5-24-2021

On Properties of Weil Sums of Binomials

Liem P. Nguyen

ON PROPERTIES OF WEIL SUMS OF BINOMIALS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Liem Nguyen
B.S., University of Wisconsin Oshkosh, 2011
M.S., Clemson University, 2013
M.S., Louisiana State University, 2017
August 2021

Acknowledgments

This dissertation would not be possible without many support. First, I would like to express my deepest gratitude to my advisor, Dr. Ling Long, for her constant support and guidance throughout my graduate studies. Thank you for always pushing me to reach further.

I would like to thank Dr. Juhan Frank for serving on my thesis committee. I want to thank Dr. Karl Mahlburg for his excellent number theory classes, which I have learned a lot from. Thank you, Dr. James Oxley, for your advice and for being a great teaching mentor. I would like to thank Dr. Fang-Ting Tu for always supporting and believing in me, in math and in life. Thank you, Dr. Stephen Shipman, for always believing in me and being such a great friend.

I thank the LSU math department and all my friends in grad school. You have made the past few years pleasant and memorable to me. Special thanks to Bao Pham, Shashika Nuwan, and Yu-Chan Chang. I want to thank my tango family in Baton Rouge for the hugs, smile, and lovely milongas.

Last but not least, I am very grateful for my parents. I couldn't have been here without your love and support throughout my journeys. This dissertation is dedicated to you.

Table of Contents

Abstract

This dissertation explores questions regarding the Weil sum of binomials, a finite field character sum originated from information theory. The Weil spectrum counts distinct values of the Weil sum through invertible elements in the finite field. The value of these sums and the size of the Weil spectrum are of particular interest, as they link problems in information theory, coding theory, and cryptography to other areas of math such as number theory and arithmetic geometry. In the setting of Niho exponents, we prove the Vanishing Conjecture of Helleseth (1971) on the presence of zero values in the Weil spectrum and deduce bounds on the Weil sum. At certain roots of unity, we derive an exact formula for the Weil sum. Finally, we state a conjecture on when the Weil spectrum contains at least five elements, and prove it for a certain class of Niho exponents.

Chapter 1. Introduction

1.1. The Weil Sum and Motivation

Let F be a finite field of characteristic p and size $q = p^n$. Let $\mu : F \to \mathbb{C}$ be the canonical additive character, i.e $\mu(x) = \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(x)}$, where $\zeta_p = e^{2\pi i/p}$ is a pth root of unity and $\mathrm{Tr}_{F/\mathbb{F}_p}(x)$ is the absolute trace function from $F \to \mathbb{F}_p$. If L is an extension of F, i.e $|L| = q^m$ for some positive integer m, then μ extends to L by $\mu(x) = \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(\mathrm{Tr}_{L/F}(x))}$ where $\mathrm{Tr}_{L/F}(x)$ is the trace function from $L \to F$.

We are interested in a character sum of binomials over a finite field F of the form:

$$\sum_{y \in F} \mu(ay^d + by^e), \tag{1.1.1}$$

where $a, b \in F^\times$ and $d \neq e$. We say d is an **invertible exponent** over F if $\gcd(d, q-1) = 1$. In such case the power mapping $x \mapsto x^d$ permutes the elements of F.

If d and e are invertible over F then we can reparameterize the character sum above by setting $y = a^{-1/d}x^{1/e}$ to obtain

$$\sum_{x \in F} \mu(x^{d/e} + ba^{-e/d}x). \tag{1.1.2}$$

So it is natural to define the **Weil sum** for each $a \in F$ as follows:

$$W_{F,s}(a) = \sum_{x \in F} \mu(x^s - ax).$$

where $\gcd(s, q-1) = 1$.

One observes that

$$W_{F,s}(0) = \sum_{x \in F} \mu(x^s) = \sum_{x \in F} \mu(x) = 0, \tag{1.1.3}$$

since the map $x \mapsto x^s$ permutes the elements of F.

The Weil sum relates many problems from number theory to discreet mathematics. Properties of the Weil sum including its values, number of values over the finite field, and its bounds are still not well understood. We note that in Eq. (1.1.1) and Eq. (1.1.2), if $d = 1$ and $e = q - 2$, then we obtain the Kloosterman sum $\sum_{x \in F^\times} \mu(ax + bx^{-1}) = W_{F,q-2}(ab) - 1$. The Kloosterman sum has many important applications in analytic number theory; see [15]. Moreover, questions associated to these aspects can also be translated to equivalent open problems in current research in information theory and cryptography. For instance, determining the values of $W_{F,s}(a)$ for $a \in F^\times$ is equivalent to the study of cross-correlation functions between maximal linear sequences in information theory.

A maximal linear sequence, or an m-sequence has been used to generate pseudo-random sequences in communication networks. One important criterion that makes such sequences useful in remote sensing and communications is that they should have low cross-correlation (See [7, 19, 6, 20, 5, 17, 1, 2, 9]). An m-sequence over the finite field F always has the trace representation $(\mathrm{Tr}(\alpha^{sj+d}))_{j \in \mathbb{Z}/(p^n-1)\mathbb{Z}}$, where α is a primitive element of the field, d is an integer called the shift, and $\gcd(s, p^n - 1) = 1$. We usually take $d = 0$ and $s = 1$ as our reference sequence.

To measure how similar a pair of m-sequences is in a network, we define the concept of a cross correlation function between them.

Definition 1.1.1. *Let m be a positive integer, and let $f = (f_j)_{j \in \mathbb{Z}/m\mathbb{Z}}$ and $g = (g_j)_{j \in \mathbb{Z}/m\mathbb{Z}}$ be m-sequences, where $j \in \mathbb{Z}/(p^n - 1)\mathbb{Z}$. The cross correlation of f with g at shift d is defined as*

$$C_{f,g}(s) = \sum_{j \in \mathbb{Z}/m\mathbb{Z}} e^{2\pi i (f_{j+d} - g_j)/p}.$$

Consider the cross-correlation function between the sequence $f = (f_j) = (\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha^{sj}))$ and the reference sequence $g = (g_j) = (\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha^{sj}))$ at a shift d. These cross correlation functions turn out to be Weil sums:

$$\begin{aligned} C_{f,g}(d) &= \sum_{j \in \mathbb{Z}/(q-1)\mathbb{Z}} \mu(\alpha^{s(j+d)} - \alpha^j) \\ &= \sum_{j \in \mathbb{Z}/(q-1)\mathbb{Z}} \mu(\alpha^{sj} - \alpha^{j-d}) \\ &= \sum_{x \in F^\times} \mu(x^s - \alpha^{-d}x) \\ &= -1 + W_{F,s}(\alpha^{-d}). \end{aligned}$$

1.2. Properties and Conjectures

Since the Weil sum is a sum of roots of unity, it is an algebraic integer. In fact, the Weil sum is a real number. This is clear when $p = 2$ since $\zeta_2 = -1$. When p is odd, note that s is odd since $\gcd(s, q-1) = 1$. Then taking the conjugate of $W_{F,s}(a)$ yields

$$\begin{aligned} \overline{W_{F,s}(a)} &= \overline{\sum_{x \in F} \mu(x^s - ax)} \\ &= \sum_{x \in F} \overline{\mu(x^s - ax)} \\ &= \sum_{x \in F} \mu(-(x^s - ax)) \\ &= \sum_{x \in F} \mu((-x)^s - a(-x)) \\ &= W_{F,s}(a). \end{aligned}$$

So when does the Weil sum become a rational integer? This was answered in a paper of Tor Helleseth [7].

Theorem 1.2.1 (Helleseth [7]). *$W_{F,s}(a) \in \mathbb{Z}$ for all $a \in F^\times$ if and only if $s \equiv 1 \pmod{p-1}$.*

Next, it is natural to wonder what kind of value one would get from the Weil sum. We have seen that the $W_{F,s}(a)$ is always 0 at $a = 0$, and interestingly, this presence of zero value is not known for nonzero elements a. We define s to be *singular* if there is an $a \in F^\times$ such that $W_{F,s}(a) = 0$. In 1971 Tor Helleseth proposed the following conjecture [6, 7] on the presence of zero value.

Conjecture 1.2.2 (Helleseth Vanishing Conjecture). *If $q = |F| > 2$ and s is an invertible exponent over F such that $s \equiv 1 \pmod{p-1}$, then s is singular.*

Now, if we put some restrictions on the exponent s, some partial results on the Vanishing Conjecture can be obtained. For the finite field L of order $q = p^{2n}$, an exponent s is called a **Niho exponent** if s is not a power of $p \pmod{p^{2n}-1}$ and $s \equiv p^j \pmod{p^n-1}$. If $j = 0$, then such exponent is called a **normalized Niho exponent**. Niho exponents were first introduced by Yoji Niho in 1972 in his PhD thesis on the cross-correlation function between an m-sequence and its d-decimation [19]. Since then further research has been done using Niho exponents, and it has resulted in various applications in coding theory, sequence design and cryptography [16]. Moreover, the Helleseth Vanishing Conjecture was proved for Niho exponents for a field of characteristic 2 [3].

One useful fact about Weil sums with Niho exponents is that we can replace them with normalized Niho exponents due to a result discussed in Aubry, Katz and Langevin paper [22] (also see Lemma 4.2.2).

In this thesis, we prove the Helleseth Vanishing Conjecture holds true for the case of Niho exponents, i.e extending the result in [3] for all characteristics p.

Theorem 1.2.3. *Let L be a finite field where $|L| = q = p^{2n}$ for some odd prime p and positive integer n. Suppose that s is an invertible Niho exponent over L. Then s is singular.*

The next questions of interest would be how many distinct values $W_{F,s}(a)$ takes as a ranges over F, and what they are. We define the **Weil spectrum** for some fixed s to be the set $\{W_{F,s}(a) \mid a \in F^\times\}$, and say that it is **r-valued** if $|\{W_{F,s}(a) \mid a \in F^\times\}| = r$.

If s is a power of p modulo $(q-1)$, s is said to be **degenerate**. In fact, if $s \equiv p^j \pmod{q-1}$ for some nonnegative integer j, then

$$\begin{aligned} W_{F,s}(a) &= \sum_{a \in F} \mu(x^s - ax) \\ &= \sum_{a \in F} \mu(x^{p^j} - ax) \\ &= \sum_{a \in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(x^{p^j} - ax)} \\ &= \sum_{a \in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(x^{p^j}) - \mathrm{Tr}_{F/\mathbb{F}_p}(ax)} \\ &= \sum_{a \in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(x(1-a))}, \end{aligned}$$

since Trace is an additive function (see Proposition 2.2.2) and $\mathrm{Tr}_{F/\mathbb{F}_p}(x^{p^j}) = \mathrm{Tr}_{F/\mathbb{F}_p}(x)$.

From here we can easily see that for a degenerate power s, $W_{F,s}(a)$ takes only two values as follows.

Theorem 1.2.4 (Helleseth [7])**.** *If s is degenerate, then the Weil spectrum of $W_{F,s}(a)$ is two-valued over F, where*

$$W_{F,s}(a) = \begin{cases} q & \text{if } a = 1, \\ 0 & \text{otherwise} \end{cases}$$

If s is nondegenerate, then $W_{F,s}(a)$ takes at least three values over $F^\times$.

The natural question from here is: When exactly is the Weil spectrum three-valued? In fact, this does not seem to occur often. Currently, only eleven families of three-valued Weil spectra are known [22, Table 1] and [13]. These are also conjectured to be the only ones that occur. The numerical data of the rare occurrence of three-valued spectra prompted Tor Helleseth in 1971 to give the following criteria for when this three-valued property is never met [6, 7].

Conjecture 1.2.5 (Helleseth Three-valued Conjecture, 1971)**.** *Let F be a finite field of characteristic p. If $[F : \mathbb{F}_p]$ is a power of 2, then for any invertible exponent s, the spectrum of the Weil sum $W_{F,s}(a)$ is not three-valued.*

More progress has been made towards the Three-valued Conjecture in comparison to the Vanishing Conjecture, using various approaches from coding theory, cryptography and number theory [1, 2, 3, 4, 9, 11, 12, 13, 14, 18, 22]. The cases for characteristic $p = 2$ and $p = 3$ in the Three-Valued Conjecture were proven by Daniel Katz in [11] and in [12], respectively. Special families of the three-valued Weil sum for all characteristics p are also addressed via the Welch Conjecture and the Niho Conjecture. Canteaut, Charpin, and Dobbertin gave a proof to the Welch Conjecture in [2] and Hollmann and Xiang proved both the Welch and Niho Conjectures in [9].

Notice that The Helleseth Three-valued Conjecture gives a criteria for the Weil spectrum of a nondegenerate exponent to be at least four values. We propose a similar conjecture for the five-valued behavior.

