Cyclotomy of Weil Sums of Binomials

Yves Aubry, Daniel J. Katz, Philippe Langevin

CYCLOTOMY OF WEIL SUMS OF BINOMIALS

YVES AUBRY, DANIEL J. KATZ, AND PHILIPPE LANGEVIN

Abstract. The Weil sum $W_{K,d}(a) = \sum_{x\in K} \psi(x^d + ax)$ where K is a finite field, ψ is an additive character of K, d is coprime to $|K^\times|$, and $a \in K^\times$ arises often in number-theoretic calculations, and in applications to finite geometry, cryptography, digital sequence design, and coding theory. Researchers are especially interested in the case where $W_{K,d}(a)$ assumes three distinct values as a runs through $K^\times$. A Galois-theoretic approach, combined with p-divisibility results on Gauss sums, is used here to prove a variety of new results that constrain which fields K and exponents d support three-valued Weil sums, and restrict the values that such Weil sums may assume.

1. Introduction

Let K be a finite field of characteristic p. Let ψ_K be the canonical additive character of K, that is, $\psi_K(x) = \exp(2i\pi \operatorname{Tr}_{K/\mathbb{F}_p}(x)/p)$ where $\operatorname{Tr}_{K/\mathbb{F}_p}$ is the absolute trace. *Weil sums* with ψ_K applied to binomials, that is, sums of the form $\sum_{x\in K} \psi_K(bx^j + cx^k)$, have been studied extensively from the early twentieth century to present [32, 37, 41, 14, 1, 23, 6, 7, 33, 31, 11, 9, 10]. We are interested in such sums when j and k are coprime to $|K^\times|$, in which case we reparameterize them to obtain sums of the form

$$\mathrm{W}_{K,d}(a) = \sum_{x\in K} \psi_K(x^d + ax) \tag{1}$$

with $\gcd(d, |K^\times|) = 1$ and $a \in K$. This definition will remain in force throughout the paper, and we shall always insist that $\gcd(d, |K^\times|) = 1$ whenever we write $\mathrm{W}_{K,d}$. The sums $\mathrm{W}_{K,d}(a)$ are always real algebraic integers [20, Theorem 3.1(a)], and furthermore, are all rational integers if and only if $d \equiv 1 \pmod{p-1}$ [20, Theorem 4.2]. Apart from arising often in number-theoretic calculations, these sums are also the key to problems in finite geometry, cryptography, digital sequence design, and coding theory, as discussed in [27, Appendix].

For a fixed K and d, we consider $\mathrm{W}_{K,d}(a)$ as a function of $a \in K^\times$, and are interested in how many different values it assumes as a runs through $K^\times$. $\mathrm{W}_{K,d}(a)$ with $a = 0$ is passed over, as it is the Weil sum of the monomial x^d, and since $x \mapsto x^d$ is a permutation of K, we always have $\mathrm{W}_{K,d}(0) = 0$. We call $\{\mathrm{W}_{K,d}(a) : a \in K^\times\}$ the *value set* of $\mathrm{W}_{K,d}$, and say that $\mathrm{W}_{K,d}$ is *v-valued* over K to mean that this set is of cardinality v.

Date: first version: 12 December 2013; this version: 02 April 2015.

If $d \equiv p^j \pmod{|K^\times|}$ for some j, we say that d is *degenerate over* K, because $\mathrm{Tr}_{K/\mathbb{F}_p}(x^d + ax) = \mathrm{Tr}_{K/\mathbb{F}_p}((1+a)x)$, and so the binomial effectively becomes zero (if $a = -1$) or a nonvanishing linear form (if $a \neq -1$). Thus if d is degenerate over K, one readily obtains for $a \in K$ that

$$\mathrm{W}_{K,d}(a) = \begin{cases} |K| & \text{if } a = -1, \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

Helleseth [20, Theorem 4.1] shows that one always obtains a richer value set in the nondegenerate case.

Theorem 1.1 (Helleseth, 1976)**.** *If d is nondegenerate over K, then $\mathrm{W}_{K,d}(a)$ takes at least three values as a runs through $K^\times$.*

Here we want to know when Weil sums of this form can be three-valued, and if so, what are the three values they may take. We indicate all known infinite families of three-valued examples, arranged according to analogy, in Table 1 below.

TABLE 1. Three-Valued Weil Sums

order of K	d (nondegenerate)	values of $W_{K,d}$	reference
$q = 2^e$	$d = 2^i + 1$ $\mathrm{val}_2(i) \geq \mathrm{val}_2(e)$	$0, \pm\sqrt{2^{\gcd(e,i)}q}$	[24, 26, 18]
$q = p^e$ p odd	$d = \frac{1}{2}(p^{2i} + 1)$ $\mathrm{val}_2(i) \geq \mathrm{val}_2(e)$	$0, \pm\sqrt{p^{\gcd(e,i)}q}$	[40] (e odd) [19, 20] (e even)
$q = 2^e$	$d = 2^{2i} - 2^i + 1$, $\mathrm{val}_2(i) \geq \mathrm{val}_2(e)$	$0, \pm\sqrt{2^{\gcd(e,i)}q}$	[42, 25]
$q = p^e$ p odd	$d = p^{2i} - p^i + 1$ $\mathrm{val}_2(i) \geq \mathrm{val}_2(e)$	$0, \pm\sqrt{p^{\gcd(e,i)}q}$	[40] (e odd) [19, 20] (e even)
$q = 2^e$ $\mathrm{val}_2(e) = 1$	$d = 2^{e/2} + 2^{(e+2)/4} + 1$	$0, \pm 2\sqrt{q}$	[12]
$q = 2^e$ $\mathrm{val}_2(e) = 1$	$d = 2^{(e+2)/4} + 3$	$0, \pm 2\sqrt{q}$	[12]
$q = 2^e$ e odd	$d = 2^{(e-1)/2} + 3$	$0, \pm\sqrt{2q}$	[4, 5, 21]
$q = 3^e$ e odd	$d = 2 \cdot 3^{(e-1)/2} + 1$	$0, \pm\sqrt{3q}$	[15]
$q = 2^e$ e odd	$d = 2^{2i} + 2^i - 1$ $e \mid 4i + 1$	$0, \pm\sqrt{2q}$	[21, 22]
$q = 3^e$ e odd	$d = 2 \cdot 3^i + 1$ $e \mid 4i + 1$	$0, \pm\sqrt{3q}$	[30]

In several entries, we make use of the *p-adic valuation* of an integer a, denoted $\mathrm{val}_p(a)$, which is the maximum k such that $p^k \mid a$ (or ∞ if $a = 0$). We write "nondegenerate" in the column heading for d values to impose the

condition that d be nondegenerate over K throughout the table, so that, for example, we cannot have $i = 0$ in the first four rows. If K has characteristic p and $1/d$ is interpreted modulo $|K^\times|$, then $\mathrm{W}_{K,pd}$ and $\mathrm{W}_{K,1/d}$ take the same values as $\mathrm{W}_{K,d}$ [20, Theorem 3.1], so the table records representative d modulo these equivalences.

First of all, note that all these value sets consist of three rational integers, one of which is 0, with the other two being opposites of each other. The first two properties are inevitable facts, as shown in [27, Theorems 1.7, 1.9].

