DIVISIBILITY OF WEIL SUMS OF BINOMIALS

DANIEL J. KATZ

(Communicated by Matthew A. Papanikolas)

Abstract. Consider the Weil sum
\[ W_{F,d}(u) = \sum_{x \in F} \psi(x^d + ux), \]
where \( F \) is a finite field of characteristic \( p \), \( \psi \) is the canonical additive character of \( F \), \( d \) is coprime to \( |F^*| \), and \( u \in F^* \). We say that \( W_{F,d}(u) \) is three-valued when it assumes precisely three distinct values as \( u \) runs through \( F^* \): this is the minimum number of distinct values in the nondegenerate case, and three-valued \( W_{F,d} \) are rare and desirable. When \( W_{F,d} \) is three-valued, we give a lower bound on the \( p \)-adic valuation of the values. This enables us to prove the characteristic 3 case of a 1976 conjecture of Helleseth: when \( p = 3 \) and \( [F:F_3] \) is a power of 2, we show that \( W_{F,d} \) cannot be three-valued.

1. Introduction

In this paper, we are concerned with Weil sums of binomials of the form
\[ W_{F,d}(u) = \sum_{x \in F} \psi(x^d + ux), \]
where \( F \) is a finite field of characteristic \( p \), the exponent \( d \) is a positive integer such that \( \gcd(d, |F^*|) = 1 \), the coefficient \( u \) is in \( F^* \), and \( \psi: F \to \mathbb{C} \) is the canonical additive character \( \psi(x) = e^{2\pi i \Tr_{F/F_p}(x)/p} \). Nontrivial Weil sums of form
\[ \sum_{x \in F} \psi(ax^m + bx^n), \]
with \( \gcd(m, |F^*|) = \gcd(n, |F^*|) = 1 \), can be reparameterized to the form \( (1) \). Such sums and their relatives arise often in number-theory \([4,5,7–10,14,16–18,21]\), and in applications to finite geometry, digital sequence design, error-correcting codes, and cryptography. See \([15,\text{Appendix}]\) on the various guises in which these sums appear in these applications, and for a bibliography.

We fix \( F \) and \( d \), and consider the values \( W_{F,d}(u) \) attains as \( u \) varies over \( F^* \), but typically ignore the trivial \( W_{F,d}(0) = 0 \), which is the Weil sum of a monomial. We say that \( W_{F,d} \) is \( \nu \)-valued to mean that \( |\{W_{F,d}(u) : u \in F^*\}| = \nu \).

If \( F \) is of characteristic \( p \) and \( d \) is a power of \( p \) modulo \( |F^*| \), then \( \psi(x^d) = \psi(x) \), so \( W_{F,d}(u) \) effectively becomes the Weil sum of the monomial \((1 + u)x\), so that
\[ W_{F,d}(u) = \begin{cases} |F| & \text{if } u = -1, \\ 0 & \text{otherwise}, \end{cases} \]
and in this case we say that \( d \) is degenerate over \( F \). For nondegenerate \( d \), Helleseth \([13, \text{Theorem 4.1}]\) showed that one obtains more than two values.
Theorem 1.1 (Helleseth, 1976). If \( d \) is nondegenerate over \( F \), then \( W_{F,d} \) is at least three-valued.

Much interest has focused on which choices of \( F \) and \( d \) make \( W_{F,d} \) precisely three-valued, and ten infinite families have been found (see [1] Table 1). From these, one finds that if \( F \) is of characteristic \( p \), and if \([F : \mathbb{F}_p]\) is divisible by an odd prime, then there is a \( d \) such that \( W_{F,d} \) is three-valued. However, no three-valued examples have ever been found for fields \( F \) where \([F : \mathbb{F}_p]\) is a power of 2. This prompted the following conjecture [13] Conjecture 5.2.

Conjecture 1.2 (Helleseth, 1976). If \( F \) is of characteristic \( p \) with \([F : \mathbb{F}_p]\) a power of 2, then \( W_{F,d} \) is not three-valued.

Many attempts have been made to test or prove this conjecture in the case where \( F \) is of characteristic 2, and many fruitful discoveries were made in the process [2][3][6][11][12][20]. The \( p = 2 \) case was at last proved in [15] Corollary 1.10. Now the \( p = 3 \) case is proved in this paper as a corollary of a new bound on the \( p \)-divisibility of Weil sums.

For a nonzero integer \( n \), the \( p \)-adic valuation of \( n \), written \( v_p(n) \), is the largest \( k \) such that \( p^k \mid n \), and \( v_p(0) = \infty \). If we extend this valuation to the cyclotomic field \( \mathbb{Q}(e^{2\pi i/p}) \) where the Weil sums lie, we may state the first fundamental result on the \( p \)-divisibility of Weil sums from [13] Theorem 4.5.

Theorem 1.3 (Helleseth, 1976). If \( F \) is of characteristic \( p \), then we have \( v_p(W_{F,d}(u)) > 0 \) for every \( u \in F \).