Conjecture 1.2.6. *Let L be a quadratic extension of a finite field F of order p^n, where p is an odd prime. Let $s = 1 + k(p^n - 1)$ be an invertible Niho exponent over L, $d_1 = \gcd(k, p^n + 1)$, and $d_2 = \gcd(k - 1, p^n + 1)$.*

If either

(i) $d_1 + d_2 \geq 5$, *or*

(ii) $d_1 + d_2 = 3$ *and* $p^n \equiv 11 \pmod{12}$,

satisfies, then the Weil spectrum over L *is at least five-valued. Moreover, in case (i), the five values are* $\{0, -p^n, p^n, 2\alpha p^n, (2\beta+1)p^n\}$ *where* $\alpha, \beta \geq 1$ *are integers. In case (ii), at least four values are* $\{0, -p^n, p^n, 2p^n\}$.

A special case of the condition $d_1 + d_2 \geq 5$ in Conjecture 1.2.6 is $p^n \equiv 2 \pmod{3}$. Hence, we can restate the conjecture with simpler assumptions as follows.

Conjecture 1.2.7. *Let* p *be an odd prime and* L *be a quadratic extension of a finite field* F *of order* p^n. *Suppose* $s = 1 + k(p^n - 1)$ *is an invertible Niho exponent over* L. *If* $p^n \equiv 2 \pmod{3}$, *then the Weil spectrum has at least five values of the form* $\{0, -p^n, p^n, 2\alpha p^n, (2\beta+1)p^n\}$ *for integers* $\alpha, \beta \geq 1$.

Remark 1.2.8. *Since* s *is an invertible exponent over* L, $\gcd(s, p^{2n} - 1) = 1$. *Hence, if* $p^n \equiv 2 \pmod{3}$, *then* $s \equiv 1$ *or* $2 \pmod{3}$. *Thus,* $k \equiv 0 \pmod{3}$ *and* $(k-1) \equiv 2 \pmod{3}$, *or* $k \equiv 1 \pmod{3}$ *and* $(k-1) \equiv 0 \pmod{3}$. *Moreover,* $p^n + 1$ *is divisible by* 2 *and* 3. *Therefore either* d_1 *or* d_2 *in Conjecture 1.2.6 is divisible by* 3. *The same conclusion can be made for the divisibility of either* d_1 *or* d_2 *by* 2. *Hence,* $d_1 + d_2 \geq 5$.

As partial progress to our above conjectures, we show case (i) of Conjecture 1.2.6 holds true for sufficiently large primes. Finally, we obtain the proof for case (ii). We have the following theorems.

Theorem 1.2.9. *Let* L *be a quadratic extension of a finite field* F *of order* p^n, *where* p *is an odd prime and* $n \geq 2$ *is an integer. Let* $k \geq 2$ *be an integer such that* $k < \frac{p}{2} + 1$, *and* $s = 1 + k(p^n - 1)$ *be an invertible Niho exponent over* L. *Let* $d_1 = \gcd(k, p^n + 1)$, *and*

$d_2 = \gcd(k-1, p^n+1)$. *If* $d_1 + d_2 \geq 5$, *then the Weil spectrum over* L *is at least five-valued. Moreover, four of those five values are* $\{0, -p^n, 2\alpha p^n, (2\beta+1)p^n\}$, *where* $\alpha, \beta \geq 1$.

Remark 1.2.10. *If* $k = 0$ *or* 1 *then* s *is degenerate. So in general, we can take* $2 \leq k \leq p^n$, *since* $k + p^n + 1$ *gives the same exponent* $s \pmod{p^{2n}-1}$ *as* k *over* L.

For the case of $n = 1$ *in Theorem 1.2.9, taking integer* k *such that* $p^{1/2} > 2(k-1)$ *would yield the same conclusion.*

Theorem 1.2.11. *Let* L *be a quadratic extension of a finite field* F *of order* p^n, *where* p *is an odd prime. Let* $s = 1 + k(p^n - 1)$ *be an invertible Niho exponent over* L, $d_1 = \gcd(k, p^n + 1)$, *and* $d_2 = \gcd(k-1, p^n+1)$. *If* $d_1 + d_2 = 3$ *and* $p^n \equiv 11 \pmod{12}$, *then the Weil spectrum over* L *is at least five-valued. Moreover, four of those five values are* $\{0, -p^n, p^n, 2p^n\}$.

1.3. Outline of Thesis

The organization of our thesis is as follows. In Chapter 2, we review some backgrounds on finite fields, character sums from additive characters and multiplicative characters. We link the discussion of additive character sum to the Weil sum of binomials and show an interpretation of the Weil sum as a projection coefficient. The chapter ends with a discussion of how Gauss sum relates to the Weil sum. Chapter 3 discusses the power moment property of the Weil sum and show how this plays a role in our proof of the Helleseth Vanishing Conjecture in the case of Niho exponents. From here, we deduce some bounds on the Weil sum in the setting of Niho exponents. Chapter 4 first proves a formula for the Weil sum at certain roots of unity. We then move on to the discussion of Galois action over the finite field on the Weil sum values. The final section of this chapter

gives the proofs of Theorem 1.2.9 and Theorem 1.2.11. Finally, we give some concluding remarks and future directions.

Chapter 2. Preliminaries

In this chapter, we review some background on finite fields and character sums over finite fields. We will discuss character sums formed by additive characters then multiplicative characters.

2.1. Finite Fields

Throughout this discussion, we let F be a finite field of order q. The prime field of F must be of the form $\mathbb{F}_p$ for some prime p. Moreover, $q = p^n$, where $[F : \mathbb{F}_p] = n$. We recall some properties about finite fields and direct the readers to the discussion of finite fields in [8].

Theorem 2.1.1. *[8, Lemma 5.3.2] A polynomial of degree d over a field can have at most d roots in any extension field.*

Theorem 2.1.2. *[8, Theorem 7.1.2] The multiplicative group $F^\times$ has $q-1$ elements and is cyclic.*

Lemma 2.1.3. *F is a finite field with $q = p^n$ elements if and only if F is the splitting field of the polynomial $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$.*

Proof. Suppose F is a finite field of order $q = p^n$. Then every element of F satisfy $x^{p^n} = x$. Since $x^{p^n} - x$ has at most p^n roots over F, F contains all the roots of $x^{p^n} - x$. Hence, F is the splitting field of the polynomial $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$.

Now, suppose F is the splitting field of the polynomial $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$. Let $F' \subset F$ be the subfield containing all roots of $x^{p^n} - x$. Thus, F' is a splitting field, and $F' = F$. So $|F| = |F'| \leq p^n$. Since $x^{p^n} - x$ has a formal derivative of -1, it is separable. Therefore, $|F| = p^n$. □

Definition 2.1.4. *Let $\sigma : F \to \mathbb{F}_p$ be defined by $\sigma(x) = x^p$, for every $x \in F$. Then σ is a field automorphism called the* ***Frobenius automorphism.***

Theorem 2.1.5. *$F/\mathbb{F}_p$ is Galois and* $\mathrm{Gal}(F/\mathbb{F}_p) = \langle\sigma\rangle$.

Proof. By Lemma 2.1.3, F is the splitting field of the separable polynomial $x^{p^n} - x$ over $\mathbb{F}_p$, so $F/\mathbb{F}_p$ is Galois.

Let $\mathrm{Fix}(\langle\sigma\rangle)$ be the fixed field of $\langle\sigma\rangle$. For $x \in \mathbb{F}_p$, $\sigma(x) = x^p = x$. Hence, $\mathbb{F}_p \subset \mathrm{Fix}(\langle\sigma\rangle)$. On the other hand, every element fixed by σ is a root of the polynomial $x^p - x$ so $\mathrm{Fix}(\langle\sigma\rangle)$ has at most p elements. Since $\langle\sigma\rangle$ is a subgroup of $\mathrm{Gal}(F/\mathbb{F}_p)$ and the fixed field of $\langle\sigma\rangle$ is precisely $\mathbb{F}_p$, $\mathrm{Gal}(F/\mathbb{F}_p) = \langle\sigma\rangle$. □

The above theorem has the following consequence for an extension field of F.

Corollary 2.1.6. *Let L be a finite extension of a finite field F, with $|L| = q^m$, $|F| = q = p^n$. Then L/F is a Galois extension. Moreover,* $\mathrm{Gal}(L/F)$ *is cyclic and is generated by the general Frobenius automorphism $\tau(x) = x^{p^n}$, for every $x \in L$.*

Proof. The proof is the same as that of Theorem 2.1.5 when we replace $\mathbb{F}_p$ by F, σ by τ, and x^p by x^{p^n}. □

2.2. Additive Characters

Let $\psi : \mathbb{F}_p \to \mathbb{C}^\times$ be the homomorphism defined by $\psi(x) = \zeta_p^x = e^{2\pi i x/p}$ for all $x \in \mathbb{F}_p$ (we consider as $x \in \mathbb{Z}_p \cong \mathbb{F}_p$). This is the canonical additive character on the prime field $\mathbb{F}_p$.

Now, to define such a character for a general field F, we need to construct an additive homomorphism from this field to the prime field $\mathbb{F}_p$. We will do this generally for an extension L of degree m of a finite field F.

Definition 2.2.1. *The trace map is defined by* $\mathrm{Tr}_{L/F}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}$.

Proposition 2.2.2. *[10] Let L be an extension of degree m of a field F, where $|F| = q = p^n$. If $\alpha, \beta \in L$ and $a \in F$, then*

(1) $\mathrm{Tr}(\alpha) \in F$.

(2) $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$.

(3) $\mathrm{Tr}(a\alpha) = a\,\mathrm{Tr}(\alpha)$.

(4) Tr *is surjective.*

(5) $\mathrm{Tr}_{F/\mathbb{F}_p}(\mathrm{Tr}_{L/F}(\alpha)) = \mathrm{Tr}_{L/\mathbb{F}_p}(\alpha)$.

Proof. (1) Note that

$$\begin{aligned}(\mathrm{Tr}_{L/F}(\alpha))^q &= (\alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}})^q \\ &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} + \alpha^{q^m} \\ &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} + \alpha \\ &= \mathrm{Tr}_{L/F}(\alpha).\end{aligned}$$

Hence, $\mathrm{Tr}(\alpha) \in F$.

(2) We have that

$$\begin{aligned}\mathrm{Tr}(\alpha + \beta) &= (\alpha + \beta) + (\alpha + \beta)^q + (\alpha + \beta)^{q^2} + \cdots + (\alpha + \beta)^{q^{m-1}}) \\ &= (\alpha + \beta) + (\alpha^q + \beta^q) + (\alpha^{q^2} + \beta^{q^2}) + \cdots + (\alpha^{q^{m-1}} + \beta^{q^{m-1}}) \\ &= (\alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}) + (\beta + \beta^q + \beta^{q^2} + \cdots + \beta^{q^{m-1}}) \\ &= \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta).\end{aligned}$$

(3) We have that

$$\begin{aligned}\mathrm{Tr}(a\alpha) &= a\alpha + a^q\alpha^q + a^{q^2}\alpha^{q^2} + \cdots + a^{q^{m-1}}\alpha^{q^{m-1}} \\ &= a(\alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}) \\ &= a\,\mathrm{Tr}(\alpha).\end{aligned}$$

(4) Consider the polynomial

$$\mathrm{Tr}_{L/F}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}},$$

which has at most q^{m-1} roots in L.

Since L has q^m elements, $\mathrm{Tr}_{L/F}(\alpha) = \gamma \neq 0$, for some $\alpha \in L$.

Now, for every $c \in F$, by part (3), $\mathrm{Tr}((c/\gamma)\alpha) = c/\gamma \,\mathrm{Tr}(\alpha) = c$.

(5) We have that

$$\begin{aligned}
\mathrm{Tr}_{F/\mathbb{F}_p}(\mathrm{Tr}_{L/F}(\alpha)) &= \mathrm{Tr}_{F/\mathbb{F}_p}(\alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}) \\
&= \mathrm{Tr}_{F/\mathbb{F}_p}(\alpha) + \mathrm{Tr}_{F/\mathbb{F}_p}(\alpha^q) + \cdots + \mathrm{Tr}_{F/\mathbb{F}_p}(\alpha^{q^{m-1}}) \\
&= \mathrm{Tr}_{F/\mathbb{F}_p}(\alpha) + \mathrm{Tr}_{F/\mathbb{F}_p}(\alpha^{p^n}) + \cdots + \mathrm{Tr}_{F/\mathbb{F}_p}(\alpha^{p^{n(m-1)}}) \\
&= (\alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}) + (\alpha^{p^n} + \alpha^{p^{n+1}} + \cdots + \alpha^{p^{n+n-1}}) + \\
&\cdots + (\alpha^{p^{n(m-1)}} + \alpha^{p^{n(m-1)+1}} + \cdots + \alpha^{p^{n(m-1)+n-1}}) \\
&= \alpha + \alpha^p + \cdots + \alpha^{p^{nm-1}} \\
&= \mathrm{Tr}_{L/\mathbb{F}_p}(\alpha).
\end{aligned}$$

□

Remark 2.2.3. $\mathrm{Tr}_{F/\mathbb{F}_p}(x) = x + x^p + \cdots + x^{p^{n-1}}$ *is called the* ***absolute trace function****.*

To define a **canonical additive character** $\mu : F \to \mathbb{C}^\times$, we compose the trace map with ψ, i.e $\mu(x) = \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(x)}$. Over the extension field L, μ extends to $\mu(x) = \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(\mathrm{Tr}_{L/F}(x))}$.