Theorem 1.2 (Katz, 2012)**.** *Let K be a finite field of characteristic p. If $\mathrm{W}_{K,d}$ is three-valued for some exponent d, then $d \equiv 1 \pmod{p-1}$, and the values must be rational integers, one of which is zero.*

Concerning the two nonzero values of a three-valued Weil sum, one must be positive and the other negative, since it is known that $\sum_{a\in K^\times} \mathrm{W}_{K,d}(a)^2 = \left(\sum_{a\in K^\times} \mathrm{W}_{K,d}(a)\right)^2$. (See Lemma 2.1 and Corollary 2.3 below for details.) However, it has not been proved that these values must have the same magnitude, although this is always what has been observed. We say that a three-valued Weil sum $\mathrm{W}_{K,d}$ is *symmetric* when the two nonzero values are opposites of each other. If we assume that a three-valued Weil sum is symmetric, we can make further conclusions about the possible values.

Proposition 1.3. *If K is the finite field of characteristic p and order q, and if $\mathrm{W}_{K,d}(a)$ is three-valued with values 0 and $\pm A$, then $|A| = p^k$ for some positive integer k with $\sqrt{q} < p^k < q$.*

This follows easily from well-known facts, which are arranged in Section 2, where the above proposition is proved as Proposition 2.4.

Our first main result shows that in many cases, $\mathrm{W}_{K,d}$ cannot be symmetric three-valued.

Theorem 1.4. *Let K be a finite field, and suppose that I and J are subfields of K with $[J : I] = 2$, with d degenerate over I but not over J. Then the set of values assumed by $\mathrm{W}_{K,d}(a)$ as a runs through $K^\times$ is not of the form $\{-A, 0, +A\}$ for any A.*

We prove this in Section 6. This means that a field obtained by a tower of quadratic extensions over a prime field can never support a symmetric three-valued sum.

Corollary 1.5. *Let K be a finite field of characteristic p, and suppose that $[K : \mathbb{F}_p]$ is a power of 2. Then the set of values assumed by $\mathrm{W}_{K,d}(a)$ as a runs through $K^\times$ is not of the form $\{-A, 0, +A\}$ for any A.*

For if $\mathrm{W}_{K,d}$ were three-valued, Theorem 1.2 and eq. (2) would make d degenerate over $\mathbb{F}_p$ but not over K, and then as we proceed from $\mathbb{F}_p$ toward K up the tower of quadratic extensions, we must find a step where d passes from degenerate to nondegenerate. This corollary generalizes a result of Calderbank-McGuire-Poonen-Rubinstein [3, Theorem 3]. Our proof is quite

different from that of Calderbank et al., who used McEliece's Theorem from coding theory (a relative of Stickelberger's Theorem on the p-divisibility of Gauss sums) and a delicate calculation in additive number theory to obtain Corollary 1.5 in the case where $p = 2$. The proof for Theorem 1.4 in full generality given here is much more straightforward, and is the consequence of some useful observations about the p-adic valuation of Weil sums. These observations come as a consequence of relations (explored in Section 4) between Weil and Gauss sums over a field and sums of the same form over a subfield: the Gauss sums play a role since Weil sums can be written in terms of Gauss sums, and the Davenport-Hasse relation supplies the connection between Gauss sums over the field and Gauss sums over the subfield.

Note that if K is a field of characteristic p and order $q = p^e$, with e not equal to a power of 2, then we can set $i = 2^{\mathrm{val}_2(e)}$ in the first four rows of Table 1 to obtain a d such that $W_{q,d}$ is three-valued. On the other hand, Table 1 furnishes no example of a three-valued $W_{K,d}$ with $[K : \mathbb{F}_p]$ a power of 2. (Recall that our table prohibits parameters which make d degenerate, so we cannot have i a multiple of e in the first four rows.) Helleseth conjectured [20, Conjecture 5.2] that for such fields there is no d that makes the Weil sum $W_{K,d}$ three-valued.

Conjecture 1.6 (Helleseth, 1976)**.** *Let K be a finite field of characteristic p. If $[K : \mathbb{F}_p]$ is a power of 2, then $\mathrm{W}_{K,d}$ is not three-valued.*

If it were proved that three-valued Weil sums must be symmetric, this would follow from Corollary 1.5. The $p = 2$ and 3 cases of Conjecture 1.6 have been proved. First, Feng [16, Theorem 2] showed that if $p = 2$, one could strengthen the conclusion of Corollary 1.5 to say that the value set is not only non-symmetric, but entirely lacks the value 0. Then when Katz [27, Theorem 1.9] proved that a three-valued Weil sum must take the value 0, Conjecture 1.6 was established for $p = 2$. Further work of Katz [28, Theorem 1.7] shows that Conjecture 1.6 is also true when $p = 3$.

A symmetric three-valued Weil sum is called *preferred* if the magnitude of the nonzero values is as small as possible in view of Proposition 1.3, that is, if the nonzero values are $\pm\sqrt{pq}$ when q is an odd power of p, or if the nonzero values are $\pm p\sqrt{q}$ when q is an even power of p. This terminology originates from digital sequence design, wherein smaller magnitude Weil sums of binomials correspond to smaller cross-correlation between a pair of maximal linear recursive sequences, which is desirable. The known infinite families of preferred three-valued Weil sums can be deduced from Table 1 above: the last seven rows furnish preferred Weil sums, and in the first four rows, one must have $\gcd(e, i) = 1$ if e is odd, or $\gcd(e, i) = 2$ if e is even.

Our second main result is a lower bound on the magnitude of the nonzero values of a symmetric three-valued Weil sum $\mathrm{W}_{K,d}$. This bound grows as the 2-divisibility of the degree of K over its prime field increases.

Theorem 1.7. *Let K be the finite field of characteristic p and order q. If $\mathrm{val}_2([K : \mathbb{F}_p]) = s$ and $\mathrm{W}_{K,d}$ is symmetric three-valued with values $0, \pm A$, then $|A| \geq p^{2^{s-1}}\sqrt{q}$.*

We prove this in Section 7. One consequence is that if the degree of K over its prime field is a multiple of 4, then $\mathrm{W}_{K,d}$ cannot be preferred.

Corollary 1.8. *Let K be the finite field of characteristic p and order q. If $[K : \mathbb{F}_p] \equiv 0 \pmod 4$, then the set of values assumed by $\mathrm{W}_{K,d}$ as a runs through $K^\times$ is not of the form $\{0, \pm p\sqrt{q}\}$.*

This generalizes the result of Calderbank-McGuire [2], who proved a conjecture of Sarwate and Pursley [39, p. 603], which is the special case of Corollary 1.8 where $p = 2$. Our proof technique for Theorem 1.7 in full generality is much simpler than the original proof of Calderbank-McGuire, as it obviates the need for McEliece's Theorem or Stickelberger's Theorem.

Our first two results give restrictions on the types of fields that support symmetric and preferred Weil sums. Our third result shows that certain exponents d of the polynomial in the Weil sum prevent the Weil sum from being three-valued at all.

Theorem 1.9. *Let K be a finite field of characteristic p with $[K : \mathbb{F}_p]$ even. If d is a power of p modulo $\sqrt{|K|} - 1$, then $\mathrm{W}_{K,d}$ is not three-valued.*

In other words, it is impossible for $\mathrm{W}_{K,d}$ to be three-valued if K is the quadratic extension of a field F in which d is degenerate. We prove this in Section 8. Such an exponent d is called a *Niho exponent*, since they were first studied by Niho in [38]. Theorem 1.9 generalizes the result of Charpin [8, Theorem 2], who proved the $p = 2$ case. Some steps of Charpin's proof for characteristic two do not hold in odd characteristic, so new arguments are devised.

