RESEARCH STATEMENT

LIEM NGUYEN

1. Introduction

1.1. **Motivation.** Number theory is a branch of mathematics that involves the study of integers. Its influence is vast, not just throughout mathematics, but also in realms such as physics, computer science and cryptography. Originating from problems in number theory, the method of exponential sums is a powerful tool that enables proofs of many results in the field. My research objective is to investigate different types of exponential sums and character sums and their applications in number theory and related fields.

An **exponential sum** is a finite sum of the form $S(P) = \sum_{n} e^{2\pi i f(n)}$, where $\{f(n)\}$ is a finite sequence of real numbers as n runs over all integers (or some of them) on a certain interval, and P is the number of summands [28]. Over a finite field of characteristic p, we can replace the sequence by $f(x)/p$, where $f(x)$ is a function on the field. The first example of an exponential sum was due to Gauss in his book in 1801 *Disquisitions Arithmeticae* [11], where he introduced the quadratic Gauss sum.

A **character sum** has the form $\sum_{n} \chi(n)$, where χ is a multiplicative character taken over a range in a finite field of characteristic p (or a finite ring). Character sums are closely linked to exponential sums; for instance, this can be seen in the Gauss sum $g_m(\chi) = \sum_{n=0}^{k-1} \chi(n) e^{2\pi i mn/k}$, which was introduced by Dirichlet in his studies of arithmetic progression [6]. In fact, 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 example, in the finite field setting, functions including the exponential functions can be expressed using the set of additive characters (or multiplicative characters together with the delta function at 0), whose coefficients can be computed using discrete Fourier transforms. This proves to be extremely useful in working with functions over finite fields.

The general framework surrounding exponential and character sums has been continually developed to solve a wide range of problems—from the interface of algebraic geometry, number theory and classical analysis of Fourier transforms and convolutions, to applications in combinatorics and discrete mathematics. The list of applications is immense, but to name a few: Gauss and Jacobi sums in the counting of points on variety over finite fields and the study of corresponding zeta functions [32], the study of cyclotomic fields [31], the developments of reciprocity laws [16], the study of power residue distributions [2, 30], Kloosterman sum and its applications in analytic number theory [28, 20]; for instance, in the constructions of families of Ramanujan graphs [22], hypergeometric character sums in the developments of hypergeometric functions over finite fields, and relation to traces of Hecke operators [12, 8, 23, 9].

My dissertation work involves the study of the **Weil sum**, a character sum over finite fields originating from the study of cross-correlation functions in information theory. Various aspects of the Weil sums in terms of bounds, number of distinct values (called the Weil spectrum) and divisibility are of interest due to their applications to equivalent problems in information theory (in sequence design, remote sensing, and synchronization), coding theory (weight distribution of p-arry cyclic error-correcting codes), and cryptography (s-boxes of symmetric key cryptosystems); see section 2.2 discussion for more details.

In 1971, Tor Helleseth formulated two conjectures concerning two ideas: The presence of zero value in the Weil spectrum (The Vanishing Conjecture), and the criteria for when the Weil spectrum contains more than three values (The Three-valued Conjecture) [14]. Until now, these two conjectures remain unsolved, except for some special cases. My work uses tools from algebraic number theory, finite fields, and character theory to address these conjectures, and to expand the literature knowledge of the Weil sum.

1.2. **Outline of statement.**

My main contributions are as follows:

- I proved the Helleseth Vanishing Conjecture in the case of Niho exponents (defined below) for all odd characteristics.
- I derived bounds on the Weil sum and gave an exact formula for the Weil sum at specific roots of unity.
- I conjectured a criterion for when the Weil spectrum contains at least five values and showed that it is true for a class of Weil sum.

Here is the outline of my research statement: In section 2, I discuss some background on the Weil sum, the connection to different areas, and open conjectures surrounding it. In section 3, I explain my result of the Helleseth Vanishing Conjecture for the case of Niho exponents in odd characteristics. I then propose a new conjecture on the five-valued property for the Weil sum and discuss some progress made towards this. Section 4 contains future directions of this project, followed by a list of citations.

2. Background: Weil Sum and the Helleseth Conjectures

2.1. **The Weil sum.**

Our finite field setting is as follows: 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 nonnegative integer m, then we take $\mu(x) = \zeta_p^{\mathrm{Tr}_{F/\mathbb{F}_p}(\mathrm{Tr}_{L/F}(x))}$ where $\mathrm{Tr}_{L/F}(x)$ is the trace function from $L \to F$.