It was recently proved [15] Theorems 1.7, 1.9] that when \( W_{F,d} \) is three-valued, the values must be rational integers.

Theorem 1.4 (Katz, 2012). If \( F \) is of characteristic \( p \), and if \( W_{F,d} \) is three-valued, then the three values are in \( \mathbb{Z} \), one of the values is 0, and \( d \equiv 1 \pmod{p-1} \).

So if \( W_{F,d} \) is three-valued, these two theorems show that \( p \mid W_{F,d}(u) \) for all \( u \in F \). Our main result is a much stronger lower bound on the \( p \)-divisibility.

Theorem 1.5. If \( F \) is of characteristic \( p \) and order \( q = p^n \), and if \( W_{F,d} \) is three-valued with values 0, \( a \), and \( b \), then one of the following holds:

(i). \( v_p(a), v_p(b) > n/2 \); or
(ii). \( v_p(a) = v_p(b) = n/2 \), and \( |a-b| \) is a power of \( p \) with \( |a-b| > \sqrt{q} \);

and case (ii) cannot occur if \( p = 2 \) or 3.

For the fields of interest in Conjecture 1.2, we use the techniques of [1] to show an upper bound on the \( p \)-divisibility of some \( W_{F,d}(u) \).

Theorem 1.6. Let \( F \) be of characteristic \( p \) and order \( q = p^n \), with \( n \) a power of 2. If \( W_{F,d} \) is three-valued, then there is some \( u \in F^* \) such that \( v_p(W_{F,d}(u)) \leq n/2 \).

This generalizes the result of Calderbank, McGuire, Poonen, and Rubinstein, who proved the \( p = 2 \) case in [3]. Theorems 1.5 and 1.6 immediately combine to prove Conjecture 1.2 in characteristic 2 and 3.

Theorem 1.7. If \( F \) is of characteristic \( p = 2 \) or 3 with \([F : \mathbb{F}_p]\) a power of 2, then \( W_{F,d} \) is not three-valued.
In Section 2, we outline a group algebra approach to this problem inspired by the work of Feng [11], and in Section 3 we use a group-theoretic approach of McGuire [20] to determine congruences on the zero counts of critical polynomials that arise in our proofs. We then prove Theorem 1.5 in Section 4 and prove Theorem 1.6 in Section 5.

2. The group algebra and the Fourier transform

This section generalizes the group ring techniques of Feng [11] to arbitrary characteristic. As in the Introduction, $F$ is a finite field.

Consider the group algebra $\mathbb{C}[F^\ast]$ over $\mathbb{C}$, whose elements are written as formal sums $S = \sum_{u \in F^\ast} S_u[u]$ with $S_u \in \mathbb{C}$. We identify any subset $U$ of $F^\ast$ with $\sum_{u \in U} [u]$ in $\mathbb{C}[F^\ast]$. For example, $F^\ast$ itself is identified with $\sum_{u \in F^\ast} [u]$. If $S \in \mathbb{C}[F^\ast]$, we let $|S| = \sum_{u \in F} S_u$; if $S$ represents a subset of $F^\ast$, this is indeed the cardinality of that set. Note that $SF^\ast = |S|F^\ast$ for any $S \in \mathbb{C}[F^\ast]$.

For $t \in \mathbb{Z}$ and $S = \sum_{u \in F^\ast} S_u[u] \in \mathbb{C}[F^\ast]$, we write $S^{(t)}$ to denote $\sum_{u \in F^\ast} S_u[u^t]$. Note that $|S^{(t)}| = |S|$. If $S \in \mathbb{C}[F^\ast]$, its conjugate is defined to be $\overline{S} = \sum_{u \in F^\ast} \overline{S_u}[u^{-1}]$, and note that $|\overline{S}| = |S|$.

We let $\widehat{F^\ast}$ denote the group of multiplicative characters from $F^\ast$ to $\mathbb{C}$. If $S = \sum_{u \in F^\ast} S_u[u] \in \mathbb{C}[F^\ast]$, and $\chi \in \widehat{F^\ast}$, we define $\chi(S) = \sum_{u \in F^\ast} S_u \chi(u)$. We call $\chi(S)$ the Fourier coefficient of $S$ at $\chi$, and we define the Fourier transform of $S$, denoted $\hat{S}$, to be a function from $\widehat{F^\ast}$ to $\mathbb{C}$, where the value of $\hat{S}$ at $\chi$ is $\hat{S}(\chi) = \chi(S)$.

It is straightforward to show that the Fourier transform $S \mapsto \hat{S}$ is an isomorphism of $\mathbb{C}$-algebras from $\mathbb{C}[F^\ast]$ with its convolutional multiplication to the $\mathbb{C}$-algebra $\mathbb{C}[\widehat{F^\ast}]$ of functions from $\widehat{F^\ast}$ into $\mathbb{C}$, with pointwise multiplication. This affords an inverse Fourier transform,

$$S_u = \frac{1}{|F^\ast|} \sum_{\chi \in \widehat{F^\ast}} \chi(S) \overline{\chi(u)},$$

so that $S = T$ if and only if $\chi(S) = \chi(T)$ for all $\chi \in \widehat{F^\ast}$.