Finally, the techniques developed here can be used to simplify the proof that the values of a three-valued Weil sum must be rational integers, a result that appears above in Theorem 1.2, and which originally appeared in [27, Theorem 1.7]. The new proof is presented in Section 9.

Our proofs of all the above results make extensive use of Galois theory. Since Weil sums connect calculations in finite fields to calculations in cyclotomic extensions of $\mathbb{Q}$, there are two realms, both cyclotomic, where Galois groups come into play. On the one hand, there are Galois groups for finite fields, which act on the terms of the polynomial arguments of the characters in the Weil sums; this is explored in Section 3. On the other hand, there are Galois groups for cyclotomic fields, which are applied to the values of the Weil sums; this is explored in Section 5. This dual Galois-theoretic approach has proved to be both powerful for obtaining new results, and at the same time, simplifies the proofs of previous results that we recapitulate.

We should note that Weil sums assuming four, five, or more values are also studied (see [20, Theorems 2.2, 2.3, 4.8, 4.10, 4.11, 4.13] for some examples), but we focus on the three-valued ones, as they are extremal in

view of Theorem 1.1. It has been asked [29, Problem 3.6] whether there is an analogue of Theorem 1.2 for four-valued Weil sums. Four-valued Weil sums $W_{K,d}(a)$ are known that assume irrational values and do not assume the value 0 for $a \in K^\times$. For example, if K is the field with 5 elements and $d = 3$, then $W_{K,d}(a)$ assumes four distinct irrational values ($\pm\sqrt{5}$ and $(5 \pm \sqrt{5})/2$) as a runs through $K^\times$. Thus any analogue of Theorem 1.2 for four-valued sums would need to be significantly different from the original.

The organization of this paper is as follows: in Section 2, we prove some preliminary results using the well-known methodology of power moments. In Section 3, we explore the action of the Galois groups of finite fields on the terms inside the Weil sums. In Section 4, we look at the Fourier transform of the value set of our Weil sums, which is expressible in terms of Gauss sums, from which we deduce results about the p-adic valuation of Weil sum values. In Section 5, we explore the action of the Galois groups of cyclotomic fields on the values of the Weil sums. In Sections 6, 7, and 8, we prove Theorems 1.4, 1.7, and 1.9, respectively. In Section 9, we finish with our new simpler proof of the rationality of the values of three-valued Weil sums.

2. Power Moments of Weil Sums

In this section we state some of the basic results about Weil sums that will be useful later on. These facts are proved using character sums known as power moments. Recall the definition (1) of $\mathrm{W}_{K,d}$, and our tacit insistence that $\gcd(d, |K^\times|) = 1$ whenever we write $\mathrm{W}_{K,d}$. The mth *power moment* of the Weil sum $\mathrm{W}_{K,d}$ is the sum

$$\sum_{a \in K^\times} \mathrm{W}_{K,d}(a)^m.$$

The first few power moments can be calculated as straightforward character sums.

Lemma 2.1. *Let K be a finite field. Then*

(i). $\sum_{a \in K^\times} \mathrm{W}_{K,d}(a) = |K|$,
(ii). $\sum_{a \in K^\times} \mathrm{W}_{K,d}(a)^2 = |K|^2$, *and*
(iii). $\sum_{a \in K^\times} \mathrm{W}_{K,d}(a)^3 = |K|^2 \cdot |R|$,

where R is the set of roots of the polynomial $(x+1)^d - x^d - 1$ in K.

Proof. See [27, Proposition 3.1]. □

Corollary 2.2. *If K is a finite field, and d is nondegenerate over K, then $|\mathrm{W}_{K,d}(a)| < |K|$ for all $a \in K^\times$.*

Proof. From Lemma 2.1(ii), the only way to escape this conclusion would be to have $|\mathrm{W}_{K,d}(b)| = |K|$ for some $b \in K^\times$, and $\mathrm{W}_{K,d}(a) = 0$ for all other a, which would make the Weil sum two-valued, contrary to Theorem 1.1. □

Corollary 2.3. *If d is nondegenerate over K, then $\mathrm{W}_{K,d}$ assumes at least one positive value and at least one negative value.*

Proof. Recall that the Weil sum values are real algebraic integers [20, Theorem 3.1(a)]. By Theorem 1.1, we know that $\mathrm{W}_{K,d}$ must assume at least two nonzero values. If all the nonzero values it assumes were of the same sign, then $\left(\sum_{a\in K^\times} \mathrm{W}_{K,d}(a)\right)^2 > \sum_{a\in K^\times} \mathrm{W}_{K,d}(a)^2$, contradicting Lemma 2.1(i) and (ii). □

The following is an easy consequence of this power moment analysis, and provides the proof of Proposition 1.3 in the Introduction.

Proposition 2.4. *If K is the finite field of characteristic p and order q, and if $\mathrm{W}_{K,d}(a)$ is three-valued with values 0 and $\pm A$, then $d \equiv 1 \pmod{p-1}$ and $|A| = p^k$ for some positive integer k. If R denotes the set of roots of $(x+1)^d - x^d - 1$ in K, then $\sqrt{q} < \sqrt{|R|\,q} = |A| < q$.*

Proof. By Theorem 1.2, we must have $A \in \mathbb{Z}$ and $d \equiv 1 \pmod{p-1}$. Let N_A be the number of $a \in K^\times$ with $\mathrm{W}_{K,d}(a) = A$. Since the other two values $\mathrm{W}_{K,d}(a)$ assumes are 0 and $-A$, we have $\sum_{a\in K^\times} \mathrm{W}_{K,d}(a)(\mathrm{W}_{K,d}(a) + A) = 2A^2 N_A$, and by Lemma 2.1(i),(ii), this sum also equals $q^2 + qA$, so that $N_A = (q^2 + qA)/(2A^2)$, and so A can not be divisible by any prime other than p. We know $|A| < q$ by Corollary 2.2.

Similarly, $\sum_{a\in K^\times} \mathrm{W}_{K,d}(a)(\mathrm{W}_{K,d}(a)^2 - A^2) = 0$, and by Lemma 2.1(i),(iii) equals $q^2\,|R| - qA^2$, so $|A| = \sqrt{|R|\,q}$. Then note that $0, -1 \in R$. (This is clear for $p = 2$, and for p odd, note that $\gcd(d, q-1) = 1$ forces d to be odd.) Thus $A \geq \sqrt{2q}$. □

It will also be useful to consider a version of the first power moment of a Weil sum, but where we restrict the summation to a smaller subfield.

Lemma 2.5. *Let K be a finite field and let L be the quadratic extension of K. Then*

$$\sum_{a\in K^\times} \mathrm{W}_{L,d}(a) = |L|\,.$$

Proof. Let $q = |K|$. Since $\mathrm{W}_{L,d}(0) = 0$, we have

$$\begin{aligned}\sum_{a\in K^\times} \mathrm{W}_{L,d}(a) &= \sum_{x\in L} \psi_L(x^d) \sum_{a\in K} \psi_K(a\,\mathrm{Tr}_{L/K}(x)) \\ &= q \sum_{\substack{x\in L \\ \mathrm{Tr}_{L/K}(x)=0}} \psi_L(x^d).\end{aligned}$$

If $x \in L$ with $\mathrm{Tr}_{L/K}(x) = 0$, then $x^q = -x$, so that $\mathrm{Tr}_{L/K}(x^d) = x^{qd} + x^d = (-x)^d + x^d = 0$. (In odd characteristic, $\gcd(d, q-1) = 1$ makes d odd.) Thus $\sum_{a\in K^\times} \mathrm{W}_{L,d}(a) = q \cdot \left|\{x \in L : \mathrm{Tr}_{L/K}(x) = 0\}\right| = q^2 = |L|$. □

3. Action of Galois Groups of Finite Fields

We begin this section by seeing that the automorphisms of a finite field K act trivially with respect to the Weil sum $\mathrm{W}_{K,d}(a)$. As always $\mathrm{W}_{K,d}(a)$ is as defined in (1), and $\gcd(d, |K^\times|) = 1$ whenever we write $\mathrm{W}_{K,d}$.

