ON THE NUMBER OF DISTINCT VALUES OF A CLASS OF FUNCTIONS OVER A FINITE FIELD

ROBERT S. COULTER AND REX W. MATTHEWS

Abstract. Several authors have recently shown that a planar function over a finite field of order \( q \) must have at least \( (q + 1)/2 \) distinct values. In this note this result is extended by weakening the hypothesis significantly and strengthening the conclusion. We also give an algorithm for determining whether a given bivariate polynomial \( \phi(X,Y) \) can be written as \( f(X + Y) - f(X) - f(Y) \) for some polynomial \( f \). Using the ideas of the algorithm, we then show a Dembowski-Ostrom polynomial is planar over a finite field of order \( q \) if and only if it yields exactly \( (q + 1)/2 \) distinct values under evaluation; that is, it meets the lower bound of the image size of a planar function.

1. Introduction and notation

Throughout \( \mathbb{F}_q \) denotes the finite field of order \( q = p^e \), \( p \) a prime. The classical notation \( \mathbb{F}_q[X] \) and \( \mathbb{F}_q[X,Y] \) is used to denote the rings of polynomials over \( \mathbb{F}_q \) in \( X \) and \( X \) and \( Y \), respectively. The standard trace mapping from \( \mathbb{F}_q \) to \( \mathbb{F}_p \) is denoted \( \text{Tr} \). Let \( \omega \) be a primitive \( p \)-th root of unity. Recall that the canonical additive character, \( \chi_1 \), of \( \mathbb{F}_q \) is defined by \( \chi_1(x) = \omega^{\text{Tr}(x)} \) for any \( x \in \mathbb{F}_q \), and that all additive characters of \( \mathbb{F}_q \) are given by \( \chi_h(x) = \chi_1(hx) \) for any \( h \in \mathbb{F}_q \). For any polynomial \( f \in \mathbb{F}_q[X] \), the Weil sum of \( f \) under \( \chi_h \) is denoted by \( S_h(f) \); that is,

\[
S_h(f) = \sum_{x \in \mathbb{F}_q} \chi_h(f(x)).
\]

Let \( f \in \mathbb{F}_q[X] \). Define the difference operator, \( \Delta_f(X,Y) \), to be the bivariate polynomial given by \( \Delta_f(X,Y) = f(X + Y) - f(X) - f(Y) \). Let \( V(f) \) denote the number of distinct values \( f(x), x \in \mathbb{F}_q \). The polynomial \( f \) is called a permutation polynomial over \( \mathbb{F}_q \) if \( V(f) = q \). The polynomial \( f \) is called a planar function over \( \mathbb{F}_q \) if for every non-zero \( a \in \mathbb{F}_q \), the polynomial \( \Delta_f(X,a) \) is a permutation polynomial over \( \mathbb{F}_q \). It is easily seen that no function can be planar over a field of characteristic 2. Planar functions were introduced by Dembowski and Ostrom [6], where they were used to construct affine planes. They are also closely connected to commutative semifields [3] and difference sets [7].

For \( n \in \mathbb{N} \) and \( p \) prime, define \( w_p(n) \) to be the \( p \)-weight of \( n \); that is, if \( n = \sum_i a_i p^i \) is the base \( p \) expansion of \( n \), then \( w_p(n) = \sum_j a_i \). A polynomial \( f \in \mathbb{F}_q[X] \) is called a linearised polynomial if each non-zero term \( X^n \) of \( f \) satisfies \( w_p(n) = 1 \). Under evaluation, linearised polynomials induce homomorphisms of the additive group of the field, and any such homomorphism can be represented by a linearised polynomial. Consequently, they have been studied in great depth, see [11] for more information.

A polynomial \( f \in \mathbb{F}_q[X] \) is called a Dembowski-Ostrom (or DO) polynomial if each non-zero term \( X^n \) of \( f \) satisfies \( w_p(n) = 2 \). When \( q \) is odd, DO polynomials
induce even functions under evaluation and so $V(f) \leq (q + 1)/2$ in such cases. Dembowski-Ostrom polynomials play a significant role in the study of planar functions. It was conjectured that any planar function over a finite field was equivalent to a DO polynomial, give or take a linearised polynomial. Though the conjecture was shown to be false in characteristic 3 by the authors [5], it remains open for all larger characteristics. The significance of planar DO polynomials was further underlined in [3], where it was shown that there is a one-to-one correspondence between commutative presemifields and planar DO polynomials.