Note that if $t$ is an integer, then $\chi(S^{(t)}) = \chi^t(S)$. Similarly, $\chi(\overline{S}) = \overline{\chi(S)}$. If $\chi_0$ is the principal character, then $\chi_0(S) = |S|$ for all $S \in \mathbb{C}[F^\ast]$.

As in the Introduction, we let $d$ be a positive integer with $\gcd(d, |F^\ast|) = 1$, let $\psi: F \to \mathbb{C}$ be the canonical additive character, and we set

$$W_u = W_{F,d}(u) = \sum_{x \in F} \psi(x^d + ux).$$

We are interested in the Fourier analysis of the group algebra element

$$W = \sum_{u \in F^\ast} W_u[u],$$

which records the various values of $W_{F,d}$ as its coefficients. To this end, we introduce the group algebra element

$$\Psi = \sum_{u \in F^\ast} \psi(u)[u],$$

which has a close connection to $W$.

**Lemma 2.1.** $W = \Psi \Psi^{(-1/d)} + F^\ast$, where $1/d$ denotes the multiplicative inverse of $d$ modulo $|F^\ast|$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. Note that \( \Psi \Psi^{(-1/d)} = \sum_{y, z \in F^*} \psi(y) \psi(z) [yz^{-1/d}] \), but then reparameterize with \( z = x^d \) and \( y = ux \) to get
\[
\Psi \Psi^{(-1/d)} = \sum_{u, x \in F^*} \psi(ux) \psi(x^d)[u] = \sum_{u \in F^*} (W_u - 1)[u],
\]
so that \( \Psi \Psi^{(-1/d)} + F^* = W \).

Now we may carry out the Fourier analysis of \( \Psi \) and \( W \).

**Corollary 2.3.** If \( \chi \in \hat{F}^* \) is not the principal character \( \chi_0 \), then \( |\chi(\Psi)| = \sqrt{|F|} \), whereas \( \chi_0(\Psi) = |\Psi| = -1 \).

Proof. For any \( \chi \in \hat{F}^* \), we have
\[
\chi(\Psi) = \sum_{u \in F^*} \psi(u) \chi(u),
\]
which is a Gauss sum, of which the magnitude in general and the value when \( \chi = \chi_0 \) is well known (see [19, Theorem 5.11]).

**Corollary 2.4.** \( W \bar{W} = |F|^2 \).

Proof. In view of Lemma 2.1, we multiply \( W = \Psi \Psi^{(-1/d)} + F^* \) by its conjugate. Note that \( \bar{F}^* = F^* \), recall that \( SF^* = |S| F^* \) for any \( S \in \mathbb{C}[F^*] \), and use Lemma 2.2 to see that \( |\Psi^{(-1/d)}| = |\Psi| = -1 \) and thus \( |\Psi^{(-1/d)}| = |\overline{\Psi}| = -1 \), so that \( W \overline{W} = \Psi \overline{\Psi} \Psi^{(-1/d)} \overline{\Psi}^{(-1/d)} + (|F^*| + 2)F^* \). Then apply Corollary 2.3 to the first term to finish.

Now define
\[
X = \sum_{u \in F^*} W_u^2 [u]
\]
and
\[
V = \sum_{v \in F} [(v^d + (1 - v)^d)^{1/d}],
\]
where the \( 1/d \) is understood modulo \( |F^*| \). We claim that \( v^d + (1 - v)^d \neq 0 \) for any \( v \in F \), because \( v \neq v - 1 \), and the condition \( \gcd(d, |F^*|) = 1 \) makes \( x \mapsto x^d \) a permutation of \( F \) and makes \( d \) odd when the characteristic of \( F \) is odd. This makes \( V \) a legitimate element of \( \mathbb{C}[F^*] \) with
\[
|V| = |F|.
\]
We can now relate \( W, X, \) and \( V \).
Lemma 2.5. \( X = WV \).

Proof. Note that

\[
(WV)_u = \sum_{z \in F^*} W_{u/z} V_z \\
= \sum_{v \in F} W_{u(v^d + (1 - v)^d)^{-1/d}} \\
= \sum_{v, w \in F} \psi(w^d + u(v^d + (1 - v)^d)^{-1/d})W \\
= |F| + \sum_{v \in F} \sum_{w \in F^*} \psi(w^d + u(v^d + (1 - v)^d)^{-1/d}w).
\]

Since \( \gcd(d, |F^*|) = 1 \) makes \( d \) odd when \( F \) is of odd characteristic, the map \((x, y) \mapsto (x/(x + y), (x^d + y^d)^{1/d})\) is a bijection from \( \{(x, y) \in F^2 : x + y \neq 0\} \) to \( F \times F^* \), with inverse \((v, w) \mapsto (v^d + (1 - v)^d)^{-1/d}(vw, (1 - v)w) \). We may then reparameterize our sum to obtain

\[
(WV)_u = |F| + \sum_{x, y \in F \atop x + y \neq 0} \psi(x^d + y^d + u(x + y)) \\
= \sum_{x, y \in F \atop x + y \neq 0} \psi(x^d + y^d + u(x + y)) \\
= W_u^2.
\]

It is now easy to calculate the first four power moments of the Weil sum.