Lemma 3.1. *Let K be a finite field of characteristic p. If $\sigma \in \mathrm{Gal}(K/\mathbb{F}_p)$, then $\mathrm{W}_{K,d}(\sigma(a)) = \mathrm{W}_{K,d}(a)$.*

Proof. Since Galois conjugates have the same trace, they have the same character value. Thus $\mathrm{W}_{K,d}(a) = \sum_{x\in K} \psi_K(\sigma(x^d + ax))$, and by reparameterizing with $y = \sigma(x)$, we have $\mathrm{W}_{K,d}(a) = \sum_{y\in K} \psi_K(y^d + \sigma(a)y) = \mathrm{W}_{K,d}(\sigma(a))$. □

The action of the Galois group also shows that some exponents give equivalent Weil sums.

Lemma 3.2. *Let K be a finite field of characteristic p. Then $\mathrm{W}_{K,d}(a) = \mathrm{W}_{K,p^j d}(a)$ for any $a \in K$ and $j \in \mathbb{Z}$.*

Proof. This follows immediately from the fact that $x^{p^j d}$ is a Galois conjugate of x^d, and so $\psi_K(x^{p^j d}) = \psi_K(x^d)$. □

Now we use finite field automorphisms to prove a congruence between the Weil sum over a field and the Weil sum over its extensions.

Lemma 3.3. *Let K be a finite field of characteristic p, and let L be an extension of K with $[L : K]$ a power of a prime ℓ distinct from p. Then for any $a \in K$, we have*

$$\mathrm{W}_{L,d}(a) \equiv \mathrm{W}_{K,d}([L : K]^{1-1/d}a) \pmod{\ell},$$

where $1/d$ indicates the multiplicative inverse of d modulo $p - 1$.

Proof. For $a \in K$, we have

$$\mathrm{W}_{L,d}(a) = \sum_{x\in K} \psi_K(\mathrm{Tr}_{L/K}(x^d + ax)) + \sum_{x\in L\smallsetminus K} \psi_L(x^d + ax).$$

The first sum equals $\sum_{x\in K} \psi_K([L : K](x^d + ax))$, and if we reparameterize with $w = [L : K]^{1/d}x$, then we see that this sum is $\mathrm{W}_{K,d}([L : K]^{1-1/d}a)$. For the second sum, the action of $\mathrm{Gal}(L/K)$ partitions $L\smallsetminus K$ into orbits of Galois conjugates whose sizes are positive powers of ℓ. For any $\sigma \in \mathrm{Gal}(L/K)$, we have $\psi_L(x^d + ax) = \psi_L(\sigma(x^d + ax)) = \psi_L(\sigma(x)^d + a\sigma(x))$, so that the value of $\psi_L(x^d + ax)$ is constant on orbits, and thus the sum over $L \smallsetminus K$ is ℓ times a sum of algebraic integers. □

We then explore what this tells us in the case where d is degenerate in the smaller field.

Corollary 3.4. *Let K be a finite field of characteristic p, and let L be an extension of L with $[L : K]$ a power of a prime ℓ distinct from p. Let d be degenerate over K. Then $\mathrm{W}_{L,d}(-1) \equiv |K| \pmod{\ell}$ and $\mathrm{W}_{L,d}(a) \equiv 0 \pmod{\ell}$ for every $a \in K \smallsetminus \{-1\}$.*

Proof. Combine Lemma 3.3 with (2), and note that since d is degenerate over K, we have $d \equiv 1 \pmod{p-1}$, so the factor of $[K : L]^{1-1/d}$ mentioned in Lemma 3.3 is equal to 1. □

4. Gauss Sum and Valuation

In this section, we explore the Fourier transform of the value set of the Weil sum, which is expressible in terms of Gauss sums. This will enable us to prove some criteria about the p-divisibility of Weil sum values.

Throughout this section K is a finite field of characteristic p and order q and, as always, we assume that $\gcd(d, q-1) = 1$. For any multiplicative character $\chi \in \widehat{K^\times}$, we consider the Gauss sum

$$\tau_K(\chi) = \sum_{a \in K^\times} \chi(a)\psi_K(a).$$

By Fourier inversion, if $a \in K^\times$, we find that

$$\psi_K(a) = \frac{1}{q-1} \sum_{\chi \in \widehat{K^\times}} \tau_K(\chi)\bar{\chi}(a).$$

Thus for $a \in K^\times$,

$$\begin{aligned} \mathrm{W}_{K,d}(a) &= 1 + \frac{1}{(q-1)^2} \sum_{b \in K^\times} \sum_{\chi,\varphi \in \widehat{K^\times}} \tau_K(\chi)\tau_K(\varphi)\bar{\chi}^d(b)\bar{\varphi}(ab) \\ &= 1 + \frac{1}{q-1} \sum_{\substack{\chi,\varphi \in \widehat{K^\times} \\ \varphi = \bar{\chi}^d}} \tau_K(\chi)\tau_K(\varphi)\bar{\varphi}(a) \\ &= \frac{q}{q-1} + \frac{1}{q-1} \sum_{\chi \neq 1} \tau_K(\chi)\tau_K(\bar{\chi}^d)\chi^d(a). \end{aligned} \tag{3}$$

If we denote by t the inverse of $-d$ modulo $q-1$, the above formula shows that q and the $\tau_K(\chi)\tau_K(\bar{\chi}^d)$ are the Fourier coefficients of the mapping $a \mapsto \mathrm{W}_{K,d}(a^t)$ from $K^\times$ to $\mathbb{C}$, whence by Fourier inversion

$$\sum_{a \in K^\times} \mathrm{W}_{K,d}(a^t)\chi(a) = \begin{cases} \mathrm{q} & \text{if } \chi = 1, \\ \tau_K(\chi)\tau_K(\bar{\chi}^d) & \text{otherwise.} \end{cases} \tag{4}$$

Recall from the Introduction that for any nonzero integer n, the *p-adic valuation* of n, written $\mathrm{val}_p(n)$, is the largest k such that p^k divides n, and we set $\mathrm{val}_p(0) = \infty$. Then $\mathrm{val}_p(ab) = \mathrm{val}_p(a) + \mathrm{val}_p(b)$ and $\mathrm{val}_p(a + b) \geq \min\{\mathrm{val}_p(a), \mathrm{val}_p(b)\}$, which becomes an equality whenever $\mathrm{val}_p(a) \neq \mathrm{val}_p(b)$. We can extend the definition to $\mathbb{Q}$, wherein $\mathrm{val}_p(a/b) = \mathrm{val}_p(a) - \mathrm{val}_p(b)$. If ζ_p and ζ_{q-1} are, respectively, primitive pth and $(q-1)$th roots of unity over $\mathbb{Q}$, we can further extend val_p to the field $\mathbb{Q}(\zeta_p, \zeta_{q-1})$ where the Gauss sums reside, while still retaining the relations given above concerning products and sums of elements. In this last field, elements can have fractional valuations: for instance $\mathrm{val}_p(1 - \zeta_p) = 1/(p-1)$.