Recently, Kyureghyan and Pott [10], and Qiu et al [12] have independently shown that if $f$ is a planar function over $\mathbb{F}_q$, then $V(f) \geq (q + 1)/2$. We show this is, in fact, a consequence of a far weaker condition, a condition which is necessary but clearly not sufficient for a polynomial $f$ to be planar, see Section 2. Next, we give an algorithm for determining whether a given polynomial $\phi(X,Y)$ satisfies $\phi = \Delta f$ for some polynomial $f$. The paper ends by showing that $V(f) = (q + 1)/2$ is a necessary and sufficient condition for a DO polynomial to be planar over $\mathbb{F}_q$.

2. The number of distinct images

Theorem 1. Let $f \in \mathbb{F}_q[X]$ be a polynomial for which $|S_h(f)| = q^{1/2}$ for all $h \neq 0$. Then $M_1(f) \geq 1$ and

$$M_1(f) + M_2(f) \geq \frac{q + 1}{2},$$

where $M_r(f)$ is the number of $y \in \mathbb{F}_q$ having $r$ pre-images under the function induced by $f$. Moreover, equality holds if and only if $M_1(f) = 3M_3(f) + 1$ and $M_r(f) = 0$ for all $r \geq 4$.

Proof. Define $N(f)$ to be the number of $(x,y) \in \mathbb{F}_q \times \mathbb{F}_q$ satisfying $f(x) = f(y)$. For ease of notation, set $d = \text{Degree}(f)$. The following identities are clear:

(i) $V(f) = \sum_{r=1}^d M_r(f)$.
(ii) $q = \sum_{r=1}^d rM_r(f)$.
(iii) $N(f) = \sum_{r=1}^d r^2 M_r(f)$.

It follows from the orthogonality relations of characters that

$$qN(f) = \sum_{h \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \chi_1(h(f(x) - f(y)))$$

$$= \sum_{h \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_q} \chi_h(f(x)) \sum_{y \in \mathbb{F}_q} \chi_h(-f(y))$$

$$= \sum_{h \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_q} \chi_h(f(x)) \sum_{y \in \mathbb{F}_q} \chi_h(f(y))$$

$$= \sum_{h \in \mathbb{F}_q} |S_h(f)|^2.$$

Now suppose $|S_h(f)| = q^{1/2}$ for all $h \neq 0$. Immediately $N(f) = 2q - 1$. Combining identities (ii) and (iii) yields

$$M_1(f) - 1 = \sum_{r=3}^d (r^2 - 2r) M_r(f),$$
from which $M_1(f) \geq 1$ is forced. Further, $M_1(f) - 1 \geq \sum_{r=3}^{d} rM_r(f)$, so that
\[
2M_1(f) + 2M_2(f) - 1 \geq \sum_{r=1}^{d} rM_r(f) = q,
\]
establishing the claim.(0.03,0.11) Note for equality to hold, $M_r(f) = 0$ for $r > 3$, and so $M_1(f) - 1 = 3M_3(f)$, completing the proof. \hfill \Box

By [4], Theorem 2.3, a polynomial $f \in \mathbb{F}_q[X]$ is planar over $\mathbb{F}_q$ if and only if $|S_h(f(x) + \lambda x)| = q^{1/2}$ for all $h, \lambda \in \mathbb{F}_q$, $h \neq 0$. The theorem therefore holds for planar functions, in particular. That the hypothesis of Theorem 1 holds for (mod $p$) prime fields, the only case for which planar functions have been classified, gives additional proof that Theorem 1 holds for functions other than planar functions. Since any planar function over $\mathbb{F}_p$ is necessarily equivalent to a quadratic (see any of [8], [9], [13]), the number of planar functions over $\mathbb{F}_p$ is $p^2(p - 1)$. On the other hand, Cavor [1] shows that the total number $T$ of functions $f$ on $\mathbb{F}_p$ for which $|S_h(f)| = p^{1/2}$ is given by
\[
T = \frac{2p \cdot p!}{2^{(p-1)/2}}.
\]
Since $V(f) \geq M_1(f) + M_2(f)$, the following corollary is immediate.

