RATIONALITY OF FOUR-VALUED FAMILIES OF WEIL SUMS OF BINOMIALS

DANIEL J. KATZ AND ALLISON E. WONG

Abstract. We investigate the rationality of Weil sums of binomials of the form $W_u^{K,s} = \sum_{x \in K} \psi(x^s - ux)$, where K is a finite field whose canonical additive character is ψ, and where u is an element of $K^\times$ and s is a positive integer relatively prime to $|K^\times|$, so that $x \mapsto x^s$ is a permutation of K. The Weil spectrum for K and s, which is the family of values $W_u^{K,s}$ as u runs through $K^\times$, is of interest in arithmetic geometry and in several information-theoretic applications. The Weil spectrum always contains at least three distinct values if s is nondegenerate (i.e., if s is not a power of p modulo $|K^\times|$, where p is the characteristic of K). It is already known that if the Weil spectrum contains precisely three distinct values, then they must all be rational integers. We show that if the Weil spectrum contains precisely four distinct values, then they must all be rational integers, with the sole exception of the case where $|K| = 5$ and $s \equiv 3 \pmod 4$.

1. Introduction

In this paper, we assume that K is a finite field of characteristic p and order $q = p^n$. Let $\zeta = \exp(2\pi i/p)$. The canonical additive character of K is $\psi\colon K \to \mathbb{Q}(\zeta)$ given by $\psi(x) = \zeta^{\mathrm{Tr}(x)}$, where $\mathrm{Tr}\colon K \to \mathbb{F}_p$ with $\mathrm{Tr}(x) = x + x^p + \cdots + x^{q/p}$. We use s to denote an *invertible exponent over* K, that is, a positive integer with $\gcd(s, q-1) = 1$. This ensures that s has a multiplicative inverse, $1/s$, modulo $q-1$ and makes $x \mapsto x^s$ a permutation of the field K with inverse map $x \mapsto x^{1/s}$. For each $u \in K$, we define

$$W_u^{K,s} = \sum_{x \in K} \psi(x^s - ux) = \sum_{x \in K} \zeta^{\mathrm{Tr}(x^s - ux)}, \tag{1}$$

which is a Weil sum of a binomial (if $u \neq 0$) or a Weil sum of a monomial (if $u = 0$). When the field K and the exponent s are clear from context, we omit the superscript and write W_u. Note that Weil sum values lie in $\mathbb{Z}[\zeta]$, the ring of algebraic integers in $\mathbb{Q}(\zeta)$. In fact, it is known that they lie in

---

Date: 06 April 2024.

Daniel J. Katz is with the Department of Mathematics, California State University, Northridge, USA. Allison E. Wong was with the Department of Mathematics, California State University, Northridge and is with the Department of Mathematics, University of California, Davis. This paper is based upon work of both authors supported in part by the National Science Foundation under Grant CCF-1815487, and upon work of Daniel J. Katz supported in part by the National Science Foundation under Grant CCF-2206454.

$\mathbb{Z}[\zeta] \cap \mathbb{R}$; see [Kat12, Theorem 2.1(c)], or see [Tra70, Theorem 2.3] for an earlier equivalent statement in terms of crosscorrelation of linear recursive sequences.

Theorem 1.1 (Trachtenberg, 1970)**.** *If K is a finite field and s is an invertible exponent over K, then $W_u^{K,s} \in \mathbb{R}$ for every $u \in K$.*

A *multiset* of elements from a set X is a function μ from X into the nonnegative integers, where for $x \in X$ the value $\mu(x)$ is the *frequency* (number of instances) of x in the multiset. Thus, μ represents a normal set if and only if it maps X into $\{0,1\}$ (in which case μ is identified with the subset $\mu^{-1}(\{1\})$ of X). The *Weil spectrum for the field K and the exponent s* is the multiset of values $W_u^{K,s}$ as u runs through $K^\times$. That is, the Weil spectrum is a multiset of elements from $\mathbb{Z}[\zeta]$, where a given value $A \in \mathbb{Z}[\zeta]$ has a frequency, written $N_A^{K,s}$ (or N_A when K and s are clear from context), with

$$N_A^{K,s} = |\{u \in K^\times : W_u^{K,s} = A\}|. \tag{2}$$

We define the *value set for the field K and the exponent s*, written $\mathcal{W}_{K,s}$, to be the set of distinct values in the Weil spectrum, that is,

$$\mathcal{W}_{K,s} = \{W_u^{K,s} : u \in K^\times\}. \tag{3}$$

Note that we do not record $W_0^{K,s}$ in $\mathcal{W}_{K,s}$, but this value is always 0 because $x \mapsto x^s$ is a permutation of K and $\sum_{x \in K} \psi(x) = 0$.

The evaluation and estimation of Weil sums has been studied extensively [Klo27, DH36, Aku65, Kar67, Car78, Car79, Cou98, CP03, CP11, SV20], including special cases such as Kloosterman sums, which are of the form $W_u^{K,|K|-2} - 1$. Weil sums are used to count points in algebraic sets over finite fields; see, for example, Sections 7.7 and 7.11 of [Kat19] and Section 5 of this paper. In the Kloosterman case, the Weil spectra for fields of characteristic 2 and 3 were studied in [LW87] and [KL89], and Sections 7.2–7.4 of [Kat19] describe applications of Weil spectra in information theory, which we summarize here. The Walsh spectrum of the permutation $x \mapsto x^s$ of K is obtained from the Weil spectrum by also including the value $W_0^{K,s} = 0$. The Walsh spectrum measures the nonlinearity of the permutation, which indicates its resistance to linear cryptanalysis. The crosscorrelation spectrum of two maximum length linear recursive sequences is obtained by subtracting 1 from each value in the Weil spectrum. This crosscorrelation spectrum determines the performance of communications networks and remote sensing systems employing these sequences for modulation. Weil spectra also determine the weight distribution of certain error correcting codes, thus indicating the performance of the codes.

For a finite field K, we say that two exponents s and s' are *equivalent* to mean that $s' \equiv p^k s^\ell \pmod{q-1}$ for some $k \in \mathbb{Z}$ and $\ell \in \{-1,1\}$; this defines an equivalence relation, and equivalent exponents produce the same Weil spectrum by [Tra70, Theorems 2.4, 2.5] (in the language of crosscorrelation), or see [Kat19, Lemmas 7.5.2, 7.5.6][1]. We say that s is *degenerate over* K to mean that it is equivalent to 1, that is, s is a power of p modulo $q-1$. If K has four or fewer elements, then all exponents are degenerate over K; larger finite fields always have at least one nondegenerate exponent (see [Kat19, Lemma 7.5.4]). If s is degenerate, then $\mathcal{W}_{K,s} = \{0, q\}$ if $q > 2$ and $\mathcal{W}_{K,s} = \{q\}$ if $q = 2$; see [Kat19, Corollary 7.5.5].

We say the Weil spectrum for K and s is *v-valued* (resp., *at least v-valued*, *at most v-valued*) to mean that $|\mathcal{W}_{K,s}| = v$ (resp., $|\mathcal{W}_{K,s}| \geq v$, $|\mathcal{W}_{K,s}| \leq v$). Thus, Weil spectra of degenerate exponents are at most 2-valued, and Helleseth showed that Weil spectra of nondegenerate exponents are always at least 3-valued in [Hel76, Theorem 4.1].

Theorem 1.2 (Helleseth, 1976)**.** *Let K be a finite field and s be an invertible exponent over K. Then the Weil spectrum for K and s is at least 3-valued if and only if s is nondegenerate over K.*

There is much interest in which pairs (K, s) produce Weil spectra with few values (e.g., 3-valued or 4-valued spectra). All known 3-valued spectra have been classified into ten infinite families (see [Kat19, Table 7.1]), and 4-valued spectra have been studied in [Nih72, Theorems 3-6, 3-7], [Hel76, Theorem 4.13], [Dob98, Proposition 1], [HR05, Theorem 6], [DFHR06, Theorem 23], [ZLFG14, Theorem II.5], and [XHW14, Theorem 1]. Although each Weil sum value is always an algebraic integer in some cyclotomic extension of $\mathbb{Q}$, one observes that Weil spectra with few distinct values often have all of their values in $\mathbb{Z}$. We say that the Weil spectrum for K and s is *rational* (or that $\mathcal{W}_{K,s}$ is *rational*) to mean $\mathcal{W}_{K,s} \subseteq \mathbb{Z}$. Helleseth proved a simple criterion for rationality in [Hel76, Theorem 4.2].

Theorem 1.3 (Helleseth, 1976)**.** *Let K be a finite field of characteristic p and s be an invertible exponent over K. Then the Weil spectrum for K and s is rational if and only if $s \equiv 1 \pmod{p-1}$.*

Later, in [Kat12, Theorem 1.7], it was proved that 3-valued Weil spectra are invariably rational.

Theorem 1.4 (Katz, 2012)**.** *Let K be a finite field and s be an invertible exponent over K. If the Weil spectrum for K and s is 3-valued, then it is rational.*

Thus, in view of Theorem 1.3, when K is a field of characteristic p and $s \not\equiv 1 \pmod{p-1}$, the Weil spectrum for K and s cannot be 3-valued. Katz and Langevin set an open problem [KL16, Problem 3.6], part of which is to find an analogue of Theorem 1.4 for 4-valued spectra. The main result of this paper is this analogue, which we now state.

[1]Lemma 7.5.6 of [Kat19] has a typographical error: $a^{1/d}$ should be fixed to read $a^{-1/d}$ there.

Theorem 1.5. *Let K be a finite field and s be an invertible exponent over K. If the Weil spectrum for K and s is 4-valued, then it is rational unless $K = \mathbb{F}_5$ and $s \equiv 3 \pmod 4$ (in which case $\mathcal{W}_{K,s} = \{(5 \pm \sqrt{5})/2, \pm\sqrt{5}\}$).*

By Theorem 1.3, this means that, other than in the exceptional case when $|K| = 5$ and $s \equiv 3 \pmod 4$, the condition $s \equiv 1 \pmod{p-1}$ is necessary for the Weil spectrum to be 4-valued. Since the Walsh spectrum of the power permutation $x \mapsto x^s$ over K is obtained from the Weil spectrum for K and s by including $W_0^{K,s} = 0$, Theorems 1.4 and 1.5 show that all the values in a four-valued Walsh spectrum must lie in $\mathbb{Z}$.

The remainder of this paper is devoted to proving Theorem 1.5. We start in Section 2 by using Galois theory and algebraic number theory to study the structure of Weil spectra. Then, in Section 3, we present some archimedean and p-adic bounds on Weil sum values. Section 4 introduces some algebraic sets over finite fields, which we then relate to Weil sums in Section 5 via a group algebra. Finally, we prove Theorem 1.5 in Section 6.

2. Algebraic number theory

In this section we introduce the number systems that are used in our proof of Theorem 1.5. Algebraic number theory provides several results that constrain the structure of Weil spectra and thus help us achieve our proof.

Recall that K is a finite field of characteristic p and order $q = p^n$, that s is a positive integer such that $\gcd(s, q-1) = 1$, and that $\zeta = \exp(2\pi i/p)$. We use $\mathbb{N}$ to denote the set of nonnegative integers and $\mathbb{Z}_+$ to denote the set of strictly positive integers. We know that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is a cyclic group of order $p-1$; an element of this Galois group fixes all elements of $\mathbb{Q}$ and maps ζ to ζ^j for some $j \in \mathbb{F}_p^\times$. Let γ denote a primitive element of the prime subfield $\mathbb{F}_p$ and let σ denote the automorphism in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ that maps ζ to ζ^γ: note that σ is a generator of the Galois group. Then [Kat12, Theorem 2.1(b)] shows that $\sigma(W_u) = W_{\gamma^{1-1/s}u}$ for every $u \in K$, where $1/s$ is interpreted as the multiplicative inverse of s modulo $p-1$. Thus, σ maps the value set $\mathcal{W}_{K,s}$ (see (3)) to itself. From now on, we let $\tau\colon \mathcal{W}_{K,s} \to \mathcal{W}_{K,s}$ be the permutation obtained by restricting σ, so that for every $u \in K$, we have

$$\tau(W_u) = W_{\gamma^{1-1/s}u}, \tag{4}$$

where $1/s$ is interpreted as the multiplicative inverse of s modulo $p-1$.

The following result indicates important relationships between the exponent s, the characteristic p of the field K, the order of τ, the order of the element $\gamma^{1-1/s}$ in (4), and the degree of the extension of $\mathbb{Q}$ generated by the values in the Weil spectrum.

Proposition 2.1. *The following are all equal:*

(i) the order of the permutation τ of $\mathcal{W}_{K,s}$,

(ii) the degree, $[\mathbb{Q}(\mathcal{W}_{K,s}) : \mathbb{Q}]$*, of the field extension of the rationals generated by* $\mathcal{W}_{K,s}$*,*

(iii) the order of $\gamma^{1-1/s}$ *in* $\mathbb{F}_p^\times$ *(where* $1/s$ *indicates the multiplicative inverse of* s *modulo* $p-1$*), and*

(iv) the quantity $(p-1)/\gcd(p-1, s-1)$*.*

Let m *denote the common value of these. If* $p = 2$*, then* $m = 1$*, but if* $p > 2$*, then* $p \equiv 1 \pmod{2m}$*.*

Proof. Since $\mathbb{Q}(\mathcal{W}_{K,s})$ is a subfield of $\mathbb{Q}(\zeta)$ and since $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is a cyclic group generated by σ, the Galois correspondence shows that $[\mathbb{Q}(\mathcal{W}_{K,s}) : \mathbb{Q}]$ equals the order of the restriction to $\mathbb{Q}(\mathcal{W}_{K,s})$ of σ, which is the same as the order of τ. Lemma 5.3 of [AKL15] shows that $[\mathbb{Q}(\mathcal{W}_{K,s}) : \mathbb{Q}]$ equals $(p-1)/\gcd(p-1, s-1)$, which is the order of $\gamma^{1-1/s} = (\gamma^{1/s})^{s-1}$ because γ has order $p-1$ and s is invertible modulo $p-1$ (since $\gcd(s, q-1) = 1$).