We introduce the useful notation

$$\mathrm{V}_{K,d} = \min_{a \in K^\times} \mathrm{val}_p(\mathrm{W}_{K,d}(a)).$$

It is well known [35], [36, Section 6] that Stickelberger's congruence on Gauss sums can be used to obtain the value of $\mathrm{V}_{K,d}$ but we do not need it to reach our goal.

Lemma 4.1. *For K a finite field of order q, and d an integer coprime to $q-1$, we have*

$$\mathrm{V}_{K,d} = \min_{\substack{\chi \in \widehat{K^\times} \\ \chi \neq 1}} \mathrm{val}_p(\tau_K(\chi)\tau_K(\bar{\chi}^d)).$$

Proof. This is straightforward once we note that $\mathrm{val}_p(\chi(a)) = 0$ for any $\chi \in \widehat{K^\times}$ and any $a \in K^\times$, because $(q-1)\mathrm{val}_p(\chi(a)) = \mathrm{val}_p(\chi(a)^{q-1}) = \mathrm{val}_p(1) = 0$. Using the relation (3), one has $\mathrm{V}_{K,d} \geq \min_{\chi\neq 1} \mathrm{val}_p(\tau_K(\chi)\tau_K(\bar{\chi}^d))$, and the reverse inequality is obtained by using the relation (4), once we establish that $\min_{\chi\neq 1} \mathrm{val}_p(\tau_K(\chi)\tau_K(\bar{\chi}^d)) \leq \mathrm{val}_p(q)$. This last fact follows because $\tau_K(\bar{\chi}) = \chi(-1)\tau_K(\chi)$ and $|\tau_K(\chi)|^2 = q$ for any nontrivial multiplicative character χ, and so $\prod_{\chi\neq 1} \tau_K(\chi)\tau_K(\bar{\chi}^d) = \pm q^{q-2}$. □

Corollary 4.2. *Let L be a finite extension of K. For a positive integer d,*

$$\mathrm{V}_{L,d} \leq [L:K] \times \mathrm{V}_{K,d}$$

Proof. Denoting by $\mathrm{N}_{L/K}$ the norm from L over K, the Davenport-Hasse relation (see [13]) tells us that if $\chi \in \widehat{K^\times}$, we have

$$-\tau_L(\chi \circ \mathrm{N}_{L/K}) = (-\tau_K(\chi))^{[L:K]},$$

and the set of lifted characters $\chi \circ \mathrm{N}_{L/K}$ as χ runs through the nontrivial elements of $\widehat{K^\times}$ is a subset of the nontrivial elements of $\widehat{L^\times}$. □

The remaining results in this section are specific to quadratic extensions of finite fields, which are involved in our three main results (Theorems 1.4, 1.7, and 1.9).

Lemma 4.3. *Let K be a finite field, and let L be the quadratic extension of K. Let d be degenerate over K, but not over L. Let Y be a set of representatives of cosets of $K^\times$ in $L^\times$. Then for $a \in L$, we have*

$$\mathrm{W}_{L,d}(a) = |K|\,(Z(a) - 1),$$

where $Z(a)$ is the number of $y \in Y$ such that $\mathrm{Tr}_{L/K}(y^d + ay) = 0$.

Proof. If K has characteristic p, then Lemma 3.2 allows us to replace d with $p^j d$ for any j, so we may take $d \equiv 1 \pmod{|K^\times|}$ without loss of generality. Then

$$\begin{aligned}\mathrm{W}_{L,d}(a) &= 1 + \sum_{y\in Y} \sum_{x\in K^\times} \psi_L((y^d + ay)x) \\ &= -|K| + \sum_{y\in Y} \sum_{x\in K} \psi_K(x\,\mathrm{Tr}_{L/K}(y^d + ay)),\end{aligned}$$

since $|Y| = (|L|-1)/(|K|-1) = |K| + 1$. The sum over x is $|K|$ when $\mathrm{Tr}_{L/K}(y^d + ay) = 0$; otherwise the sum is 0. □

This calculation has immediate consequences for the p-adic valuation of Weil sum values.

Corollary 4.4. *Let K be a finite field of characteristic p, and let L be the quadratic extension of K. Let d be degenerate over K, but not over L. Then*

$$\mathrm{V}_{L,d} = [K : \mathbb{F}_p],$$

and furthermore, $\mathrm{W}_{L,d}(a) = -|K|$ for some $a \in L^\times$.

Proof. Let Y and $Z(a)$ be as defined in Lemma 4.3, which tells us that

$$\mathrm{W}_{L,d}(a) = |K|\,(Z(a) - 1),$$

for each $a \in L$. All these numbers have a valuation greater or equal to $[K : \mathbb{F}_p]$. Since d is not degenerate over L, $\mathrm{W}_{L,d}(a)$ must be negative for some $a \in L^\times$ by Corollary 2.3. The only way to make $\mathrm{W}_{L,d}(a)$ negative is to have $Z(a) = 0$, which makes $\mathrm{W}_{L,d}(a) = -\,|K|$, and then the valuation of $\mathrm{W}_{L,d}(a)$ is precisely $[K : \mathbb{F}_p]$. □

The calculation of Lemma 4.3 also gives a nonnegativity condition that will be useful in our proof of Theorem 1.9.

Corollary 4.5. *Let K be a finite field, and let L be the quadratic extension of K. Let d be degenerate over K. Then $\mathrm{W}_{L,d}(a) \geq 0$ for all $a \in K$.*

Proof. We may take d nondegenerate over L, since (2) settles the degenerate case. Let $a \in K$. By Lemma 4.3, it suffices to find some $y \in L^\times$ such that $\mathrm{Tr}_{L/K}(y^d + ay) = 1$. In characteristic 2, take $y \in K^\times$, so that $\mathrm{Tr}_{L/K}(y^d + ay) = 2(y^d + ay) = 0$. In odd characteristic, take $y \in L$ with $y^2 \in K$ but $y \notin K$. Then y and $-y$ are conjugates under the action of $\mathrm{Gal}(L/K)$, and so $\mathrm{Tr}_{L/K}(y^d + ay) = (-y)^d + a(-y) + y^d + ay = 0$. □

5. Action of Galois Groups of Cyclotomic Fields

Throughout this section, ζ_p denotes a primitive pth root of unity over $\mathbb{Q}$. If K is a field of characteristic p, then the Weil sum values $\mathrm{W}_{K,d}(a)$ reside in $\mathbb{Q}(\zeta_p)$ by definition (1). First we see how Galois automorphisms permute the Weil sum values. Recall that we always have d invertible modulo $|K^\times|$ whenever we write the sum $\mathrm{W}_{K,d}$.

Lemma 5.1. *Let K be a finite field of characteristic p. If σ is the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ with $\sigma(\zeta_p) = \zeta_p^j$, then $\sigma(\mathrm{W}_{K,d}(a)) = \mathrm{W}_{K,d}(j^{1-(1/d)}a)$, where $1/d$ indicates the multiplicative inverse of d modulo $p-1$.*

Proof. This is [27, Theorem 2.1(b)]. □

This shows that if two Weil sum values are Galois conjugates over $\mathbb{Q}$, then they occur equally often.