We are interested in a character sum of binomials, let's say over F, of the form

$$\sum_{y\in F} \mu(ay^d + by^e), \tag{2.1}$$

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

$$\sum_{x\in F} \mu(x^{d/e} + ba^{-e/d}x). \tag{2.2}$$

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

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

One observes that

$$W_{F,s}(0) = \sum_{x\in F} \mu(x^s) = \sum_{x\in F} \mu(x) = 0, \tag{2.3}$$

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

2.2. **Connections to other problems in number theory and related fields.** Properties of the Weil sum including its values, number of values over the finite field, and its bounds are still not well understood. First, these aspects are certainly of interest from a purely number-theoretic standpoint. We note that in eq. (2.1) and eq. (2.2), 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 [20]. Second, questions associated to these aspects can also be translated to equivalent open problems in current research in cryptography, coding and information theory. For instance, in sequence design in information theory, the cross-correlation function between two p-ary maximal linear recursive sequences (called p-ary m-sequences; p-ary means the terms are taken over a finite field of characteristic p) measures how similar they are, and can be realized as a character sum, specifically as the Weil sum plus (-1). One important criterion that makes such sequences useful in remote sensing and communications is that they should have low cross-correlation (see [14, 27, 13, 29, 10, 24, 3, 4, 15]).

In coding theory, p-ary m-sequence (by restricting to a finite subsequence) above can be regarded as a codeword in the p-ary cyclic code. We can define the Hamming weight of a codeword to measure the number of substitutions to change one string to another. We can relate this weight to the cross-correlation function, which in turn relates to the Weil sum. We are interested in the distinct values of these weights, and the number of the weights, and hence the corresponding properties of the Weil sum (see [25, 5, 7] for more details).

2.3. **Properties and open conjectures.** Since $W_{F,s}(a)$ is a sum of roots of unity, $W_{F,s}(a)$ is an algebraic integer. One may ask when the sum becomes a rational integer. In fact, Tor Helleseth has stated the necessary and sufficient conditions for $W_{F,s}(a)$ to be a rational integer for every $a \in F$ in the following theorem [14].

Theorem 2.1 (Helleseth). *$W_{F,s}(a) \in \mathbb{Z}$ for all $a \in F^\times$ if and only if $s \equiv 1 \pmod{p-1}$.*

It is natural to wonder what kind of values one would get from the Weil sum. We have seen in eq. (2.3) that the $W_{F,s}(a)$ is always 0 at $a = 0$, and interestingly, this presence of zero value is not obvious for nonzero elements a. We say that s is **singular** if there is an $a \in F^\times$ such that $W_{F,s}(a) = 0$. In 1971, based on numerous computations on the cross-correlation function, Tor Helleseth proposed the conjecture [13, 14] that this presence of zero value always held.

Conjecture 2.2 (Helleseth Vanishing Conjecture, [13, 14]). *If $q = |F| > 2$ and s is an invertible exponent over F such that $s \equiv 1 \pmod{p-1}$, 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 $(q - 1)$, we call s to be **degenerate**. For any degenerate power s, we know that $W_{F,s}(a)$ takes two values via a theorem by Helleseth [14].

Theorem 2.3 (Helleseth [14]). *If s is degenerate, $W_{F,s}(a)$ 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 $F^\times$.

Now, the natural question is: When exactly is the Weil spectrum three-valued? In the same paper that Helleseth proposed the Vanishing Conjecture in 1971, he also gave another conjecture for when this three-valued property is never met [13, 14].

Conjecture 2.4 (Helleseth Three-valued Conjecture [13, 14]). *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.*

In comparison to the Vanishing Conjecture, more progress has been made to the Three-valued Conjecture using various approaches from coding theory, cryptography and number theory [3, 4, 15, 25, 5, 7, 17, 1, 18, 19]. Currently, only ten families of three-valued Weil sum are known [1, Table 1], and these are conjectured to be the only ones that occur. The cases of characteristic 2 and 3 were proven by Daniel Katz in [17, 18].

