J Syst Sci Complex (2021) 34: 1225–1278

# Exponential Sums over Finite Fields*

**WAN Daqing**

DOI: 10.1007/s11424-021-0066-8
Received: 10 March 2021


**Abstract** This is an expository paper on algebraic aspects of exponential sums over finite fields. This is a new direction. Various examples, results and open problems are presented along the way, with particular emphasis on Gauss periods, Kloosterman sums and one variable exponential sums. One main tool is the applications of various $p$-adic methods. For this reason, the author has also included a brief exposition of certain $p$-adic estimates of exponential sums. The material is based on the lectures given at the 2020 online number theory summer school held at Xiamen University. Notes were taken by Shaoshi Chen and Ruichen Xu.

**Keywords** Degrees of exponential sums, finite fields, Gauss sums, Kloosterman sums, $L$-functions.

## 1 Introduction

Exponential sums over finite fields are of central importance in number theory and its wide applications. Much of the modern study focuses on their analytic estimates as complex numbers. In this expository paper, we take a different point of view. Our main purpose is to view exponential sums as algebraic integers and study their degrees as algebraic numbers, see Section 3 for a precise description of our main problems to be studied. This is a new direction. Various examples, results and open problems are presented along the way, with particular emphasis on Gauss periods, Kloosterman sums and one variable exponential sums.

As it would become clear, $p$-adic methods would be particularly helpful in this global study of exponential sums. For this purpose, we have also included a brief exposition of both classical and recent results on $p$-adic estimates of exponential sums. The final part on the $p$-adic slope variation for $L$-function of higher $p$-power order exponential sums is itself another emerging new direction.

The material of this paper is based on lecture notes given at the 2020 Xiamen online number theory mini-course. The audience consists of a mixture of undergraduate students, graduate

WAN Daqing
*Department of Mathematics, University of California, Irvine, CA* 92697-3875*, USA.*
Email: dwan@math.uci.edu.
*This paper was partially supported by the National Natural Science of Foundation under Grant No. 1900929.
◇ *This paper was recommended for publication by Editor CHEN Shaoshi.*

students and young people working in number theory and related applied areas. For this reason, we have tried to keep the background as minimal as possible. It is a pleasure to thank Xiamen University to organize this fruitful and enjoyable summer school. I would also like to thank the participants for their many interesting questions, and in particular to Shaoshi Chen and Ruichen Xu for their tremendous help in taking and preparing the notes. I would also like to thank the anonymous referees for their constructive and helpful comments. For brevity and clarity, we have kept these notes in their original lecture style. However, various references are given for those who wish to look up more details.

## 2 Preliminaries

In this section, we shall first introduce some preliminaries on algebraic numbers and their various absolute values.

### 2.1 Absolute Values over Rational Numbers

Recall that the set of natural numbers

$$\mathbb{N} = \{1, 2, \cdots\}$$

has two operations, namely $+$ and $\times$. For $n \in \mathbb{N}$, write

$$n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}.$$

Then the "traditional" absolute value is defined by

$$|n| = \text{the number of 1's in the addition.}$$

Also, by prime factorization, we can write $n$ as

$$n = \underbrace{p \cdot p \cdot \cdots \cdot p}_{v_p(n) \text{ times}} \cdot u,$$

where $p$ is a prime and $u$ is not divided by $p$. The $v_p(n)$ above is called the **$p$-adic valuation** of $n$. It is the number of $p$ in the multiplication. Then we define the **$p$-adic absolute value** of $n$ as

$$|n|_p = \left(\frac{1}{p}\right)^{v_p(n)}.$$

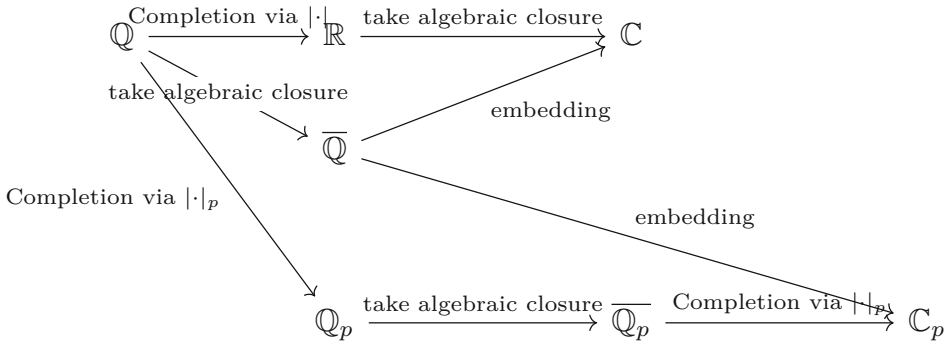
By unique factorization of integers, it is clear that we have

$$n = \prod_p |n|_p^{-1}.$$

In other words, we have the following principle:

Integer factorization $\Leftrightarrow$ Computation of $p$-adic absolute value for all primes $p$.

We can extend $|\cdot|$ and $|\cdot|_p$ to $\mathbb{Q}$ by $|0|_p = 0$ and $\left|\frac{\pm a}{b}\right|_p = \frac{|a|_p}{|b|_p}$. To sum up, we have




Here are some examples.

**Example 2.1** The sequence $\{p^n | n = 1, 2, \cdots\}$ converges to zero in $|\cdot|_p$, diverges in $|\cdot|_\ell$ for all primes $\ell \neq p$ and in $|\cdot|$.