Proposition 2.2.4. *[10] The additive character sum μ has the following properties:*

(1) $\mu(\alpha + \beta) = \mu(\alpha)\mu(\beta)$.

(2) There is an $\alpha \in F$ *such that* $\mu(\alpha) \neq 1$.

(3) (Orthogonal property) $\sum_{\alpha \in F} \mu(\alpha) = 0$.

Proof. (1) Since Trace is additive we have that

$$\mu(\alpha + \beta) = \zeta_p^{\mathrm{Tr}(\alpha+\beta)} = \zeta_p^{\mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta)} = \mu(\alpha)\mu(\beta).$$

(2) Since Trace map is onto, $\mathrm{Tr}(\alpha) = 1$ for some $\alpha \in F$. Then $\mu(\alpha) = \zeta_p \neq 1$.

(3) Let $\beta \in F$ such that $\mu(\beta) \neq 1$. Then

$$\begin{aligned}\mu(\beta)\sum_{\alpha\in F}\mu(\alpha) &= \sum_{\alpha\in F}\mu(b)\mu(\alpha)\\ &= \sum_{\alpha\in F}\mu(\alpha+\beta)\\ &= \sum_{\alpha\in F}\mu(\alpha),\end{aligned}$$

since the map $\alpha \mapsto \beta + \alpha$ for all $\alpha \in F$ gives a bijection on F.

Hence, $\sum_{\alpha\in F}\mu(\alpha) = 0$.

□

Definition 2.2.5. *For all functions $f, g : F \to \mathbb{C}$, we define the inner product*

$$\langle f, g\rangle = \frac{1}{q}\sum_{x\in F} f(x)\overline{g(x)},$$

where $\bar{\cdot}$ stands for complex conjugation.

For $a \in F$, let $\mu_a(x) = \mu(ax)$. Then the set of additive characters $\{\mu_a : a \in F\}$ form an orthonormal basis, with respect to the above inner product, for the space of functions from F to $\mathbb{C}$. In fact, for $a, b \in F$,

$$\begin{aligned}\langle \mu_a, \mu_b\rangle &= \frac{1}{q}\sum_{x\in F}\mu_a(x)\overline{\mu_b(x)}\\ &= \frac{1}{q}\sum_{x\in F}\zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}((a-b)x)}\\ &= \begin{cases}1 & \text{if } b = a,\\ \\ 0 & \text{if } b \neq a\end{cases},\end{aligned}$$

by the orthogonal property of additive characters in Proposition 2.2.4.

We also note that $\mu_0(x) = 1$ for all $x \in F$. One observes that the additive character $\mu(x)$ in our introduction is $\mu_1(x)$.

If we let f_s be the function $f_s(x) := \mu(x^s)$, our Weil sum is the coordinates (or the Fourier coefficients) up to a factor of $1/q$ of f_s with respect to the orthonormal basis $\{\mu_a : a \in F\}$. More precisely, the Weil sum becomes

$$\begin{aligned} W_{F,s}(a) &= \sum_{x \in F} \mu(x^s - ax) \\ &= \sum_{x \in F} \mu(x^s)\overline{\mu_a(x)} \\ &= q \cdot \langle f_s, \mu_a \rangle, \end{aligned}$$

and

$$f_s = \frac{1}{q} \sum_{a \in F} W_{F,s}(a) \cdot \mu_a.$$

On the other hand,

$$\langle f_s, f_s \rangle = 1,$$

and hence,

$$1 = \left\langle \sum_{a \in F} \frac{1}{q} W_{F,s}(a) \cdot \mu_a, \sum_{b \in F} \frac{1}{q} W_{F,s}(b) \cdot \mu_b \right\rangle = \frac{1}{q^2} \sum_{a \in F} |W_{F,s}(a)|^2.$$

The Weil sum is shown to only take real values [11, Theorem 2.1(c)], so the relation above becomes

$$1 = \frac{1}{q^2} \sum_{a \in F} W_{F,s}(a)^2. \tag{2.2.1}$$

This relation is also called the **second power moment** of the Weil sum (see Section 3.1).

2.3. Multiplicative Characters

A multiplicative character on $\mathbb{F}_p$ is a homomorphism $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$. The trivial multiplicative character is defined by $\epsilon(a) = 1$ for all $a \in \mathbb{F}_p$. We can extend the domain to

$\mathbb{F}_p$ by letting $\epsilon(0) = 1$ and $\chi(0) = 0$ if $\chi \neq \epsilon$.

Proposition 2.3.1. *[10] Let χ be a multiplicative character and $a \in \mathbb{F}_p^\times$. Then*

(a) $\chi(1) = 1$.

(b) $\chi(a)$ *is a* $(p-1)^{st}$ *root of unity.*

(c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Proof. (a) $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$. Since $\chi(1) \neq 0$, $\chi(1) = 1$.

(b) We have that

$$1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}.$$

Thus, $\chi(a)$ is a $(p-1)^{\text{st}}$ root of unity.

(c) We have that

$$\overline{\chi(a)}\chi(a) = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a).$$

This means that $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

□

A multiplicative character sum on $\mathbb{F}_p$ is defined as $\sum_{a \in \mathbb{F}_p} \chi(a)$.

Proposition 2.3.2. *[10] Let χ be a multiplicative character. If $\chi \neq \epsilon$, then* $\sum_{a \in \mathbb{F}_p} \chi(a) = 0$.

This is called the ***orthogonal property of multiplicative characters****. If $\chi = \epsilon$, then*

$$\sum_{a \in \mathbb{F}_p} \chi(a) = p$$

Proof. Suppose $\chi \neq \epsilon$. Let $b \in \mathbb{F}_p$ be such that $\chi(b) \neq 1$. Now

$$\begin{aligned}
\chi(b) \sum_{a \in \mathbb{F}_p} \chi(a) &= \sum_{a \in \mathbb{F}_p} \chi(b)\chi(a) \\
&= \sum_{a \in \mathbb{F}_p} \chi(ba) \\
&= \sum_{a \in \mathbb{F}_p} \chi(a),
\end{aligned}$$

since $a \mapsto ba$ gives a bijection on $\mathbb{F}_p$. Since $\chi(b) \neq 1$, $\sum_{a \in \mathbb{F}_p} \chi(a) = 0$. If $\chi = \epsilon$, then

$$\sum_{a \in \mathbb{F}_p} \epsilon(a) = \sum_{a \in \mathbb{F}_p} 1 = p.$$

□

The multiplicative characters over $\mathbb{F}_p^\times$ form a group under multiplication, i.e $\chi\gamma(x) = \chi(x)\gamma(x)$ for characters χ, γ over $\mathbb{F}_p^\times$, with the trivial character ϵ as the identity element, and the inverse of χ as $\overline{\chi}$ in Proposition 2.3.1. We denote this group by $\widehat{\mathbb{F}_p}$.

Proposition 2.3.3. *[10] $\widehat{\mathbb{F}_p}$ is cyclic of order $p-1$. If $a \in \mathbb{F}_p^\times$ and $a \neq 1$, then there is a character χ such that $\chi(a) \neq 1$.*

Proof. Since $\mathbb{F}_p^\times$ is cyclic, let g be a generator for $\mathbb{F}_p^\times$.

For every $a \in \mathbb{F}_p^\times$, $a = g^l$. Then $\chi(a) = \chi(g)^l$. So we only need to determine $\chi(g)$ to find the values of χ at each element in the field.

Recall that $\chi(g)$ is a $(p-1)$st root of unity, and there are exactly $p-1$ of these. Hence, $|\widehat{\mathbb{F}_p}| \leq p-1$.

Let γ be such that

$$\gamma(g^k) = e^{2\pi i \frac{k}{p-1}}.$$

One can easily check that γ is a character.

Claim: $p-1$ is the smallest integer such that $\gamma^n = \epsilon$.

To see this , if $\gamma^n = \epsilon$ for some integer n, then

$$1 = \epsilon(g) = \gamma^n(g) = e^{2\pi i \frac{n}{p-1}}.$$

Hence, $p-1$ divides n. Since

$$\gamma^{p-1}(a) = \gamma(a)^{p-1} = \gamma(a^{p-1}) = \gamma(1) = 1,$$

we have $\gamma^{p-1} = \epsilon$. Therefore, $p-1$ is the smallest integer such that $\gamma^n = \epsilon$. Combine this fact with $|\widehat{\mathbb{F}_p}| \leq p-1$, we see that $\widehat{\mathbb{F}_p}$ has exactly $p-1$ characters. Moreover, it is cyclic with γ as its generator.

Let $a \in \mathbb{F}_p^\times$ and $a \neq 1$. Then $a = g^l$ where $p-1 \nmid l$. We have that

$$\gamma(a) = \gamma(g)^l = e^{2\pi i \frac{l}{p-1}} \neq 1.$$

□

Corollary 2.3.4. *[10] If $a \in \mathbb{F}_p^\times$ and $a \neq 1$, then $\sum_\chi \chi(a) = 0$, where the summation is over the group of characters on $\mathbb{F}_p$.*

Proof. Since $a \neq 1$, there is a character λ such that $\lambda(a) \neq 1$. We have

$$\lambda(a) \sum_\chi \chi(a) = \sum_\chi \lambda(a)\chi(a) = \sum_\chi \lambda\chi(a) = \sum_\chi \chi(a),$$

since $\lambda\chi$ runs over the group of characters. Therefore, $\sum_\chi \chi(a) = 0$. □

To extend the concept of a multiplicative character over a general field of order $q = p^n$, we need to construct a multiplicative homomorphism this field back to the prime field $\mathbb{F}_p$, similar to our construction of the additive character over a general field. This is called the norm map. We will do this generally for an extension L of a finite field F of degree m.

Definition 2.3.5. *Let $\alpha \in L$. The **norm** of α from L to F is defined by*

$$N_{L/F}(\alpha) = \alpha \cdot \alpha^q \dots \alpha^{q^{m-1}}.$$

For the norm map, we have the following properties.

Proposition 2.3.6. *[10] Let L be an extension of degree m of a field F, where $|F| = q = p^n$. If $\alpha, \beta \in L$ and $a \in F$, then*

(a) $N_{L/F}(\alpha) \in F$.

(b) $N_{L/F}(\alpha\beta) = N_{L/F}(\alpha)N_{L/F}(\beta)$.

(c) $N_{L/F}(a\alpha) = a^m N_{L/F}(\alpha)$.

(d) $N_{L/F}$ *maps* $L^\times$ *onto* $F^\times$.

(e) $N_{F/\mathbb{F}_p}(N_{L/F}(\alpha)) = N_{L/\mathbb{F}_p}(\alpha)$.

Proof. (a) We have that

$$\begin{aligned} N_{L/F}(\alpha)^q &= (\alpha \cdot \alpha^q \dots \alpha^{q^{m-1}})^q \\ &= \alpha^q \cdot \alpha^{q^2} \dots \alpha^{q^m} \\ &= \alpha^q \cdot \alpha^{q^2} \dots \alpha \\ &= N_{L/F}(\alpha). \end{aligned}$$

(b) We have that

$$\begin{aligned} N_{L/F}(\alpha\beta) &= (\alpha\beta) \cdot (\alpha\beta)^q \dots (\alpha\beta)^{q^{m-1}} \\ &= (\alpha \cdot \alpha^q \dots \alpha^{q^{m-1}}) \cdot (\beta \cdot \beta^q \dots \beta^{q^{m-1}}) \\ &= N_{L/F}(\alpha)N_{L/F}(\beta). \end{aligned}$$

(c) Since $a^q = a$, $N_{L/F}(a) = a \cdot a^q \dots a^{q^{m-1}} = a^m$.

(d) We compute the kernel of $N_{L/F}$. An element $\alpha \in Ker(N_{L/F})$ if and only if

$$1 = \alpha \cdot \alpha^q \dots \alpha^{q^{m-1}} = \alpha^{1+q+\dots+q^{m-1}} = \alpha^{\frac{q^s-1}{q-1}}.$$

Since $L^\times$ is cyclic and $\dfrac{q^s-1}{q-1} \mid q^s - 1$, the equation $x^{\frac{q^s-1}{q-1}} = 1$ has $\dfrac{q^s-1}{q-1}$ solutions.

By part (b), $N_{L/F} : L^\times \to F^\times$ is a group homomorphism and

$$Ker(N_{L/F}) = \{\alpha \in L \mid \alpha^{\frac{q^s-1}{q-1}}\}.$$

By the First Isomorphism Theorem, the image of $N_{L/F}$ has $q-1$ elements.

Therefore, $N_{L/F}$ is onto.