If $p = 2$, then $\mathbb{Q}(\zeta) = \mathbb{Q}(-1) = \mathbb{Q}$, so $\mathbb{Q}(\mathcal{W}_{K,s}) = \mathbb{Q}$ and $m = 1$. When $p > 2$, Theorem 1.1 shows that $\mathbb{Q}(\mathcal{W}_{K,s})$ is a subfield of $\mathbb{Q}(\zeta) \cap \mathbb{R} = \mathbb{Q}(\zeta + \zeta^{-1})$, an extension of $\mathbb{Q}$ of degree $(p-1)/2$, and so $m \mid (p-1)/2$. □

Remark 2.2. Proposition 2.1 shows that $\mathcal{W}_{K,s}$ is rational when $p = 2$ or 3.

Recall from (2) that the frequency of a value A in the Weil spectrum is $N_A = |\{u \in K^\times : W_u = A\}|$. The action of τ on the Weil spectrum gives us information about these frequencies.

Lemma 2.3. *Suppose that* τ *has order* m*, and let* $A_0, A_1, \ldots, A_{k-1}$ *be distinct elements of* $\mathcal{W}_{K,s}$ *that* τ *permutes in a* k*-cycle, that is,* $\tau(A_i) = A_{i+1}$ *for every* $i \in \mathbb{Z}/k\mathbb{Z}$*. Then* $k \mid m$ *and* $N_{A_0} = N_{A_1} = \cdots = N_{A_{k-1}}$*, which is a multiple of* m/k*.*

Proof. Let $U_i = \{u \in K^\times : W_u = A_i\}$ for each $i \in \mathbb{Z}/k\mathbb{Z}$ and let $\lambda = \gamma^{1-1/s}$, where we interpret $1/s$ as the multiplicative inverse of s modulo $p-1$. For $u \in U_0$ and $j \in \mathbb{Z}$ we have, by (4), that $W_{\lambda^j u} = \tau^j(W_u) = \tau^j(A_0) = A_{j \bmod k}$. In particular, we have $k \mid m$ since τ has order m. Moreover, $W_{\lambda^k u} = A_0 = W_u$, so U_0 is a union of cosets of the subgroup $\langle \lambda^k \rangle$ of the group $K^\times$. Since λ is of order m by Proposition 2.1 and $k \mid m$, this subgroup is of order m/k, and so $N_{A_0} = |U_0|$ is a multiple of m/k. Lastly, for any $j \in \mathbb{Z}$, the map $u \mapsto \lambda^j u$ provides a bijection from U_0 to $U_{j \bmod k}$ because we have seen that $W_{\lambda^j u} = A_{j \bmod k}$ for every $u \in U_0$, and we can similarly prove $W_{\lambda^{-j} v} = \tau^{-j}(W_v) = \tau^{-j}(A_{j \bmod k}) = A_0$ for every $v \in U_{j \bmod k}$. □

Let f be a permutation of a finite set X. The *cycle type of* f is the multiset of lengths of cycles that is obtained when f is written as a composition of disjoint cycles. Note that the sum of the values in the cycle type of a permutation f is equal to the size of the set being permuted. We say that f *is a single cycle* to mean that f can be written as a single cycle that contains all elements of X. The next two results explore constraints on the cycle type of τ.

Lemma 2.4. *When $p = 2$, the cycle type of τ is a collection of $|\mathcal{W}_{K,s}|$ instances of 1. When p is odd, the cycle type of τ contains no number larger than $(p-1)/2$.*

Proof. Let m be the order of τ. When $p = 2$, the field $\mathbb{Q}(\zeta) = \mathbb{Q}(-1) = \mathbb{Q}$, so σ and τ are identity maps. When p is odd, Proposition 2.1 implies that $m \leq (p-1)/2$, so the desired result follows since m is the least common multiple of all the numbers in the cycle type of τ. □

Proposition 2.5. *The permutation τ is a single cycle if and only if $K = \mathbb{F}_2$ (and then s is degenerate and τ is a 1-cycle).*

Proof. Suppose $p = 2$. Lemma 2.4 shows that τ is a single cycle if and only if $|\mathcal{W}_{K,s}| = 1$, which happens exactly when $K = \mathbb{F}_2$ (and then every exponent is degenerate and τ is a 1-cycle).

Now suppose p is odd. Let $\mathcal{W}_{K,s} = \{A_0, \ldots, A_{k-1}\}$ and suppose for a contradiction that τ is a single cycle. Then $N_{A_0} = \cdots = N_{A_{k-1}}$ by Lemma 2.3. The sum $\sum_{u \in K^\times} W_u$ of $q-1$ Weil sum values is equal to q by [Kat12, Proposition 3.1(b)], so that

$$\begin{aligned} kN_{A_0} &= q - 1 \text{ and} \\ N_{A_0}(A_0 + \cdots + A_{k-1}) &= q. \end{aligned}$$

Note that $A_0 + \cdots + A_{k-1} \in \mathbb{Z}$ since it is an algebraic integer fixed by σ (of which τ is a restriction). Thus, N_{A_0} is a common divisor of q and $q-1$, and hence $N_{A_0} = 1$ and $k = q-1$. But then, by Lemma 2.4, we must have $(p-1)/2 \geq k = q-1 \geq p-1$, which is impossible. □

3. Bounds on Weil sum values

In this section we discuss some archimedean and non-archimedean bounds on the Weil sum $W_u^{K,s}$ that are used in proving the main result (Theorem 1.5). Recall that we use $\mathbb{N}$ to refer to the set of nonnegative integers. We use the p-adic valuation, v_p. One begins with $v_p \colon \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$, where $v_p(0) = \infty$ and $v_p(a) = \max\{j \in \mathbb{N} : p^j \mid a\}$ when $a \neq 0$. Then one extends the domain of v_p to $\mathbb{Q}$ by letting $v_p(a/b) = v_p(a) - v_p(b)$ when $a, b \in \mathbb{Z}$ and $b \neq 0$. Furthermore, one can extend the domain of v_p to $\mathbb{Q}(\zeta)$, in which case $v_p(\zeta - 1) = 1/(p-1)$; see [Lan02, Theorem 4.1], [Lan90, p. 7], and [Hel76, p. 218]. For the purposes of this paper, the most important facts about v_p (which we shall use without proof) are that $v_p(ab) = v_p(a) + v_p(b)$ and that $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$, with $v_p(a+b) = \min\{v_p(a), v_p(b)\}$ if $v_p(a) \neq v_p(b)$.

From (1), we know that Weil sums are sums of pth roots of unity, so we first explore linear combinations of these roots.

Lemma 3.1. *For any $t \in \mathbb{Q}$ and any $v \in \mathbb{Q}(\zeta)$, there is one and only one way to write v as a $\mathbb{Q}$-linear combination of $1, \zeta, \ldots, \zeta^{p-1}$ such that the coefficients sum to t.*

Proof. Our claim will follow if we show that the map $\varphi\colon \mathbb{Q}^p \to \mathbb{Q}(\zeta)\times\mathbb{Q}$ with $\varphi(w_0, w_1, \ldots, w_{p-1}) = (w_0 + w_1\zeta + \cdots + w_{p-1}\zeta^{p-1}, w_0 + w_1 + \cdots + w_{p-1})$ is an isomorphism of $\mathbb{Q}$-vector spaces. Since φ is clearly a $\mathbb{Q}$-linear map between two $\mathbb{Q}$-vector spaces of dimension p, it suffices to show that $\ker(\varphi)$ is trivial. Let $\mathrm{pr}_1\colon \mathbb{Q}(\zeta) \times \mathbb{Q} \to \mathbb{Q}(\zeta)$ and $\mathrm{pr}_2\colon \mathbb{Q}(\zeta) \times \mathbb{Q} \to \mathbb{Q}$ be the projection maps. Since $\{1, \zeta, \ldots, \zeta^{p-1}\}$ spans the $(p-1)$-dimensional $\mathbb{Q}$-space $\mathbb{Q}(\zeta)$ and has dependence relation $1+\zeta+\cdots+\zeta^{p-1} = 0$, we know that $\mathrm{pr}_1 \circ\varphi$ is surjective, which makes $\ker(\mathrm{pr}_1 \circ\varphi)$ equal to the 1-dimensional space $\mathrm{span}_{\mathbb{Q}}\{(1, 1, \ldots, 1)\}$. Then $\ker(\varphi)$ is a subspace of $\ker(\mathrm{pr}_1 \circ\varphi)$, but $(\mathrm{pr}_2 \circ\varphi)(1, 1, \ldots, 1) \neq 0$, so $\ker(\varphi)$ must be trivial. □

Now we shall apply the previous result to obtain an archimedean bound on nondegenerate Weil sums. Recall that we let K be a finite field with characteristic p and order $q = p^n$ and that s is a positive integer with $\gcd(s, q-1) = 1$.

Lemma 3.2. *For any $u \in K$, there exist unique $w_0, \ldots, w_{p-1} \in \mathbb{N}$ with $w_0 > 0$ such that $\sum_{i=0}^{p-1} w_i = q$ and $W_u = \sum_{i=0}^{p-1} w_i\zeta^i$. If s is nondegenerate, then $w_i < q$ for every $i \in \{0, 1, \ldots, p-1\}$ and $|W_u| < q$.*

Proof. By definition (1), a Weil sum W_u is a sum of q terms from the set $\{\zeta^0, \zeta^1, \ldots, \zeta^{p-1}\}$, so we can write $W_u = \sum_{i=0}^{p-1} w_i\zeta^i$ for some $w_0, \ldots, w_{p-1} \in \mathbb{N}$ such that $\sum_{i=0}^{p-1} w_i = q$. The uniqueness of this representation follows from Lemma 3.1. Note that $w_0 > 0$ because one term in W_u is $\psi(0^s - u \cdot 0) = \zeta^0$.

When s is nondegenerate, [Kat12, Theorem 2.1(f)] tells us $|W_u| < q$, which makes it impossible for $w_i = q$ for any i (else $|W_u| = |q\zeta^i| = q$). □

The next two results explore p-adic bounds on Weil sums.

Lemma 3.3. *For all $u \in K$, we have $v_p(W_u) > 0$.*

Proof. This is [Kat12, Theorem 2.1(e)]. For an equivalent version in terms of crosscorrelation, see [Hel76, Theorem 4.5]. □

Lemma 3.4. *Suppose that s is nondegenerate. If $u \in K$ and $v_p(W_u) \geq v_p(q) = n$, then $W_u = 0$. In particular, either $v_p(W_u) < v_p(q)$ or else $v_p(W_u) = \infty$.*

Proof. Let $u \in K$ and use Lemma 3.2 to write $W_u = \sum_{0\leq i<p} w_i\zeta^i$, where $w_0, \ldots, w_{p-1}$ are nonnegative integers that are strictly less than q with $\sum_{0\leq i<p} w_i = q$. Suppose that $v_p(W_u) \geq v_p(q) = n$. Then $q = p^n$ divides W_u in $\mathbb{Z}[\zeta]$, so that $W_u = qr$ for some $r \in \mathbb{Z}[\zeta]$, which we write as $\sum_{0\leq i<p} r_i\zeta^i$, where each $r_i = w_i/q$ is a nonnegative rational number strictly less than 1 with $\sum_{0\leq i<p} r_i = 1$. Then we write r as $\sum_{0\leq i<p-1}(r_i - r_{p-1})\zeta^i$, which is the unique $\mathbb{Q}$-linear combination of $1, \zeta, \ldots, \zeta^{p-2}$ equal to r, and since $r \in \mathbb{Z}[\zeta]$, the coefficients $r_i - r_{p-1}$ are all in $\mathbb{Z}$. Since $0 \leq r_i < 1$ for every i, this forces $r_0 = \cdots = r_{p-1}$, so that $r = 0$, and then $W_u = 0$. □

Recall from Section 2 that γ is a primitive element of the prime subfield $\mathbb{F}_p$ and σ is the generator of $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ that maps ζ to ζ^γ. If $p \equiv 1 \pmod 4$, then it is well known from algebraic number theory that $\mathbb{Q}(\zeta) \supseteq \mathbb{Q}(\sqrt{p})$ and that $\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{p})$ is an extension of degree $(p-1)/2$ with Galois group $\langle \sigma^2 \rangle$. The algebraic integers in $\mathbb{Q}(\sqrt{p})$ are precisely elements of the form $(a+b\sqrt{p})/2$ with $a, b \in \mathbb{Z}$ and $a \equiv b \pmod 2$. We are interested in how one obtains such elements from Weil sums. To explore this, we use Gauss's determination of the quadratic Gauss sum when $p \equiv 1 \pmod 4$ (see [LN97, Theorem 5.15]):

$$\sum_{i \in \mathbb{F}_p^\times} \eta(i)\zeta^i = \sqrt{p}, \tag{5}$$

where η is the quadratic character (Legendre symbol) of $\mathbb{F}_p^\times$.