**Corollary 2.** Let $f \in \mathbb{F}_q[X]$ be a polynomial for which $|S_h(f)| = q^{1/2}$ for all $h \neq 0$. Then $V(f) \geq (q + 1)/2$, with equality holding if and only if $M_1(f) = 1$, $M_2(f) = (q - 1)/2$, and $M_r(f) = 0$ for all $r \geq 3$.

Note that when equality holds in the corollary, without loss of generality, the polynomial $f \in \mathbb{F}_q[X]$ can be assumed to satisfy $f(0) = 0$ and to act 2 to 1 on the non-zero elements of $\mathbb{F}_q$. Such a function is called a 2-1 function. We shall return to such functions at the end of the following section.

3. The difference operator and planar DO polynomials

For $n \in \mathbb{N}$ and $p$ prime, define $\nu_p(n)$ to be the $p$-order of $n$. Any term $X^tY^s \in \mathbb{F}_q[X,Y]$ is defined to be $p$-admissible if $\nu_p(s + t) = \min(\nu_p(s), \nu_p(t))$. We say $\phi \in \mathbb{F}_q[X,Y]$ is $p$-admissible if each non-zero term of $\phi$ is $p$-admissible.

Define an equivalence relation $\approx$ on $\mathbb{F}_q[X]$ by $f \approx g$ if and only if $f - g$ is a linearised polynomial. We say $f$ is $L$-normalised if $f$ contains no linearised term. For any $f \in \mathbb{F}_q[X]$ there exists a unique $L$-normalised polynomial $g$ with $f \approx g$. Clearly $f$ is linearised if and only if $f \approx 0$. Equivalently, $\Delta_f(X,Y) = 0$ if and only if $f \approx 0$.

If $f(X) = \sum_i c_i X^i$ has no term $X^t$ with $t \equiv -1$ (mod $p$), then define the antiderivative $\Lambda f(X)$ to be
\[
\Lambda f(X) = \sum_i c_i X^{i+1}/(i + 1).
\]
Given any polynomial $f$, set $g(X) = f'(X)$, the derivative of $f$. Then $\Lambda g$ is the unique $L$-normalised polynomial satisfying $f = \Lambda g$.

We are interested in solving the following problem:
Let \( \phi \in \mathbb{F}_q[X,Y] \). Describe an algorithm which will determine whether there exists a polynomial \( f \in \mathbb{F}_q[X] \) with \( \Delta_f = \phi \). If this returns TRUE then return \( f \) and indicate whether \( f \) is a DO polynomial.

We begin by presenting an algorithm which produces a candidate for such an \( f \).

Given \( \phi \in \mathbb{F}_q[X,Y] \).

Step 1. If \( \phi(X,Y) \neq \phi(Y,X) \), then return FALSE.

Step 2. Write \( \phi(X,Y) \) as a sum \( \psi_i(X,Y) \) where \( \psi_i \) is the sum of the non-zero terms of \( \phi \) whose total degree satisfies \( p \)-order \( i \). Define \( \phi_i \) by \( \psi_i = \phi_i^p \).

Step 3. For each \( i > 0 \), if \( \phi_i \) has a non-constant term with \( X \)-degree or \( Y \)-degree 0, then return FALSE.

Step 4. For each \( i > 0 \), if \( \phi_i \) is not \( p \)-admissible, then return FALSE.

Step 5. For each \( i \), let \( Y \mathcal{g}_i(X) \) be the sum of the terms whose degree in \( Y \) is 1. Let \( f_i(X) \) be the unique \( L \)-normalised antiderivative of \( g_i \). Verify \( f_i(X+Y) - f_i(Y) = \phi_i(X,Y) \). If not, return FALSE.

Step 6. Set \( f(X) = \sum_i f_i^p \). Return TRUE. Note that \( f \) is a DO polynomial if and only if \( g_i(X) \) is a linearised polynomial for each \( i \).