**Example 2.2** The sequence $\left\{\left(\frac{1}{p}\right)^n | n = 1, 2, \cdots\right\}$ converges to zero in $|\cdot|$, diverges in $|\cdot|_\ell$ for all primes $\ell$.

By the two examples above, we obtain that $\{|\cdot|, |\cdot|_2, \cdots, |\cdot|_p, \cdots\}$ are inequivalent absolute values on $\mathbb{Q}$. Actually, we have

**Theorem 2.3** (Ostrowski) *Up to the equivalence of topology,* $\{|\cdot|, |\cdot|_2, \cdots, |\cdot|_p, \cdots\}$ *are all the nontrivial absolute values of* $\mathbb{Q}$.

*Proof* Omitted. ∎

### 2.2 Absolute Values over Number Fields

We first introduce the basic notion of number fields. A field $K$ is called a **number field** if $K$ is a finite extension of $\mathbb{Q}$. Such an extension can be written as $K = \mathbb{Q}[x]/(h(x))$, where $h(x)$ is a monic irreducible polynomial of degree $n$ in $\mathbb{Q}[x]$. Let $\beta$ be a root of $h(x)$ in $K$, then $K$ can also be written as $K = \mathbb{Q}[\beta]$.

For $\alpha \in K$, we hope to define the absolute values $|\alpha|$ and $|\alpha|_p$. We have defined absolute values in $\mathbb{C}$ and $\mathbb{C}_p$, hence it is enough to choose field embeddings $\sigma : K \to \mathbb{C}$ and $\sigma : K \to \mathbb{C}_p$, not unique in general. Such an embedding is determined by $\sigma(\beta)$.

**Absolute value $|\cdot|$ over number fields** We can factor $h(x)$ as

$$h(x) = \prod_{i=1}^{r_1}(x - \beta_i)\prod_{j=1}^{r_2}(x^2 + a_j x + b_j)$$

in $\mathbb{R}[x]$ and

$$h(x) = \prod_{i=1}^{n}(x - \beta_i)$$

in $\mathbb{C}[x]$. Here $r_1+2r_2=n$, $\beta_1,\beta_2,\cdots,\beta_{r_1}\in\mathbb{R}$, $\beta_{r_1+1},\beta_{r_1+2},\cdots,\beta_{r_1+r_2}\in\mathbb{C}-\mathbb{R}$ and $\beta_{r_1+r_2+1}=\overline{\beta_{r_1+1}},\cdots,\beta_{r_1+2r_2}=\overline{\beta_{r_1+r_2}}$.

Now since $h(\beta)=0$, applying $\sigma$ to both sides, we deduce

$$\sigma(h(\beta))=h(\sigma(\beta))=0.$$

It follows that $\sigma(\beta)\in\{\beta_1,\beta_2,\cdots,\beta_n\}$. This gives $n=r_1+2r_2$ different embeddings

$$\sigma_i:K\to\mathbb{C};\quad \sigma(\beta)=\beta_i.$$

Define the absolute value

$$|\alpha|_{\sigma_i}=|\sigma_i(\alpha)|$$

and note that

$$|\alpha|_{\sigma_{r_1+r_2+j}}=|\sigma_{r_1+r_2+j}(\alpha)|=\left|\overline{\sigma_{r_1+j}(\alpha)}\right|=|\alpha|_{\sigma_{r_1+j}}.$$

Hence, there are only $r_1+r_2$ distinct absolute values of $K$, namely the absolute value given by the embeddings $\{\sigma_1,\cdots,\sigma_{r_1},\sigma_{r_1+1},\cdots,\sigma_{r_1+r_2}\}$. The first $r_1$ of them are real embeddings, and the last $r_2$ of them are pairs of complex embeddings.

**Absolute value $|\cdot|_p$ over number fields** Similarly, we factor $h(x)$ as

$$h(x)=\prod_{i=1}^{g}h_i(x)$$

in $\mathbb{Q}_p[x]$, where $h_i(x)\in\mathbb{Q}_p[x]$ is a monic irreducible polynomial of degree $f_i$. Then

$$h(x)=\prod_{i=1}^{g}\prod_{j=1}^{f_i}(x-\beta_{ij})$$

in $\mathbb{C}_p[x]$. Hence we get $n=\sum_{i=1}^{g}f_i$ different embeddings, viz.

$$\sigma_{ij}:K\to\mathbb{C}_p;\quad \sigma_{ij}(\beta)=\beta_{ij}.$$

Then

$$|\alpha|_p=|\sigma_{ij}(\alpha)|_p$$

is a $p$-adic absolute value of $K$. For fixed $1\le i\le g$, the $f_i$ embeddings $\{\sigma_{i1},\sigma_{i2},\cdots,\sigma_{if_i}\}$ are Galois conjugates over $\mathbb{Q}_p$, and hence they define the same absolute value of $K$. It follows that we only get $g$ distinct $p$-adic absolute values of $K$, namely $\{\sigma_1,\sigma_2,\cdots,\sigma_g\}$, where

$$|\alpha|_{\sigma_i}:=|\alpha|_{\sigma_{i1}},\quad 1\le i\le g.$$

**Factorization of algebraic integers** Let $\mathcal{O}_K$ be the ring of integers in $K$. Given non-zero algebraic integer $\alpha \in \mathcal{O}_K - \{0\}$, we have the unique factorization of ideals,