Lemma 3.5. *Suppose that $p \equiv 1 \pmod 4$. An expression of the form $\sum_{i \in \mathbb{F}_p} w_i \zeta^i$ with rational coefficients w_i lies in $\mathbb{Q}(\sqrt{p})$ if and only if, for every $i, j \in \mathbb{F}_p$, we have $w_i = w_j$ when $\eta(i) = \eta(j)$. In this case, if we write w_+ for the common value of the w_i's with $\eta(i) = +1$ and w_- for the common value of the w_i's with $\eta(i) = -1$, then our sum becomes*

$$\left(w_0 - \frac{w_+ + w_-}{2}\right) + \left(\frac{w_+ - w_-}{2}\right)\sqrt{p}.$$

Proof. Since $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{p})) = \langle \sigma^2 \rangle$, we know that $A = \sum_{i \in \mathbb{F}_p} w_i \zeta^i \in \mathbb{Q}(\sqrt{p})$ if and only if it is fixed by σ^2, that is, if and only if

$$\sum_{i \in \mathbb{F}_p} w_i \zeta^i = \sum_{i \in \mathbb{F}_p} w_i \zeta^{i\gamma^2} = \sum_{i \in \mathbb{F}_p} w_{\gamma^{-2} i} \zeta^i,$$

and then Lemma 3.1 tells us that this happens if and only if $w_i = w_{\gamma^{-2} i}$ for every $i \in \mathbb{F}_p$, which is true if and only if $w_i = w_j$ whenever $j \in i\langle \gamma^2 \rangle$, i.e., whenever $\eta(i) = \eta(j)$. In this case, write w_+ and w_- as in the statement of this lemma, and then our sum becomes

$$\begin{aligned} A &= w_0 + w_+ \sum_{i \in \langle \gamma^2 \rangle} \zeta^i + w_- \sum_{i \in \mathbb{F}_p^\times \smallsetminus \langle \gamma^2 \rangle} \zeta^i \\ &= w_0 + \left(\frac{w_+ + w_-}{2}\right) \sum_{i \in \mathbb{F}_p^\times} \zeta^i + \left(\frac{w_+ - w_-}{2}\right) \sum_{i \in \mathbb{F}_p^\times} \eta(i)\zeta^i, \end{aligned}$$

where the penultimate summation is clearly -1 and the ultimate one is the quadratic Gauss sum (5). □

We now apply the previous result to Weil sums.

Lemma 3.6. *Let p be a prime with $p \equiv 1 \pmod 4$ and suppose that s is an invertible exponent over K. Any Weil sum $W_u^{K,s}$ in $\mathbb{Q}(\sqrt{p})$ can be written uniquely in the form $(I + J\sqrt{p})/2$, where $I, J \in \mathbb{Z}$. Furthermore, $I \equiv J \pmod 2$ and $v_p(I) \geq 1$. If s is nondegenerate, then $-q < -2(q-1)/(p-1) < I < 2q$ and $|J| \leq 2(q-1)/(p-1) < q$.*

Proof. From Lemmas 3.2 and 3.5, it follows that any Weil sum in $Q(\sqrt{p})$ can be written as

$$\left(\frac{2w_0 - (w_+ + w_-)}{2}\right) + \left(\frac{w_+ - w_-}{2}\right)\sqrt{p},$$

where $w_0, w_+, w_- \in \mathbb{Z}$. Thus, if we let $I = 2w_0 - (w_+ + w_-)$ and $J = w_+ - w_-$, then $I, J \in \mathbb{Z}$ and our Weil sum is $(I + J\sqrt{p})/2$; since $\{1, \sqrt{p}\}$ is $\mathbb{Q}$-linearly independent, the I and J are uniquely determined. Since $J \in \mathbb{Z}$, we know that $v_p(J\sqrt{p})$ has strictly positive p-adic valuation, as does the entire Weil sum (by Lemma 3.3), and so $v_p(I)$ must be a strictly positive integer. Note also that $I \equiv J \pmod 2$ since, as we stated in the paragraph before Lemma 3.5, algebraic integers in $\mathbb{Q}(\sqrt{p})$ are of the form $(a + b\sqrt{p})/2$ where $a, b \in \mathbb{Z}$ and $a \equiv b \pmod 2$.

From now on, let us suppose that s is nondegenerate. Then by Lemma 3.2, we know that w_0, w_+, w_- are all nonnegative integers that are strictly less than q with $w_0 \geq 1$ and $w_0 + (w_+ + w_-)(p-1)/2 = q$. Thus,

$$|J| \leq w_+ + w_- \leq 2\left(\frac{q-1}{p-1}\right),$$

and since $w_0 < q$, we know that $w_+ + w_- > 0$, so

$$-2\left(\frac{q-1}{p-1}\right) < 2 - 2\left(\frac{q-1}{p-1}\right) \leq I < 2w_0 + (w_+ + w_-)(p-1) = 2q,$$

where since $p - 1 > 2$, we have $2(q-1)/(p-1) < q - 1 < q$.

□

4. Algebraic sets over finite fields

In this section, we study a certain type of algebraic set over the finite field K. It turns out that these sets are closely related to sums of products of Weil sum values (as we shall see in Section 5), and thus will help us prove our main result (Theorem 1.5).

Recall that K is a finite field of characteristic p and order $q = p^n$ and that s is a positive integer such that $\gcd(s, q-1) = 1$. First, we introduce two notations that enable us to express our algebraic sets very compactly.

Notation 4.1. If $k \in \mathbb{Z}_+$ and $u = (u_1, \ldots, u_k), v = (v_1, \ldots, v_k) \in K^k$ then $u \cdot v$ denotes $u_1v_1 + \cdots + u_kv_k$ and $\|u\|_s$ denotes $(u_1^s + \cdots + u_k^s)^{1/s}$, so that $\|u\|_s^s = u_1^s + \cdots + u_k^s$.

Notation 4.2. For $k \in \mathbb{Z}_+$, $t = (t_1, \ldots, t_k) \in (K^\times)^k$, and $a, b \in K$, we use $Q_{a,b}^t$ to denote the number of solutions $v = (v_1, \ldots, v_k) \in K^k$ to the system of equations

$$t \cdot v = a$$
$$\|v\|_s = b.$$

The next four results relate various values of $Q_{a,b}^t$ with each other.

Lemma 4.3. *For any $k \in \mathbb{Z}_+$, any $t \in (K^\times)^k$, and any $b \in K$ we have $\sum_{a\in K} Q^t_{a,b} = \sum_{a\in K} Q^t_{b,a} = q^{k-1}$.*

Proof. The second summation counts the points in the hyperplane $t \cdot v = b$ in K^k, while the first sum counts points with $\|v\|_s^s = b^s$, which has the same cardinality because $x \mapsto x^s$ is a permutation of K. □

Lemma 4.4. *For $k \in \mathbb{Z}_+$, any $u \in K^\times$, any $t \in (K^\times)^k$, and any $a, b \in K$, we have $Q^{ut}_{a,b} = Q^t_{a/u,b}$ and $Q^t_{ua,ub} = Q^t_{a,b}$.*

Proof. The first equality follows from observing that $ut \cdot v = a$ if and only if $t \cdot v = a/u$. The second follows from the bijection $(v_1, \ldots, v_k) \mapsto (v_1/u, \ldots, v_k/u)$ from the set of points counted by $Q^t_{ua,ub}$ to that counted by $Q^t_{a,b}$. □

Lemma 4.5. *Let $k \in \mathbb{Z}_+$ and $t \in (K^\times)^k$. For any $a \in K^\times$, we have*

$$Q^t_{a,0} = Q^t_{0,a} = \frac{q^{k-1} - Q^t_{0,0}}{q-1}. \tag{6}$$

Moreover, if $b \in K$, we have

$$\sum_{a\in K^\times} Q^t_{a,b} = \sum_{a\in K^\times} Q^t_{b,a} = \begin{cases} q^{k-1} - Q^t_{0,0} & \text{if } b = 0 \\ \frac{q^k - 2q^{k-1} + Q^t_{0,0}}{q-1} & \text{if } b \neq 0. \end{cases} \tag{7}$$

Proof. Lemma 4.4 shows that $Q^t_{a,0}$ (resp., $Q^t_{0,a}$) has the same value for every $a \in K^\times$, so (6) and the $b = 0$ case of (7) follow from Lemma 4.3. The $b \neq 0$ case of (7) then similarly follows from Lemma 4.3, using (6). □

Lemma 4.6. *For any $k \in \mathbb{Z}_+$, any $b, t_1, \ldots, t_k \in K^\times$, and any $a \in K$, we have*

$$Q^{(t_1,\ldots,t_k)}_{a,b} = \frac{Q^{(a/b,t_1,\ldots,t_k)}_{0,0} - Q^{(t_1,\ldots,t_k)}_{0,0}}{q-1}.$$

Proof. For the rest of this proof, let $t = (t_1, \ldots, t_k)$ and $t' = (a/b, t_1, \ldots, t_k)$, and let u and v' be shorthand for $(u_1, \ldots, u_k)$ and $(v_0, v_1, \ldots, v_k)$, respectively. Then

$$\begin{aligned} Q^{t'}_{0,0} - Q^t_{0,0} &= |\{v' \in K^{k+1} : v_0 \neq 0, t' \cdot v' = 0, \|v'\|_s = 0\}| \\ &= |\{(v_0, u) \in K^\times \times K^k : t \cdot u = a, \|u\|_s = b\}| \\ &= (q-1)Q^t_{a,b}, \end{aligned}$$

where the second equality uses the reparameterization with $u_j = -bv_j/v_0$ for $j \in \{1, \ldots, k\}$ and the fact that the invertibility of s makes $(-1)^s = -1$. □

Now we compute certain values of $Q^t_{a,b}$ that will be useful later.

Lemma 4.7. *Let $t_1, t_2 \in K^\times$ and let δ denote the Kronecker delta.*

(i) *We have $Q^{(t_1)}_{a,b} = \delta_{a,t_1 b}$.*

(ii) If at least one of a or b is zero, then

$$Q_{a,b}^{(t_1,t_2)} = \begin{cases} 1+(q-1)\delta_{t_1,t_2} & \text{if } a=b=0, \\ 1-\delta_{t_1,t_2} & \text{otherwise.} \end{cases}$$

Proof. The first claim is clear because $Q_{a,b}^{(t_1)}$ counts the number of $v_1 \in K$ such that $t_1 v_1 = a$ and $(v_1^s)^{1/s} = b$. Applying this result to the fact that $Q_{0,0}^{(t_1,t_2)} = (q-1)Q_{t_1,1}^{(t_2)} + Q_{0,0}^{(t_2)}$ by Lemma 4.6 gives the expression in the first case of the second claim, and then the second case follows from using Lemma 4.5 to deduce the value of $Q_{a,0}^{(t_1,t_2)}$ and $Q_{0,a}^{(t_1,t_2)}$. □

We explore certain special values of $Q_{a,b}^t$ that are critical for our proof of Theorem 1.5.

Lemma 4.8. *Let $w \in K$.*

(i) We have $Q_{1,w}^{(1,-1)} = Q_{1,-w}^{(1,-1)}$.

(ii) If p is odd, then $Q_{1,1}^{(1,-1)} - 1 = Q_{1,-1}^{(1,-1)} - 1 = Q_{1,-1}^{(1,1)}$.

(iii) When p is odd and $w = 2^{1/s-1}$, then $Q_{1,w}^{(1,1)}$ is odd; otherwise $Q_{1,w}^{(1,1)}$ is even.

Proof. Recall that $(-1)^s = -1$ since s is invertible.

The first result follows from the observation that $(x_1, x_2) \in K^2$ satisfies the system of equations corresponding to $Q_{1,w}^{(1,-1)}$ if and only if $(-x_2, -x_1)$ satisfies the system of equations corresponding to $Q_{1,-w}^{(1,-1)}$.

Now $Q_{1,-1}^{(1,1)}$ counts how many $(x_1, x_2) \in K^2$ satisfy $x_1 + x_2 = 1$ and $x_1^s + x_2^s = (-1)^s$, and since these equations preclude $x_2 = 0$ in odd characteristic, we can reparameterize with $x_2 = -1/y$ for $y \in K^\times$ and eliminate x_1 to see that $Q_{1,-1}^{(1,1)}$ is the same as the number of $y \in K^\times$ such that $(y+1)^s + y^s = 1$, which is $Q_{1,1}^{(1,-1)} - 1$ because $(0+1)^s + 0^s = 1$.

For the third result, note that the system of equations that corresponds to $Q_{1,w}^{(1,1)}$ is symmetric in both unknowns, so (x_1, x_2) satisfies this system if and only if (x_2, x_1) does. This implies that $Q_{1,w}^{(1,1)}$ is even except when there is some $x \in K$ such that $2x = 1$ and $2^{1/s}x = w$, which happens exactly when p is odd, $x = 1/2$, and $w = 2^{1/s-1}$. □

5. Group algebra

In this section, we use a group algebra that gives us a convenient way to encapsulate all the Weil spectrum values in a single object; this builds upon the methods of Feng [Fen12] and developments in [Kat15]. After introducing the relevant group algebra here, we define the key group algebra elements of interest in Section 5.1 and demonstrate their relation to the cardinalities of algebraic sets studied in Section 4. Then we present other related group algebra elements designed to have a particular symmetry in Section 5.2, and focus on a particularly important case of this symmetry in Section 5.3.

Let $L = \mathbb{Q}(\zeta, \xi)$, where $\xi = \exp(2\pi i/(q-1))$, and consider the group L-algebra $L[K^\times]$, whose elements are of the form $S = \sum_{u \in K^\times} S_u[u]$, where $S_u \in L$ for each $u \in K^\times$. We write the elements of $K^\times$ in brackets to distinguish them from similar-appearing elements in L. We identify any subset U of $K^\times$ with $\sum_{u \in U}[u]$ in $L[K^\times]$. For $S = \sum_{u \in K^\times} S_u[u] \in L[K^\times]$, we define its conjugate to be $\overline{S} = \sum_{u \in K^\times} \overline{S_u}[u^{-1}]$. We also let $|S| = \sum_{u \in K^\times} S_u$; this is the cardinality of S if S is a group algebra element representing a subset of $K^\times$. Moreover, if $t \in \mathbb{Z}$, we write $S^{(t)}$ to denote $\sum_{u \in K^\times} S_u[u^t]$.

Below, we record some easily proved observations.

Lemma 5.1. *For any $S, T \in L[K^\times]$ and any $t \in \mathbb{Z}$, we have*

(i) $|S^{(t)}| = |S|$;
(ii) $|\overline{S}| = \overline{|S|}$;
(iii) $|S+T| = |S| + |T|$;
(iv) $|ST| = |S||T|$;
(v) $SK^\times = |S|K^\times$;
(vi) if S is a subgroup of $K^\times$, then $\overline{S} = S^{(-1)} = S$ and $S^2 = |S|S$; and
(vii) $(S\overline{S})_1 = \sum_{u \in K^\times} |S_u|^2$.