(e) We have that

$$\begin{aligned}
N_{F/\mathbb{F}_p}(N_{L/F}(\alpha)) &= N_{F/\mathbb{F}_p}(\alpha \cdot \alpha^q \dots \alpha^{q^{m-1}}) \\
&= N_{F/\mathbb{F}_p}(\alpha) N_{F/\mathbb{F}_p}(\alpha^q) \dots N_{F/\mathbb{F}_p}(\alpha^{q^{m-1}}) \\
&= N_{F/\mathbb{F}_p}(\alpha) N_{F/\mathbb{F}_p}(\alpha^{p^n}) \dots N_{F/\mathbb{F}_p}(\alpha^{p^{n(m-1)}}) \\
&= (\alpha \cdot \alpha^p \dots \alpha^{p^{n-1}})(\alpha^{p^n} \cdot \alpha^{p^{n+1}} \dots \alpha^{p^{n+n-1}}) \\
&\dots (\alpha^{p^{n(m-1)}} \cdot \alpha^{p^{n(m-1)+1}} \dots \alpha^{p^{n(m-1)+n-1}}) \\
&= \alpha \cdot \alpha^p \dots \alpha^{p^{nm-1}} \\
&= N_{L/\mathbb{F}_p}(\alpha).
\end{aligned}$$

□

To define a multiplicative character $\chi' : F \to \mathbb{C}^\times$, we compose the norm map with χ, i.e $\chi'(\alpha) = \chi(N_{F/\mathbb{F}_p}(\alpha))$. Over the extension field L, χ' extends to $\mu(\alpha) = \chi(N_{F/\mathbb{F}_p}(N_{L/F}(\alpha)))$. For simplicity, from now on, we will just relabel a multiplicative character over a given field χ.

2.4. Gauss Sums

In this section we review Gauss sum at a character and show how it relates to the Weil sum.

Definition 2.4.1. *Let χ be a multiplicative character on F of order $q = p^n$ and $r \in F$. The Gauss sum on F at χ is defined as*

$$g_r(\chi) = \sum_{a \in F} \chi(a)\mu(ra).$$

Proposition 2.4.2. *[10] We have the following*

$$g_r(\chi) = \begin{cases} q & \text{if } r = 0 \text{ and } \chi = \epsilon, \\ 0 & \text{if } r = 0 \text{ and } \chi \neq \epsilon, \\ 0 & \text{if } r \neq 0 \text{ and } \chi = \epsilon, \\ \chi(r^{-1})g_1(\chi) & \text{otherwise.} \end{cases}$$

Proof. We have that

$$g_0(\epsilon) = \sum_{a \in F} \epsilon(a) = q.$$

If $\chi \neq \epsilon$, then

$$g_0(\chi) = \sum_{a \in F} \chi(t) = 0,$$

by the orthogonal property of multiplicative characters. If $r \neq 0$, then

$$g_r(\epsilon) = \sum_{a \in F} \mu(ra) = 0,$$

by the orthogonal property of additive characters.

If $r \neq 0$ and $\chi \neq \epsilon$, then

$$\chi(r)g_r(\chi) = \chi(r) \sum_{a \in F} \chi(a)\mu(ra) = \sum_{a \in F^\times} \chi(ra)\mu(ra) = g_1(\chi)$$

Hence, $g_r(\chi) = \chi(r^{-1})g_1(\chi)$. □

One sees that the Gauss sum can be viewed as the discrete Fourier transform of the character χ at m. This realization can be further generalized in other exponential or character sums to give a useful perspective to study an exponential function of interest by understanding its Fourier transform with a character. This is one of the main reasons why

exponential and character sums would naturally arise in various settings. For instance, in the finite field setting, functions including the exponential functions can be expressed using the set of additive characters, whose coefficients can be computed using discrete Fourier transforms. This proves to be extremely useful in working with functions over finite fields.

Consider $g_1(\chi) = \sum_{a \in F} \chi(a)\mu(a) = \sum_{a \in F^\times} \chi(a)\mu(a)$. Note that

$$\begin{aligned}
\overline{g_1(\chi)} &= \sum_{a \in F} \overline{\chi(a)\mu(a)} \\
&= \sum_{a \in F} \overline{\chi(a)}\mu(-a) \\
&= \chi(-1) \sum_{a \in F} \overline{\chi(-a)}\mu(-a) \\
&= \chi(-1) g_1(\overline{\chi}).
\end{aligned}$$

Now, we consider the absolute value of $g_1(\chi)$.

Proposition 2.4.3. *If $\chi \neq \epsilon$, then $|g_1(\chi)| = \sqrt{q}$.*

Proof. Let $r \neq 0$. By Proposition 2.4.2,

$$\overline{g_r(\chi)} = \overline{\chi(r^{-1})g_1(\chi)} = \chi(r)\overline{g_1(\chi)},$$

and

$$g_r(\chi) = \chi(r^{-1})g(\chi).$$

Hence,

$$g_r(\chi)\overline{g_r(\chi)} = \chi(r^{-1})\chi(r)g_1(\chi)\overline{g_1(\chi)} = |g_1(\chi)|^2. \tag{2.4.1}$$

Summing the right hand side of Eq. (2.4.1) over all $r \in F$ we have

$$\sum_{r\in F}|g_1(\chi)|^2= (q-1)|g_1(\chi)|^2,$$

because $g_0(\chi) = 0$.

We also have that

$$\begin{aligned}\sum_{r\in F} g_r(\chi)\overline{g_r(\chi)} &= \sum_{r\in F}\left(\sum_{a\in F}\chi(a)\mu(ra)\right)\left(\sum_{b\in F}\overline{\chi(b)\mu(rb)}\right)\\ &= \sum_{r\in F}\sum_{a\in F}\sum_{b\in F}\chi(a)\overline{\chi(b)}\mu(ra-rb)\\ &= \sum_{a\in F}\sum_{b\in F}\chi(a)\overline{\chi(b)}\left(\sum_{r\in F}\mu(r(a-b))\right).\end{aligned}$$

If $a = b$ then the inner sum becomes q. If $a \neq b$, then it is 0.

We can rewrite the above sum

$$\sum_{r\in F} g_r(\chi)\overline{g_r(\chi)} = \sum_{a\in F}\chi(a)\overline{\chi(a)}q = (q-1)q.$$

It now follows that

$$(q-1)|g_1(\chi)|^2= (q-1)q,$$

or $|g_1(\chi)|= \sqrt{q}$. □

Finally, we are interested to relate the Weil sum to the Gauss sum. This is discussed extensively in [22].

By Fourier inversion, if $a \in F^\times$, we have that

$$\mu(a) = \frac{1}{q-1}\sum_{\chi\in\widehat{F^\times}} g_1(\chi)\overline{\chi}(a).$$

Hence, for $a \in F^\times$,

$$\begin{aligned}
W_{F,s}(a) &= \sum_{x\in F} \mu(x^s - ax) \\
&= 1 + \sum_{x\in F^\times} \mu(x^s)\overline{\mu(ax)} \\
&= 1 + \frac{1}{(q-1)^2} \sum_{x\in F^\times} \left(\sum_{\chi\in\widehat{F^\times}} g_1(\chi)\overline{\chi}(x^s) \right) \left(\sum_{\varphi\in\widehat{F^\times}} g_1(\overline{\varphi})\varphi(-ax) \right) \\
&= 1 + \frac{1}{(q-1)^2} \sum_{x\in F^\times} \sum_{\chi,\varphi\in\widehat{F^\times}} g_1(\chi)g_1(\overline{\varphi})\overline{\chi}^s(x)\varphi(-a)\varphi(x) \\
&= 1 + \frac{1}{(q-1)^2} \sum_{\chi,\varphi\in\widehat{F^\times}} g_1(\chi)g_1(\overline{\varphi})\varphi(-a) \left(\sum_{x\in F^\times} \overline{\chi}^s\varphi(x) \right) \\
&= 1 + \frac{1}{(q-1)^2} \sum_{\substack{\chi,\varphi\in\widehat{F^\times} \\ \varphi=\chi^s}} g_1(\chi)g_1(\overline{\varphi})\varphi(-a) \left(\sum_{x\in F^\times} \overline{\chi}^s\varphi(x) \right) \\
&= 1 + \frac{1}{(q-1)} \sum_{\chi\in\widehat{F^\times}} g_1(\chi)g_1(\overline{\chi}^s)\chi^s(-a) \\
&= \frac{q}{q-1} + \frac{1}{(q-1)} \sum_{\substack{\chi\in\widehat{F^\times} \\ \chi\neq\epsilon}} g_1(\chi)g_1(\overline{\chi}^s)\chi^s(-a).
\end{aligned}$$

Chapter 3. Weil Sums of Binomials

3.1. Power Moments

Relation (2.2.1) can also be proved using the cross-correlation function in [11]. In fact, it is called the second power moment of the Weil sum. In general we can consider the summation of all Weil sums in the finite field raised to a positive integer m. This is called the mth power moment. For the first few moments we have the following result which was proved in [11].

Lemma 3.1.1. *[11] Let F be a finite field of order p^n and s be a fixed invertible exponent. Then*

(i) $\sum_{a\in F} W_{F,s}(a) = p^n$,

(ii) $\sum_{a\in F} W_{F,s}(a)^2 = p^{2n}$, *and*

(iii) $\sum_{a\in F} W_{F,s}(a)^3 = p^{2n}\cdot|R|$, *where* $R = \{x \in F \mid (1-x)^s + x^s - 1 = 0\}$.

As for the settings of a quadratic extension L over F, we have the following moment property of the Weil sum in different orbits under the multiplication action of $F^\times$ on $L^\times$.

Lemma 3.1.2. *Let F be a finite field of order p^n and L be a quadratic extension of F. Suppose that s is an invertible exponent over L and $s \equiv 1 \pmod{p^n-1}$. Then for a fixed $b \in L^\times$,*

$$\sum_{a\in F} W_{L,s}(ab) = \begin{cases} p^{2n} & \text{if } b \in F^\times, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The first case for $b \in F$ was proved in [22, lemma 2.5]. We restate that proof here, then prove the second equality afterwards.

Case 1: Suppose $b \in F^\times$.

We have that

$$\begin{aligned}\sum_{a\in F} W_{L,s}(ab) &= \sum_{a\in F} W_{L,s}(a) \\ &= \sum_{a\in F}\sum_{x\in L} \mu(x^s - ax) \\ &= \sum_{x\in L} \mu(x^s) \sum_{a\in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(-a(Tr_{L/F}(x)))}.\end{aligned}$$

For each $x \in L$ such that $u = \mathrm{Tr}_{L/F}(x) \neq 0$, then the inner sum becomes

$$\sum_{a\in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(-au)} = 0.$$

Hence the above sum becomes

$$\sum_{a\in F} W_{L,s}(a) = p^n \cdot \sum_{\substack{x\in L \\ \mathrm{Tr}_{L/F}(x)=0}} \mu(x^s).$$

Notice that if $\mathrm{Tr}_{L/F}(x) = 0$, then $0 = \mathrm{Tr}_{L/F}(x) = x^{p^n} + x$, or $x^{p^n} = -x$. Hence, $\mathrm{Tr}_{L/F}(x^s) = x^{sp^n} + x^s = (-x)^s + x^s$. If s is odd then this makes $\mathrm{Tr}_{L/F}(x^s) = 0$. Now, suppose s is even. Since $\gcd(s, q-1) = 1$, this case is only possible if $p = 2$. Then $\mathrm{Tr}_{L/F}(x^s) = 2x^s = 0$. Thus,

$$\sum_{a\in F} W_{L,s}(a) = p^n \cdot \sum_{\substack{x\in L \\ \mathrm{Tr}_{L/F}(x)=0}} 1 = p^{2n}.$$

For odd p, the last equality follows since the elements in L such that $0 = \mathrm{Tr}_{L/F}(x) = x^{p^n} + x$ (or $x^{p^n} = -x$) are precisely 0 or in $H \setminus F^\times$, where H is the unique subgroup of $L^\times$ with $[H : F^\times] = 2$. For $p = 2$, the equality follows since $0 = \mathrm{Tr}_{L/F}(x) = x^{2^n} + x = x^{2^n} - x$ means $x \in F$.

Case 2: Suppose $b \notin F^\times$.

Observe that

$$\sum_{a\in F} W_{L,s}(ab) = \sum_{a\in F}\sum_{x\in L} \mu(x^s - abx)$$
$$= \sum_{x\in L} \mu(x^s) \sum_{a\in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(-a(Tr_{L/F}(bx)))}.$$

For each $x \in L$ such that $u = \mathrm{Tr}_{L/F}(bx) \neq 0$, then the inner sum becomes

$$\sum_{a\in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(-au)} = 0.$$

Hence,

$$\sum_{a\in F} W_{L,s}(ab) = p^n \cdot \sum_{\substack{x\in L \\ \mathrm{Tr}_{L/F}(bx)=0}} \mu(x^s).$$

Now we consider the equation $0 = \mathrm{Tr}_{L/F}(y) = y^{p^n} + y = y(y^{p^n-1} + 1)$ over L. Note that the polynomial $y^{p^n} + y$ has formal derivative of 1 so it is separable over L with p^n distinct roots. Let x_0 be a non-zero element such that bx_0 is a nonzero solution to $\mathrm{Tr}_{L/F}(y) = 0$. Then all the roots of the polynomial are of the form cbx_0, where $c \in F$. Note that $\mathrm{Tr}_{L/F}(x_0) \neq 0$ because $b \notin F$.