$$\alpha\mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)},$$

where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. Define

$$|\alpha|_{\mathfrak{p}} := \left(\frac{1}{\mathrm{N}(\mathfrak{p})}\right)^{v_{\mathfrak{p}}(\alpha)},$$

where $\mathrm{N}(\mathfrak{p}) = \sharp(\mathcal{O}_K/\mathfrak{p}) = p^r$, and $r$ is the degree of residue field, i.e., $r = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$. This also defines a $p$-adic absolute value of $K$. Hence $|\alpha|_{\mathfrak{p}} = |\alpha|_p^c$, where $|\cdot|_p = |\cdot|_\sigma$ is one of the above $p$-adic absolute values of $K$ and $c$ is a normalization factor. To determine the factor $c$, consider

$$p\mathcal{O}_K = \mathfrak{p}^e \cdots, \quad v_{\mathfrak{p}}(p) = e,$$

and then

$$|p|_{\mathfrak{p}} = \left(\frac{1}{p^r}\right)^e = \left(\frac{1}{p}\right)^{er} = |p|_p^{er}.$$

Hence $c = er$. Now we recover the principle in $p$-adic case:

Ideal factorization of $\alpha \Leftrightarrow$ Computation of all $p$-adic absolute values of $\alpha$.

### 2.3 Degrees of Algebraic Numbers

A number $\alpha$ in an extension field of $\mathbb{Q}$ is called **algebraic** if $h(\alpha) = 0$ for some monic polynomial $h(x) \in \mathbb{Q}[x]$. The **minimal polynomial** of $\alpha$ is the lowest degree monic polynomial $h(x) \in \mathbb{Q}[x]$ such that $h(\alpha) = 0$. The minimal polynomial of $\alpha$ is unique and irreducible.

If $\alpha$ is algebraic over $\mathbb{Q}$, then we define $\deg(\alpha) := [\mathbb{Q}(\alpha) : \mathbb{Q}]$, which is equal to the degree of the minimal polynomial of $\alpha$ over $\mathbb{Q}$.

**Example 2.4** $\zeta_p$ is algebraic since $\zeta_p$ is a root of $x^p - 1$. Furthermore, $\deg(\zeta_p) = p - 1$, since its minimal polynomial is the $p$-th cyclotomic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, which is an irreducible polynomial in $\mathbb{Q}[x]$ of degree $p - 1$.

**$p$-Eisenstein Criterion** We frequently encounter the problem of deciding whether a polynomial is irreducible. A useful tool is the $p$-Eisenstein criterion.

**Definition 2.5** Let $g(x) = x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{Z}[x]$ be a monic polynomial. We say that $g(x)$ is **$p$-Eisenstein** for some prime $p$, if $p|a_i$ for all $1 \le i \le d$ and $p^2 \nmid a_d$. More generally, we say that $g(x)$ is **generalized $p$-Eisenstein**[1] if $v_p(a_i) \ge \frac{i}{d} v_p(a_d)$ for all $1 \le i \le d$, and $(d, v_p(a_d)) = 1$.

**Proposition 2.6** *If $g(x)$ is generalized $p$-Eisenstein, then $g(x)$ is irreducible over $\mathbb{Q}_p$, and hence irreducible over $\mathbb{Q}$.*

*Proof* We first factor $g(x) = \prod_{i=1}^{d}(x - \alpha_i) \in \mathbb{C}_p[x]$. Then our assumption implies that the Newton polygon has only one slope, see [2]. Equivalently,

$$v_p(\alpha_1) = v_p(\alpha_2) = \cdots = v_p(\alpha_d) = \frac{1}{d} v_p(\alpha_1\alpha_2\cdots\alpha_d) = \frac{1}{d} v_p(a_d).$$

If $g(x)$ is reducible over $\mathbb{Q}_p$, then a partial product of the roots will be in $\mathbb{Q}_p$, say $\alpha_1\alpha_2\cdots\alpha_h \in \mathbb{Q}_p$ for some $1 \le h < d$. Then the valuation of the product

$$v_p(\alpha_1\alpha_2\cdots\alpha_h) = h\frac{v_p(a_d)}{d}$$

is an integer, since it is the valuation of $\alpha_1\alpha_2\cdots\alpha_h \in \mathbb{Q}_p$. Note that $(d, v_p(\alpha_d)) = 1$, we conclude $d \mid h$, a contradiction. Thus, $g(x)$ is irreducible over $\mathbb{Q}_p$. ∎

**Example 2.7** For positive integers $d$ and $s$, the polynomial $x^d - p^s$ is irreducible over $\mathbb{Q}$ if and only if $(d, s) = 1$.

Given $\alpha \in \mathcal{O}_K$, our main problems are simply to understand the following three questions:

$$|\alpha| = ?, \quad |\alpha|_p = ?, \quad \deg \alpha = [\mathbb{Q}(\alpha) : \mathbb{Q}] = ?$$

In this paper, $\alpha$ is the "exponential sum" to be defined in next section. We study the above three questions. The first two questions on the absolute values are local. The third question on the degree as an algebraic integer is global. The first question on the complex absolute value has been studied extensively in the literature, in relation to the celebrated Weil conjectures. In this paper, we focus on the second question on the $p$-adic absolute value and the third question on the degree of $\alpha$. The local $p$-adic information will be useful for the global degree problem. Recently, $p$-adic lattices in local fields have been studied in [3] with application in cryptology.