Let $\widehat{K^\times}$ denote the group of multiplicative characters from $K^\times$ to $L^\times$. The identity element of $\widehat{K^\times}$ is called the *principal character* and is written χ_0; it maps every element of $K^\times$ to 1. We define the application of a multiplicative character $\chi \in \widehat{K^\times}$ to a group algebra element $S = \sum_{u \in K^\times} S_u[u] \in L[K^\times]$ by linear extension:

$$\chi(S) = \sum_{u \in K^\times} S_u \chi(u),$$

and we call $\chi(S)$ *the Fourier coefficient of S at χ.*

The following facts, which we record without proof, are easy to verify.

Lemma 5.2. *The following facts hold for any $S, T \in L[K^\times]$ and any $\chi \in \widehat{K^\times}$:*

(i) $\chi_0(S) = |S|$,
(ii) $\chi(S^{(t)}) = \chi^t(S)$ *for any $t \in \mathbb{Z}$,*
(iii) $\chi(\overline{S}) = \overline{\chi(S)}$,
(iv) $\chi(S+T) = \chi(S) + \chi(T)$, *and*
(v) $\chi(ST) = \chi(S)\chi(T)$.

The next lemma follows from Theorem 5.4 of [LN97].

Lemma 5.3. *We have*

$$\sum_{u \in K^\times} \chi(u) = \chi(K^\times) = \begin{cases} q-1 & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise.} \end{cases}$$

The next result says that a group algebra element is determined by its Fourier transform.

Lemma 5.4. *If $S, T \in L[K^\times]$, then $S = T$ if and only if $\chi(S) = \chi(T)$ for all $\chi \in \widehat{K^\times}$.*

Proof. This follows from the fact that the Fourier transform (the map from $L[K^\times]$ to $L^{\widehat{K^\times}}$ that takes S to the function $\widehat{S}\colon \widehat{K^\times} \to L$ with $\widehat{S}(\chi) = \chi(S)$) is an isomorphism of L-algebras with the inverse map

$$\begin{aligned} L^{\widehat{K^\times}} &\to L[K^\times] \\ R &\mapsto \check{R} = \sum_{u \in K^\times} \check{R}_u [u], \end{aligned}$$

where

$$\check{R}_u = \frac{1}{|K^\times|} \sum_{\chi \in \widehat{K^\times}} R(\chi)\overline{\chi(u)}. \qquad \square$$

5.1. **Weil sums in the group algebra.** Recall that $\psi : K \to \mathbb{Q}(\zeta)$ is the canonical additive character of K. We define

$$\Psi = \sum_{u \in K^\times} \psi(u)[u]$$

and

$$W^{K,s} = \sum_{u \in K^\times} W_u^{K,s}[u], \tag{8}$$

and when the field K and the exponent s are clear from context, we simply write $W = \sum_{u \in K^\times} W_u[u]$. We now relate W to Ψ.

Lemma 5.5. *We have $W = \Psi\overline{\Psi^{(1/s)}} + K^\times$.*

Proof. Applying the reparameterization $z = -x^s, y = -ux$ to $\Psi\overline{\Psi^{(1/s)}} = \sum_{y,z \in K^\times} \psi(y)\overline{\psi(z)}[yz^{-1/s}]$ gives

$$\Psi\overline{\Psi^{(1/s)}} = \sum_{u,x \in K^\times} \psi(x^s)\psi(-ux)[u] = \sum_{u \in K^\times} (W_u - 1)[u],$$

from which the result follows. $\square$

Let $\chi \in \widehat{K^\times}$. Then the *Gauss sum* $G(\chi)$ is given by $\sum_{u \in K^\times} \psi(u)\chi(u)$. Note that $G(\chi) = \chi(\Psi)$. We list some useful facts about Gauss sums, which will be useful later when we calculate the Fourier transform of group algebra elements that generalize W.

Lemma 5.6. *Let χ_0 be the principal character and $\chi \in \widehat{K^\times}$. Then*

(i) $|\Psi| = \chi_0(\Psi) = G(\chi_0) = -1$,
(ii) $|\chi(\Psi)| = |G(\chi)| = \sqrt{q}$ *for* $\chi \neq \chi_0$, *and*
(iii) $\overline{G(\chi)} = \chi(-1)G(\overline{\chi})$.

Proof. For a proof of the first and second parts, see [LN97, Theorem 5.11]; for a proof of the third part, see [LN97, Theorem 5.12(iii)]. ☐

We record two more useful calculations concerning Ψ and W.

Lemma 5.7. *If $t \in \mathbb{Z}$ and $\gcd(t, q-1) = 1$, then $\Psi^{(t)}\overline{\Psi^{(t)}} = q[1] - K^\times$.*

Proof. See [Kat15, Corollary 2.3]. ☐

Lemma 5.8. *We have $|W| = q$ and $W\overline{W} = q^2[1]$.*

Proof. The first result follows from Lemmas 5.5, 5.1, and 5.6, which give us $|W| = |\Psi||\overline{\Psi^{(1/s)}}| + |K^\times| = (-1)^2 + q - 1$. The second is proved as follows:

$$\begin{aligned}
W\overline{W} &= (\Psi\overline{\Psi^{(1/s)}} + K^\times)(\overline{\Psi\overline{\Psi^{(1/s)}} + K^\times}) \\
&= \Psi\overline{\Psi}\Psi^{(1/s)}\overline{\Psi^{(1/s)}} + \Psi\overline{\Psi^{(1/s)}}K^\times + \overline{\Psi}\Psi^{(1/s)}K^\times + K^\times K^\times \\
&= (|K|[1] - K^\times)^2 + |\Psi\overline{\Psi^{(1/s)}}|K^\times + |\overline{\Psi}\Psi^{(1/s)}|K^\times + |K^\times|K^\times \\
&= |K|^2[1] - 2|K|K^\times + |K^\times|K^\times + (|K^\times| + 2)K^\times \\
&= |K|^2[1],
\end{aligned}$$

where the third equality uses Lemmas 5.7 and 5.1, and the fourth equality uses Lemmas 5.1 and 5.6. ☐

The proof of our main result requires us to use generalizations of W whose coefficients are products of Weil sum values rather than individual ones. We introduce a convenient notation for these.

Notation 5.9. Let $k \in \mathbb{Z}_+$ and let $t = (t_1, t_2, \ldots, t_k) \in (K^\times)^k$. We write

$$W^{[t]} = \sum_{u \in K^\times} W_{t_1 u} \cdots W_{t_k u}[u].$$

Often, we just write $W^{[t_1,\ldots,t_k]}$ instead of $W^{[(t_1,\ldots,t_k)]}$ and $W^{[t]}_u$ for $(W^{[t]})_u$. Also, note that $W^{[1]} = W$.

Lemma 5.10 and Proposition 5.13 below make a connection between the group algebra elements just defined in Notation 5.9 and the cardinalities of algebraic sets defined in Notation 4.2. The connecting object is defined in Notation 5.11.

Lemma 5.10. *Let $k \in \mathbb{Z}_+$ and let $t = (t_1, \ldots, t_k) \in (K^\times)^k$. Then*

$$|W^{[t]}| = \sum_{u \in K^\times} W_{t_1 u} \cdots W_{t_k u} = \frac{q^2 Q^t_{0,0} - q^k}{q-1}.$$

Proof. This is Lemma 7.7.2 of [Kat19]. ☐

Recall the notations $\cdot$ and $\|\cdot\|_s$ from Notation 4.1, which we use for the rest of this section.

Notation 5.11. Let $k \in \mathbb{Z}_+$ and let $t = (t_1, t_2, \ldots, t_k) \in (K^\times)^k$. Then, adopting the convention that $[0]$ is the 0 of the group algebra $L[K^\times]$, we write

$$V^{[t]} = \sum_{\substack{v \in K^k \\ t \cdot v = 1}} [\|v\|_s] - Q^t_{1,0} K^\times,$$

so that

$$V^{[t]} = \sum_{u \in K^\times} (Q^t_{1,u} - Q^t_{1,0})[u].$$

We often write $V^{[t_1,\ldots,t_k]}$ instead of $V^{[(t_1,\ldots,t_k)]}$ and use the notation $V^{[t]}_u$ to mean $(V^{[t]})_u$.

The following calculation is needed for our proof of Proposition 5.13, which connects $W^{[t]}$ to $V^{[t]}$.

Lemma 5.12. *Let $k \in \mathbb{Z}_+$ and $t \in (K^\times)^k$. Then*

$$|V^{[t]}| = q^{k-1} - q \cdot Q^t_{1,0} = \frac{q Q^t_{0,0} - q^{k-1}}{q-1}.$$

Proof. The first equality comes from using Notation 5.11 to write $|V^{[t]}| = \sum_{u \in K^\times} Q^t_{1,u} - (q-1) \cdot Q^t_{1,0} = \sum_{u \in K} Q^t_{1,u} - q \cdot Q^t_{1,0}$ and then applying Lemma 4.3. The second equality then follows from Lemma 4.5. □

Now we show the relation between $V^{[t]}$ and $W^{[t]}$.

Proposition 5.13. *For $k \in \mathbb{Z}_+$ and $t \in (K^\times)^k$, we have*

$$W^{[t]} = W V^{[t]}.$$

Proof. Since both sides of this equation are elements of $L[K^\times]$, it suffices to show that $\chi(W^{[t]}) = \chi(W V^{[t]})$ for all $\chi \in \widehat{K^\times}$ by Lemma 5.4.

For the principal character χ_0 we have

$$\chi_0(W V^{[t]}) = |W||V^{[t]}| = \frac{q^2 Q^t_{0,0} - q^k}{q-1} = |W^{[t]}| = \chi_0(W^{[t]}),$$

where the first and last equalities follow from Lemma 5.2, the second comes from Lemmas 5.8 and 5.12, and the third comes from Lemma 5.10.

Now let χ be any non-principal character. On one hand, we have

$$\begin{aligned}
\chi\left(W^{[t]}\right) &= \sum_{u \in K^\times} \left(\sum_{x_1 \in K} \psi(x_1^s - t_1 u x_1) \right) \cdots \left(\sum_{x_k \in K} \psi(x_k^s - t_k u x_k) \right) \chi(u) \\
&= \sum_{\substack{x \in K^k \\ t \cdot x \neq 0}} \psi(\|x\|_s^s) \sum_{u \in K^\times} \psi(-(t \cdot x) u) \chi(u) \\
&= G(\chi) \sum_{w \in K^\times} \sum_{\substack{x \in K^k \\ t \cdot x = w}} \psi(\|x\|_s^s) \chi^{-1}(-w)
\end{aligned}$$

$$
\begin{aligned}
&= G(\chi) \sum_{z\in K^\times} \sum_{\substack{v\in K^k\\ t\cdot v=1}} \psi(\|v\|_s^s z)\chi^{-1}(-z^{1/s}) \\
&= G(\chi) \sum_{\substack{v\in K^k\\ t\cdot v=1\\ \|v\|_s\neq 0}} \sum_{z\in K^\times} \psi(\|v\|_s^s z)\chi^{-1/s}(-1)\chi^{-1/s}(z) \\
&= G(\chi)G(\chi^{-1/s})\chi^{-1/s}(-1) \sum_{\substack{v\in K^k\\ t\cdot v=1\\ \|v\|_s\neq 0}} \chi^{1/s}(\|v\|_s^s) \\
&= G(\chi)G(\chi^{-1/s})\chi^{-1/s}(-1)\chi\left(\sum_{\substack{v\in K^k\\ t\cdot v=1}} [\|v\|_s]\right),
\end{aligned}
$$

where we use Lemma 5.3 to impose $t \cdot x \neq 0$ following the second equals sign, and we use the Gauss sum in the third and second-to-last equalities and the reparameterization $w = z^{1/s}, x = z^{1/s}v$ in the fourth equality.

On the other hand, Lemmas 5.5, 5.2, 5.3, and Notation 5.11 give us

$$
\chi(WV^{[t]}) = \chi(\Psi)\chi(\overline{\Psi^{(1/s)}}) \cdot \chi\left(\sum_{\substack{v\in K^k\\ t\cdot v=1}} [\|v\|_s]\right),
$$

where

$$
\chi(\Psi)\chi(\overline{\Psi^{(1/s)}}) = G(\chi)\overline{\chi^{1/s}(\Psi)} = G(\chi)\overline{G(\chi^{1/s})} = G(\chi)G(\chi^{-1/s})\chi^{-1/s}(-1)
$$

by Lemmas 5.6 and 5.2, so the result is proved. □

For future convenience, we explicitly calculate some values of $|W^{[t]}|$ and $V^{[t]}$.

Lemma 5.14. *For any $t_1, t_2, t_3 \in K^\times$, we have*

(i) $|W| = q$,

(ii) $|W^{[t_1,t_2]}| = \begin{cases} q^2 & \text{if } t_1 = t_2 \\ 0 & \text{if } t_1 \neq t_2, \end{cases}$

(iii) $|W^{[t_1,t_2,t_3]}| = q^2 V^{[t_1,t_2]}_{1/t_3}$, *and*

(iv) $|W^{[1,1,1,1]}| = q^2 \sum_{u\in K^\times} \left(V_u^{[1,1]}\right)^2$.

Proof. The first result is from Lemma 5.8.