Corollary 5.2. *Let K be a finite field, and let A and B be values assumed by $\mathrm{W}_{K,d}$. If A and B are Galois conjugates over $\mathbb{Q}$, then the number of $a \in K^\times$ such that $\mathrm{W}_{K,d}(a) = A$ is equal to the number of $a \in K^\times$ such that $\mathrm{W}_{K,d}(a) = B$.*

Proof. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ with $\sigma(A) = B$, and let $j \in \mathbb{F}_p^\times$ such that $\sigma(\zeta_p) = \zeta_p^j$. By Lemma 5.1, $\mathrm{W}_{K,d}(a) = A$ precisely when $\mathrm{W}_{K,d}(j^{1-1/d}a) = B$. □

Often the Weil sums lie in a proper subfield of $\mathbb{Q}(\zeta_p)$. We give a criterion for determining when this happens.

Lemma 5.3. *Let K be a finite field of characteristic p. Let E be the extension of $\mathbb{Q}$ generated by all the values of $\mathrm{W}_{K,d}(a)$ for $a \in K^\times$. Let m be the smallest divisor of $p-1$ such that $d \equiv 1 \pmod{(p-1)/m}$. Then E is the unique subfield of $\mathbb{Q}(\zeta_p)$ with $[E : \mathbb{Q}] = m$.*

Proof. An arbitrary $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ takes ζ_p to ζ_p^j for some $j \in \mathbb{F}_p^\times$. So by Lemma 5.1, we have

$$\sigma^n(\mathrm{W}_{K,d}(a)) = \mathrm{W}_{K,d}(j^{n(1-1/d)}a) \tag{5}$$

for any $a \in K^\times$ and $n \in \mathbb{Z}$.

Since $d \equiv 1 \pmod{(p-1)/m}$, we see that $j^{m(1-1/d)} = 1$ for any $j \in \mathbb{F}_p^\times$. Thus if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, then σ^m fixes all the values of $\mathrm{W}_{K,d}$. So the subgroup of index m in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ fixes all values in E, and so $[E : \mathbb{Q}]$ is a divisor of m.

Conversely, if we set $n = [E : \mathbb{Q}]$ and Fourier transform both sides of (5) with a multiplicative character $\chi \in \widehat{K^\times}$, we obtain

$$\sum_{a \in K^\times} \mathrm{W}_{K,d}(a)\chi(a) = \sum_{a \in K^\times} \mathrm{W}_{K,d}(j^{n(1-1/d)}a)\chi(a).$$

The right hand side is $\bar{\chi}(j^{n(1-1/d)})$ times the left hand side. The left hand side is nonzero, since it is either q if χ is principal, or a product of Gauss sums involving nontrivial characters (use (4) with χ^t in place of χ, where t is the inverse of $-d$ modulo $q-1$). Thus we must have $\chi(j^{n(1-1/d)}) = 1$ for all $j \in \mathbb{F}_p^\times$ and all $\chi \in \widehat{K^\times}$, which forces $d \equiv 1 \pmod{(p-1)/n}$. By the minimality of m, this means that $[E : \mathbb{Q}] = n \geq m$. □

Remark 5.4. Values of $\mathrm{W}_{K,d}$ are always algebraic integers, so that if these lie in a field E, they actually lie in the ring of algebraic integers in E.

Remark 5.5. In view of the previous remark, the special case of Lemma 5.3 when $m = 1$ states that the values of $\mathrm{W}_{K,d}(a)$ for $a \in K^\times$ all lie in $\mathbb{Z}$ if and only if $d \equiv 1 \pmod{p-1}$. This was proved in [20, Theorem 4.2].

The next result is reminiscent of the power moments of Section 2. We shall combine it with Lemma 5.1 in Corollary 5.7 below.

Lemma 5.6. *Let K be a finite field. For any $b \in K$ with $b \neq 1$, we have*

$$\sum_{a \in K^\times} \mathrm{W}_{K,d}(a)\mathrm{W}_{K,d}(ba) = 0.$$

Proof. Since $\mathrm{W}_{K,d}(0) = 0$, we may include the $a = 0$ term in

$$\begin{aligned}\sum_{a \in K^\times} \mathrm{W}_{K,d}(a)\mathrm{W}_{K,d}(ba) &= \sum_{x,y \in K} \psi_K(x^d + y^d) \sum_{a \in K} \psi_K(a(x + by)) \\ &= |K| \sum_{\substack{x,y \in K \\ x+by=0}} \psi_K(x^d + y^d) \\ &= |K| \sum_{y \in K} \psi_K(y^d(1 + (-b)^d)),\end{aligned}$$

which vanishes because $y \mapsto y^d$ is a permutation of K, and $1 + (-b)^d \neq 0$ since $b \neq 1$. □

Now we combine Lemmata 5.1 and 5.6.

Corollary 5.7. *If K is a finite field and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ permutes the values of $\mathrm{W}_{K,d}$ nontrivially, then*

$$\sum_{a \in K^\times} \mathrm{W}_{K,d}(a)\sigma(\mathrm{W}_{K,d}(a)) = 0.$$

Proof. Lemma 5.1 furnishes an element b such that $\sigma(\mathrm{W}_{K,d}(a)) = \mathrm{W}_{K,d}(ba)$ for all $a \in K^\times$, and clearly $b \neq 1$, for otherwise σ would fix each value taken by $\mathrm{W}_{K,d}$. Lemma 5.6 finishes the proof. □

6. Proof of Theorem 1.4

We have three fields $I \subseteq J \subseteq K$ with $[J : I] = 2$. Let p be the characteristic of our fields. As always, $\gcd(d, |K^\times|) = 1$. We are given that d is degenerate in I, but not in J.

We want to show that the value set of $\mathrm{W}_{K,d}$ is not of the form $\{0, \pm A\}$. Suppose the contrary. By Proposition 2.4, $|A|$ must be an integral power of p with $\sqrt{|K|} < |A| < |K|$, so then

$$\begin{aligned}\mathrm{V}_{K,d} &= \mathrm{val}_p(A) \\ &> \mathrm{val}_p(\sqrt{|K|}) \\ &= \frac{1}{2}[K : \mathbb{F}_p].\end{aligned}$$

On the other hand, by Corollary 4.2 and Corollary 4.4, we get a contradiction because

$$\begin{aligned} \mathrm{V}_{K,d} &\leq [K : J] \times \mathrm{V}_{J,d} \\ &= [K : J] \times [I : \mathbb{F}_p] \\ &= \frac{1}{2}[K : \mathbb{F}_p]. \end{aligned}$$

7. Proof of Theorem 1.7

We have K a finite field of characteristic p and order q with $[K : \mathbb{F}_p]$ divisible by 2^s. As always, $\gcd(d, q-1) = 1$. We suppose that $\mathrm{W}_{K,d}$ is symmetric three-valued with values 0 and $\pm A$, and our goal is to show that $|A| \geq p^{2^{s-1}}\sqrt{q}$.

Note that $\mathbb{F}_{p^{2^s}} \subseteq K$. Since $\mathrm{W}_{K,d}$ is three-valued, d is degenerate over $\mathbb{F}_p$ by Theorem 1.2. If d were nondegenerate over $\mathbb{F}_{p^{2^s}}$, then there must be subfields I and J of $\mathbb{F}_{p^{2^s}}$ with $[J : I] = 2$ and d degenerate over I but not over J. Then Theorem 1.4 tells us that $\mathrm{W}_{K,d}$ is not symmetric three-valued, contrary to our hypothesis.

So d is degenerate over $\mathbb{F}_{p^{2^s}}$, and thus every point of $\mathbb{F}_{p^{2^s}}$ is an element of the set R of roots of $(x+1)^d - x^d - 1$. Thus $|R| \geq p^{2^s}$, so Proposition 2.4 tells us that $|A| = \sqrt{|R|\,q} \geq p^{2^{s-1}}\sqrt{q}$.