Corollary 2.6. We have

(i). \( \sum_{u \in F^*} W_u = |F| \),

(ii). \( \sum_{u \in F^*} W_u^2 = |F|^2 \),

(iii). \( \sum_{u \in F^*} W_u^3 = |F|^2 V_1 \), and

(iv). \( \sum_{u \in F^*} W_u^4 = |F|^2 \sum_{u \in F^*} V_u^2 \).

Proof. First of all, \( \sum_{u \in F^*} W_u = |W| \), which equals \( |\Psi| \cdot |\Psi^{(-1/d)}| + |F^*| = (-1)^2 + |F^*| \) by Lemmas 2.3 and 2.2.

Secondly, \( \sum_{u \in F^*} W_u^2 = |X| \), which equals \( |W| \cdot |V| = |F|^2 \) by Lemma 2.5, equation (7), and the previous part.

Thirdly, \( \sum_{u \in F^*} W_u^3 \) is the coefficient for the element \([1]\) in \( W \), and \( W = (WV)V = |F|^2 V \) by Lemma 2.3 and Corollary 2.1.

Finally, \( \sum_{u \in F^*} W_u^4 \) is the coefficient of \([1]\) in \( XW \), and we see that \( XW = (WV)(WV) = |F|^2 V^2 \) by Lemma 2.5 and Corollary 2.1.

3. Congruences for \( V_1 \)

As in previous sections, \( F \) is a finite field and \( d \) is a positive integer with \( \gcd(d, |F^*|) = 1 \). We recall \( V \) from equation (4), whose coefficient \( V_1 \) appears in Corollary 2.6. We deduce useful congruences for \( V_1 \) by means of a group action studied by McGuire [20].
Proposition 3.1. Let \( V_1 = |\{v \in F : v^d + (1-v)^d = 1\}|. \)

(i). If \(|F| \equiv 0 \pmod{3}\), then \( V_1 \equiv 3 \pmod{6} \).

(ii). If \(|F| \equiv 1 \pmod{3}\), then

(a). if \( 2^{d-1} = 1 \) in \( F \), then \( V_1 \equiv 1 \pmod{6} \), but

(b). if \( 2^{d-1} \neq 1 \) in \( F \), then \( V_1 \equiv 4 \pmod{6} \).

(iii). If \(|F| \equiv 2 \pmod{3}\), then

(a). if \( 2^{d-1} = 1 \) in \( F \), then \( V_1 \equiv 5 \pmod{6} \), but

(b). if \( 2^{d-1} \neq 1 \) in \( F \), then \( V_1 \equiv 2 \pmod{6} \).

Before proving the proposition, we interject two remarks.

Remark 3.2. When \( F \) is of order \( 2^n \), then we have \( 2 = 0 \) in \( F \), so that \( 2^{d-1} \neq 1 \), and we recover the result of McGuire (cf. [20] Corollary 1) that \( V_1 \equiv 4 \pmod{6} \) if \( n \) is even, and \( V_1 \equiv 2 \pmod{6} \) if \( n \) is odd.

Remark 3.3. When we are dealing with three-valued Weil sums, Theorem 1.4 shows that \( d \equiv 1 \pmod{p-1} \), in which case \( 2^{d-1} = 1 \) in \( F \) by Fermat’s Little Theorem whenever \( p \neq 2 \).

Proof of Proposition 3.1. We are counting modulo 6 the roots of \( f(X) = X^d + (1-X)^d - 1 \) in \( F \). First of all, note that 0 and 1 are always roots of \( f \). Consider the action of the two involutions \( \sigma(x) = 1-x \) and \( \tau(x) = 1/x \) on \( F \setminus \{0,1\} \). Note that \( f(\sigma(x)) = f(x) \) and \( f(\tau(x)) = -f(x)/x^d \), because \( \gcd(d,|F^*|) = 1 \) makes \( d \) odd when \(|F|\) is odd. Thus \( \sigma \) and \( \tau \) map the roots of \( f \) in \( F \setminus \{0,1\} \) to themselves.

For generic \( F \), our \( \sigma \) and \( \tau \) generate a group \( G \) isomorphic to \( S_3 \), consisting of the identity, \( \sigma, \tau, \sigma \circ \sigma(x) = 1/(1-x), \sigma \circ \tau(x) = (x-1)/x, \) and \( \sigma \circ \tau \circ \sigma(x) = \tau \circ \sigma \circ \tau(x) = x/(x-1) \). The set of roots of \( f \) in \( F \setminus \{0,1\} \) is preserved by \( G \), so is partitioned into orbits under its action.