Next, we use Theorem 1.1 and Lemma 5.8 to obtain

$$
|W^{[t_1,t_2]}| = \sum_{\substack{x,y\in K^\times\\ xy=t_1/t_2}} W_x\overline{W_{1/y}} = (W\overline{W})_{t_1/t_2} = \begin{cases} q^2 & \text{if } t_1/t_2 = 1 \\ 0 & \text{otherwise.} \end{cases}
$$

For (iii), we use Theorem 1.1 to show that $|W^{[t_1,t_2,t_3]}| = \left(W^{[t_1,t_2]}\overline{W}\right)_{1/t_3}$. Then, Lemmas 5.13 and 5.8 and Notation 5.11 give us that

$$\left(W^{[t_1,t_2]}\overline{W}\right)_{1/t_3} = \left(WV^{[t_1,t_2]}\overline{W}\right)_{1/t_3} = q^2 V^{[t_1,t_2]}_{1/t_3}.$$

Lastly, we observe that $\sum_{u\in K^\times} W_u^4 = (W^{[1,1]}\overline{W^{[1,1]}})_1$, so the fourth result follows from Lemmas 5.13 and 5.8, which tell us that

$$W^{[1,1]}\overline{W^{[1,1]}} = (WV^{[1,1]})(\overline{WV^{[1,1]}}) = q^2 V^{[1,1]}\overline{V^{[1,1]}}. \qquad \square$$

Lemma 5.15. *If $t = (t_1,t_2) \in (K^\times)^2$, then we have*

$$V^{[t]} = \begin{cases} \sum_{\substack{v\in K^2\\ v\cdot t=1}} [\|v\|_s] & \text{if } t_1 = t_2 \\ \sum_{\substack{v\in K^2\\ v\cdot t=1}} [\|v\|_s] - K^\times & \text{otherwise,} \end{cases}$$

that is,

$$V^{[t]} = \begin{cases} \sum_{u\in K^\times} Q^t_{1,u}[u] & \text{if } t_1 = t_2 \\ \sum_{u\in K^\times} (Q^t_{1,u}-1)[u] & \text{otherwise,} \end{cases}$$

so that $V_u^{[t]} \ge -1$ for every $u \in K^\times$, and if $t_1 = t_2$ then $V_u^{[t]} \ge 0$ for every $u \in K^\times$. Furthermore,

$$|V^{[t]}| = \begin{cases} q & \text{if } t_1 = t_2 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. These facts follow from Notation 5.11 and Lemma 5.12, as well as the formula for $Q^t_{1,0}$ found in Lemma 4.7 and the fact that $Q^t_{1,u}$ values are always nonnegative, since they count solutions to systems of equations. $\square$

5.2. **Symmetrized Weil sums.** In later sections we study Weil spectra where there is a symmetry among the Weil sums $W_u^{K,s}$. Here we present some general results.

Fix some $k \in \mathbb{Z}_+$ and suppose that $p \equiv 1 \pmod{k}$. Then we let

$$T = \sum_{i=0}^{k-1} [\lambda^i],$$

where λ is a primitive kth root of unity in $\mathbb{F}_p^\times$. We also let

$$\Omega = \sum_{u\in K^\times} \left(\sum_{i=0}^{k-1} W_{\lambda^i u}\right)[u].$$

We call $\Omega_u = \sum_{i=0}^{k-1} W_{\lambda^i u}$ *the k-laterally symmetrized Weil sum at u*, and we use the word *bilateral* to mean 2-lateral. Note that Ω has real coefficients by Theorem 1.1. First, we relate Ω to W and T.

Lemma 5.16. *We have $\Omega = WT$.*

Proof. Reordering the sums in the definition of Ω gives us

$$\Omega = \sum_{i=0}^{k-1} \sum_{u \in K^\times} W_{\lambda^i u}[u] = \sum_{i=0}^{k-1} W \cdot [\lambda^{-i}] = W \cdot \sum_{i=0}^{k-1} [\lambda^i]. \qquad \square$$

We compute power moments for Ω.

Lemma 5.17. *We have*

(i) $\sum_{u \in K^\times} \Omega_u^0 = q-1$*;*
(ii) $\sum_{u \in K^\times} \Omega_u = kq$*;*
(iii) $\sum_{u \in K^\times} \Omega_u^2 = kq^2$*; and*
(iv) if $k=2$*, then* $\sum_{u \in K^\times} \Omega_u^3 = 2q^2(V_1^{[1,1]} + 3V_{-1}^{[1,1]})$*.*

Proof. The first equation comes from the fact that $|K^\times| = q-1$. The second and third results follow from Lemmas 5.16 and 5.8 as well as the fact that the coefficients of Ω are real, so that $\sum_{u \in K^\times} \Omega_u = |\Omega| = |W||T| = qk$ and $\sum_{u \in K^\times} \Omega_u^2 = (\Omega\overline{\Omega})_1 = (WT\overline{WT})_1 = q^2(T^2)_1 = q^2 k$. Lastly, if $k=2$, then

$$\sum_{u \in K^\times} \Omega_u^3 = \sum_{u \in K^\times} (W_u + W_{-u})^3 = 2 \sum_{u \in K^\times} W_u^3 + 6 \sum_{u \in K^\times} W_u^2 W_{-u},$$

so the desired result follows from Lemma 5.14(iii). $\square$

When p is odd and $k=2$, we have further results, which we explore in the next section.

5.3. **Bilateral symmetry in the group algebra.**

In Propositions 6.4 and 6.5 below we study bilaterally symmetrized Weil sums. Here, we present some general results that hold in this situation. To this end, suppose that p is odd and let

$$S = [1] - [-1], \quad \Phi = \sum_{u \in K^\times} (W_u - W_{-u})[u], \quad \Upsilon = \sum_{u \in K^\times} (W_u - W_{-u})^2 [u],$$
$$T = [1] + [-1], \quad \Omega = \sum_{u \in K^\times} (W_u + W_{-u})[u].$$

Note that this use of T and Ω is consistent with the notation introduced in Section 5.2 when $k=2$. Also, note that Φ, Ω, and Υ have real coefficients by Theorem 1.1. For convenience of notation, we set

$$V = V^{[1,1]} \quad \text{and} \quad U = V^{[1,-1]}.$$

We relate the various group algebra elements that we have just defined.

Lemma 5.18. *We have* $\Phi = WS$ *and* $\Upsilon = W(TV - 2U)$*.*

Proof. These results come from the above notation and Proposition 5.13. $\square$

Before we prove further results, we shall restate in the notation of this section a few key facts that we have proved earlier.

Lemma 5.19. *We have*

(i) $U_u = Q_{1,u}^{(1,-1)} - 1$ *and* $V_u = Q_{1,u}^{(1,1)}$ *so in particular,* $U_u \geq -1$ *and* $V_u \geq 0$ *for all* $u \in K^\times$*;*
(ii) $U_u = U_{-u}$ *for any* $u \in K^\times$*;*
(iii) $U_1 = U_{-1} = V_{-1}$*; and*
(iv) $\sum_{u \in K^\times} U_u = 0$ *and* $\sum_{u \in K^\times} V_u = q$*.*

Proof. Part (i) follows from the definitions of U and V and Lemma 5.15. Then, using the result in part (i) and the assumption that p is odd, parts (ii) and (iii) follow from the first two parts of Lemma 4.8. Lastly, the part (iv) comes from Lemma 5.15. □

We compute some power moments for Φ and a related sum that involves both Φ and Ω.

Lemma 5.20. *We have*
(i) $\sum_{u \in K^\times} \Phi_u = 0$*,*
(ii) $\sum_{u \in K^\times} \Phi_u^2 = 2q^2$*,*
(iii) $\sum_{u \in K^\times} \Phi_u^2 \cdot \Omega_u = 2q^2(V_1 - V_{-1})$*, and*
(iv) $\sum_{u \in K^\times} \Phi_u^4 = q^2 \sum_{u \in K^\times} (V_u + V_{-u} - 2U_u)^2$*.*

Proof. Recall that Φ and Υ have real coefficients.

To prove the first part, we use Lemmas 5.18 and 5.1(iv) to get $|\Phi| = |W||S| = 0$. The second part follows from Lemmas 5.18, 5.8, and 5.1(vii), which give us $\sum_{u \in K^\times} \Phi_u^2 = (\Phi\overline{\Phi})_1 = (WS\overline{WS})_1 = q^2(S\overline{S})_1 = 2q^2$.

We can prove the third part by observing that $\sum_{u \in K^\times} \Phi_u^2 \cdot \Omega_u = (\Upsilon \cdot \overline{\Omega})_1$ and then using Lemmas 5.18, 5.16, 5.8, and 5.19(iii) to get that

$$(\Upsilon \cdot \overline{\Omega})_1 = \left(W\overline{W}(2TV - 2UT)\right)_1 = 2q^2(V_1 + V_{-1} - U_1 - U_{-1}) = 2q^2(V_1 - V_{-1}).$$

The fourth and final part is a consequence of Lemmas 5.1(vii) (using the fact that all coefficients in our group algebra elements here are real), 5.18 and 5.8, since we have

$$\begin{aligned} \sum_{u \in K^\times} \Phi_u^4 &= (\Upsilon\overline{\Upsilon})_1 \\ &= \left(W\overline{W}(TV - 2U)(\overline{TV - 2U})\right)_1 \\ &= q^2 \sum_{u \in K^\times} ((TV - 2U)_u)^2 \\ &= q^2 \sum_{u \in K^\times} (V_u + V_{-u} - 2U_u)^2. \end{aligned}$$ □

6. Cyclotomic actions on value sets of size four

In this section, we examine the action on the value set $\mathcal{W}_{K,s}$ (see (3)) of τ, the restriction of the generator σ of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ to $\mathcal{W}_{K,s}$. We shall prove our main theorem (Theorem 1.5), which is:

Theorem 6.1. *Let K be a finite field and s be an invertible exponent over K. If the Weil spectrum for K and s is 4-valued, then it is rational unless $K = \mathbb{F}_5$ and $s \equiv 3 \pmod 4$ (in which case $\mathcal{W}_{K,s} = \{(5 \pm \sqrt{5})/2, \pm\sqrt{5}\}$).*

Suppose $\mathcal{W}_{K,s} = \{A, B, C, D\}$, where A, B, C, and D are distinct. Recall that σ is a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and that τ is the restriction of σ to $\mathcal{W}_{K,s}$. We saw in (4) that τ always permutes the elements of $\mathcal{W}_{K,s}$, so here τ must act trivially, as a transposition (while keeping two values fixed), as a composition of two disjoint transpositions, as a 3-cycle (while keeping one value fixed), or as a 4-cycle on the set $\{A, B, C, D\}$. We shall address each of the non-trivial actions in the next four propositions, and then finally prove the theorem. Throughout this section, we shall use the notation (from (2) in the Introduction) where $N_A^{K,s}$ (or simply N_A) denotes the frequency of a value A in the Weil spectrum for the field K and the exponent s.

Proposition 6.2 (**No action as a 4-cycle**)**.** *If $|\mathcal{W}_{K,s}| = 4$, then τ does not permute $\mathcal{W}_{K,s}$ as a 4-cycle.*

Proof. This follows from Proposition 2.5, since $|\mathcal{W}_{K,s}| = 1$ when $K = \mathbb{F}_2$. □

Proposition 6.3 (**No action as a 3-cycle**)**.** *If $|\mathcal{W}_{K,s}| = 4$, then τ does not permute $\mathcal{W}_{K,s}$ as a 3-cycle (while fixing one value).*

Let $|\mathcal{W}_{K,s}| = 4$. Assume that τ permutes $\mathcal{W}_{K,s}$ as a 3-cycle to show a contradiction, so we write $\mathcal{W}_{K,s} = \{A, B, C, D\}$ and $\tau = (A)(BCD)$, i.e., $\tau(A) = A$, $\tau(B) = C$, $\tau(C) = D$, and $\tau(D) = B$. For clarity, we break the proof into steps.

Step 1. The exponent s is nondegenerate.

Proof. This is from Theorem 1.2.

Step 2. We have $p \equiv 1 \pmod 6$, so $p \geq 7$, and there is a primitive third root of unity $\lambda \in \mathbb{F}_p^\times$ such that $\tau(W_u) = W_{\lambda u}$ for all $u \in K^\times$.

Proof. This is from Proposition 2.1 and (4), since τ has order 3.

Step 3. We have $3 \mid N_A$ and $N_B = N_C = N_D$.

Proof. This is from Lemma 2.3, since τ has order 3, permutes A in a 1-cycle, and permutes B, C, D in a 3-cycle.

Step 4. Let $X = 3A$ and $Y = B + C + D$. Then X and Y are rational integers with $3 \mid X$ and

$$3q^2 - 3q(X + Y) + (q - 1)XY = 0. \tag{9}$$

Proof. We know that A and Y are in $\mathbb{Z}$ because σ (of which τ is a restriction) fixes both of these algebraic integers. Thus, X is a rational integer with $3 \mid X$. By Step 2, we can let $\Omega_u = W_u + W_{\lambda u} + W_{\lambda^2 u} = W_u + \tau(W_u) + \tau^2(W_u)$ for all $u \in K^\times$, as in Section 5.2 (with $k = 3$). Notice that Ω_u only assumes two values as u runs through $K^\times$, namely $X = 3A$ (N_A times) and $Y = B+C+D$ ($3N_B$ times by Step 3). This means that $\sum_{u \in K^\times} (\Omega_u - X)(\Omega_u - Y) = 0$, so we obtain (9) from the first three results in Lemma 5.17.

Step 5. We have $\max\{v_p(X), v_p(Y)\} \geq v_p(q)$.

Proof. If $\max\{v_p(X), v_p(Y)\} < v_p(q)$, then $v_p((q-1)XY) < v_p(3q^2-3q(X+Y))$, contradicting (9) in Step 4.

Step 6. We have $0 \notin \{X, Y\}$.

Proof. We assume $0 \in \{X, Y\}$ to show contradiction. Then $\{X, Y\} = \{0, q\}$ by (9). Now q is a power of the prime p with $p \geq 7$ (by Step 2), but X is a rational integer with $3 \mid X$ (by Step 4), so we cannot have $X = q$. Thus, $X = 3A = 0$ and $Y = B+C+D = q$. Since s is nondegenerate by Step 1, we have $|B|, |C|, |D| < q$ by Lemma 3.2, so that $B+C+D = q$ makes at least two of B, C, D positive, while [AKL15, Corollary 2.3] makes at least one negative, and so $BCD < 0$. Now Lemma 5.14(iii) gives us $|W^{[1,\lambda,\lambda^2]}| = q^2 V_\lambda^{[1,\lambda]}$, that is, $\sum_{u \in K^\times} W_u W_{\lambda u} W_{\lambda^2 u} = q^2 V_\lambda^{[1,\lambda]}$. Recalling the relation involving τ and λ from Step 2, this means that $\sum_{u \in K^\times} W_u \, \tau(W_u) \, \tau^2(W_u) = q^2 V_\lambda^{[1,\lambda]}$. Then in view of the fact that $\mathcal{W}_{K,s} = \{A, B, C, D\}$ with $\tau(B) = C$, $\tau(C) = D$, and $\tau(D) = B$, and since we have shown that $A = 0$ here and $N_B = N_C = N_D$ in Step 3, we have $3N_B BCD = q^2 V_\lambda^{[1,\lambda]}$. Since $BCD < 0$, Lemma 5.15 forces $V_\lambda^{[1,\lambda]} = -1$, and hence $3N_B BCD = -q^2$. But $BCD \in \mathbb{Z}$ since it is an algebraic integer fixed by τ, which is a restriction of σ, the generator of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. This means that $3 \mid q^2$, contradicting $p \geq 7$ from Step 2.