## 3 Exponential Sums and Main Problems

Let $p$ be a prime. Let $\zeta_p$ be a fixed primitive $p$-th root of 1. Depending on the situation, $\zeta_p$ will be taken as an element in $\mathbb{C}$ (complex numbers), or $\mathbb{C}_p$ ($p$-adic numbers), or $\overline{\mathbb{Q}}$ (algebraic numbers). We use $\mathbb{F}_p$ to denote the finite field of $p$ elements. In this section, we define exponential sums over finite fields, and formulate our main problems to be studied.

### 3.1 Exponential Sums over $\mathbb{F}_p$

Let $f(x_1, x_2, \cdots, x_n)$ be a polynoimal in $\mathbb{F}_p[x_1, x_2, \cdots, x_n]$. We define the **exponential sum** over the prime finite field $\mathbb{F}_p$ to be the following algebraic integer

$$S(f) = \sum_{x_1, x_2, \cdots, x_n \in \mathbb{F}_p} \zeta_p^{f(x_1, x_2, \cdots, x_n)} \in \mathbb{Z}[\zeta_p] \subset \mathbb{Q}(\zeta_p).$$

This is usually viewed as a character sum, namely

$$S(f) = \sum_{x_1, x_2, \cdots, x_n \in \mathbb{F}_p} \psi_p(f(x_1, x_2, \cdots, x_n)),$$

where

$$\psi_p : (\mathbb{F}_p, +) \to \mathbb{Q}(\zeta_p); \quad \psi_p(a) = \zeta_p^a$$

is the additive character of order $p$ defined by $\zeta_p$.

Our basic questions are:

PROBLEM 1: Analytic number theory: $\zeta_p \in \mathbb{C}$, $|S(f)| =?$;

PROBLEM 2: $p$-adic number theory: $\zeta_p \in \mathbb{C}_p$, $|S(f)|_p =?$;

PROBLEM 3: Algebraic number theory: $\zeta_p \in \overline{\mathbb{Q}}$, $\deg_{\mathbb{Q}} S(f) =?$.

For the first problem, as a complex number, the complex absolute value $|S(f)|$ depends on the choice of the $p$-th root $\zeta_p$. For the second and third problems, it turns out that the $p$-adic absolute value and algebraic degree of $S(f)$ are independent of the choice of $p$-th root $\zeta_p$. There is actually a fourth problem, namely, studying the $\ell$-adic absolute value of $S(f)$, where $\ell$ is a prime different from $p$. We shall however not touch this fourth problem in this paper.

All three questions above are difficult in general, as there are no clean formulas. Our first step is to work with examples, discover and formulate good general properties.

Note that $p\mathbb{Z}[\zeta_p] = ((\zeta_p - 1)\mathbb{Z}[\zeta_p])^{p-1}$, which means that $p$ is totally ramified in $\mathbb{Z}[\zeta_p]$. Meanwhile, the cyclotomic polynomial $\Phi_p(x)$ is irreducible over $\mathbb{Q}_p$, hence $|\cdot|_p$ is uniquely determined on the field $\mathbb{Q}_p(\zeta_p)$, and $|\zeta_p - 1|_p = \left(\frac{1}{p}\right)^{\frac{1}{p-1}}$.

The aim of this paper, is to study the global "PROBLEM 3", which is a new direction. In the process, it is likely that we need the two local problems 1 and 2 as well, which have been studied extensively in the literature.

### 3.2 Exponential Sums over $\mathbb{F}_q$

In addition to exponential sums over the prime field $\mathbb{F}_p$, it is important to work with exponential sums over *all* finite extensions $\mathbb{F}_{p^k}$, not just $\mathbb{F}_p$, as in the Weil conjectures. Let $\overline{\mathbb{F}_p}$ be a fixed algebraic closure of $\mathbb{F}_p$. For each $k \in \mathbb{N}$, there is a unique finite subfield $\mathbb{F}_{p^k}$ of $p^k$ elements in $\overline{\mathbb{F}_p}$. Consider the trace map

$$\mathrm{Tr}_{\mathbb{F}_p}^{\mathbb{F}_{p^k}} : \mathbb{F}_{p^k} \to \mathbb{F}_p; \quad \alpha \mapsto \sum_{\sigma \in \mathrm{Gal}\left(\mathbb{F}_{p^k} | \mathbb{F}_p\right)} \sigma(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{k-1}}.$$

We will denote this trace map as $\mathrm{Tr}_k$ from now on. Then we can define the exponential sum over $\mathbb{F}_{p^k}$, i.e.,

$$S_k(f) = \sum_{x_1, x_2, \cdots, x_n \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(f(x_1, x_2, \cdots, x_n))} \in \mathbb{Z}[\zeta_p].$$

In this way, for a given polynomial $f$, we have a sequence $S_k(f)$ of exponential sums indexed by $k \in \mathbb{N}$. We can ask how our questions on the exponential sum $S_k(f)$ vary when the integer parameter $k$ varies. This leads to the following questions.

QUESTION 1: If $\zeta_p \in \mathbb{C}$, as complex numbers, how $S_k(f)$ varies with $k$?

QUESTION 2: If $\zeta_p \in \mathbb{C}$, as real numbers, how $|S_k(f)|$ varies with $k$?

QUESTION 3: If $\zeta_p \in \mathbb{C}_p$, as real numbers, how $|S_k(f)|_p$ varies with $k$?