Now, suppose that $0 = \mathrm{Tr}_{L/F}(x_0^s) = x_0^s(1 + x_0^{s(p^n-1)})$. This means $x_0^{s(p^n-1)} = -1$ since x_0 is nonzero. Then $x_0^{p^n-1} = (-1)^{1/s}$, where $1/s$ is the inverse of s modulo $p^{2n} - 1$. If p is odd, then $1/s$ is odd and $x_0^{p^n-1} = -1$, which contradicts $\mathrm{Tr}_{L/F}(x_0) \neq 0$. If $p = 2$, then $x_0^{p^n-1} = 1$. This also contradicts $\mathrm{Tr}_{L/F}(x_0) \neq 0$ in $L = \mathbb{F}_{2^{2n}}$. Therefore, $\mathrm{Tr}_{L/F}(x_0^s) \neq 0$.

Hence,

$$\begin{aligned}\sum_{a\in F} W_{L,s}(ab) &= p^n \cdot \sum_{c\in F} \mu((cx_0)^s) \\ &= p^n \cdot \sum_{c\in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(c\,\mathrm{Tr}_{L/F}(x_0^s))} \\ &= 0.\end{aligned}$$

Note that the second-to-last equality follows from $s \equiv 1 \pmod{p^n - 1}$ and $c^s = c$ in F.

□

The conclusion of Lemma 3.1.2 also implies the first moment property of the Weil sum.

3.2. The Helleseth Vanishing Conjecture in the Case of Niho Exponents

Our goal in this section is to prove the Vanishing Conjecture for the case of Niho exponent s:

Theorem 3.2.1. *Let L be a finite field where $q = p^{2n}$ for some odd prime p and positive integer n. Suppose that s is an invertible Niho exponent over L. Then s is singular.*

We first start with a lemma that gives a formula for Weil sum $W_{L,s}(a)$ based on the cardinality of a relevant set.

Lemma 3.2.2. *Let L be the quadratic extension of the finite field F. Assume that s is an invertible Niho exponent over L. Let $K_{a,s} = \{x \in L^\times \mid \mathrm{Tr}_{L/F}(x^s - ax) = 0\}$.*

Then $|K_{a,s}|$ is a multiple of $(p^n - 1)$ and

$$W_{L,s}(a) = p^n \cdot \frac{|K_{a,s}|}{p^n - 1} - p^n.$$

Furthermore, $W_{L,s}(a)$ is divisible by p^n.

Remark 3.2.3. *The first statement of the theorem was also proved in [22].*

Proof. By Lemma 4.2.2, we can replace the condition $s \equiv p^j \pmod{p^n-1}$ by $s \equiv 1 \pmod{p^n-1}$.

As seen in the proof of Lemma 3.1.2, the equation $y^{p^n}+y=0$ has p^n distinct roots over L. Hence,

$$|K_{0,s}| = |\{x \in L^\times \mid (x^s)^{p^n} + x^s = 0\}| = p^n - 1.$$

So the identity $0 = W_{L,s}(0) = p^n \cdot \dfrac{|K_{0,s}|}{p^n-1} - p^n$ holds. We now assume $a \neq 0$.

We have

$$W_{L,s}(a) = \sum_{x \in L^\times} \mu(x^s - ax) + \mu(0) = \sum_{x \in L^\times} \mu(x^s - ax) + 1.$$

For any $y \in L^\times$, we can write $y = bx$ for some $b \in F^\times$, and

$$\mathrm{Tr}_{L/F}((bx)^s - a(bx)) = \mathrm{Tr}_{L/F}(bx^s - abx) = b\,\mathrm{Tr}_{L/F}(x^s - ax).$$

Therefore, each element y in the coset $\bar{x} := xF^\times$ either lies in $K_{a,s}$ or not depending on whether x lies in $K_{a,s}$ or not. This implies that $|K_{a,s}|$ is a multiple of $|F^\times| = p^n - 1$. We then rewrite $\displaystyle\sum_{x \in L^\times} \mu(x^s - ax)$ as follows.

$$\begin{aligned}
\sum_{x \in L^\times} \mu(x^s - ax) &= \sum_{x \in \{\bar{x}\}} \sum_{b \in F^\times} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(\mathrm{Tr}_{L/F}((bx)^s - a(bx)))} \\
&= \sum_{x \in \{\bar{x}\}} \sum_{b \in F^\times} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(b(\mathrm{Tr}_{L/F}(x^s - ax)))} \\
&= \sum_{x \in \{\bar{x}\}} \sum_{b \in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(b(\mathrm{Tr}_{L/F}(x^s - ax)))} - (p^n + 1).
\end{aligned}$$

If $x \notin K_{a,s}$, then for a fixed equivalence class $\bar{x}$ the inner sum

$$\sum_{b \in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(b(\mathrm{Tr}_{L/F}(x^s - ax))} = \sum_{u \in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(u)}$$

is 0; otherwise it is p^n.

Thus,

$$\begin{aligned} W_{L,s}(a) &= \frac{p^n |K_{a,s}|}{p^n - 1} - (p^n + 1) + 1 \\ &= p^n \cdot \frac{|K_{a,s}|}{p^n - 1} - p^n. \end{aligned}$$

This completes the proof.

□

Now we are ready to give a proof of Theorem 3.2.1.

Proof of Theorem 3.2.1. By Lemma 3.2.2, $W_{L,s}(a) = p^n \cdot h_a$ for some $h_a \in \mathbb{Z}$. Specifically, $h_0 = 0$ since $W_{L,s}(0) = 0$. Applying this and relation (2.2.1) to the setting of a field L of order $q = p^{2n}$, we have

$$q = p^{2n} = \sum_{a \in L^\times} h_a^2. \tag{3.2.1}$$

If $h_a = 0$ for some $a \in L^\times$, then the Vanishing conjecture holds. To prove this, we use proof by contradiction and assume that $h_a \neq 0$ for all $a \in L^\times$. If $|h_a| = 1$ for all $a \in L^\times$, then from (3.2.1), we have that $q - 1 = q$, which is not possible. So $|h_{a'}| \geq 2$ for some $a' \in L$, then

$$\sum_{a \in L^\times} h_a^2 \geq \sum_{\substack{a \in L^\times \\ a \neq a'}} h_a^2 + 2^2 = (q-2) + 4 = q + 2 > q,$$

which also contradicts (3.2.1).

So at least $W_{L,s}(a) = 0$ for some $a \in L^\times$. □

As a consequence to Theorem 3.2.1, the Helleseth Vanishing Conjecture holds true for $\mathbb{F}_{p^2}$.

Corollary 3.2.4. *Suppose s is an invertible exponent over $\mathbb{F}_{p^2}$ and $s \equiv 1 \pmod{(p-1)}$, then the Helleseth Vanishing Conjecture holds for the field $\mathbb{F}_{p^2}$.*

3.3. Bounds on the Weil Sum

Recall that F is a finite field of order $q = p^n$. First, we consider the Weil sum $W_{F,s}(a)$. Since the Weil sum is a sum of roots of unity and by triangle inequality, we always have $|W_{F,s}(a)| \leq q$. In fact, $W_{F,s}(a)$ is only equal to q if the exponent s is degenerate.

Lemma 3.3.1. *[11] If s is nondegenerate, $|W_{F,s}(a)| < q$.*

Proof. Since each p^{th} root of unity has length ≤ 1, $|W_{F,s}(a)| = q$ if and only if all the roots of unity equal 1. That means, for all $x \in F$, $\mathrm{Tr}(x^s - ax) = \mathrm{Tr}(x^s) - \mathrm{Tr}(ax) = 0$. In other words, the polynomial

$$x^s + x^{sp} + \cdots + x^{sp^{n-1}} - (ax + a^p x^p + \cdots + a^{p^{n-1}} x^{p^{n-1}}) = 0 \pmod{x^q - x}.$$

If s is nondegenerate then $s \not\equiv 1, p, \ldots, p^{n-1} \pmod{q-1}$. Hence all the exponents of x in the above polynomial are distinct modulo $q-1$ and cannot be reduced to zero modulo $x^q - x$. □

The above bound is considered a "naive" bound on the Weil sum. Using the Weil-Carlitz-Uchiyama bound on character sums in [21], we can obtain a better bound as follows.

Theorem 3.3.2. *Let F be a finite field and d a nondegenerate invertible exponent over F. Then $|W_{F,s}(a)| \leq (s-1)\sqrt{|F|}$ for every $a \in F$.*

Now we revisit our setting with a Niho exponent over a quadratic extension L over F. We utilize results in Section 3.2 to obtain bounds for $W_{L,s}(a)$.

Lemma 3.2.2 gives a formula for $W_{L,s}(a)$ based on the cardinality of the set $K_{a,s}$. By identifying field elements in $K_{a,s}$, we can bound $|K_{a,s}|$ in order to deduce bounds on $W_{L,s}(a)$.

Proposition 3.3.3. *Let $a \in F$ and p be an odd prime. Suppose $x^{2(p^n-1)} = 1$ and $x \notin F$, then $\mathrm{Tr}_{L/F}(x^s - ax) = 0$.*

Proof. Since $x^{2(p^n-1)} = 1$ and $x \notin F$, $x^{p^n-1} = -1$.

We have that $x^{(p^n-1)^2} = x^{p^{2n}-1-2(p^n-1)} = (x^{2(p^n-1)})^{-1} = 1$. Now,

$$\begin{aligned}
\mathrm{Tr}_{L/F}(x^s - ax) &= \mathrm{Tr}_{L/F}(x^s) - a\,\mathrm{Tr}_{L/F}(x) \\
&= x^s + x^{sp^n} - a(x + x^{p^n}) \\
&= x^s(1 + x^{(k(p^n-1)+1)(p^n-1)}) - ax(1 + x^{p^n-1}) \\
&= x^s(1 + x^{p^n-1}) - ax(1 + x^{p^n-1}) \\
&= 0.
\end{aligned}$$

□

Note that there are $2(p^n - 1)$ solutions for the equation $x^{2(p^n-1)} = 1$ in L, since $\gcd(2(p^n - 1), p^{2n} - 1) = 2(p^n - 1)$. This gives a bound on the size of $K_{a,s}$, hence a bound on the Weil sum.

Proposition 3.3.4. *Let $p^n \equiv 2 \pmod 3$. If $x^{3(p^n-1)} = 1$, then $\mathrm{Tr}_{L/F}(x^s - x) = 0$.*

Proof. We have that

$$\begin{aligned}\mathrm{Tr}_{L/F}(x^s - x) &= \mathrm{Tr}_{L/F}(x^s) - \mathrm{Tr}_{L/F}(x) \\ &= x^s + x^{sp^n} - (x + x^{p^n}) \\ &= x^{k(p^n-1)+1}(1 + x^{(k(p^n-1)+1)(p^n-1)}) - x(1 + x^{p^n-1}) \\ &= x(x^{k(p^n-1)} + x^{(p^n-1)(2k+1)} - 1 - x^{(p^n-1)}), \qquad (3.3.1)\end{aligned}$$

using the relation

$$x^{(p^n-1)^2} = x^{p^{2n}-1-2(p^n-1)} = x^{-2(p^n-1)} = x^{(p^n-1)}.$$

If $k \equiv 0 \pmod 3$ or $k \equiv 1 \pmod 3$, then the expression (3.3.1) becomes 0.

If $k \equiv 2 \pmod 3$, then $s \equiv 0 \pmod 3$, but $q - 1 = p^{2n} - 1 \equiv 0 \pmod 3$. So $\gcd(s, q-1) \geq 3$, which is a contradiction. □

Theorem 3.3.5. *For an odd prime p, we have the following bounds on $W_{L,s}(a)$:*

(1) If $a \in L$, then $W_{L,s}(a) \geq -p^n$.

(2) If $a \in F$, then $W_{L,s}(a) \geq 0$.

(3) In particular, $W_{L,s}(1) \geq p^n$. If $p^n \equiv 2 \pmod 3$, then $W_{L,s}(1) \geq 3p^n$.

Proof. Since $|K_{a,s}| \geq 0$, $|W_{L,s}(a)| \geq -q$ for $a \in L$.

If $a \in F$, then by Proposition 3.3.3 there are at least $2(p^n - 1) - (p^n - 1) = p^n - 1$ points in $K_{a,s}$. So $W_{L,s}(a) \geq 0$ by Lemma 3.2.2.

For part (3), if $x \in F$, then $x^s = x$ and $\mathrm{Tr}_{L/F}(x^s - x) = 0$. So such x lies in $K_{1,s}$. Combining this fact and Proposition 3.3.3, there are at least $2(p^n - 1)$ points in $K_{1,s}$.

