most $n - g/d$.

**Proof.** Without loss of generality, we can assume that $f_1(0) = f_2(0) = 0$. The remainder of the proof is similar to the proof of the previous theorem except we use Lemma 3.2 instead of Lemma 3.1.

**Example 4.1.** Suppose $m$ is a positive integer such that $m|q - 1$. Let $G$ be the group $m$th powers, i.e., $G = (\mathbb{F}_q^*)^m$. Let $S_1$ and $S_2$ be any two cosets of $G$. Finally, let $f \in \mathbb{F}_q[x]$ be a polynomial of degree $d \geq 1$. Then $f[S_1]$ and $f[S_2]$ are either equal (with multiplicities), or they have at most $(q - 1)/m - (q - 1)/md$ terms in common (including multiplicities).

**Example 4.2.** Suppose $m$ is a positive integer such that $m|q - 1$. Let $G = (\mathbb{F}_q^*)^m$. Finally, let $f_1, f_2 \in \mathbb{F}_q[x]$ be two nonconstant polynomials of degree at most $d$ with the same constant term. Then $f_1[G]$ and $f_2[G]$ are
either equal (with multiplicities), or they have at most \((q - 1)(1 - 1/d)/m\) terms in common.

**Example 4.3.** Suppose \(m\) is a positive integer such that \(m|q - 1\). Let \(G = (\mathbb{F}_q^*)^m\), and let \(f \in \mathbb{F}_q[x]\) be a polynomial of degree \(d \geq 1\) with no constant term. Then \(f(G) = G\), or \(f(G)\) contains at most \((q - 1)/m - (q - 1)/md\) elements of \(G\). To see this, just take \(f_1 = f, f_2 = x\).

5. A REFINEMENT

Now we will derive a refinement of the above results for the case of the group of squares in \(\mathbb{F}_q^*\):

**Theorem 6.** Suppose \(q\) is odd, and let \(G = (\mathbb{F}_q^*)^2\). Let \(S_1 = G, S_2 = \mathbb{F}_q^* - G\) be the two cosets of \(G\) in \(\mathbb{F}_q^*\), and let \(f \in \mathbb{F}_q[x]\) be a polynomial of degree \(d > 1\) such that \(f(0) = 0\). Then either (1) both \(f(S_1) \cap f(S_2) \cap S_1\) and \(f(S_1) \cap f(S_2) \cap S_2\) have at most \((q - 1)/2 - (q - 1)/d\) elements, or (2) \(f(S_1) \cap f(S_2) \subset S_j\) for some coset \(S_j\) and

\[
f(S_1) \cap f(S_2) = f(S_1) \cap S_j = f(S_2) \cap S_j.
\]

Before proving this we will prove the following lemma:

**Lemma 5.1.** The polynomial \(\Phi_{f,S_1}(T) + \Phi_{f,S_2}(T) - 2T^{(q - 1)/2} \in \mathbb{F}_q[T]\) has degree at most \(\frac{q - 1}{2} - \frac{q - 1}{d}\), or it is the zero polynomial.

**Proof of Lemma 5.1.** Observe that \(T \cdot \Phi_{f,S_1}(T) \cdot \Phi_{f,S_2}(T) = \Phi_f(T)\). By Lemma 3.1 and Lemma 3.2, if \(\Phi_f(T) - T^{(q - 1)/2} (i = 1, 2)\) is not the zero polynomial then it has degree at most \((q - 1)/2 - (q - 1)/2d\), and if \(\Phi_f(T) - T^q\) is not the zero polynomial then it has degree at most \(q - (q - 1)/d\). Consider the following:

\[
- T^{(q - 1)/2}(\Phi_{f,S_1}(T) + \Phi_{f,S_2}(T) - 2T^{(q - 1)/2}) = (\Phi_{f,S_1}(T) - T^{(q - 1)/2})(\Phi_{f,S_2}(T) - T^{(q - 1)/2}) - \frac{\Phi_f(T) - T^q}{T}.
\]

We see that either the right hand side is the zero polynomial or it has degree at most \(q - 1 - (q - 1)/d\). Therefore, \(\Phi_{f,S_1}(T) + \Phi_{f,S_2}(T) - 2T^{(q - 1)/2}\) has degree at most \((q - 1)/2 - (q - 1)/d\) or is the zero polynomial.