QUESTION 4: If $\zeta_p \in \overline{\mathbb{Q}}$, an integers, how $\deg_{\mathbb{Q}} S_k(f)$ varies with $k$?

Our basic stability conjecture is:

**Conjecture 3.1** Each of the above four sequences in $k$ is determined by its first few terms.

More precisely, we can ask about the possible rationality for the generating function of the corresponding sequence.

QUESTION 1: $\sum_{k=1}^{\infty} S_k(f)T^k \in \mathbb{Q}(\zeta_p)(T)$?

QUESTION 2: $\sum_{k=1}^{\infty} |S_k(f)|\, T^k \in \mathbb{R}(T)$?

QUESTION 3: $\sum_{k=1}^{\infty} |S_k(f)|_p\, T^k \in \mathbb{R}(T)$?

QUESTION 4: $\sum_{k=1}^{\infty} \deg(S_k(f))T^k \in \mathbb{Q}(T)$?.

It turns out that a lot is already known to these problems. For the first two problems, we have

**Theorem 3.2** *The two sequences $\{S_k(f)\}$ and $\{|S_k(f)|^2\}$ are linear recurring sequences.*

As a corollary, we obtain

**Corollary 3.3** *The two sequences $\{S_k(f)\}$ and $\{|S_k(f)|^2\}$ are determined by their first few terms.*

*Proof* [Proof of Theorem 3.2] By the rationality theorem of Dwork-Bombieri-Grothendieck[4, 5], the following $L$-function is a rational function

$$L(f,T) = \exp\left(\sum_{i=1}^{\infty} \frac{S_k(f)}{k} T^k\right) \in \mathbb{Q}(\zeta_p)(T).$$

Then the generating function

$$\sum_{k=1}^{\infty} S_k(f)T^k = T\frac{d}{dT}\log(L(f,T)) = T\frac{L'(f,T)}{L(f,T)} \in \mathbb{Q}(\zeta_p)(T)$$

is rational. It follows that the sequence $S_k(f)$ in $k$ is a linear recurring sequence.

To show that the sequence $|S_k(f)|^2$ in $k$ is also a linear recurring sequence, note that

$$\begin{aligned} |S_k(f)|^2 &= S_k(f(x_1, x_2, \cdots, x_n))S_k(-f(y_1, y_2, \cdots, y_n)) \\ &= S_k(f(x_1, x_2, \cdots, x_n) - f(y_1, y_2, \cdots, y_n)) \\ &= S_k(g), \end{aligned}$$

where $g = f(x_1, x_2, \cdots, x_n) - f(y_1, y_2, \cdots, y_n)$ is a polynomial in $2n$ variables. Hence, we are done. ∎

**Remark 3.4** All rationality proofs for $L(f,T)$ use either $p$-adic method or $\ell$-adic method. Any proof over $\mathbb{C}$ will be revolutionary!

**Remark 3.5** The sequence $|S_k(f)|$ itself is probably NOT a linear recurrence sequence. We leave the problem of finding a counter-example (or proving no counter-example) to the reader.

For the sequence of degrees, we have the following stronger periodicity conjecture:

**Conjecture 3.6** (Periodicity) The degree sequence $\{\deg S_k(f)\}$ is periodic for $k >> 0$.

This conjecture was proposed at the beginning of this summer course. Luckily, it was already proved to be true by the end of the course, in collaboration with several participants. This result and its proof will appear in a joint work with Jason P. Bell, Shaoshi Chen, Rong-hua Wang and Hang Yin. As a corollary, we obtain the following rationality result.

**Corollary 3.7** (Rationality) *The generating function* $\sum_{k=1}^{\infty} \deg(S_k(f))T^k \in \mathbb{Q}(T)$.

The proof of the above conjecture depends on the celebrated Skolem-Mahler-Lech theorem, hence it is not effective. It is interesting to understand this degree sequence more explicitly in various important special cases. This was the main purpose of this course. The explicit results and problems studied in the course remain very interesting, and are not superseded by the general structural but non-effective periodicity result.

The third question, the $p$-adic stability conjecture for the sequence of $p$-adic absolute value $|S_k(f)|_p$, seems more difficult. In all cases where we can compute the degree sequence explicitly, the $p$-adic absolute value sequence $|S_k(f)|_p$ is indeed stable. The general case of the $p$-adic stability conjecture seems to be a very challenging problem. An effective solution of this $p$-adic conjecture should shed light on the effective solution of the global degree sequence problem. We hope to return to this topic on another occasion.

## 4 Degree of Exponential Sums: Basic Examples

In this section, we shall introduce basic examples and results on the degree of exponential sums.

### 4.1 The $p = 2$ Case

First we discuss the trivial $p = 2$ case.

**Proposition 4.1** *For the degree of the exponential sum,* $\deg S_k(f)$ *divides* $p-1$ *for all* $k \in \mathbb{N}$ *and all prime* $p$.

*Proof* Since $S_k(f) \in \mathbb{Q}(\zeta_p)$, apply the tower formula

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}(S_k(f))][\mathbb{Q}(S_k(f)) : \mathbb{Q}].$$

Then

$$\deg S_k(f) = [\mathbb{Q}(S_k(f)) : \mathbb{Q}] \,|\, [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1.$$

The proof is finished. ∎

As a corollary, we have

**Corollary 4.2** *If $p = 2$, then $\deg S_k(f) = 1$, for all $k \in \mathbb{N}$.*

This is also obvious from the definition, as $\zeta_2 = -1$.