Therefore, $W_{L,s}(1) \geq p^n$. Moreover, if $p^n \equiv 2 \pmod 3$, then there are $3(p^n - 1)$ solutions to the equation $x^{3(p^n-1)} = 1$, and by Proposition 3.3.4 and Lemma 3.2.2, $W_{L,s}(1) \geq 3p^n$. $\square$

Chapter 4. Weil Spectrum

4.1. A Formula for the Weil Sum at Roots of Unity

In this section, we begins by considering the value of the Weil sum at a root of unity in the field for certain primes p. The formula is obtained by realizing the relation between the elements in the set $K_{a,s} = \{x \in L^\times \mid \mathrm{Tr}_{L/F}(x^s - ax) = 0\}$ in Lemma 3.2.2 and the roots of unity.

Proposition 4.1.1. *Let $s = 1 + k(p^n - 1)$ be an invertible Niho exponent over L, where $2 \leq k \leq p^n$. Let $d_1 = \gcd(k, p^n + 1)$, $d_2 = \gcd(k - 1, p^n + 1)$, and t be a positive integer with $t \mid p^n + 1$. Let ζ_t be a primitive t-th root of unity in L. For $i = 1$ or 2, let*

$$\delta_{i,t} = \begin{cases} 1 & \text{if } t \mid \dfrac{p^n + 1}{d_i}, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$W_{L,s}(\zeta_t) = \begin{cases} p^n(d_1 + d_2 - 2) & \text{if } t = 1, \\ p^n(d_1\delta_{1,t} + d_2\delta_{2,t} - 1) & \text{otherwise.} \end{cases}$$

Proof. We compute $|K_{\zeta_t,s}|$ in Lemma 3.2.2. Let $x \in K_{\zeta_t,s}$ then $\mathrm{Tr}_{L/F}(x^s) = \mathrm{Tr}_{L/F}(\zeta_t x)$. We also have that $N_{L/F}(x^s) = N_{L/F}(\zeta_t x)$, since $\zeta_t^{p^n+1} = 1$. Hence, $\zeta_t x$ and x^s satisfy the same degree two minimal polynomial over F. So we can consider two cases $x^s = \zeta_t x$ or $x^s = (\zeta_t x)^{p^n}$. Let

$$L^\times = \langle g \rangle$$

for some generator g in the field. Then $x = g^i$ for some $i \in \mathbb{Z}_{p^{2n}-1}$. We can pick $\zeta_t = g^{(p^{2n}-1)j/t}$ where $\gcd(j, t) = \gcd(j, p^{2n} - 1) = 1$. For the case $x^s = \zeta_t x$, we have that

$x^{k(p^n-1)} = \zeta_t$. Then $g^{ik(p^n-1)} = g^{(p^{2n}-1)j/t}$, so

$$(p^n-1)ik \equiv \frac{(p^{2n}-1)j}{t} \pmod{p^{2n}-1}, \tag{4.1.1}$$

which implies that

$$ik \equiv \frac{(p^n+1)j}{t} \pmod{p^n+1}. \tag{4.1.2}$$

Let $d_1 = \gcd(k, p^n+1)$. Then (4.1.2) is solvable if $\frac{p^n+1}{t} \equiv 0 \pmod{d_1}$. If it is solvable then there are d_1 solutions. When $t = 1$, (4.1.2) is always solvable. Hence (4.1.1) has $d_1(p^n-1)$ solutions if $t = 1$, and $d_1\delta_{1,t}(p^n-1)$ solutions otherwise.

Similarly, for the case $x^s = (\zeta_t x)^{p^n} = \zeta_t^{-1}x^{p^n}$, we have that

$$x^{(k-1)(p^n-1)} = \zeta_t^{-1} = g^{-(p^{2n}-1)j/t}.$$

Let $d_2 = \gcd(k-1, p^n+1)$, then there are $d_2(p^n-1)$ solutions to this case if $t = 1$ and $d_2\delta_{2,t}(p^n-1)$ for other values of t. For both cases to have simultaneous solutions, we have that $\zeta_t x = x^s = (\zeta_t x)^{p^n}$. This means $x^s = \zeta_t x \in F^\times$ and $x^{s(p^n-1)} = 1$. Since the power map $x \mapsto x^s$ permutes both L and the subfield F, $x^s \in F$ if and only if $x \in F$. Therefore, we have $x \in F^\times$. We also note that $\zeta_t = x^{s-1} = x^{k(p^n-1)} = 1$.

Hence, when $t = 1$ the solutions for both cases were counted twice for $x \in F^\times$. Therefore,

$$|K_{\zeta_t,s}| = \begin{cases} (p^n-1)(d_1+d_2-1) & \text{if } t = 1, \\ (p^n-1)(d_1\delta_{1,t}+d_2\delta_{2,t}) & \text{otherwise.} \end{cases}$$

Apply this to the formula for $W_{L,s}(\zeta_t)$ in Lemma 3.2.2, we have

$$W_{L,s}(\zeta_t) = \begin{cases} p^n(d_1+d_2-2) & \text{if } t = 1, \\ p^n(d_1\delta_{1,t}+d_2\delta_{2,t}-1) & \text{otherwise.} \end{cases}$$

□

Remark 4.1.2. *Theorem 3.3.5(3), can be obtained by Proposition 4.1.1. As noted in Remark 1.2.8, for an odd prime p, either d_1 or d_2 must be divisible by 2, so $d_1 + d_2 \geq 3$. Moreover, if $p^n \equiv 2 \pmod 3$, then $d_1 + d_2 \geq 5$, and thus, $W_{L,s}(1) = p^n(d_1 + d_2 - 2) \geq 3p^n$.*

From Proposition 4.1.1, we deduce the following corollary for the Weil sum at $a = -1$.

Corollary 4.1.3. *Let p be an odd prime, L be a quadratic extension of order p^{2n} over the finite field F, s be an Niho exponent over L, and d_1, d_2 be defined as in Proposition 4.1.1. Then*

$$W_{L,s}(-1) = p^n \left(d_1 \cdot \frac{1 + (-1)^{(p^n+1)/d_1}}{2} + d_2 \cdot \frac{1 + (-1)^{(p^n+1)/d_2}}{2} - 1 \right).$$

If $p^n \equiv 3 \pmod 4$ and $d_1 + d_2 = 3$, then $W_{L,s}(-1) = 2p^n$.

Proof. Applying the formula of 4.1.1 for $t = 2$, and notice that $\delta_{1,2}$ and $\delta_{2,2}$ are precisely given by $\frac{1 + (-1)^{(p^n+1)/d_1}}{2}$ and $\frac{1 + (-1)^{(p^n+1)/d_2}}{2}$, respectively. □

4.2. Galois Action and Weil Spectrum

In this section we consider the Galois action on elements of the finite field and the influence on the Weil sum values. These discussion are from [22].

Lemma 4.2.1. *[22] Let F be a finite field of characteristic p. If $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$, then $W_{F,s}(\sigma(a)) = W_{F,s}(a)$.*

Proof. Let $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$. Galois conjugates have the same trace, so

$$\begin{aligned} W_{F,s}(a) &= \sum_{x \in F} \mu(x^s - ax) \\ &= \sum_{x \in F} \mu(\sigma(x^s - ax)) \\ &= \sum_{y \in F} \mu(y^s - \sigma(a)y) \\ &= W_{F,s}(\sigma(a)), \end{aligned}$$

where $y = \sigma(x)$. □

Lemma 4.2.2. *[22] Let F be a finite field of characteristic p and s be an invertible exponent over F. Then $W_{F,s}(a) = W_{F,p^j s}(a)$ for any $a \in F$ and $j \in \mathbb{Z}$.*

Proof. Since $x^{p^j s}$ and x^s are Galois conjugates, they have the same trace and hence, $W_{F,s}(a) = W_{F,p^j s}(a)$. □

Lemma 4.2.1 implies that we can replace Niho exponents with normalized Niho exponents in the Weil sum.

The next two results [22] show congruences between Weil sums in the finite field, which are useful in our proof of the values in the Weil spectrum in Conjecture 1.2.6.

Lemma 4.2.3. *[22] Let L be an extension of a finite field F of characteristic p. Suppose that $[L : F]$ is a power of a prime ℓ distinct from p. Then for any $a \in F$, we have*

$$W_{L,s}(a) \equiv W_{F,s}([L : F]^{1-1/s} a) \pmod{\ell},$$

where $1/s$ indicates the multiplicative inverse of $s \pmod{p-1}$.

Proof. We have that

$$W_{L,s}(a) = \sum_{x \in L} \mu(x^s - ax) \tag{4.2.1}$$

$$= \sum_{x \in F} \mu(x^s - ax) + \sum_{x \in L \setminus F} \mu(x^s - ax) \tag{4.2.2}$$

The first sum becomes

$$\begin{aligned}
\sum_{x \in F} \mu(x^s - ax) &= \sum_{x \in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(\mathrm{Tr}_{L/F}(x^s - ax))} \\
&= \sum_{x \in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}((x^s - ax)\,\mathrm{Tr}_{L/F}(1))} \\
&= \sum_{x \in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}([L:F](x^s - ax))} \\
&= \sum_{x \in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(([L:F]^{1/s}x)^s - [L:F]^{1-1/s}a([L:F]^{1/s}x))} \\
&= \sum_{x \in F} \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(y^s - [L:F]^{1-1/s}ay)} \\
&= W_{F,s}([L:F]^{1-1/s}a),
\end{aligned}$$

where $y = [L:F]^{1/s}x$.

Now, consider the second sum in Eq. (4.2.2). The action of $\mathrm{Gal}(L/F)$ partitions the set $L \setminus F$ into orbits of Galois conjugates. The size of each orbit is a power of ℓ. Let $\sigma \in \mathrm{Gal}(L/F)$. By Lemma 4.2.1,

$$\mu(x^s - ax) = \mu(\sigma(x^s - ax)) = \mu(\sigma(x)^s - a\sigma(x)).$$

Hence, in each orbit, the values are constant. Therefore, the second sum in Eq. (4.2.2) is a multiple of ℓ.

Thus,

$$W_{L,s}(a) \equiv W_{F,s}([L:F]^{1-1/s}a) \pmod{\ell}.$$

□

For Niho exponent s over L, we have the following corollary to the above lemma.

Corollary 4.2.4. *[22] Let F be a finite field of characteristic p, and let L be an extension of F with $[L:F]$ a power of a prime ℓ distinct from p. Let s be degenerate over F but not over L. Then $W_{L,s}(1) \equiv |F| \pmod{\ell}$ and $W_{L,s}(a) \equiv 0 \pmod{\ell}$ for every $a \in F \setminus \{1\}$.*

Proof. Since s is a Niho exponent, $s \equiv 1 \pmod{p^n-1} \equiv 1 \pmod{p-1}$. So $[L:F]^{1-1/s} = 1$. Hence by Eq. (4.2.2),

$$\begin{aligned} W_{L,s}(1) \equiv W_{F,s}(1) &= \sum_{x \in F} \mu(x^s - x) \\ &= \sum_{x \in F} \mu(0) \\ &= |F| \pmod{\ell}. \end{aligned}$$

Moreover, for every $a \in F \setminus \{1\}$,

$$\begin{aligned} W_{L,s}(a) \equiv W_{F,s}(a) &= \sum_{x \in F} \mu(x^s - ax) \\ &= \sum_{x \in F} \mu(x - ax) \\ &= \sum_{x \in F} \mu(x(1-a)) \\ &= 0 \pmod{\ell}. \end{aligned}$$

□

Combining this corollary with our previous results, we can deduce the following four values in the Weil spectrum in the cases of Conjecture 1.2.6.

Corollary 4.2.5. *Let L be a quadratic extension of a finite field F of order p^n, where p is an odd prime. Let $s = 1+k(p^n-1)$ be an invertible Niho exponent over L, $d_1 = \gcd(k, p^n+1)$, and $d_2 = \gcd(k-1, p^n+1)$.*

(i) If $d_1 + d_2 \geq 5$, then the spectrum of $W_{L,s}(a)$ contains at least 4 values of the form

$$\{0, -p^n, 2\alpha p^n, (2\beta+1)p^n\},$$

where $\alpha, \beta \geq 1$ are integers.

(ii) If $d_1 + d_2 = 3$ and $p^n \equiv 11 \pmod{12}$, then the spectrum of $W_{L,s}(a)$ contains

$$\{0, -p^n, 2p^n, p^n\}.$$

Proof. In both cases: By Theorem 1.2.4, the Weil spectrum contains at least three values, and one of which is 0 by Theorem 3.2.1. If all the nonzero values were positive, we would have

$$\left(\sum_{a\in L} W_{L,s}(a)\right)^2 > \sum_{a\in L} W_{L,s}^2(a).$$

This would contradicts the first and second moments in Lemma 3.1.1. Hence, the spectrum must contain at least a negative value. From Lemma 3.2.2 and Theorem 3.3.5 (part 1), this negative value must be $-p^n$.