Step 7. We have $v_p(X) < v_p(q)$ and $v_p(Y) \geq v_p(q)$.

Proof. Recall from Step 4 that $X = 3A$. Therefore, by Step 2 we have $v_p(X) = v_p(3A) = v_p(A)$, and then by Step 6 and Lemma 3.4, we know that $v_p(A) < v_p(q)$. Thus $v_p(X) < v_p(q)$ and so by Step 5 we know that $v_p(Y) \geq v_p(q)$.

Step 8. We have $Y = rq$ for some $r \in \{\pm 1, \pm 2\}$.

Proof. Recall from Step 4 that $Y = B + C + D$. By Steps 6 and 1 combined with Lemma 3.2, we know that $0 < |Y| = |B + C + D| < 3q$. Thus, $0 < |Y| < pq$ by Step 2. Now Step 4 shows that $Y \in \mathbb{Z}$, so by Step 7 we have $v_p(Y) = v_p(q)$. Then $Y = rq$ for some $r \in \mathbb{Z}$ and recall that $0 < |Y| < 3q$.

Step 9. We conclude that τ does not permute $\mathcal{W}_{K,s}$ as a 3-cycle.

Proof. We rule out each of the four possible values of r in Step 8 using the following formula for $X \in \mathbb{Z}$, which comes from (9) and $Y = rq$:

$$X = \frac{3q(r-1)}{(q-1)r-3} \tag{10}$$

(note that the denominator is not zero because $q-1 \geq p-1 \geq 6$ by Step 2).

If $r = 1$, then $X = 0$, which contradicts Step 6. If $r = -2$ (resp., -1, 2), then (10) becomes $4+(q-4)/(2q+1)$ (resp., $6-12/(q+2)$, $1+(q+5)/(2q-5)$). None of these expressions can be a rational integer, since q is a power of some prime $p \geq 7$ by Step 2, so Step 4 is contradicted. □

Proposition 6.4 (Action as a composition of two disjoint 2-cycles). *The following are equivalent:*

(i) $|\mathcal{W}_{K,s}| = 4$ *and* τ *permutes* $\mathcal{W}_{K,s}$ *as a composition of two disjoint transpositions;*

(ii) $q = 5$ *and* $s \equiv 3 \pmod 4$.

When these hold, $\mathcal{W}_{K,s} = \{(5 \pm \sqrt{5})/2, \pm\sqrt{5}\}$.

Suppose that $q = 5$ and $s \equiv 3 \pmod 4$. In fact, we may assume $s = 3$ since $\mathcal{W}_{K,s'} = \mathcal{W}_{K,s''}$ if $s' \equiv s'' \pmod{q-1}$ (see the definition of equivalent exponents in Section 1). Let $\zeta = e^{2\pi i/5}$. The polynomial $x^3 - x$ represents 0 thrice and each of ± 1 only once over $K = \mathbb{F}_5$, and so $W_1^{K,s} = 3 + (\zeta + \zeta^{-1}) = (5 + \sqrt{5})/2$ by Lemma 3.5. Similarly, $x^3 - 2x$ represents 0 once and each of ± 1 twice over K; $x^3 - 3x$ represents 0 once and each of ± 2 twice; and $x^3 - 4x$ represents 0 three times and each of ± 2 once over K, so we can calculate that $W_2^{K,s} = \sqrt{5}$, $W_3^{K,s} = -\sqrt{5}$, and $W_4^{K,s} = (5 - \sqrt{5})/2$. Then since $\sigma(\sqrt{5}) = -\sqrt{5}$ (because σ restricts to the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$), it is clear that τ acts on $\mathcal{W}_{K,s}$ as a product of two disjoint transpositions.

Now suppose that $|\mathcal{W}_{K,s}| = 4$ and suppose that τ acts on $\mathcal{W}_{K,s}$ as a composition of two disjoint transpositions. For clarity, the remainder of the proof is broken up into steps.

Step 1. We have $p \equiv 1 \pmod 4$, so $p \geq 5$, and $\tau(W_u) = W_{-u}$ for all $u \in K^\times$.

Proof. This is from Proposition 2.1 and (4), since τ has order 2.

Step 2. We write $\mathcal{W}_{K,s} = \{A, B, C, D\}$ with

$$A = \frac{E + F\sqrt{p}}{2}, B = \frac{E - F\sqrt{p}}{2}, C = \frac{G + H\sqrt{p}}{2}, \text{ and } D = \frac{G - H\sqrt{p}}{2},$$

where $E, F, G, H \in \mathbb{Z}$ with $E \equiv F \pmod 2$, $G \equiv H \pmod 2$, $v_p(E) \leq v_p(G)$, and $\tau = (AB)(CD)$, i.e., $\tau(A) = B$, $\tau(B) = A$, $\tau(C) = D$, and $\tau(D) = C$.

Proof. Since τ has order 2 and since Step 1 tells us that $p \equiv 1 \pmod 4$, Proposition 2.1 shows that the elements of $\mathcal{W}_{K,s}$ are algebraic integers in $\mathbb{Q}(\sqrt{p})$, the unique degree 2 extension of $\mathbb{Q}$ that lies in $\mathbb{Q}(\zeta)$. Thus, each element of $\mathcal{W}_{K,s}$ has the form described in Lemma 3.6, and the four elements consist of two pairs of Galois conjugates because of the action of τ. This establishes the existence of the integers E, F, G, and H which are used to describe our four elements of $\mathcal{W}_{K,s}$ above (making sure to arrange so that $v_p(E) \leq v_p(G)$), and we also name the elements A, B, C, and D as above, so that the Galois conjugate pairs are $\{A, B\}$ and $\{C, D\}$; this means that τ must act as $(AB)(CD)$.

Step 3. We have $N_A = N_B$ and $N_C = N_D$.

Proof. This is due to Lemma 2.3 since $\tau = (AB)(CD)$ from Step 2.

Step 4. We have the following equations:

$$N_A + N_C = \frac{q-1}{2} \tag{11}$$

$$N_A E + N_C G = q \tag{12}$$

$$N_A E^2 + N_C G^2 = q^2 \tag{13}$$

$$N_A F^2 p + N_C H^2 p = q^2 \tag{14}$$

$$N_A(E^3 + 3pEF^2) + N_C(G^3 + 3pGH^2) = 4q^2 V_1^{[1,1]}. \tag{15}$$

Proof. For $u \in K^\times$, let $\Omega_u = W_u + W_{-u}$ and $\Phi_u = W_u - W_{-u}$. This is consistent with the notation we introduced in Section 5.2 (with $k = 2$) and in Section 5.3 since $p \equiv 1 \pmod 2$ by Step 1. Thus, by Step 1, we have $\Omega_u = W_u + \tau(W_u)$ and $\Phi_u = W_u - \tau(W_u)$ for every $u \in K^\times$.

As we run through $u \in K^\times$, Steps 2 and 3 tell us that Ω_u has

$2N_A$ instances of E $\qquad$ $2N_C$ instances of G

while Φ_u has

N_A instances of $F\sqrt{p}$ $\qquad$ N_A instances of $-F\sqrt{p}$

N_C instances of $H\sqrt{p}$ $\qquad$ N_C instances of $-H\sqrt{p}$,

so that (11), (12), and (13) follow from parts (i), (ii), and (iii) of Lemma 5.17 and (14) follows from 5.20(ii). The left-hand side of Lemma 5.14(iii) (with $t_1 = t_2 = t_3 = 1$) is summing W_u^3 over all $u \in K^\times$, and since $N_A = N_B$ and $N_C = N_D$ by Step 3, we obtain (15).

Step 5. We have $G = 0$.

Proof. Add EG times (11) and $-(E+G)$ times (12) to (13) to get

$$0 = EG\left(\frac{q-1}{2}\right) - (E+G)q + q^2. \tag{16}$$

Recall from Step 2 that $v_p(E) \le v_p(G)$. Note that if either $v_p(G) < v_p(q)$ or $v_p(E) > v_p(q)$, then one of the terms in (16) would have strictly lower p-adic valuation than the other terms. Thus, $v_p(E) \le v_p(q) \le v_p(G)$, so that $E \neq 0$ and $q \mid G$. On the other hand, since $N_A, N_C \in \mathbb{Z}_+$, (13) tells us that

$$q^2 = N_A E^2 + N_C G^2 > N_C G^2 \ge G^2,$$

and so $G = 0$.

Step 6. We have $E = q$ and $N_A = 1$.

Proof. Since $G = 0$ by Step 5, (12) and (13) imply that $E = q$ and $N_A = 1$.

Step 7. We have $N_C = (q-3)/2$.

Proof. Since $N_A = 1$ by Step 6, (11) gives us that $N_C = (q-3)/2$.

Step 8. The quantity F is odd and $H = 2I$ for some $I \in \mathbb{Z} \setminus \{0\}$.

Proof. We know that $G = 0$ by Step 5 and $E = q$ by Step 6. Furthermore, q is odd since p is odd by Step 1. Step 2 tells us that $E \equiv F \pmod{2}$ and $G \equiv H \pmod{2}$, so F is odd and H is even. But $H \neq 0$, else $C = D$ (see Step 2), so $H = 2I$ for some $I \in \mathbb{Z} \setminus \{0\}$.

Step 9. We must have $q \leq 5$.

Proof. We can substitute the results from Steps 5–8 into (15) and (14) to obtain

$$3F^2 = \frac{q}{p} \cdot (4V_1^{[1,1]} - q) \tag{17}$$

$$F^2 + 2(q-3)I^2 = \frac{q^2}{p}. \tag{18}$$

Since $p \equiv 1 \pmod{4}$ by Step 1, we have $\gcd(q/p, 3) = \gcd(q/p, 2(q-3)) = 1$, and therefore since $V_1^{[1,1]} \in \mathbb{Z}$, (17) and (18) consecutively give us that $(q/p) \mid F^2$ and $(q/p) \mid I^2$. Now we know from Step 8 that $F, I \neq 0$, so $F^2/(q/p), I^2/(q/p) \geq 1$. If we substitute this into (18), the equality becomes the inequality

$$q = \frac{q^2/p}{q/p} = \frac{F^2}{q/p} + 2(q-3) \cdot \frac{I^2}{q/p} \geq 1 + 2(q-3) = 2q - 5,$$

so that $q \leq 5$.

Step 10. We conclude that $q = 5$ and $s \equiv 3 \pmod{4}$.

Proof. Steps 1 and 9 give us that an action with two disjoint transpositions can only occur when $q = p = 5$. We now consider the possible values for s. Since $\mathcal{W}_{K,s'} = \mathcal{W}_{K,s''}$ if $s' \equiv s'' \pmod{q-1}$ (see the definition of equivalent exponents in Section 1), it suffices to consider the cases when $s \equiv 0, 1, 2, 3 \pmod{4}$. We cannot have $s \equiv 0, 2 \pmod{4}$, for then $\gcd(s, q-1) = \gcd(s, 4) \neq 1$, so s would not be invertible. Nor can we have $s \equiv 1 \pmod{4}$, for then s would be degenerate and this would make $|\mathcal{W}_{K,s}| \leq 2$ by Theorem 1.2. Thus $s \equiv 3 \pmod{4}$. □

Proposition 6.5 (**No action as a transposition).** *If $|\mathcal{W}_{K,s}| = 4$, then τ does not permute the elements of $\mathcal{W}_{K,s}$ as a transposition.*

Suppose that $|\mathcal{W}_{K,s}| = 4$. Assume that τ permutes $\mathcal{W}_{K,s}$ as a transposition to show a contradiction. For clarity, the proof of this proposition is broken into steps.

Step 1. We have $p \equiv 1 \pmod{4}$, so $p \geq 5$, and there exist $A, B, E, F \in \mathbb{Z}$ with $|A| \leq |B|$, $F > 0$, and $E \equiv F \pmod{2}$ such that $\mathcal{W}_{K,s} = \{A, B, C = (E + F\sqrt{p})/2, D = (E - F\sqrt{p})/2\}$ and τ acts on $\mathcal{W}_{K,s}$ as $(A)(B)(CD)$, i.e., $\tau(A) = A$, $\tau(B) = B$, $\tau(C) = D$, and $\tau(D) = C$. Moreover, both N_A and N_B are even and $N_C = N_D$.

Proof. Since τ has order 2, we know by Proposition 2.1 that $p \equiv 1 \pmod{4}$ and that $\mathbb{Q}(\mathcal{W}_{K,s}) = \mathbb{Q}(\sqrt{p})$, the unique degree 2 extension of $\mathbb{Q}$ that lies in $\mathbb{Q}(\zeta)$. This means that the two elements of $\mathcal{W}_{K,s}$ exchanged by τ are Galois conjugate algebraic integers in $\mathbb{Q}(\sqrt{p})$, and hence can be written as $C = (E + F\sqrt{p})/2$ and $D = (E - F\sqrt{p})/2$ for some $E, F \in \mathbb{Z}$ where $E \equiv F \pmod 2$ and $F > 0$ by Lemma 3.6. The other two elements of $\mathcal{W}_{K,s}$ are algebraic integers fixed by τ (and hence by σ), so they must be rational integers; we label these A and B in such a way that $|A| \leq |B|$. Then both N_A and N_B are even and $N_C = N_D$ by Lemma 2.3.