**So we shall assume $p > 2$ from now on.**

### 4.2 Low Degree Case

Recall the periodicity conjecture (see Conjecture 3.6), i.e.,

*The degree sequence $\{\deg S_k(f)\}$ is periodic for $k >> 0$.*

In this subsection, we give an explicit formula for the degree sequence when $\deg(f) \leq 2$. In particular, we obtain

**Theorem 4.3** *Let $f(x_1, x_2, \cdots, x_n) \in \mathbb{F}_p[x_1, x_2, \cdots, x_n]$. Assume $\deg(f) \leq 2$. Then the degree periodicity conjecture holds. Furthermore, the $p$-adic absolute value sequence $|S_k(f)|_p$ is also stable.*

#### 4.2.1 Degree zero case

In this case, $f(x_1, x_2, \cdots, x_n) = c \in \mathbb{F}_p$ is a constant. Then the exponential sum

$$S_k(f) = \sum_{x_1, x_2, \cdots, x_n \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(c)} = p^{kn} \zeta_p^{kc}.$$

Hence,

$$\deg S_k(f) = \begin{cases} 1, & \text{if } kc = 0 \text{ in } \mathbb{F}_p, \\ p-1, & \text{if } kc \neq 0 \text{ in } \mathbb{F}_p, \end{cases}$$

and

$$|S_k(f)|_p = p^{-kn}.$$

So the sequence $\{\deg(S_k(f))\}$ is periodic, and the $p$-adic absolute value sequence $|S_k(f)|_p$ is stable in $k$.

#### 4.2.2 Degree one case

Let $f(x_1, x_2, \cdots, x_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n + c \in \mathbb{F}_p[x_1, x_2, \cdots, x_n]$. Without loss of generality, we may assume that $a_1 \neq 0$. Then the exponential sum

$$\begin{aligned} S_k(f) &= \sum_{x_1, x_2, \cdots, x_n \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(a_1x_1 + \cdots + a_nx_n + c)} \\ &= \sum_{x_1 \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(a_1x_1)} \cdot \sum_{x_2, \cdots, x_n \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(a_2x_2 + \cdots + a_nx_n + c)} \\ &= \sum_{t \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(t)} \cdot \sum_{x_2, \cdots, x_n \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(a_2x_2 + \cdots + a_nx_n + c)} \\ &= 0 \cdot \sum_{x_2, \cdots, x_n \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(a_2x_2 + \cdots + a_nx_n + c)} \\ &= 0. \end{aligned}$$

Hence, $\deg S_k(f) = 1, \forall k \in \mathbb{N}$. So in particular, the sequence $\{\deg(S_k(f))\}$ is periodic in $k$, and the $p$-adic absolute value sequence $|S_k(f)|_p$ is the zero sequence.

### 4.2.3 Degree two case

First assume $n = k = 1$, then

$$S_1(x^2) = \sum_{x\in\mathbb{F}_p} \zeta_p^{x^2} = \sqrt{(-1)^{\frac{p-1}{2}}p}.$$

This sum is called the **quadratic Gauss sum**, and the second equality was proved by Gauss in 1804, which yields another proof of the quadratic reciprocity law. With this explicit formula, we obtain $\deg S_1(x^2) = 2$, $\left|S_1(x^2)\right| = \sqrt{p}$ and $\left|S_1(x^2)\right|_p = \frac{1}{\sqrt{p}}$.

For $k \geq 1$, by Hasse-Davenport relation (1935), i.e.,

$$-S_k(x^2) = (-S_1(x^2))^k,$$

the exponential sum $S_k(x^2)$ becomes

$$S_k(x^2) = -\left(-\sqrt{(-1)^{\frac{p-1}{2}}p}\right)^k.$$

Hence

$$\deg S_k(x^2) = \begin{cases} 1, & \text{if } 2 \mid k, \\ 2, & \text{if } 2 \nmid k. \end{cases}$$

So the degree sequence $\{\deg(S_k(x^2))\}$ is periodic in $k$, and the $p$-adic absolute value sequence $|S_k(x^2)|_p = p^{-k/2}$ is stable in $k$.

Now if $f(x) = ax^2+bx+c \in \mathbb{F}_p[x]$, where $a \in \mathbb{F}_p^\times$. By completing the square, we can assume that $f(x) = ax^2 + c$, and

$$\begin{aligned} S_k(ax^2 + c) &= S_k(ax^2)\zeta_p^{kc} \\ &= \eta_k(a)S_k(x^2)\zeta_p^{kc} \\ &= \pm\left(-\sqrt{(-1)^{\frac{p-1}{2}}p}\right)^k \zeta_p^{kc}, \end{aligned}$$

where $\eta_k : \left(\mathbb{F}_{p^k}\right)^\times \to \{\pm 1\}$ is the quadratic character. Hence,

$$\deg S_k(ax^2 + c) = \begin{cases} 1, & \text{if } p|kc, 2 \mid k, \\ 2, & \text{if } p|kc, 2 \nmid k, \\ p-1, & \text{if } p \nmid kc. \end{cases}$$

Again, the degree sequence $\{\deg(S_k(ax^2 + bx + c))\}$ is periodic in $k$, and the $p$-adic absolute value sequence $|S_k(ax^2+bx+c)|_p = p^{-k/2}$ is stable in $k$. Note that when calculating the degree, we used the following fact:

**Fact 1** $\deg(\sqrt{\pm p}\zeta_p) = p-1$.

*Proof* Since $p-1 = \deg(\zeta_p^2) = \deg((\sqrt{\pm p}\zeta_p)^2)$. This number divides $\deg(\sqrt{\pm p}\zeta_p)$, which in turn divides $p-1$. ∎

Now we turn to the case when $n > 1$. Since $p > 2$, by an invertible linear transformation, the polynomial $f(x_1, x_2, \cdots, x_n)$ is equivalent to

$$g(x_1, x_2, \cdots, x_n) = a_1x_1^2 + \cdots + a_rx_r^2 + b_{r+1}x_{r+1} + \cdots + b_nx_n + c,$$

where $a_1, a_2, \cdots, a_r \in (\mathbb{F}_p)^\times$. Then the exponential sum

$$S_k(f) = S_k(g) = S_k(a_1x_1^2)\cdots S_k(a_rx_r^2)S_k(b_{r+1}x_{r+1})\cdots S_k(b_nx_n)\cdot\zeta_p^{kc}.$$

Hence

$$S_k(f) = \begin{cases} 0, & \text{if some } b_j \neq 0, \\ \pm p^{k(n-r)}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)^{kr}\zeta_p^{kc}, & \text{if all } b_j = 0. \end{cases}$$

So the degree sequence $\{\deg(S_k(f))\}$ is periodic in $k$, and the $p$-adic absolute value sequence $|S_k(f)|_p = p^{-k(2n-r)/2}$ is stable in $k$.

### 4.3 Reduction to Low Degree Cases

The higher degree cases $\deg(f) \geq 4$ can be reduced to lower degree case $\deg(f) = 3$, at the expense of increasing $n$. However, the cubic case $\deg(f) = 3$ is not much easier, except for $n = 1$ which is doable. No explicit formula exists in general. We have the following

**Theorem 4.4** *Assume that the periodicity conjecture (resp., the p-adic stability conjecture) is true for all polynomials $f(x_1, x_2, \cdots, x_n)$ in $\mathbb{F}_p[x_1, x_2, \cdots, x_n]$ with degree three and all $n \in \mathbb{N}$. Then the periodicity conjecture (resp., the p-adic stability conjecture) is true for all polynomials $g(x_1, x_2, \cdots, x_m) \in \mathbb{F}_p[x_1, x_2, \cdots, x_m]$ of any degree and all $m \in \mathbb{N}$.*

We will first give an illustration on a specific polynomial and then provide a proof in general.

#### 4.3.1 An illustrating example

Consider the monomial $f(x_1, x_2) = x_1^3x_2$ of degree four. Write $f$ as $f(x_1, x_2) = ((x_1^2)x_1)x_2$ and define a system of quadratic equations

$$V = \begin{cases} x_3 = x_1^2, \\ x_4 = x_1x_3 = x_1^3, \\ x_5 = x_4x_2 = x_1^3x_2. \end{cases} \hookrightarrow \mathbb{A}^5.$$

Then

$$\begin{aligned} S_k(f) &= \sum_{x_1,x_2\in\mathbb{F}_{p^k}} \psi_k(x_1^3x_2) \\ &= \sum_{(x_1,x_2,\cdots,x_5)\in V} \psi_k(x_5) \\ &= \frac{1}{p^{3k}} \sum_{x_1,x_2,\cdots,x_8\in\mathbb{F}_{p^k}} \psi_k(x_5 + x_6(x_3 - x_1^2) + x_7(x_4 - x_1x_3) + x_8(x_5 - x_4x_2)) \end{aligned}$$

$$= \frac{1}{p^{3k}} S_k(g(x_1, x_2, \cdots, x_8)),$$

where the polynomial $g$ satisfies $\deg g = 3$. Here we used the standard lemma:

**Lemma 4.5** (Orthogonality of characters) *Let $b \in \mathbb{F}_{p^k}$, then*

$$\sum_{a \in \mathbb{F}_{p^k}} \psi_k(ba) = \begin{cases} p^k, & \text{if } b = 0, \\ 0, & \text{if } b \neq 0. \end{cases}$$

*Proof* Trivial when $b = 0$. If $b \neq 0$, then

$$\begin{aligned} \sum_{a \in \mathbb{F}_{p^k}} \psi_k(ba) &= \sum_{a \in \mathbb{F}_{p^k}} \psi_k(a) \\ &= \sum_{i=0}^{p-1} \sharp\{a \in \mathbb{F}_{p^k} | \mathrm{Tr}_k(a) = i\} \cdot \zeta_p^i \\ &= p^{k-1} \sum_{i=0}^{p-1} \zeta_p^i \\ &= p^{k-1} \frac{\zeta_p^p - 1}{\zeta_p - 1} \\ &= 0. \end{aligned}$$

The proof is now complete. ∎

### 4.3.2 General proof

*Proof* [Proof of Theorem 4.4] For general $f(x_1, x_2, \cdots, x_n) \in \mathbb{F}_p[x_1, x_2, \cdots, x_n]$ of $\deg f \geq 4$, we can write

$$f(x_1, x_2, \cdots, x_n) = \sum_{j=1}^{J} a_j x_1^{u_{j1}} \cdots x_n^{u_{jn}}, \quad a_j \neq 0.$$