A \( G \)-orbit contains 6 elements unless it contains a point fixed by some nonidentity element of \( G \). An \( x \in F \setminus \{0,1\} \) is fixed by a nonidentity element of \( G \) if and only if it satisfies at least one of the following equations: \( x = 1-x, x = 1/x, x = 1/(1-x), x = (x-1)/x, \) or \( x = x/(x-1) \). Equivalently, \( x \) equals at least one of: (i) \(-1\), (ii) \(2\), (iii) the multiplicative inverse of 2 (which we shall call \( 1/2 \) when it exists), or (iv) a root of \( \Phi_6(X) = X^2 - X + 1 \), the cyclotomic polynomial of index 6.

If \(|F| \equiv 0 \pmod{3}\), then \(-1 = 2 = 1/2\), which is the double root of \( \Phi_6 \). Furthermore, \( f(-1) = 0 \) since \( d \) is odd. Thus the roots of \( f \) consist of \( 0, 1, \) and orbits of size 6, so that \( V_1 \equiv 3 \pmod{6} \).

If \( F \) is of characteristic 2, then (i) \(-1 = 1\), (ii) \(2 = 0\), and (iii) the multiplicative inverse of 2 does not exist, so these are not points in \( F \setminus \{0,1\} \), and (iv) the roots of \( \Phi_6 \) are the primitive third roots of unity, \( \omega \) and \( \omega^{-1} = 1 - \omega \), which lie in \( F \) if and only if \(|F| \equiv 1 \pmod{3}\). In this case \( f(\omega) = f(\omega^{-1}) = 0 \) since \( d \equiv \pm 1 \pmod{3} \), because \( \gcd(d,|F^*|) = 1 \). So the roots of \( f \) consist of 0 and 1 always, the third roots of unity if \(|F| \equiv 1 \pmod{3}\), and orbits of size 6. Thus \( V_1 \equiv 4 \pmod{6} \) if \(|F| \equiv 1 \pmod{3}\) and \( V_1 \equiv 2 \pmod{6} \) if \(|F| \equiv 2 \pmod{3}\).

Now suppose that \( F \) is of characteristic \( p \geq 5 \). Then (i) \(-1, 2\), (ii) \(1/2\), and (iv) the roots of \( \Phi_6 \) are five distinct elements in characteristic \( p \). The roots \( \zeta \) and \( \zeta^{-1} = 1-\zeta \) of \( \Phi_6 \) lie in \( F \) if and only if \(|F| \equiv 1 \pmod{6} \), or equivalently, if and only if \(|F| \equiv 1 \pmod{3}\). In this case \( f(\zeta) = f(\zeta^{-1}) = 0 \) since \( d \equiv \pm 1 \pmod{6} \) because \( \gcd(d,|F^*|) = 1 \), so the roots of \( \Phi_6 \) are roots of \( f \) if they are present in \( F \). The three elements \(-1, 2, \) and \(1/2\) make up a \( G \)-orbit, and are roots of \( f \) if and only if \( 0 = f(1/2) = (1/2)^d + (1/2)^d - 1 = (1/2)^{d-1} - 1 \), that is, if and only if \( 2^{d-1} = 1 \).
So the roots of $f$ consist of 0 and 1 always, the roots of $\Phi_6$ if and only if $|F| \equiv 1 \pmod{3}$, the elements $-1$, $2$, and $1/2$ if and only if $2^{d-1} = 1$ in $F$, and orbits of size 6. Adding these counts together modulo 6 according to the four possible cases finishes the proof. \hfill \Box

4. Proof of Theorem 1.5

Throughout this section, we assume that $F$ is a finite field of characteristic $p$ and order $q$, and that $d$ is a positive integer with $\gcd(d, q - 1) = 1$. We let $\psi: F \to \mathbb{C}$ be the canonical additive character, and set

$$W_u = W_{F,d}(u) = \sum_{x \in F} \psi(x^d + ux),$$

and assume that $W_{F,d}$ is three-valued. Per Theorem 1.4, these three values must all be in $\mathbb{Z}$, and one of them must be 0. Call the other two values $a$ and $b$; these are of opposite sign since $\sum_{u \in F^*} W_u^2 = (\sum_{u \in F^*} W_u)^2$ by Corollary 2.6. We calculate the power moments in this three-valued case.

Lemma 4.1. For any positive integer $k$, we have

$$\sum_{u \in F^*} W_u^k = \frac{q^2(a^{k-1} - b^{k-1}) - qab(a^{k-2} - b^{k-2})}{a - b}.$$

Proof. The $k = 1$ and 2 cases are proved in Corollary 2.6. For $k > 2$, we note that $W_u^{k-2}(W_u - a)(W_u - b) = 0$ for all $u \in F^*$, whence

$$\sum_{u \in F^*} W_u^k = (a + b) \sum_{u \in F^*} W_u^{k-1} - ab \sum_{u \in F^*} W_u^{k-2},$$

from which the identity for $\sum_{u \in F^*} W_u^k$ follows by induction. \hfill \Box

We let $V$ be as defined in equation (6), and note the consequences that our power moment results have for the coefficients of $V$.