Step 2. We have $\tau(W_u) = W_{-u}$ for all $u \in K^\times$, so as in Sections 5.2 (with $k = 2$) and 5.3 we can let

$$\Omega = \sum_{u \in K^\times} (W_u + W_{-u})[u] = \sum_{u \in K^\times} (W_u + \tau(W_u))[u],$$

$$\Phi = \sum_{u \in K^\times} (W_u - W_{-u})[u] = \sum_{u \in K^\times} (W_u - \tau(W_u))[u],$$

$$V = V^{[1,1]}, \qquad U = V^{[1,-1]}, \qquad \text{and} \qquad T = [1] + [-1].$$

Proof. Since Step 1 implies that τ has order 2 and $p \equiv 1 \pmod 2$, Proposition 2.1 and (4) give us that $\tau(W_u) = W_{-u}$ for all $u \in K^\times$ and we have the bilateral symmetry alluded to in Sections 5.2 (with $k = 2$) and 5.3.

Step 3. The integer E is odd and there exist rational integers $X < Y < Z$ such that $\{X, Y, Z\} = \{2A, 2B, E\}$. Let $M_R = |\{u \in K^\times : \Omega_u = R\}|$ for $R \in \{X, Y, Z\}$. Then we have $\{(X, M_X), (Y, M_Y), (Z, M_Z)\} = \{(2A, N_A), (2B, N_B), (E, 2N_C)\}$ and the following equations hold:

$$q - 1 = M_X + M_Y + M_Z \tag{19}$$

$$2q = M_X X + M_Y Y + M_Z Z \tag{20}$$

$$2q^2 = M_X X^2 + M_Y Y^2 + M_Z Z^2 \tag{21}$$

$$M_X = \frac{2q^2 - 2q(Y + Z) + (q - 1)YZ}{(X - Y)(X - Z)} \tag{22}$$

$$M_Y = \frac{2q^2 - 2q(X + Z) + (q - 1)XZ}{(Y - X)(Y - Z)} \tag{23}$$

$$M_Z = \frac{2q^2 - 2q(X + Y) + (q - 1)XY}{(Z - X)(Z - Y)} \tag{24}$$

$$V_1 + 3V_{-1} = (X + Y + Z) - \frac{XY + YZ + ZX}{q} + \frac{(q - 1)XYZ}{2q^2} \tag{25}$$

$$q^2 = N_C F^2 p \tag{26}$$

$$V_1 - V_{-1} = E \tag{27}$$

$$2F^2 p = \sum_{u \in K^\times} (V_u + V_{-u} - 2U_u)^2. \tag{28}$$

Proof. Since $N_C = N_D$ by Step 1, we observe that as u runs through $K^\times$,

Φ_u has	Ω_u has
$N_A + N_B$ instances of 0	N_A instances of $2A$
N_C instances of $F\sqrt{p}$	N_B instances of $2B$
N_C instances of $-F\sqrt{p}$	$2N_C$ instances of E

and $\Omega_u = E$ for those u such that $\Phi_u \neq 0$. Thus, we obtain (26)–(28) from Lemma 5.20(ii)–(iv). Note that (26) and Step 1 imply that E and F are odd, whereas $2A$ and $2B$ must be distinct and even, so that there are rational integers $X < Y < Z$ with $\{X, Y, Z\} = \{2A, 2B, E\}$ and we can let M_X, M_Y, and M_Z be as stated above. Equations (19)–(21) then follow from Lemma 5.17(i)–(iii), which we also use to prove (22) from the following observation:

$$M_X(X - Y)(X - Z) = \sum_{u \in K^\times} (\Omega_u - Y)(\Omega_u - Z),$$

and (23) and (24) follow similarly by exchanging the roles of X, Y, and Z. Similarly, one can prove (25) using all parts of Lemma 5.17 (and the fact that $V = V^{[1,1]}$) from the following observation:

$$0 = \sum_{u \in K^\times} (\Omega_u - X)(\Omega_u - Y)(\Omega_u - Z).$$

Step 4. We have $-q < -2(q-1)/(p-1) < X < Y < Z < 2q$ and $v_p(X), v_p(Y), v_p(Z) \geq 1$. If any of X, Y, or Z is nonzero, then its p-adic valuation is less than the p-adic valuation of q. If none of X, Y, and Z is zero, then $v_p(XY), v_p(YZ), v_p(ZX) > v_p(q)$.

Proof. The first chain of inequalities follows from Step 3 and Lemma 3.6 (which applies due to Step 1 and Theorem 1.2), once we notice that $2A$, $2B$, and E take the place of I in Lemma 3.6. Lemma 3.6 also tells us that $v_p(X), v_p(Y), v_p(Z) \geq 1$. Next, $M_X X^2$, $M_Y Y^2$, and $M_Z Z^2$ are all even rational integers by Step 3, so if $X \neq 0$ but $v_p(X) \geq v_p(q)$, then $2q^2 \mid M_X X^2$, and hence $M_X X^2 = 2q^2$ and $Y = Z = 0$ by (21). This contradicts Step 3. Analogous arguments show that the same result holds for Y and Z. In particular, if $0 \notin \{X, Y, Z\}$, then $v_p(X), v_p(Y), v_p(Z) < v_p(q)$. Thus, if we write (25) as

$$2q^2(V_1 + 3V_{-1}) = 2q^2(X + Y + Z) - 2q(XY + YZ + ZX) + (q-1)(XYZ),$$

then $(q-1)XYZ$ has a strictly smaller p-adic valuation than every other term on the right-hand side of the above equation. This implies that

$$v_p(X) + v_p(Y) + v_p(Z) = v_p(2q^2(V_1 + 3V_{-1})) \geq 2v_p(q),$$

and so the desired inequalities follow from subtracting one of the terms on the left-hand side from both sides.

Step 5. We have $-q < X < Y = 0 < Z < q$.

Proof. Recall from Step 3 that M_X is a strictly positive count, so the numerator and denominator in (22) must have the same sign. Thus, to prove this step, it suffices to show that $Y = 0$ since $-q < X < Y < Z$ by Step 4, for then the numerator in (22), which is positive, becomes $2q(q - Z)$.

Suppose that $Y \neq 0$. By Step 3, we know that $Z > 0$, since otherwise the right-hand side of (20) would be negative. Moreover, the numerator in (22) is positive, that is,

$$2q^2 - 2q(Y + Z) + (q - 1)YZ > 0. \tag{29}$$

Thus, using Step 4 and the fact that $p \geq 5$ from Step 1 in (29) gives us

$$YZ > \frac{2q(Y + Z - q)}{q - 1} > \frac{2q}{q - 1}\left(-2\left(\frac{q - 1}{5 - 1}\right) + 1 - q\right) = -3q > -pq.$$

We cannot have $Y < 0$, for that would imply both $0 \notin \{X, Y, Z\}$ and $v_p(YZ) \leq v_p(q)$, which contradicts Step 4. So we must have $Y > 0$. If we use the same argument, replacing (22) with (24), Z with Y, and Y with X, we show that $X < 0$ is also impossible, and so obtain $X \geq 0$.

If $X > 0$, then Step 4 implies that $X, Y, Z \geq p$, so (20), (19), and the fact that $q \geq p \geq 5$ by Step 1 give us the contradiction

$$2q \geq p(M_X + M_Y + M_Z) = p(q - 1) \geq 5q - p \geq 4q.$$

This forces $X = 0 < Y < Z$ by Step 3, so that (20) and (21) give

$$2qZ = (M_Y Y + M_Z Z)Z > M_Y Y^2 + M_Z Z^2 = 2q^2,$$

and hence $Z > q$. On the other hand, $M_Z Z^2 \leq 2q^2$ by (21), so $M_Z = 1$. With this information, (20) and (21) become

$$M_Y Y + Z = 2q \tag{30}$$

$$M_Y Y^2 + Z^2 = 2q^2. \tag{31}$$

Since $v_p(Z) < v_p(q)$ by Step 4, (30) and (31) imply that $v_p(M_Y Y) = v_p(Z)$ and $v_p(M_Y Y^2) = v_p(Z^2)$, and hence that $v_p(M_Y) = 0$ and $v_p(Y) = v_p(Z)$. Moreover, (23) can be rewritten as

$$M_Y Y = \frac{2q(Z - q)}{Z - Y},$$

so that $v_p(Y) = v_p(q) + v_p(Z) - v_p(Z - Y)$, and so $v_p(Z - Y) = v_p(q)$. In other words, $q \mid Z - Y$. Since $0 < Y < Z < 2q$ by Step 4, this is only possible if $Z = Y + q$. If we substitute this equation for Z into (30) and (31) and solve for Y, we obtain $3Y = q$, which is impossible because $p \equiv 1 \pmod 4$ by Step 1.

Step 6. We have $E = X < 0$ and $A = Y/2 = 0$ and $B = Z/2 > 0$. Moreover, $|E| < |B|$ and $V_{-1} > 0$ and $B = 2V_{-1}/(1 - E/q)$.

Proof. Recall from Step 3 that $\{X, Y, Z\} = \{2A, 2B, E\}$ is a set of three distinct numbers and that E is odd. Since $|A| \leq |B|$ by Step 1 and $Y = 0$ is even by Step 5, we must have $0 = Y = A$ and $\{X, Z\} = \{2B, E\}$. We obtain $B = 2V_{-1}/(1-E/q)$ by substituting these facts into (25) and using (27) (note that we can divide by $1-E/q$ since Step 5 implies that $|E| < q$).

Now, since B is nonzero, $1-E/q$ is positive (since $|E| < q$), and V_{-1} is nonnegative (by Lemma 5.19(i)), we must have $B = Z/2$ is positive, and hence $V_{-1} > 0$ and $E = X < 0$. It then follows that $1 < 1-E/q < 2$ and $V_{-1} < B < 2V_{-1}$. Lastly, Lemma 5.19(i) tells us that $V_1 \geq 0$, so $E \geq -V_{-1}$ by (27), and thus $|E| < |B|$.

Step 7. There exists an odd integer m with $0 < m < n$ such that $N_C = p^m$ and $F = p^{n-(m+1)/2}$. Let $\ell = v_p(B) - v_p(E)$. Then $v_p(N_B) = m - 2\ell$. Moreover, we have

$$N_B B + N_C E = q \tag{32}$$

$$2N_B B^2 + N_C E^2 = q^2. \tag{33}$$

Proof. The results about m, N_C, and F follow from (26) since $N_C < q$, while (32) and (33) come from equations (20) and (21) and Steps 3 and 6. Lastly, (33) implies that $v_p(N_B B^2) = v_p(N_C E^2)$ since $2N_B B^2 > 0$ and $N_C E^2 > 0$ by Step 6 and $p \nmid 2$ by Step 1, so $v_p(N_B) = m - 2\ell$.

Step 8. We have $\ell > 0$, and there exist $\beta, \varepsilon, \nu \in \mathbb{Z}_+$ all relatively prime to p such that

$$B = \beta p^{n-m+2\ell}, \qquad E = -\varepsilon p^{n-m+\ell}, \text{ and } \qquad N_B = 2\nu p^{m-2\ell}. \tag{34}$$

Moreover, we have the following equations:

$$2\nu\beta - \varepsilon p^{\ell} = 1 \tag{35}$$

$$4\nu\beta^2 + \varepsilon^2 = p^{m-2\ell}. \tag{36}$$

Proof. Steps 1, 6, and 7 allow us to write $B = \beta p^{v_p(E)+\ell}$, $N_B = 2\nu p^{m-2\ell}$, $E = -\varepsilon p^{v_p(E)}$, and $N_C = p^m$ with $\beta, \varepsilon, \nu \in \mathbb{Z}_+$ all relatively prime to p, so that (32) and (33) become

$$2\nu\beta p^{m+v_p(E)-\ell} - \varepsilon p^{m+v_p(E)} = p^n \tag{37}$$

$$4\nu\beta^2 + \varepsilon^2 = p^{2n-m-2v_p(E)}. \tag{38}$$

It thus suffices to show that $\ell > 0$, for then $m + v_p(E) - \ell < m + v_p(E)$, and hence $m + v_p(E) - \ell = n$ by (37), so that $v_p(E) = n - m + \ell$, and so the expressions for E and B at the beginning of this proof become those in (34) while (37) and (38) become (35) and (36).

Suppose $\ell \leq 0$, and let $g = n - m - v_p(E)$. Then (37) and (38) become

$$2\nu\beta p^{-\ell} - \varepsilon = p^g \tag{39}$$

$$4\nu\beta^2 + \varepsilon^2 = p^{2g+m}. \tag{40}$$

By Step 6, we have $\varepsilon = |E|/p^{v_p(E)} < |B|/p^{v_p(E)+\ell} = \beta$, so (39) gives us

$$p^g > 2\nu\beta p^{-\ell} - \beta \geq \beta(2\nu - 1), \tag{41}$$

and hence $g > 0$ since $\beta, \nu \geq 1$. Note that this implies that $\ell = 0$, for otherwise the p-adic valuation of the left-hand side of (39) would be 0. We can thus solve (39) for ε and substitute the resulting expression into (40) to get

$$4\beta^2\nu(\nu+1) - 4\nu\beta p^g + p^{2g} - p^{2g+m} = 0. \tag{42}$$

Since $g > 0$, the third and fourth terms on the left-hand side of (42) have strictly larger p-adic valuation than the second term does, so we must have $v_p(4\beta^2\nu(\nu+1)) = v_p(4\nu\beta p^g)$, that is, $v_p(\nu+1) = g$. So $\nu = -1 + \mu p^g$ for some $\mu \geq 1$ such that $p \nmid \mu$. But if we substitute this into $p^g > \beta(2\nu - 1)$ from (41) and rearrange to obtain an upper bound for μ, then (keeping in mind that $p \geq 5$ by Step 1) we obtain

$$\mu < \frac{1}{2\beta} + \frac{3}{2p^g} \leq \frac{1}{2} + \frac{3}{2 \cdot 5} = \frac{4}{5},$$

which is a contradiction. We thus have $\ell > 0$, as we wished.