Case (i): Apply Corollary 4.2.4 to our setting of the quadratic extension L over F, the prime $\ell = [L : F] = 2$. Then the Weil sum $W_{L,s}(a)$ admits an odd value for $a = 1$ and even values for all $a \in F \setminus \{1\}$. By Proposition 4.1.1, $W_{L,s}(1) = (d_1 + d_2 - 2)p^n \geq 3p^n$. If $W_{L,s}(a) = 0$ for all $a \in F \setminus \{1\}$, then taking $b = 1$ in Lemma 3.1.2 yields

$$p^{2n} = \sum_{a\in F} W_{L,s}(a) = W_{L,s}(1).$$

Together with the value $-p^n$, this would mean

$$\sum_{a\in L} W_{L,s}^2(a) > p^{4n},$$

contradicting to the second power moment relation 2.2.1. Hence, there is a nonzero even value for some $a \in F \setminus \{1\}$. Therefore, the Weil spectrum consists of $-p^n, 0, 2\alpha p^n$, and $(2\beta+1)p^n$, where $\alpha, \beta \geq 1$.

Case (ii): By Proposition 4.1.1, $W_{L,s}(1) = (d_1+d_2-2)p^n = p^n$. By Corollary 4.1.3, $W_{L,s}(-1) = 2p^n$. Hence the Weil spectrum in this case consists of $-p^n, 0, p^n$, and $2p^n$. □

Our numerical evidence suggests a stronger conclusion than Corollary 4.2.5 implies. This leads to Conjecture 1.2.6 and Conjecture 1.2.7 in the introduction.

4.3. A New Conjecture

In this section we give some partial results towards Conjecture 1.2.6. The idea behind the proofs of 1.2.9 and Theorem 1.2.11 is to apply the power moments in Lemma 3.1.1 to the four Weil sum values to derive a contradiction.

We first need to count the set $R = \{x \in L \mid (1-x)^s + x^s - 1 = 0\}$ in the third power momment of Lemma 3.1.1 for the case of Niho exponent s over a quadratic extension of F. We have the following lemma.

Lemma 4.3.1. *Let L be a quadratic extension of F, and $|F| = p^n$ and $k \geq 2$. Let $d_1 = \gcd(k, p^n+1)$ and $d_2 = \gcd(k-1, p^n+1)$. Then*

$$|R| = p^n + (d_1-1)(d_1-2) + (d_2-1)(d_2-2).$$

Proof. Clearly, all elements in F are in R. So $|R| \geq p^n$. Now suppose $x \in R \setminus F$.

We have that $(1-x)^s = 1-x^s$. Computing the norm $N_{L/F}$ of both sides, we get

$$\begin{aligned} N_{L/F}(1-x^s) &= 1 - x^{sp^n} - x^s + x^{s(p^n+1)} \\ &= 1 - \mathrm{Tr}_{L/F}(x^s) + N_{L/F}(x^s) \end{aligned}$$

and

$$\begin{aligned} N_{L/F}((1-x)^s) &= 1 - x^{p^n} - x + x^{p^n+1} \\ &= 1 - \mathrm{Tr}_{L/F}(x) + N_{L/F}(x). \end{aligned}$$

As $s = 1 + k(p^n - 1)$, we know $N_{L/F}(x) = N_{L/F}(x^s)$. Equating the norm of $1 - x^s$ gives us $\mathrm{Tr}_{L/F}(x) = \mathrm{Tr}_{L/F}(x^s)$.

Since the norm and trace of x and x^s are the same, they must satisfy the same degree-two minimal polynomial over F. Hence $x^s = x$ or $x^s = x^{p^n}$.

Case 1: $x^s = x$.

This implies $x^{k(p^n-1)} = 1$. Since $x \notin F$, $x^{p^n-1} \neq 1$. Now, $1 = x^{p^{2n}-1} = x^{(p^n-1)(p^n+1)}$. So a solution in this case must satisfy $x^{d_1(p^n-1)} = 1$, where $d_1 = \gcd(k, p^n+1)$. Let $L^\times = \langle g \rangle$ and $h = g^{(p^{2n}-1)/d_1}$ be an element of order d_1 in $L^\times$. Then x^{p^n-1} must be in $\langle h \rangle$. Without loss of generality, let $x^{p^n-1} = h^{t_1}$, where $1 \leq t_1 \leq d_1 - 1$.

On the other hand, $1 = x^s + (1-x)^s = x + (1-x)^s$. This implies $(1-x)^{s-1} = 1$ or $(1-x)^{k(p^n-1)} = 1$. Using the similar argument from above, we can say $(1-x)^{p^n-1} = h^{t_2}$, where $1 \leq t_2 \leq d_1 - 1$. Since $x \notin F$, $t_1 \neq t_2$.

Now,

$$\begin{aligned}(1-x)^{p^n-1} = h^{t_2} &\implies 1 - x^{p^n} = h^{t_2}(1-x) \\ &\implies 1 - h^{t_1}x = h^{t_2} - h^{t_2}x \\ &\implies x = \frac{1-h^{t_2}}{h^{t_1}-h^{t_2}}. \end{aligned} \tag{4.3.1}$$

With $1 \leq t_1, t_2 \leq d_1 - 1$ and $t_1 \neq t_2$, there are $(d_1-1)(d_1-2)$ choices for solution x.

Claim: These $(d_1-1)(d_1-2)$ choices are all distinct.

To see this, suppose there are pairs $(t_1, t_2) \neq (u_1, u_2)$, where $1 \leq t_1, u_1 \leq d_1 - 1$, satisfying

$$x = \frac{1-h^{t_2}}{h^{t_1}-h^{t_2}} = \frac{1-h^{u_2}}{h^{u_1}-h^{u_2}}.$$

Since h has order $d_1 = \gcd(k, p^n+1)$, $h^k = h^{p^n+1} = 1$. Thus, $h^{p^n} = h^{-1}$. Using this fact we compute

$$\begin{aligned} x^{p^n} &= \left(\frac{1-h^{t_2}}{h^{t_1}-h^{t_2}}\right)^{p^n} \\ &= \frac{1-h^{t_2 p^n}}{h^{t_1 p^n}-h^{t_2 p^n}} \\ &= \frac{1-h^{-t_2}}{h^{-t_1}-h^{-t_2}} \\ &= h^{t_1}\frac{1-h^{t_2}}{h^{t_1}-h^{t_2}} \\ &= h^{t_1}x. \end{aligned}$$

So $x^{p^n-1} = h^{t_1}$. Similarly we find $x^{p^n-1} = h^{u_1}$.

This means $t_1 = u_1$, since h has order d_1 and $1 \leq t_1, t_2, u_1, u_2 \leq d_1 - 1$. From here, we can reverse the implications of Eq. (4.3.1) to show $h^{t_2} = (1-x)^{p^n-1} = h^{u_2}$, which means $t_2 = u_2$.

Therefore, the $(d_1-1)(d_1-2)$ choices for x in this case are all distinct.

In the reverse direction, to show such $(d_1-1)(d_1-2)$ choices are in R, consider $x = \dfrac{1-h^{t_2}}{h^{t_1}-h^{t_2}}$, where h is defined as above, and $1 \leq t_1, t_2 \leq d_1 - 1$.

We have that

$$\begin{aligned}
(h^{t_1}-h^{t_2})^s &= (h^{t_1}-h^{t_2})^{(1+k(p^n-1))} && (4.3.2)\\
&= (h^{t_1}-h^{t_2})^{(1-k)}(h^{t_1p^n}-h^{t_2p^n})^k && (4.3.3)\\
&= (h^{t_1}-h^{t_2})^{(1-k)}(h^{-t_1}-h^{-t_2})^k \\
&= h^{-t_1k}h^{-t_2k}(h^{t_1}-h^{t_2})^{(1-k)}(h^{t_2}-h^{t_1})^k \\
&= (h^k)^{-t_1}(h^k)^{-t_2}(-1)^k(h^{t_1}-h^{t_2}) \\
&= (-1)^k(h^{t_1}-h^{t_2})
\end{aligned}$$

Similarly, we can show that

$$(h^{t_1}-1)^s = (-1)^k(h^{t_1}-1), \tag{4.3.4}$$

and

$$(1-h^{t_2})^s = (-1)^k(1-h^{t_2}). \tag{4.3.5}$$

Now,

$$\begin{aligned}
(1-x)^s + x^s - 1 &= \left(1 - \frac{1-h^{t_2}}{h^{t_1}-h^{t_2}}\right)^s + \left(\frac{1-h^{t_2}}{h^{t_1}-h^{t_2}}\right)^s - 1 \\
&= \left(\frac{(h^{t_1}-1)^s + (1-h^{t_2})^s}{(h^{t_1}-h^{t_2})^s}\right) - 1 \\
&= 0,
\end{aligned}$$

with the last equality following from relations (4.3.2), (4.3.4), and (4.3.5). Hence, such choice x is in R.

Case 2: $x^{p^n} = x^s = x^{1+k(p^n-1)}$.

This implies $x^{(k-1)(p^n-1)} = 1$. Suppose $x \notin F$. Similar to the argument in case 1 we let $d_2 = \gcd(k-1, p^n+1)$ and find solutions to the equation $x^{d_2(p^n-1)} = 1$. Let $\ell = g^{(p^{2n}-1)/d_2}$ be an element of order d_2, where g is the generator of $L^\times$ as in case 1. A quick check also yields us the relation $(1-x)^{(k-1)(p^n-1)} = 1$. Then x^{p^n-1} and $(1-x)^{p^n-1}$ must be in $\langle \ell \rangle$. Using the similar argument from above, we obtain $x = \dfrac{1-\ell^{r_2}}{\ell^{r_1}-\ell^{r_2}}$, where $1 \le r_1, r_2 \le d_2 - 1$. There are $(d_2-1)(d_2-2)$ choices for such x. Using similar arguments as Case 1, we can show that all these choices are distinct.

In the reverse direction, we first note that $\ell^k = \ell$ and $\ell^{p^n} = \ell^{-1}$, since ℓ has order $d_2 = \gcd(k-1, p^n+1)$.

Using a similar argument as in case 1, we have that

$$\begin{aligned}(\ell^{r_1}-\ell^{r_2})^s &= (\ell^{r_1}-\ell^{r_2})^{(1-k)}(\ell^{r_1 p^n}-\ell^{r_2 p^n})^k \\ &= (\ell^{r_1}-\ell^{r_2})^{(1-k)}(\ell^{-r_1}-\ell^{-r_2})^k \\ &= \ell^{-r_1 k}\ell^{-r_2 k}(\ell^{r_1}-\ell^{r_2})^{(1-k)}(\ell^{r_2}-\ell^{r_1})^k \\ &= (-1)^k \ell^{-r_1}\ell^{-r_2}(\ell^{r_1}-\ell^{r_2}) \\ &= (-1)^k(\ell^{-r_2}-\ell^{-r_1}).\end{aligned} \tag{4.3.6}$$

Similarly, we can show that

$$(\ell^{r_1}-1)^s = (-1)^k(1-\ell^{-r_1}), \tag{4.3.7}$$

and

$$(1-\ell^{r_2})^s = (-1)^k(\ell^{-r_2}-1). \tag{4.3.8}$$

By relations (4.3.6), (4.3.7), and (4.3.8), we can show that $(1-x)^s + x^s - 1 = 0$. Thus, such choice x is in R.

Hence there are $(d_2 - 1)(d_2 - 2)$ solutions of x in this case.

Note that since k and $k-1$ are coprime, d_1 and d_2 are coprime as well. Therefore, the solutions in case 1 and case 2 for $x \notin F$ are distinct.

Accounting for the solutions $x \in F$ we have $|R| = p^n + (d_1 - 1)(d_1 - 2) + (d_2 - 1)(d_2 - 2)$. □

Corollary 4.3.2. *Let $s = 1 + k(p^n - 1)$ for some integer k, $0 \leq k \leq p^n$. Then k and $2 - k + p^n$ gives the same number of solutions to the equation $(1-x)^s + x^s - 1 = 0$ for $x \in L$.*

Proof. From the proof of Lemma 4.3.1, the exponents s and sp^n give the same number of solutions to the equation $(1-x)^s + x^s - 1 = 0$ for $x \in L$. Now, $sp^n \equiv 1 + (1-k)(p^n - 1) \pmod{p^{2n} - 1}$, and $0 \leq 2 - k + p^n \leq p^n$ gives the same exponent modulo $(p^{2n} - 1)$ as $1 - k$ over L. □

Now we are ready to prove Theorem 1.2.9.

Proof of Theorem 1.2.9. According to Corollary 4.2.5, there are four values in the Weil spectrum. Suppose that these are the only ones in the spectrum. Let m_1, m_2, m_3 and m_4 be the number of elements whose Weil sum value is $-p^n, 0, 2\alpha p^n$ and $(2\beta + 1)p^n$, respectively, for integers $\alpha, \beta \geq 1$. In here $2\beta + 1 = d_1 + d_2 - 2$ from Proposition 4.1.1.

By Lemma 3.1.1 we have the following system of equations:

$$\begin{cases} m_1 + m_2 + m_3 + m_4 = p^{2n} & (4.3.9) \\ -m_1 + 2\alpha m_3 + (d_1 + d_2 - 2)m_4 = p^n & (4.3.10) \\ m_1 + 4\alpha^2 m_3 + (d_1 + d_2 - 2)^2 m_4 = p^{2n} & (4.3.11) \\ -m_1 + 8\alpha^3 m_3 + (d_1 + d_2 - 2)^3 m_4 = p^n |R|, & (4.3.12) \end{cases}$$

where $|R| = p^n + (d_1 - 1)(d_1 - 2) + (d_2 - 1)(d_2 - 2)$ from Lemma 4.3.1.