Lemma 4.2. $V_1 = a + b - \frac{ab}{q}$, hence $v_p(ab) \geq v_p(q)$, with strict inequality if $p = 2$ or 3.

Proof. Compare Corollary 2.6 and the $k = 3$ case of Lemma 4.1 to deduce the equation. Since $V_1 = \{v \in F : v^d + (1 - v)^d = 1\}$, and since $a, b, 1 \in \mathbb{Z}$, we know that $ab/q$ lies in $\mathbb{Z}$, so that $v_p(ab) \geq v_p(q)$. Suppose that $F$ is of characteristic $p = 2$ or 3. Since $W_{F,d}$ is three-valued, $d \equiv 1 \pmod{p - 1}$ by Theorem 1.4 and so by Proposition 3.1 and Remark 3.2 we see that $V_1 \equiv 0 \pmod{p}$. Furthermore, $a \equiv b \equiv 0 \pmod{p}$ by Theorem 1.3. Thus $ab/q \equiv 0 \pmod{p}$, so $v_p(ab) > v_p(q)$. \hfill \Box

Lemma 4.3. We have

(i). $\sum_{u \in F \setminus \{0,1\}} V_u = \frac{(q-a)(q-b)}{q} > 0$, and

(ii). $\sum_{u \in F \setminus \{0,1\}} V_u^2 = -\frac{ab(q-a)(q-b)}{q^2} > 0$.

Proof. For part (i), we have $\sum_{u \in F \setminus \{0,1\}} V_u = |V| - V_1$, and then use equation (7) and the value of $V_1$ from Lemma 4.2. For part (ii), compare Corollary 2.6 and the $k = 4$ case of Lemma 4.1 to see that

$$q^2 \sum_{u \in F^*} V_u^2 = q^2(a^2 + ab + b^2) - qab(a + b),$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
and then substitute the value of \( V_u \) from Lemma 4.4 and rearrange. Both our sums are strictly positive since \(|a|, |b| < q\), inasmuch as Corollary 2.6(i) shows that \( q^2 = \sum_{u \in F^*} W_u^2 \), which must be at least \( a^2 + b^2 \).

Now write \(|a| = a_o a_p\), \(|b| = b_o b_p\), and \(|a - b| = (a - b)_o (a - b)_p\), where \( a_p, b_p\), and \((a - b)_p\) are powers of \( p\) and \( a_o, b_o\), and \((a - b)_o\) are positive integers coprime to \( p\). So \( \gcd(a_o, b_o)\) is coprime to \( p\), and yet also a divisor of every \( W_u\), hence of \(|W| = q\) (see Corollary 2.6(i)), and so \( \gcd(a_o, b_o) = 1\). Thus \( a_o, b_o\), and \((a - b)_o\) are pairwise coprime, and now we show that they divide most of the coefficients of \( V\).

**Lemma 4.4.** \( a_o b_o (a - b)_o | V_u \) for all \( u \in F^* \) with \( u \neq 1\).

**Proof.** Recall the definitions of \( W \) and \( X \) in equations (4) and (5). Let \( A = \{u \in F^* : W_u = a\} \) and \( B = \{u \in F^* : W_u = b\} \), so that \( W = a A + b B \) and \( X = a^2 A + b^2 B \). Since \( X = W V\) by Lemma 2.6 we solve for \( A \) to get \( a(a - b) A = W(V - b)\), then multiply both sides by \( W\) and apply Corollary 2.4 to get \( a(a - b) AW = q^2(V - b)\). Since \( A \) and \( W\) have integer coefficients, \( a_o(a - b)_o\) divides all the coefficients of \( V - b\), in particular, all \( V_u\) with \( u \neq 1\). By the same method, we deduce that \( b_o(a - b)_o\) divides all \( V_u\) with \( u \neq 1\), and recall that \( a_o, b_o\), and \((a - b)_o\) are pairwise coprime. \( \square \)

Now we recall and prove our main result, Theorem 1.5.

**Theorem 4.5.** If \( q = p^n\), then one of the following holds:

(i). \( v_p(a), v_p(b) > n/2\); or

(ii). \( v_p(a) = v_p(b) = n/2\), and \(|a - b|\) is a power of \( p\) with \(|a - b| > \sqrt{q}\);

and case (ii) cannot occur if \( p = 2 \) or 3.

**Proof.** By Lemma 4.4 \( V_u^2 \geq a_o b_o (a - b)_o \) for each \( u \neq 0, 1\). Thus

\[
\sum_{u \in F \setminus \{0, 1\}} V_u^2 \geq a_o b_o (a - b)_o \sum_{u \in F \setminus \{0, 1\}} V_u,
\]

so by Lemma 4.3 we can divide by the sum on the right to obtain \(-ab/q \geq a_o b_o (a - b)_o\), which yields

\[ a_p b_p \geq q(a - b)_o. \]

If \( a_p \neq b_p\), set \( \{g, h\} = \{a_p, b_p\} \) with \( g < h\). Then \((a - b)_p = g, (a - b)_o = |a - b|/g\), and thus (5) becomes \( g^2 h \geq q|a - b|\). Now \(|a - b| > \max\{|a|, |b|\} \geq h\), so that \( g^2 > q\), and so \( a_p, b_p > \sqrt{q}\), and hence \( v_p(a), v_p(b) > n/2\).