Step 9. We have both $BE - 2CD = \beta p^{2n-2m+2\ell}$ and $C^2 + D^2 - BE = p^{2n-2m+2\ell}(p^{m-2\ell} - \beta)$.

Proof. These results come from using the expressions for C and D in Step 1 and those for B, E, and F in Steps 7 and 8 to write

$$BE - 2CD = p^{2n-2m+2\ell}\left(\frac{p^{m-2\ell} - \varepsilon^2}{2} - \beta\varepsilon p^\ell\right)$$

$$C^2 + D^2 - BE = p^{2n-2m+2\ell}\left(\frac{p^{m-2\ell} + \varepsilon^2}{2} + \beta\varepsilon p^\ell\right)$$

and then using (35) and (36) to simplify these expressions.

Step 10. Let $S_R = \{u \in K^\times : W_u = R\}$ for $R \in \mathcal{W}_{K,s}$. If we identify these subsets of $K^\times$ with group algebra elements as described before Lemma 5.1, then, using the definitions of $W = W^{K,s}$ from (8) in Section 5.1 and of T, U, V from Step 2, we have

$$WT = \sum_{u \in K^\times} (W_u + W_{-u})[u] = 2BS_B + E(S_C + S_D) \tag{43}$$

$$WU = \sum_{u \in K^\times} W_u W_{-u}[u] = B^2 S_B + CD(S_C + S_D) \tag{44}$$

$$WVT = \sum_{u \in K^\times} (W_u^2 + W_{-u}^2)[u] = 2B^2 S_B + (C^2 + D^2)(S_C + S_D). \tag{45}$$

Proof. The left-hand equalities follow from the definitions of T, U, and V and also Proposition 5.13 in the case of (44) and (45). The right-hand equalities follow from the fact that $W_{-u} = \tau(W_u)$ (by Step 2) and the values for W_u in Steps 1 and 6.

Step 11. We have $\beta = 1$, so $B = p^{n-m+2\ell}$.

Proof. We can eliminate $S_C + S_D$ from (43) and (44) to get

$$W(EU - CDT) = B(BE - 2CD)S_B. \tag{46}$$

Then we can multiply both sides of (46) by $\overline{W}/(B(BE - 2CD))$ to get, by Lemma 5.8 and Steps 8 and 9, that

$$\overline{W}S_B = \frac{q^2(EU - CDT)}{\beta^2 p^{3n-3m+4\ell}}. \tag{47}$$

Note that the coefficients of $\overline{W}S_B \in L[K^\times]$ are algebraic integers, while the coefficients of the right-hand side of (47) are rational numbers, so the coefficients in (47) must all be rational integers. In particular, β divides every coefficient of the numerator of the right-hand side of the above equation. Since $\gcd(q, \beta) = 1 = \gcd(\beta, \varepsilon) = \gcd(\beta, E)$ by Step 8 and (35), we must have $\beta \mid U_u$ for all $u \notin \{\pm 1\}$. If $\beta > 1$, then $\beta \nmid -1$, so $U_u \geq 0$ for every $u \neq \pm 1$ by Lemma 5.19(i). We also know that $U_1 = U_{-1} = V_{-1} > 0$ by Lemma 5.19(iii) and Step 6. But then $\sum_{u \in K^\times} U_u > 0$, which contradicts Lemma 5.19(iv). Thus $\beta = 1$ and $B = p^{n-m+2\ell}$ by Step 8.

Step 12. We have $3 \leq 3\ell < m < 4\ell$ and

$$\varepsilon^2 + 2p^\ell \varepsilon - (p^{m-2\ell} - 2) = 0. \tag{48}$$

Proof. Equation (48) comes from using Step 11 and eliminating ν from (35) and (36). Then (48) and Step 8 imply that $p^{m-3\ell} > 2\varepsilon > 1$, so $m > 3\ell \geq 3$.

Recall from Step 8 that $\varepsilon > 0$, so (48) implies $\varepsilon = -p^\ell + \sqrt{p^{2\ell} + p^{m-2\ell} - 2}$. If we assume that $m > 4\ell$, then $\varepsilon \geq -p^\ell + \sqrt{p^{2\ell} + p^{2\ell+1} - 2}$, and since $\ell > 0$ by Step 8, we obtain $\varepsilon \geq -p^\ell + \sqrt{p} \cdot p^\ell > p^\ell$ because $\sqrt{p} \geq \sqrt{5} > 2$ by Step 1. But then Steps 8 and 11 give us that $|E| = \varepsilon p^{n-m+\ell} > p^{n-m+2\ell} = |B|$, which contradicts Step 6. So $m \leq 4\ell$, and this inequality is actually strict since m is odd by Step 7.

Step 13. Let $\delta_0 = 1$ and $\delta_x = 0$ if $x \neq 0$. For any $u \in K^\times$, we have

$$V_u + V_{-u} = q\delta_{u^2-1} - 2(p^{m-2\ell} - 1)U_u.$$

Moreover, if $u \notin \{\pm 1\}$, then $U_u \in \{-1, 0\}$.

Proof. First, we eliminate S_B from (43) and (44) (respectively, (43) and (45)) and use Steps 9 and 11 to get

$$W(BT - 2U) = p^{2n-2m+2\ell}(S_C + S_D) \tag{49}$$

$$W(VT - BT) = (p^{m-2\ell} - 1)p^{2n-2m+2\ell}(S_C + S_D). \tag{50}$$

Then, we substitute (49) into (50) and use Step 11 to obtain

$$W\left(-2(p^{m-2\ell} - 1)U - VT + qT\right) = 0.$$

Note that W is a unit in $L[K^\times]$ because $W\overline{W} = q^2$ by Lemma 5.8, so

$$VT = qT - 2(p^{m-2\ell} - 1)U,$$

and hence we achieve the above general result. When $u \notin \{\pm 1\}$, we also have $U_u \in \{-1, 0\}$ since both V_u and V_{-u} are nonnegative and $U_u \geq -1$ by Lemma 5.19(i), while $-2(p^{m-2\ell} - 1)$ is strictly negative by Step 12.

Step 14. We conclude that τ does not permute $\mathcal{W}_{K,s}$ as a transposition.

Proof. Using the expression for F in Step 7 and the expression for $V_u + V_{-u}$ from Step 13, (28) becomes

$$2p^{2n-m} = \sum_{u \in \{\pm 1\}} (q^2 - 4qp^{m-2\ell} U_u) + 4p^{2m-4\ell} \sum_{u \in K^\times} U_u^2. \tag{51}$$

We now use the fact from Step 13 that $U_u \in \{-1, 0\}$ for $u \notin \{\pm 1\}$ to write $\sum_{u \in K^\times} U_u^2 = \sum_{u \in \{\pm 1\}} U_u(U_u + 1) - \sum_{u \in K^\times} U_u$. Then, since $\sum_{u \in K^\times} U_u = 0$ and $U_1 = U_{-1} = V_{-1}$ by Lemma 5.19(iii),(iv), we see that (51) simplifies to

$$p^{2n-m} = q^2 - 4qp^{m-2\ell} V_{-1} + 4p^{2m-4\ell} V_{-1}(V_{-1} + 1). \tag{52}$$

We also have from Step 6 that $2V_{-1} = B(1 - E/q)$, so $2p^{m-2\ell} V_{-1} = q - E$ by Step 11. Using this fact, the expression for E in Step 8, and (48) in (52), we obtain

$$\begin{aligned} p^{2n-m} &= q^2 - 2q(q - E) + 2p^{m-2\ell}(q - E) + (q - E)^2 \\ &= \varepsilon^2 p^{2n-2m+2\ell} + 2\varepsilon p^{n-\ell} + 2p^{n+m-2\ell} \\ &= p^{2n-m} - 2\varepsilon p^{2n-2m+3\ell} - 2p^{2n-2m+2\ell} + 2\varepsilon p^{n-\ell} + 2p^{n+m-2\ell}, \end{aligned}$$

that is,

$$p^{2n-2m+2\ell}(1 + \varepsilon p^\ell) = p^{n-\ell}(\varepsilon + p^{m-\ell}). \tag{53}$$

Since $\ell > 0$ and $m > \ell$ by Step 12 and since $p \nmid \varepsilon$ (see Step 8), p-adic valuation shows that $2n - 2m + 2\ell = n - \ell$. Then divide (53) by $p^{n-\ell} = p^{2n-2m+2\ell}$ and rearrange to obtain

$$\varepsilon(p^\ell - 1) = p^{m-\ell} - 1.$$

This means that $p^\ell - 1 \mid p^{m-\ell} - 1$, which implies that $\ell \mid m - \ell$, and so $\ell \mid m$. But $3\ell < m < 4\ell$ by Step 12, so we have a contradiction. □

Now we are ready to prove Theorem 1.5 (which was restated at the beginning of this section as Theorem 6.1).

Proof of Theorem 1.5. Suppose $|\mathcal{W}_{K,s}| = 4$. Since τ permutes the elements of $\mathcal{W}_{K,s}$ (see (4)), τ must act trivially, as a transposition (while keeping two values fixed), as a composition of two disjoint transpositions, as a 3-cycle (while keeping one value fixed), or as a 4-cycle on $\mathcal{W}_{K,s}$. But Propositions 6.2, 6.3, and 6.5 exclude the possibilities that τ acts as a 4-cycle, as a 3-cycle, and as a transposition, respectively, while Proposition 6.4 states that τ permutes $\mathcal{W}_{K,s}$ as a composition of two disjoint transpositions precisely when $q = 5$ and $s \equiv 3 \pmod 4$, in which case $\mathcal{W}_{K,s} = \{(5 \pm \sqrt{5})/2, \pm\sqrt{5}\}$. That is, other than the aforementioned case, τ can only act trivially on $\mathcal{W}_{K,s}$, and hence $\mathcal{W}_{K,s}$ is rational by Proposition 2.1, as we wished to prove. □

Acknowledgements

The authors thank Jason Lo and an anonymous reviewer for helpful suggestions.

References

[AKL15] Yves Aubry, Daniel J. Katz, and Philippe Langevin. Cyclotomy of Weil sums of binomials. *J. Number Theory*, 154:160–178, 2015.

[Aku65] N. M. Akuliničev. Bounds for rational trigonometric sums of a special type. *Dokl. Akad. Nauk SSSR*, 161:743–745, 1965.

[Car78] L. Carlitz. A note on exponential sums. *Math. Scand.*, 42(1):39–48, 1978.

[Car79] L. Carlitz. Explicit evaluation of certain exponential sums. *Math. Scand.*, 44(1):5–16, 1979.

[Cou98] Robert S. Coulter. Further evaluations of Weil sums. *Acta Arith.*, 86(3):217–226, 1998.

[CP03] Todd Cochrane and Christopher Pinner. Stepanov's method applied to binomial exponential sums. *Q. J. Math.*, 54(3):243–255, 2003.

[CP11] Todd Cochrane and Christopher Pinner. Explicit bounds on monomial and binomial exponential sums. *Q. J. Math.*, 62(2):323–349, 2011.

[DFHR06] Hans Dobbertin, Patrick Felke, Tor Helleseth, and Petri Rosendahl. Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums. *IEEE Trans. Inform. Theory*, 52(2):613–627, 2006.

[DH36] H. Davenport and H. Heilbronn. On an exponential sum. *Proc. London Math. Soc. (2)*, 41(6):449–453, 1936.

[Dob98] Hans Dobbertin. One-to-one highly nonlinear power functions on $\mathrm{GF}(2^n)$. *Appl. Algebra Engrg. Comm. Comput.*, 9(2):139–152, 1998.

[Fen12] Tao Feng. On cyclic codes of length $2^{2^r} - 1$ with two zeros whose dual codes have three weights. *Des. Codes Cryptogr.*, 62(3):253–258, 2012.

[Hel76] Tor Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Math.*, 16(3):209–232, 1976.

[HR05] Tor Helleseth and Petri Rosendahl. New pairs of m-sequences with 4-level cross-correlation. *Finite Fields Appl.*, 11(4):674–683, 2005.

[Kar67] A. A. Karatsuba. Estimates of complete trigonometric sums. *Mat. Zametki*, 1(2):199–208, 1967.

[Kat12] Daniel 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.

[Kat15] Daniel J. Katz. Divisibility of Weil sums of binomials. *Proc. Amer. Math. Soc.*, 143(11):4623–4632, 2015.

[Kat19] Daniel J. Katz. Weil sums of binomials: properties, applications and open problems. In Kai-Uwe Schmidt and Arne Winterhof, editors, *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications*, volume 23 of *Radon Ser. Comput. Appl. Math.*, pages 109–134. De Gruyter, Berlin, Boston, 2019.

[KL89] Nicholas Katz and Ron 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.

[KL16] Daniel J. Katz and Philippe Langevin. New open problems related to old conjectures by Helleseth. *Cryptogr. Commun.*, 8(2):175–189, 2016.

[Klo27] 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.

[Lan90] Serge Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.

[LW87] Gilles Lachaud and Jacques 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.

[Nih72] Yoji Niho. *Multi-valued cross-correlation function between two maximal linear recursive sequences*. PhD thesis, University of Southern California, Los Angeles, 1972.

[SV20] Igor E. Shparlinski and José Felipe Voloch. Binomial exponential sums. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 21:931–941, 2020.

[Tra70] Herbert Mitchell Trachtenberg. *On the cross-correlation functions of maximal linear sequences*. PhD thesis, University of Southern California, Los Angeles, 1970.

[XHW14] Yongbo Xia, Tor Helleseth, and Gaofei Wu. A note on cross-correlation distribution between a ternary m-sequence and its decimated sequence. In *Sequences and their applications—SETA 2014*, volume 8865 of *Lecture Notes in Comput. Sci.*, pages 249–259. Springer, Cham, 2014.

[ZLFG14] Tao Zhang, Shuxing Li, Tao Feng, and Gennian Ge. Some new results on the cross correlation of m-sequences. *IEEE Trans. Inform. Theory*, 60(5):3062–3068, 2014.