The above system has a unique solution over $\mathbb{Q}$, which is

$$m_1 = -\frac{p^n(d_1^2 + d_2^2 + (2\alpha - p^n - 3)(d_1 + d_2) - p^n(2\alpha - 3) + 4(1 - \alpha))}{(2\alpha + 1)(d_1 + d_2 - 1)}$$

$$m_2 = \frac{1}{2} \cdot \frac{p^n((d_1 + d_2)(2\alpha(p^n + 1) - p^n - 4) + d_1^2 + d_2^2 - 6\alpha(p^n + 1) + 2(2p^n + 3))}{\alpha(d_1 + d_2 - 2)}$$

$$m_3 = \frac{1}{2} \cdot \frac{p^n(d_1^2 + d_2^2 - (p^n + 4)(d_1 + d_2) + 2(2p^n + 3))}{(2\alpha - d_1 - d_2 + 2)(2\alpha + 1)\alpha}$$

$$m_4 = -\frac{p^n(d_1^2 + d_2^2 - 2p^n(\alpha - 1) - 3(d_1 + d_2) + 4 - 2\alpha)}{(2\alpha - d_1 - d_2 + 2)(d_1 + d_2 - 1)(d_1 + d_2 - 2)}.$$

From the numerator of m_3, we have that

$$\begin{aligned} d_1^2 + d_2^2 - (p^n + 4)(d_1 + d_2) + 2(2p^n + 3) &= (d_1 - 2)^2 + (d_2 - 2)^2 - (d_1 + d_2 - 4)p^n - 2 \\ &\leq (d_1 - 2)^2 + (d_2 - 2)^2 - p^n - 2, \end{aligned} \tag{4.3.13}$$

since $d_1 + d_2 - 4 \geq 1$.

Note that since $k < \frac{p}{2} + 1$, $d_1 < \frac{p}{2} + 1$ and $d_2 < \frac{p}{2}$. Hence, we can bound (4.3.13) by

$$\begin{aligned} \left(\frac{p}{2} - 1\right)^2 + \left(\frac{p}{2} - 2\right)^2 - p^n - 2 &= \frac{1}{2}p^2 - 3p - p^n + 3 \\ &\leq -\frac{1}{2}p^2 - 3p + 3 \\ &< 0, \end{aligned}$$

since $n \geq 2$.

So the numerator of m_3 is negative. Thus, the denominator of m_3, i.e $2(2\alpha - d_1 - d_2 + 2)(2\alpha + 1)\alpha$ is negative, which implies the factor $(2\alpha - d_1 - d_2 + 2) < 0$.

Now, this forces the denominator of m_4 to be negative, which implies that the expression $(d_1^2 + d_2^2 - 2p^n(\alpha - 1) - 3(d_1 + d_2) + 4 - 2\alpha)$ in the numerator of m_4 must be positive. If $\alpha \geq 2$, using the bounds for d_1 and d_2, we can bound the numerator of m_4 by

$$\begin{aligned}
(d_1^2 + d_2^2 - 2p^n(\alpha - 1) - 3(d_1 + d_2) + 4 - 2\alpha) &\leq d_1^2 + d_2^2 - 2p^n - 3(d_1 + d_2) \\
&= \left(d_1 - \frac{3}{2}\right)^2 + \left(d_2 - \frac{3}{2}\right)^2 - \frac{9}{2} - 2p^n \\
&< \left(\frac{p+2}{2} - \frac{3}{2}\right)^2 + \left(\frac{p}{2} - \frac{3}{2}\right)^2 - \frac{9}{2} - 2p^n \\
&= \frac{1}{2}p^2 - 2p - 2p^n - 2 \\
&\leq -\frac{1}{2}p^2 - 2p - 2 \\
&< 0,
\end{aligned}$$

which is a contradiction. Hence, α must be 1.

Replacing this for m_4, we have

$$m_4 = \frac{1}{2}\frac{p^n(d_1^2 + d_2^2 - 3(d_1 + d_2) + 2)}{(d_1 + d_2 - 4)(d_1 + d_2 - 2)(d_1 + d_2 - 1)}.$$

Observe that the factors in the denominator

$$(d_1 + d_2 - 4) < (d_1 + d_2 - 2) < (d_1 + d_2 - 1) < \frac{p+2}{2} + \frac{p}{2} - 1 = p.$$

Moreover, $(d_1 + d_2 - 2), (d_1 + d_2 - 1) \geq 3$, so these two factors do not divide p. Hence, for m_4 to be an integer, they must divide $d_1^2 + d_2^2 - 3(d_1 + d_2) + 2$.

However,

$$d_1^2 + d_2^2 - 3(d_1 + d_2) + 2 = (d_1 + d_2 - 4)(d_1 + d_2 - 1) - 2(d_1 - 1)(d_2 - 1)$$
$$< (d_1 + d_2 - 2)(d_1 + d_2 - 1).$$

This is a contradiction. Therefore, there must be a fifth value in this Weil spectrum. □

Remark 4.3.3. *For the case $n = 1$ in Theorem 1.2.9, taking odd prime p such that $p^{1/2} > 2(k-1)$, and following the argument in the proof of Theorem 1.2.9 with this bound would yield the same conclusion (i.e the Weil spectrum has at least five values).*

Finally, we show Theorem 1.2.11, which proves case (ii) of Conjecture 1.2.6.

Proof of Theorem 1.2.11. This proof is in a similar flavor to the proof of Theorem 1.2.9. Since $p^n \equiv 11 \pmod{12}$, $p^n \equiv 3 \pmod 4$. By Corollary 4.1.3, $W_{L,s}(-1) = 2p^n$. Since $d_1 + d_2 = 3$, $W_{L,s}(1) = p^n$ by Proposition 4.1.1. As in the last proof, let m_1, m_2, m_3 and m_4 be the number of elements whose Weil sum value is $-p^n, 0, 2\alpha p^n$ and $(2\beta+1)p^n$, but here we take $\alpha = 1, \beta = 0$, specifically. Now, $d_1 + d_2 = 3$, where $d_1, d_2 \geq 1$ (since $k \geq 2$) implies that one of them is 1 and the other one is 2. Hence, $d_1^2 + d_2^2 = 5$.

Replacing these values of $\alpha, \beta, d_1 + d_2 = 3$, and $d_1^2 + d_2^2 = 5$ in the solutions of m_1, m_2, m_3, and m_4 in the proof of Theorem 1.2.9, we obtain

$$m_1 = \frac{p^n(p^n - 1)}{3}$$
$$m_2 = \frac{p^n(p^n - 1)}{2}$$
$$m_3 = \frac{p^n(p^n - 1)}{6}$$
$$m_4 = p^n.$$

Since $p^n \equiv 11 \pmod{12}$, $p \neq 3$. Since m_1 must be an integer, $p^n \equiv 1 \pmod{3}$, but this is a contradiction. Therefore, there exists a fifth value in this Weil spectrum.

□

Chapter 5. Concluding Remarks and Future Directions

The study of Weil sum has many important applications in information theory. In this thesis, we prove the Helleseth Vanishing Conjecture for the case of Niho exponents, propose, and prove a criterion for when the Weil spectrum is at least five-valued, while giving some intermediate results on the bounds and behavior of the Weil sum values at roots of unity. There are some next-step projects naturally arise from this work:

(1) The general case of the Helleseth Vanishing Conjecture for non-Niho exponents remains open.

(2) Case (i) of Conjecture 1.2.6 for other invertible exponents s is still open. Also, the fifth value p^n in case (i) is conjectured to be in the spectrum, based on our computation data.

(3) A probabilistic approach to study the likelihood that the Weil spectrum takes a certain value is of interest. This maybe helpful in proving the fifth value p^n in case (i) of Conjecture 1.2.6. Some directions for this approach can start looking the averaging properties of the Weil sum using the m-th power moments in [11, Proposition 3.1] and Lemma 3.1.2.

(4) A different perspective for the Helleseth Vanishing Conjecture is to look at it as a counting point problem over hypersurfaces. In fact, [14] establishes that the conjecture is equivalent to the following problem:

Conjecture 5.0.1. *Let F be a finite field of characteristic p and order $q > 2$, and let S be*

an invertible exponent over F with $s \equiv 1 \pmod{p-1}$. Consider the system of equations

$$\begin{cases} x_1^s + x_2^s + \cdots + x_{q-1}^s = 0 \\ \\ b_1 x_1 + b_2 x_2 + \cdots + b_{q-1} x_{q-1} = 0, \end{cases}$$

where $(x_1, \ldots, x_{q-1}) \in F^{q-1}$ and $\{b_1, \ldots, b_{q-1}\} = F^\times$.

The Helleseth Vanishing Conjecture is equivalent to saying that the number of solutions of the above system is equal to q^{q-3}.

Bibliography

[1] Bjorn Poonen A. R. Calderbank, Gary McGuire and Michael Rubinstein, *On a conjecture of Helleseth regarding pairs of binary m-sequences*, IEEE Trans. Inform. Theory **42** (1996), no. 3, 988–990. MR 1445885

[2] Pascale Charpin Anne Canteaut and Hans Dobbertin, *Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture*, IEEE Trans. Inform. Theory **46** (2000), no. 1, 4–8. MR 1743572

[3] Pascale Charpin, *Cyclic codes with few weights and Niho exponents*, J. Combin. Theory Ser. A **108** (2004), no. 2, 247–259. MR 2098843

[4] Tao Feng, *On cyclic codes of length* $2^{2^r} - 1$ *with two zeros whose dual codes have three weights*, Des. Codes Cryptogr. **62** (2012), no. 3, 253–258. MR 2886276

[5] Richard A. Games, *The geometry of m-sequences: three-valued crosscorrelations and quadrics in finite projective geometry*, SIAM J. Algebraic Discrete Methods **7** (1986), no. 1, 43–52. MR 819704

[6] Tor Helleseth, *Krysskorrelasjonsfunksjonen mellom maksimale sekvenser over* $GF(q)$, Master's thesis, Universitetet i Bergen, 1971.

[7] ———, *Some results about the cross-correlation function between two maximal linear sequences*, Discrete Math. **16** (1976), no. 3, 209–232. MR 0429323

[8] I. N. Herstein, *Topics in algebra*, 2d ed ed., Xerox College Pub.

[9] Henk D. L. Hollmann and Qing Xiang, *A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences*, Finite Fields Appl. **7** (2001), no. 2, 253–286. MR 1826337

[10] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR 1070716

[11] Daniel J. Katz, *Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth*, J. Combin. Theory Ser. A **119** (2012), no. 8, 1644–1659. MR 2946379

[12] ———, *Divisibility of Weil sums of binomials*, Proc. Amer. Math. Soc. **143** (2015), no. 11, 4623–4632. MR 3391022

[13] Daniel J. Katz and Philippe Langevin, *Proof of a conjectured three-valued family of Weil sums of binomials*, Acta Arith. **169** (2015), no. 2, 181–199. MR 3359953

[14] ———, *New open problems related to old conjectures by Helleseth*, Cryptogr. Commun. **8** (2016), no. 2, 175–189. MR 3488215

[15] Nicholas M. Katz, *Gauss sums, kloosterman sums, and monodromy groups. (am-116)*, Princeton University Press, 1988.

[16] Nian Li and Xiangyong Zeng, *A survey on the applications of Niho exponents*, Cryptogr. Commun. **11** (2019), no. 3, 509–548. MR 3946534

[17] G. McGuire and A. R. Calderbank, *Proof of a conjecture of Sarwate and Pursley regarding pairs of binary m-sequences*, IEEE Transactions on Information Theory **41** (1995), no. 4, 1153–1155.

[18] Gary McGuire, *On certain 3-weight cyclic codes having symmetric weights and a conjecture of Helleseth*, Sequences and their applications (Bergen, 2001), Discrete Math. Theor. Comput. Sci. (Lond.), Springer, London, 2002, pp. 281–295. MR 1916139

[19] Yoji Niho, *Multi-valued cross-correlation functions between two maximal linear recursive sequences*, Ph.D. thesis, University of Southern California, Los Angeles, 1972.

[20] D. V. Sarwate and M. B. Pursley, *Crosscorrelation properties of pseudorandom and related sequences*, Proceedings of the IEEE **68** (1980), no. 5, 593–619.

[21] André Weil, *On some exponential sums*, Proceedings of the National Academy of Sciences **34** (1948), no. 5, 204–207.

[22] Daniel J. Katz Yves Aubry and Philippe Langevin, *Cyclotomy of Weil sums of binomials*, J. Number Theory **154** (2015), 160–178. MR 3339571

Vita

Liem Nguyen was born in Vietnam. She finished her undergraduate studies in mathematics and chemistry at the University of Wisconsin, Oshkosh, in 2011. She earned a master of science in mathematical sciences at Clemson University in 2013. She is currently a Ph.D. candidate in mathematics at Louisiana State University, which will be awarded in August 2021.