3. Main Results

We are interested in the properties and open conjectures surrounding the Weil sum in the setting of Niho exponent. For a 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 $s \equiv p^j \pmod{p^n - 1}$. Niho exponent was first introduced by Yoji Niho in 1972 in his PhD thesis on the cross-correlation function between an m-sequence and its d-decimation [27]. Since then further research has been done using Niho exponents, and it has resulted in various applications in coding theory, sequence design, and cryptography [21].

For the rest of our discussion, we take such field L of order p^{2n}, where p is an odd prime. Let s be an invertible Niho exponent over L. Then $s = 1 + k(p^n - 1)$ for some integer k. 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.

3.1. The Helleseth Vanishing Conjecture for the case of Niho exponents.

As mentioned, partial results on the Vanishing Conjecture are limited compared to the Three-valued Conjecture. It should be noted that if the spectrum is three-valued, then one of them must be 0; this is a result by D. Katz [17].

In 2004, Charpin proved the Helleseth Vanishing Conjecture for Niho exponents for fields of characteristic 2 [5]. My first main result extends this to all odd characteristic, *i.e.* proving the Helleseth Vanishing Conjecture for Niho exponents in all finite fields.

Theorem 3.1 (L. Nguyen [26]). *Suppose that s is an invertible Niho exponent over L. Then s is singular.*

3.2. Bounds on the Weil sum and some special values.

In building towards the proof of theorem 3.1, we derive some intermediate results that give the following bounds on the Weil sum.

Theorem 3.2 (L. Nguyen [26]). *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 $W_{L,s}(1) \geq 3p^n$.

At some roots of unity in the finite field L we can give a formula for the Weil sum $W_{L,s}(a)$. This is useful for my next result.

Proposition 3.3 (L. Nguyen [26]). *Let $2 \leq k \leq p^n$, $d_1 = \gcd(k, p^n + 1)$, and $d_2 = \gcd(k - 1, p^n + 1)$. Let $s = 1 + k(p^n - 1)$ be an invertible Niho exponent over L, 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

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

3.3. **The Weil spectrum: new conjecture and partial result.** In section 2.2, we discuss why the Weil spectrum is of interest. In a similar inquiry as the Three-valued Conjecture, I propose the following conjecture on when the Weil spectrum has at least five values, based on computations done in SageMath.

Conjecture 3.4. *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 3.4 is $p^n \equiv 2 \pmod 3$. Hence, we can restate part (i) of the conjecture with simpler assumptions as follows.

Conjecture 3.5. *Let $s = 1 + k(p^n - 1)$ be an invertible Niho exponent over L. If $p^n \equiv 2 \pmod 3$, then the Weil spectrum over L has at least the five values $\{0, -p^n, p^n, 2\alpha p^n, (2\beta + 1)p^n\}$ for integers $\alpha, \beta \geq 1$.*

My work was to, first, show that case (i) of conjecture 3.4 holds true for a class of Weil sum.

Theorem 3.6 (L. Nguyen [26])**.** *Let $n \geq 2$ be an integer. Let $k \geq 2$ be an integer such that $k < \dfrac{p}{2} + 1$, 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 3.7. Note that for $k = 0$ or 1, the exponent s is degenerate, so we take $k \geq 2$. For the case of $n = 1$ in theorem 3.6, taking k such that $k < \dfrac{p^{1/2}}{2} + 1$ would yield the same conclusion.

Second, I showed that case (ii) of conjecture 3.4 is true.

Theorem 3.8 (L. Nguyen [26])**.** *Given the assumptions of 3.4 where case (ii) satisfies, the Weil spectrum over L is at least five-valued. Moreover, four of those five values are $\{0, -p^n, p^n, 2p^n\}$.*

4. Future Work

There are some natural next-step projects arise from my work. I am working on some of these, and hope to continue with more in the future.

(1) The general case of the Helleseth Vanishing Conjecture remains open. I hope to be able to extend the proof to all (non-Niho) exponents.
(2) Case (i) of conjecture 3.4 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. These two aspects amount to another project.
(3) A probabilistic approach to study the likelihood that the Weil spectrum takes a certain value is of interest. As discussed in section 2.2, the question of determining certain values of the Weil sum has direct applications to study the cross-correlation functions in information theory and the Hamming weights in coding theory. Some directions for this can start from averaging properties of the Weil sum known as the m-th power moments, i.e the summation of all Weil sums in the finite field raised to a positive integer m. For the first few moments there are some results in [17, Proposition 3.1] and [26, Lemma 2.3].