**Proof of Theorem 6.** Case 1. First assume that \(\Phi_{f,S_1}(T) + \Phi_{f,S_2}(T) - 2T^{(q - 1)/2}\) has positive degree. Let \(g_j(T) \overset{\text{def}}{=} \prod_{b \in S_j}(T - b)\). By Lemma 3.2 applied to the polynomial \(x\), we see that \(g_j(T) - T^{(q - 1)/2}\) is a constant.
It follows from Lemma 5.1 that $\Phi_{f,s_1}(T) + \Phi_{f,s_2}(T) - 2g_j(T)$ has positive degree at most $(q - 1)/2 - (q - 1)/d$. Finally, note that elements of $f(S_1) \cap f(S_2) \cap S_j$ are roots of $\Phi_{f,s_1}(T) + \Phi_{f,s_2}(T) - 2g_j(T)$.

Proof of Theorem 6. Case 2. Now assume that $\Phi_{f,s_1}(T) + \Phi_{f,s_2}(T) - 2T^{(q-1)/2} = c$ for some constant $c \in \mathbb{F}_q$.

If $f(S_1) \cap f(S_2)$ is empty, then the result follows. Suppose $0 \in f(S_1) \cap f(S_2)$. Then

$$c = \Phi_{f,s_1}(0) + \Phi_{f,s_2}(0) - 2 \cdot 0^{(q-1)/2} = 0.$$ Thus $c = 0$. In particular, if $r \in f(S_1) \cap f(S_2)$ then

$$0 = \Phi_{f,s_1}(r) + \Phi_{f,s_2}(r) - 2r^{(q-1)/2} = -2r^{(q-1)/2},$$

so $r = 0$. Hence $f(S_1) \cap f(S_2) = \{0\}$, in which case the theorem follows.

Thus we can assume that there is a non-zero element $r \in f(S_1) \cap f(S_2)$, and that $0 \notin f(S_1) \cap f(S_2)$. Therefore,

$$c = \Phi_{f,s_1}(r) + \Phi_{f,s_2}(r) - 2r^{(q-1)/2} = -2r^{(q-1)/2}.$$ In particular, if $r$ is in $S_1 = G$ then $r^{(q-1)/2} = 1$, so $c = -2$. If $r$ is in $S_2$ then $r^{(q-1)/2} = -1$, so $c = 2$. Therefore, $c = \pm 2$. The above considerations hold for arbitrary elements $r$ of $f(S_1) \cap f(S_2)$. Therefore, $f(S_1) \cap f(S_2) \subseteq S_j$ where $j = 1$ if $c = -2$ and $j = 2$ if $c = 2$. Note that $c = (-1)^j \cdot 2$.

Now suppose that $r \in f(S_1) \cap S_j$. Since $r \in S_j$, $-r^{(q-1)/2} = (-1)^j$. In particular,

$$c = \Phi_{f,s_1}(r) + \Phi_{f,s_2}(r) - 2r^{(q-1)/2} = \Phi_{f,s_2}(r) + 2(-1)^j.$$ Since $c = (-1)^j \cdot 2$, this implies that $\Phi_{f,s_2}(r) = 0$. Therefore, $r \in f(S_2)$. Likewise, $r \in f(S_2) \cap S_j$ implies $r \in f(S_1)$. Therefore, $f(S_1) \cap S_j = f(S_2) \cap S_j$. ■

Example 5.2. Suppose $q$ is odd, and that $f \in \mathbb{F}_q[x]$ is a cubic polynomial such that $f(0) = 0$. Let $G$, $S_1$, and $S_2$ be as above. By Example 4.1, $f[S_1]$ and $f[S_2]$ are either equal, or they have at most $(q - 1)/3$ elements in common (including multiplicities). It will leave it to the reader to show that if $q \geq 7$, then $f[S_1]$ and $f[S_2]$ cannot be equal. (Start by observing that if $c$ is in both $f[S_1]$ and $f[S_2]$, then $-c$ has at least two, and hence usually three, distinct non-zero roots. The case $q = 7$ requires additional treatment; in this case show that it is enough to check the nine polynomials of the form $x(x - a)(x - b)$ where $a \in S_1$ and $b \in S_2$.)
Theorem 6 gives information on how the elements in $f(S_1) \cap f(S_2)$ are distributed. In particular, either $f(S_1) \cap f(S_2) \cap S_j$ has at most $(q - 1)/6$ elements for $j = 1, 2$, or $f(S_1) \cap f(S_2)$ is contained entirely within $S_1$ or $S_2$.

For example, if $q = 11$, then $f[S_1]$ and $f[S_2]$ have at most 3 elements in common. Either $f(S_1) \cap f(S_2) \cap S_j$ has at most 1 element for $j = 1, 2$, or $f(S_1) \cap f(S_2)$ is contained entirely within $S_1$ or $S_2$. The first occurs for $x^3 + x^2 + 6x$. The second for $x^3 + 2x^2 + 4x$.

REFERENCES