If \( a_p = b_p\), then \( v_p(ab) \geq v_p(q)\) by Lemma 4.2. If this inequality is strict, which it must be if \( p = 2 \) or 3, then \( v_p(a) = v_p(b) > n/2\).

So it remains to consider the case where \( p \geq 5\) and \( v_p(a) = v_p(b) = n/2\). Then \( a_p b_p = q\), so (5) forces \((a - b)_o = 1\), hence \(|a - b|\) must be a power of \( p\), and indeed must be greater than \( \sqrt{q}\) since \(|a - b| > |a|\) and \( a\) is a nonzero integral multiple of \( \sqrt{q}\). \( \square \)

We conclude with a remark about what happens when we are in case (ii) of our theorem, and what that tells us about possible counterexamples to Conjecture 1.2.

**Remark 4.6.** In case (ii) of our theorem, where \( v_p(a) = v_p(b) = n/2\), we have \(-ab/q = a_o b_o\), so that \( V_1 = a + b + a_o b_o\) by Lemma 4.2 and by Lemma 4.3 \( \sum_{v \in F} V_u (V_u - a_o b_o) = 0\). Since \( V_u\) is equal to the count

\[ |\{v \in F : v^d + (1 - v)^d = u^d\}|, \]
and since Lemma 4.3 tells us that \( a_o b_o \mid V_u \) for all \( u \in F \setminus \{0, 1\} \), we see that \( V_u \in \{0, a_o b_o\} \) for all \( u \in F \setminus \{0, 1\} \). Furthermore, \( |a - b| \) is a power of \( p \) greater than \( \sqrt{q} \), so that \( a_o + b_o \) is also a power of \( p \), and \( a_o + b_o \geq 5 \), and so \( a_o b_o \geq 4 \).

Theorem 1.6 forces us into this \( v_p(a) = v_p(b) = n/2 \) case when \( n \) is a power of 2. So if there is a counterexample to Conjecture 1.2, the field \( F \) and exponent \( d \) must have the property that \( a^d + (1 - v)^d \) represents 1 for precisely \( a + b + a_o b_o \) values of \( v \in F \), and it represents \( \frac{2 - a - b - a_o b_o}{a_o b_o} \) elements of \( F \setminus \{0, 1\} \) for precisely \( a_o b_o \) values of \( v \in F \) each, and it does not represent any other element of \( F \).

5. Proof of Theorem 1.6

Throughout this section, we use the definition of \( W_{F,d}(u) \) from (1). We prove Theorem 1.6 using two results of Aubry, Katz, and Langevin (1). The first key result is Corollary 4.2 of that paper.

**Proposition 5.1** (Aubry-Katz-Langevin, 2013). Let \( K \) be a finite field and \( L \) an extension of \( K \) of finite degree, and suppose that \( d \) is a positive integer with \( \gcd(d, |L^*|) = 1 \). Then

\[
\min_{u \in L^*} v_p(W_{L,d}(u)) \leq [L : K] \cdot \min_{u \in K^*} v_p(W_{K,d}(u)).
\]

The second result is part of Corollary 4.4 of the same paper.

**Proposition 5.2** (Aubry-Katz-Langevin, 2013). Let \( K \) be a finite field of characteristic \( p \), and let \( L \) be the quadratic extension of \( K \). Let \( d \) be a positive integer with \( \gcd(d, |L^*|) = 1 \), and suppose that \( d \) is degenerate over \( K \) but not over \( L \). Then

\[
\min_{u \in L^*} v_p(W_{L,d}(u)) = [K : F_p].
\]

We now recall and prove Theorem 1.6.

**Theorem 5.3**. Let \( F \) be a field of characteristic \( p \) and order \( q = p^n \), with \( n \) a power of 2. Let \( d \) be a positive integer with \( \gcd(d, q - 1) = 1 \) such that \( W_{F,d} \) is three-valued. Then there is some \( u \in F^* \) such that \( v_p(W_{F,d}(u)) \leq n/2 \).