8. Proof of Theorem 1.9

We have L a finite field with $[L : \mathbb{F}_p]$ even, and d is a power of p modulo $\sqrt{|L|} - 1$. We want to show that $\mathrm{W}_{L,d}$ is not three-valued.

Since we are considering $\mathrm{W}_{L,d}$, the exponent d is an invertible element modulo $|L|$. If d is degenerate over L, then $\mathrm{W}_{L,d}$ is at most two-valued by (2), so we assume that d is nondegenerate over L henceforth. The proof that $\mathrm{W}_{L,d}$ is not three-valued when L is of characteristic 2 is given as [8, Theorem 2], so we assume that we are in odd characteristic henceforth.

Assume $\mathrm{W}_{L,d}$ is three-valued to show a contradiction. By Theorem 1.2 and Corollary 2.3, these three values are all in $\mathbb{Z}$, one of them is 0, one is positive, and one is negative. Let K be the subfield of L with $[L : K] = 2$. Then by Corollary 4.5, we know that $\mathrm{W}_{L,d}(a) \geq 0$ for all $a \in K$. Corollary 3.4 shows that $\mathrm{W}_{L,d}(-1)$ is odd, and that $\mathrm{W}_{L,d}(a)$ is even for all other $a \in K$. Since these are nonnegative, the positive value of $\mathrm{W}_{L,d}$ must be $\mathrm{W}_{L,d}(-1)$, and $\mathrm{W}_{L,d}(a) = 0$ for all other $a \in K$. But Lemma 2.5 tells us that $\sum_{a \in K^\times} \mathrm{W}_{L,d}(a) = |L|$, which forces $\mathrm{W}_{L,d}(-1) = |L|$. This contradicts Corollary 2.2, since $\mathrm{W}_{L,d}$ was assumed to be nondegenerate over L.

9. New Proof of the Rationality of Three-Valued Weil Sums

We suppose that $\mathrm{W}_{K,d}$ is three-valued, and we want to show that those three values lie in $\mathbb{Z}$. As for the rest of Theorem 1.2, the conclusion that $d \equiv 1 \pmod{p-1}$ will then follow immediately from Remark 5.5, and the

proof that one of the three values is 0 is given in [27, Theorem 5.2], which is not very difficult to follow. The proof of rationality given here, while complex, is considerably easier than the original, given as [27, Theorem 4.1].

Let p and q be respectively the characteristic and order of K, and so $\gcd(d, q-1) = 1$. Let ζ_p be a primitive pth root of unity over $\mathbb{Q}$. Let $\mathrm{W}_{K,d}(a)$ take the three distinct values A, B, and C, respectively, for N_A, N_B, and N_C values of $a \in K^\times$. By Lemma 5.1, the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ permutes A, B, and C. The field $\mathbb{Q}(A, B, C)$ is a cyclic Galois extension of $\mathbb{Q}$ since it is contained in the cyclic extension $\mathbb{Q}(\zeta_p)$ of $\mathbb{Q}$. Let σ be a generator of $\mathrm{Gal}(\mathbb{Q}(A, B, C)/\mathbb{Q})$. There are three possible actions of σ upon $\{A, B, C\}$: (i) σ is the identity permutation, (ii) σ acts transitively, or (iii) σ permutes a pair of these elements, and fixes the third. As A, B, and C are algebraic integers, they lie in $\mathbb{Z}$ if and only if they lie in $\mathbb{Q}$, and this occurs precisely in Case (i). So it suffices to show that Cases (ii) and (iii) are impossible.

In Case (ii), Corollary 5.2 tells us that $N_A = N_B = N_C$, so they all equal $(q-1)/3$. Then Lemma 2.1(i) shows that $N_A A + N_B B + N_C C = q$, so that $A + B + C = 3 + \frac{3}{q-1}$. As $A + B + C$ is fixed by σ, it lies in $\mathbb{Q}$, and is at the same time an algebraic integer, so it lies in $\mathbb{Z}$. This means that $q - 1 \mid 3$, which forces $p = 2$, in which case $\zeta_p = -1$, and so the values of $\mathrm{W}_{K,d}$ lie in $\mathbb{Z}$, contradicting our supposition that σ permutes them nontrivially. So Case (ii) is impossible.

Henceforth, we suppose that we are in Case (iii). Without loss of generality, we suppose that the generator σ of $\mathrm{Gal}(\mathbb{Q}(A, B, C)/\mathbb{Q})$ has $\sigma(A) = B$, $\sigma(B) = A$, and $\sigma(C) = C$. Then σ is of order 2, and so $\mathbb{Q}(A, B, C)$ is a quadratic extension of $\mathbb{Q}$ lying in $\mathbb{Q}(\zeta_p)$. There is no such thing if $p = 2$ (since $\zeta_p = -1$, so $\mathbb{Q}(\zeta_p) = \mathbb{Q}$). Otherwise, since $\mathbb{Q}(\zeta_p)$ is cyclic of degree $p - 1$ over $\mathbb{Q}$, this means that $\mathbb{Q}(A, B, C)$ is the unique quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$. In view of the values of the quadratic Gauss sums [17], we know that this unique quadratic extension must be $\mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \pmod 4$, or $\mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod 4$. But since A, B, and C are real (see [20, Theorem 3.1(a)] or [27, Theorem 2.1(c)]), the latter case is impossible, so we must have $p \equiv 1 \pmod 4$ and $\mathbb{Q}(A, B, C) = \mathbb{Q}(\sqrt{p})$. Then $C \in \mathbb{Z}$, since it is an algebraic integer fixed by σ, and $A = a + b\sqrt{p}$ and $B = a - b\sqrt{p}$, for some a, b with $2a$, $2b$, and $a + b \in \mathbb{Z}$, since this is the form of algebraic integers in $\mathbb{Q}(\sqrt{p})$, as shown in [34, Chapter IV, Theorem 2.3].

Then Lemma 2.1(i),(ii) tells us that

$$N_A A + N_B B + N_C C = q, \tag{6}$$

$$N_A A^2 + N_B B^2 + N_C C^2 = q^2. \tag{7}$$

Also $\sum_{a \in K^\times} \mathrm{W}_{K,d}(a)\sigma(\mathrm{W}_{K,d}(a)) = 0$ by Corollary 5.7, so

$$N_A AB + N_B BA + N_C C^2 = 0. \tag{8}$$

By Corollary 5.2, we have $N_A = N_B$, and since $A = a+b\sqrt{p}$ and $B = a-b\sqrt{p}$, our three equations (6), (7), and (8) become

$$\begin{aligned} 2N_A a + N_C C &= q, \\ 2N_A(a^2 + pb^2) + N_C C^2 &= q^2, \\ 2N_A(a^2 - pb^2) + N_C C^2 &= 0, \end{aligned}$$

and this system is equivalent to the system

$$2N_A a + N_C C = q, \tag{9}$$

$$4N_A a^2 + 2N_C C^2 = q^2, \tag{10}$$

$$4N_A p b^2 = q^2. \tag{11}$$

From (11) we see that $p \mid N_A$. Note that $C \neq 0$, since otherwise (9) and (10) imply that $N_A = 1$, contradicting $p \mid N_A$. If we subtract (10) from $2(a+C)$ times equation (9), we obtain

$$2(2N_A + N_C)aC = q(2a + 2C - q),$$

and since $N_A + N_B + N_C = q - 1$, with $N_A = N_B$, this gives

$$2(q-1)aC = q(2a + 2C - q).$$

Examine the p-adic valuation of each side of this equation to see that $\max\{\mathrm{val}_p(a), \mathrm{val}_p(C)\} \geq \mathrm{val}_p(q)$. Then by Corollary 2.2, we see that $|C| < q$, and since $C \neq 0$, we must have $\mathrm{val}_p(C) < \mathrm{val}_p(q) \leq \mathrm{val}_p(a)$, so that $q \mid 2a$. If we reduce (9) modulo q, we see that $q \mid N_C C$, but since $q \nmid C$, we have $p \mid N_C$. Thus $p \mid N_A$ and $p \mid N_C$, and so $p \mid (2N_A + N_C) = q - 1$, which is absurd. Thus Case (iii) is impossible, and the proof is complete.