**Justification of algorithm:** Exit points returning FALSE correspond to necessary conditions. If we write \( f_i(X+Y) = \sum_{j \neq i} g_{i,j}(X)Y^j \), then \( g_i(X) = g_{i,1}(X) = f_i(X) \). From the conditions on \( f_i(X) \) it follows that \( f_i(X) = A \mathcal{g}_i(X) \), which uniquely determines \( f \). If \( f \) is a DO polynomial, then for each \( i \), \( f_i(X) = XL_i(X) \), where \( L_i(X) \) is linearised. Hence \( f_i(X+Y) - f_i(Y) = (X+Y)L_i(X+Y) - XL_i(X) - YL_i(Y) \), and the coefficient of \( Y \) is \( L_i(X) \). If \( g_i(X) \) is linearised, then \( f_i(X) = A \mathcal{g}_i(X) = X \mathcal{g}_i(X) \) and \( f \) is a DO polynomial.

The ideas laid out in the algorithm and its justification lead us to a short proof of the following theorem.

**Theorem 3.** Let \( f \in \mathbb{F}_q[X] \) be a Dembowski-Ostrom polynomial. Then \( f \) is planar over \( \mathbb{F}_q \) if and only if \( f \) is a 2-1 function. Equivalently, \( f \) is planar over \( \mathbb{F}_q \) if and only if \( V(f) = (q + 1)/2 \).

**Proof.** Write \( f(X) = \sum_i f_i^q(X) \). Then each \( f_i(X) \) has the shape \( XL_i(X) \), with \( L_i(X) \) a linearised polynomial. Adopting the notation of the algorithm, set \( \phi = \Delta f \). So \( \phi_i(X,Y) = YL_i(X) + XL_i(Y) \). Now make the change of variable \( X = U + V \), \( Y = U - V \). Then

\[
\phi_i(X,Y) = (U - V)L_i(U + V) + (U + V)L_i(U - V)
\]

\[
= 2(U L_i(U) - V L_i(V))
\]

\[
= 2(f_i(U) - f_i(V)),
\]

and so \( \phi(X,Y) = 2(f(U) - f(V)) \).

The planarity condition is that \( \phi(X,Y) \) has all its zeros on the curve \( XY = 0 \). In \( (U,V) \) coordinates this translates to all zeros of \( f(U) - f(V) \) lying on the curve \( U^2 - V^2 = 0 \), or that \( f(U) = f(V) \) implies \( U = V \) or \( U = -V \). Since \( f \) is an even function, this implies that \( f \) is a 2-1 function.

Conversely, if \( f \) is a 2-1 function, we need to show that \( \phi(X,Y) \) has all its zeros on \( XY = 0 \). It suffices to show \( \phi(X,Y) \) has \( 2q - 1 \) zeros or that \( f(U) - f(V) \) has \( 2q - 1 \) zeros. But if \( f(U) = c, c \neq 0 \), then \( f(-U) = c \), so \( c \) has exactly two
ON THE NUMBER OF DISTINCT VALUES OF A CLASS OF FUNCTIONS OVER A FINITE FIELD

pre-images. Consequently \( f(U) - f(V) \) has \( 1 + 2((q - 1)/2) = 2q - 1 \) zeros, as required. \( \square \)

We note that each \( f_i \) may be written as \( X^2 h_i(X^2) \) where \( h_i(X^2) = L_i(X)/X \), so \( f_i(X) = g_i(X) \) with \( g_i(X) = Xh_i(X) \). Then \( f(X) = g(X^2) \) where \( g(X) = \sum_i g_i(X) \). If \( g(X) \) is a permutation polynomial, then \( f \) is 2-1, but this is not a necessary condition. Let \( \zeta \) be a primitive element of \( \mathbb{F}_{25} \). Set \( f_a(X) = X^6 + 2aX^2 \) where \( a = \zeta^{4i+1} \) for some integer \( i \), so \( g_a(X) = X^3 + 2aX \). Then \( f_a \) is planar over \( \mathbb{F}_{25} \) but \( g_a(X) \) is not a permutation polynomial.

**Added in proof:** We have been informed Theorem 3 has also been established recently by G. Weng and X. Zeng using methods distinct from ours.

**References**