**Proof.** By Theorem 1.4 \( d \) is degenerate over \( F_p \). But \( d \) is not degenerate over \( F \) since \( W_{F,d} \) is three-valued (cf. (2)). Proceeding by successive quadratic extensions from \( F_p \) to \( F \), there must be subfields, say \( K \) and \( L \), of \( F \) with \( [L : K] = 2 \) and \( d \) degenerate over \( K \) but not \( L \). Then by Propositions 5.1 and 5.2 we have

\[
\min_{u \in F^*} v_p(W_{F,d}(u)) \leq [F : L] \cdot \min_{u \in L^*} v_p(W_{L,d}(u))
\]

\[
= [F : L][K : F_p],
\]

so that there is some \( u \in F^* \) with \( v_p(W_{F,d}(u)) \leq [F : F_p]/[L : K] = n/2 \). □

**Acknowledgement**

The author was supported in part by a Research, Scholarship, and Creative Activity Award from California State University, Northridge.
REFERENCES

[1] Yves Aubry, Daniel J. Katz, and Philippe Langevin, Cyclotomy of Weil sums of binomials, arXiv:1312.3889 (2013).

[2] Emrah Çakçak and Philippe Langevin, Power permutations in dimension 32, Sequences and their applications—SETA 2010, Lecture Notes in Comput. Sci., vol. 6338, Springer, Berlin, 2010, pp. 181–187, DOI 10.1007/978-3-642-15874-2_14. MR2830722 (2012i:05005)

[3] A. R. Calderbank, Gary McGuire, Bjorn Poonen, and Michael Rubinstein, On a conjecture of Helleseth regarding pairs of binary m-sequences, IEEE Trans. Inform. Theory 42 (1996), no. 3, 988–990, DOI 10.1109/18.490561. MR1445885 (97m:94010)

[4] L. Carlitz, A note on exponential sums, Math. Scand. 42 (1978), no. 1, 39–48. MR500144 (80d:12017)

[5] L. Carlitz, Explicit evaluation of certain exponential sums, Math. Scand. 44 (1979), no. 1, 5–16. MR544577 (80j:10042)

[6] Pascale Charpin, Cyclic codes with few weights and Niho exponents, J. Combin. Theory Ser. A 108 (2004), no. 2, 247–259, DOI 10.1016/j.jcta.2004.07.001. MR2098843 (2005h:94075)

[7] Todd Cochrane and Christopher Pinner, Stepanov’s method applied to binomial exponential sums, Q. J. Math. 54 (2003), no. 3, 243–255, DOI 10.1093/qmath/54.3.243. MR2013138 (2004k:11136)

[8] Todd Cochrane and Christopher Pinner, Explicit bounds on monomial and binomial exponential sums, Q. J. Math. 62 (2011), no. 2, 323–349, DOI 10.1093/qmath/hap041. MR2805207 (2012d:11171)

[9] Robert S. Coulter, Further evaluations of Weil sums, Acta Arith. 86 (1998), no. 3, 217–226. MR1655980 (99i:11113)

[10] H. Davenport and H. Heilbronn, On an Exponential Sum, Proc. London Math. Soc. S2-41, no. 6, 449, DOI 10.1112/plms/s2-41.6.449. MR1576618

[11] Tao Feng, On cyclic codes of length $2^{2r} - 1$ with two zeros whose dual codes have three weights, Des. Codes Cryptogr. 62 (2011), no. 3, 253–258, DOI 10.1007/s10623-011-9514-0. MR2886276 (2012m:94317)

[12] Richard A. Games, The geometry of m-sequences: three-valued crosscorrelations and quadrics in finite projective geometry, SIAM J. Algebraic Discrete Methods 7 (1986), no. 1, 43–52, DOI 10.1137/0607005. MR819704 (87d:51016)

[13] Tor Helleseth, Some results about the cross-correlation function between two maximal linear sequences, Discrete Math. 16 (1976), no. 3, 209–232. MR0429323 (55 #2341)

[14] A. A. Karacuba, Estimates of complete trigonometric sums (Russian), Mat. Zametki 1 (1967), 199–208. MR0205941 (34 #5766)

[15] Daniel J. Katz, Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth, J. Combin. Theory Ser. A 119 (2012), no. 8, 1644–1659, DOI 10.1016/j.jcta.2012.05.003. MR2946379

[16] Nicholas Katz and Ron Livné, Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3 (French, with English summary), C. R. Acad. Sci. Paris Sér. I Math. 309 (1989), no. 11, 723–726. MR1054286 (91e:11066)

[17] H. D. Kloosterman, On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$, Acta Math. 49 (1927), no. 3-4, 407–464, DOI 10.1007/BF02564120. MR1555249

[18] Gilles Lachaud and Jacques Wolfmann, Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2 (French, with English summary), C. R. Acad. Sci. Paris Sér. I Math. 305 (1987), no. 20, 881–883. MR925289 (89c:11031)

[19] Rudolf Lidl and Harald Niederreiter, Finite fields, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997. With a foreword by P. M. Cohn. MR1423994 (97i:11115)

[20] Gary McGuire, On certain 3-weight cyclic codes having symmetric weights and a conjecture of Helleseth, Sequences and their applications (Bergen, 2001), Discrete Math. Theor. Comput. Sci. (Lond.), Springer, London, 2002, pp. 281–295. MR1916139 (2003c:94104)

[21] I. Vinogradov, Some trigonometrical polynomials and their applications, C. R. Acad. Sci. URSS (N.S.) (1933), no. 6, 254–255.