Acknowledgements

The second author was supported in part by a Research, Scholarship, and Creative Activity Award from California State University, Northridge. The second author thanks Tor Helleseth for help with the history of these researches.

References

[1] N. M. Akuliničev. Bounds for rational trigonometric sums of a special type. *Dokl. Akad. Nauk SSSR*, 161:743–745, 1965. Trans. in *Soviet Math. Dokl.* 6:480–482, 1965.

[2] A. R. Calderbank and G. McGuire. Proof of a conjecture of Sarwate and Pursley regarding pairs of binary m-sequences. *IEEE Trans. Inform. Theory*, 41(4):1153–1155, 1995.

[3] A. R. Calderbank, G. McGuire, B. Poonen, and M. Rubinstein. On a conjecture of Helleseth regarding pairs of binary m-sequences. *IEEE Trans. Inform. Theory*, 42(3):988–990, 1996.

[4] A. Canteaut, P. Charpin, and H. Dobbertin. Couples de suites binaires de longueur maximale ayant une corrélation croisée à trois valeurs: conjecture de Welch. *C. R. Acad. Sci. Paris Sér. I Math.*, 328(2):173–178, 1999.

[5] A. Canteaut, P. Charpin, and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture. *IEEE Trans. Inform. Theory*, 46(1):4–8, 2000.
[6] L. Carlitz. A note on exponential sums. *Math. Scand.*, 42(1):39–48, 1978.
[7] L. Carlitz. Explicit evaluation of certain exponential sums. *Math. Scand.*, 44(1):5–16, 1979.
[8] P. Charpin. Cyclic codes with few weights and Niho exponents. *J. Combin. Theory Ser. A*, 108(2):247–259, 2004.
[9] T. Cochrane and C. Pinner. Stepanov's method applied to binomial exponential sums. *Q. J. Math.*, 54(3):243–255, 2003.
[10] T. Cochrane and C. Pinner. Explicit bounds on monomial and binomial exponential sums. *Q. J. Math.*, 62(3):323–349, 2011.
[11] R. S. Coulter. Further evaluations of Weil sums. *Acta Arith.*, 86(3):217–226, 1998.
[12] T. W. Cusick and H. Dobbertin. Some new three-valued crosscorrelation functions for binary m-sequences. *IEEE Trans. Inform. Theory*, 42(4):1238–1240, 1996.
[13] H. Davenport and H. Hasse. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *J. Reine Angew. Math.*, 172:151–182, 1935.
[14] H. Davenport and H. Heilbronn. On an exponential sum. *Proc. London Math. Soc. (2)*, 41:449–453, 1936.
[15] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen. Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type. *IEEE Trans. Inform. Theory*, 47(4):1473–1481, 2001.
[16] T. Feng. On cyclic codes of length 2^{2^r} with two zeros whose dual codes have three weights. *Des. Codes Cryptogr.*, 62(3):253–258, 2012.
[17] C. F. Gauss. Summatio quarumdam serierum singularium. *Comment. Soc. Reg. Sci. Gottingensis*, page 1, 1811.
[18] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Trans. Inform. Theory*, 14(1):154–156, 1968.
[19] T. Helleseth. Krysskorrelasjonsfunksjonen mellom maksimale sekvenser over GF(q). Master's thesis, Matematisk Institutt, Universitetet i Bergen, 1971.
[20] T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Math.*, 16(3):209–232, 1976.
[21] H. D. L. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences. *Finite Fields Appl.*, 7(2):253–286, 2001.
[22] X.-D. Hou. A note on the proof of Niho's conjecture. *SIAM J. Discrete Math.*, 18(2):313–319, 2004.
[23] A. A. Karatsuba. On estimates of complete trigonometric sums. *Mat. Zametki*, 1:199–208, 1967. Trans. in *Math. Notes* 1(2):133–139, 1967.
[24] T. Kasami. Weight distribution formula for some class of cyclic codes. Technical report, Univ. Illinois, Urbana, 1966.
[25] T. Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Information and Control*, 18:369–394, 1971.
[26] T. Kasami, S. Lin, and W. W. Peterson. Some results on cyclic codes which are invariant under the affine group and their applications. *Information and Control*, 11:475–496, 1967.
[27] D. J. Katz. Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth. *J. Combin. Theory Ser. A*, 119(8):1644–1659, 2012.
[28] D. J. Katz. Divisibility of Weil sums of binomials. *arXiv*, 1407.7923 [math.NT], 2014.
[29] D. J. Katz and P. Langevin. New open problems related to old conjectures by Helleseth. *arXiv*, 1412.8530 [math.NT], 2014.
[30] D. J. Katz and P. Langevin. Proof of a conjectured three-valued family of Weil sums of binomials. *arXiv*, 1409.2459 [math.NT], 2014.

[31] N. Katz and R. Livné. Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309(11):723–726, 1989.
[32] H. D. Kloosterman. On the representation of numbers in the form $ax^2+by^2+cz^2+dt^2$. *Acta Math.*, 49(3-4):407–464, 1927.
[33] G. Lachaud and J. Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(20):881–883, 1987.
[34] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.
[35] P. Langevin. *Les sommes de caractères et la formule de Poisson dans la théorie des codes, des séquences et des fonctions boolénnes*. PhD thesis, Université de Toulon, 1999.
[36] P. Langevin and P. Véron. On the non-linearity of power functions. *Des. Codes Cryptogr.*, 37(1):31–43, 2005.
[37] L. J. Mordell. On a sum analogous to a Gauss sum. *Quart. J. Math.*, 3:161–167, 1932.
[38] Y. Niho. *Multi-valued cross-correlation function between two maximal linear recursive sequences*. PhD thesis, University of Southern California, Los Angeles, 1972.
[39] D. V. Sarwate and M. B. Pursley. Crosscorrelation properties of pseudorandom and related sequences. *IEEE Trans. Inform. Theory*, 68(5):593–619, 1980. Correction in IEEE Trans. Inform. Theory 68(12):1554, 1980.
[40] H. M. Trachtenberg. *On the cross-correlation functions of maximal linear sequences*. PhD thesis, University of Southern California, Los Angeles, 1970.
[41] I. Vinogradow. Some trigonometrical polynomes and their applications. *C. R. Acad. Sci. URSS (N.S.)*, (6):254–255, 1933.
[42] L. R. Welch. Trace mappings in finite fields and shift register cross-correlation properties. Technical report, Dept. Electrical Engineering, University of Southern California, Los Angeles, 1969.

Institut de Mathématiques de Toulon, Université de Toulon, France and Institut de Mathématiques de Marseille, CNRS-UMR 7373, Aix-Marseille Université, France

Department of Mathematics, California State University, Northridge, United States

Institut de Mathématiques de Toulon, Université de Toulon, France