References

1. Yves Aubry, Daniel J. Katz, and Philippe Langevin, *Cyclotomy of Weil sums of binomials*, J. Number Theory **154** (2015), 160–178. MR 3339571
2. D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika **4** (1957), 106–112. MR 93504
3. A. R. Calderbank, Gary McGuire, Bjorn Poonen, and Michael Rubinstein, *On a conjecture of Helleseth regarding pairs of binary m-sequences*, IEEE Trans. Inform. Theory **42** (1996), no. 3, 988–990. MR 1445885
4. Anne Canteaut, Pascale Charpin, 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
5. Pascale Charpin, *Cyclic codes with few weights and Niho exponents*, J. Combin. Theory Ser. A **108** (2004), no. 2, 247–259. MR 2098843
6. G. L. Dirichlet, *Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes. première partie.*, Journal für die reine und angewandte Mathematik (Crelles Journal) **1842**, 291 – 371.
7. 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
8. Sharon Frechette, Ken Ono, and Matthew Papanikolas, *Gaussian hypergeometric functions and traces of Hecke operators*, Int. Math. Res. Not. (2004), no. 60, 3233–3262. MR 2096220
9. Jenny Fuselier, Ling Long, Ravi Ramakrishna, Holly Swisher, and Fang-Ting Tu, *Hypergeometric functions over finite fields*, arXiv:1510.02575 [math.NT] (2019).
10. 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
11. Carl F. Gauss, *Disquisitions Arithmeticae*, Fleischer, Leipzig, 1801.
12. John Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1987), no. 1, 77–101. MR 879564
13. Tor Helleseth, *Krysskorrelasjonsfunksjonen mellom maksimale sekvenser over GF(q)*, Master's thesis, Universitetet i Bergen, 1971.
14. Tor Helleseth, *Some results about the cross-correlation function between two maximal linear sequences*, Discrete Math. **16** (1976), no. 3, 209–232. MR 0429323
15. 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
16. 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
17. 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
18. ______, *Divisibility of weil sums of binomials*, Proc. Amer. Math. Soc. **143** (2015), no. 11, 4623–4632. MR 3391022
19. Daniel J. Katz and Philippe Langevin, *New open problems related to old conjectures by Helleseth*, Cryptogr. Commun. **8** (2016), no. 2, 175–189. MR 3488215
20. Nicholas M. Katz, *Gauss sums, kloosterman sums, and monodromy groups. (am-116)*, Princeton University Press, 1988.
21. Nian Li and Xiangyong Zeng, *A survey on the applications of Niho exponents*, Cryptogr. Commun. **11** (2019), no. 3, 509–548. MR 3946534
22. Wen-Ch'ing Winnie Li, *Character sums and abelian Ramanujan graphs*, J. Number Theory **41** (1992), no. 2, 199–217, With an appendix by Ke Qin Feng and the author. MR 1164798
23. Ling Long, *Hypergeometric evaluation identities and supercongruences*, Pacific J. Math. **249** (2011), no. 2, 405–418. MR 2782677
24. 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.
25. 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
26. Liem Nguyen, *On weil sums, conjectures of helleseth and niho exponents*, arXiv:2006.15726 [math.NT] (2020).
27. Yoji Niho, *Multi-valued cross-correlation functions between two maximal linear recursive sequences*, Ph.D. thesis, University of Southern California, Los Angeles, 1972.
28. Korobov N.M, *Exponential sums and their applications*, Springer Netherlands, 1992 (English).
29. D. V. Sarwate and M. B. Pursley, *Crosscorrelation properties of pseudorandom and related sequences*, Proceedings of the IEEE **68** (1980), no. 5, 593–619.
30. Ivan Matveevich Vinogradov, *Selected works. Prepared by the Steklov Mathematical Institute of the Academy of Sciences of the USSR on the occasion of his ninetieth birthday. Ed. by L. D. Faddeev, R. V. Gamkrelidze, A. A. Karatsuba, K. K. Mardzhanishvili and E. F. Mishchenko*, Berlin etc.: Springer-Verlag. viii, 401 p. (1985)., 1985.

31. Lawrence C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1982. MR 718674

32. André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. MR 29393