We can recursively introduce a system of quadratic equations

$$V = \begin{cases} g_1(x_1, x_2, \cdots, x_m) = 0, \\ \vdots \\ g_m(x_1, x_2, \cdots, x_m) = 0, \\ x_{m+1} - g_{m+1}(x_1, x_2, \cdots, x_m) = 0, \ (g_{m+1}(x_1, x_2, \cdots, x_m) = a_1 x_1^{u_{11}} x_2^{u_{12}} \cdots x_n^{u_{1n}}) \\ \vdots \\ x_{m+J} - g_{m+J}(x_1, x_2, \cdots, x_m) = 0, \ (g_{m+J}(x_1, x_2, \cdots, x_m) = a_J x_1^{u_{J1}} x_2^{u_{J2}} \cdots x_n^{u_{Jn}}), \end{cases} \hookrightarrow \mathbb{A}^{m+J},$$

such that

$$\begin{aligned} S_k(f) &= \sum_V \psi_k(x_{m+1} + \cdots + x_{m+J}) \\ &= \frac{1}{p^{k(m+J)}} \sum_{x,y} \psi_k(x_{m+1} + \cdots + x_{m+J} + \sum_{i=1}^{m} y_i g_i + \sum_{i=m+1}^{m+J} y_i(x_i - g_i)) \\ &= \frac{1}{p^{k(m+J)}} S_k(h(x_1, \cdots, x_{m+J}, y_1, \cdots, y_{m+J})), \end{aligned}$$

where $h(x_1, \cdots, x_{m+J}, y_1, \cdots, y_{m+J})$ is a cubic polynomial in $2(m+J)$ variables. Clearly,

$$\begin{aligned} &\deg S_k(f) = \deg S_k(h), \\ &|S_k(f)|_p = p^{-k(m+J)} |S_k(h)|_p. \end{aligned}$$

The reduction proof is now complete. ∎

### 4.4 The Monomial Case $x^d$ over $\mathbb{F}_{p^k}$

Let $f(x) = x^d$, where $d \geq 1$. In this subsection, we consider the monomial exponential sum $S_k(x^d)$ over all finite fields $\mathbb{F}_{p^k}$. Recall that the exponential sum over $\mathbb{F}_{p^k}$ is

$$S_k(x^d) = \sum_{x \in \mathbb{F}_{p^k}} \psi_k(x^d) = \sum_{x \in \mathbb{F}_{p^k}} \psi_k(x^{(d, p^k-1)}).$$

and

$$S_k(x^{pd}) = S_k(x^d).$$

Hence, we shall assume that $(d, p) = 1$. The sum $S_k(x^d)$ is called (up to a linear change of variable) the **Gauss period** or "**Gauss sum**". This is studied extensively in the literature for small $d$, see Berndt and Evans[6] for a survey. Our basic question is to find an explicit formula for $\deg S_k(x^d)$ for all $k \in \mathbb{N}$ and to show that the $p$-adic stability for $S_k(x^d)$ holds. This is already unknown, even for monomials $x^d$ for general $d$. We shall give some partial results.

For the prime field case when $k = 1$, according to Myerson[7], Gauss has already obtained

**Theorem 4.6** (Gauss) $\deg S_1(x^d) = (d, p-1)$.

For $k \geq 1$, we have.

**Theorem 4.7** (Myerson[7]) *If $d|(p-1)$ and $(d,k) = 1$, then $\deg S_k(x^d) = d$.*

In this subsection, we shall prove the following stronger result.

**Theorem 4.8** *If $d|(p-1)$, then $\deg S_k(x^d) = \frac{d}{(d,k)}$. If $d \Big| \frac{p^k-1}{p-1}$, then $\deg S_k(x^d) = 1$.*

The proof will be given a little later. As a corollary, we obtain

**Corollary 4.9** *The degree periodicity conjecture holds for the monomial $f(x) = x^d$ if either $d|(p-1)$ or $(d, p-1) = 1$ or $d$ is a prime.*

*Proof* We can assume $p \not| d$. If $d|(p-1)$, then

$$\deg S_k(x^d) = \frac{d}{(d,k)},$$

which is clearly periodic in $k$. If $(d, p-1) = 1$, then $(d, p^k - 1) | \frac{p^k-1}{p-1}$. Thus,

$$\deg S_k(x^d) = \deg S_k(x^{(d,p^k-1)}) = 1,$$

which is periodic in $k$. If $d$ is a prime, then either $d|(p-1)$ or $(d, p-1) = 1$. Hence we are done.

We also raise two problems here.

PROBLEM 1: Compute $\deg S_k(x^d)$, where $d = p_1 p_2$ is a product of two primes.

PROBLEM 2: Assume $d$ divides $(p^k - 1)/(p-1)$. The theorem shows that $S_k(x^d) \in \mathbb{Z}$. Find an explicit formula for $S_k(x^d)$. Some special cases are known. This has applications in weight distribution of cyclic codes.

**Remark 4.10** If $d|(p-1)$, using the binomial formula after writing $p$ as $1 + (p-1)$, we find that

$$d \left| \frac{p^{(p-1)k} - 1}{p-1}. \right.$$

Hence $S_{(p-1)k}(x^d) \in \mathbb{Z}$. This is a little surprising! Perhaps it is not so easy to find an explicit formula for $S_k(x^d)$ in the case $d$ divides $(p^k - 1)/(p-1)$.

Now we provide the proof of Theorem 4.8.

*Proof* [Proof of Theorem 4.8] For $a \in (\mathbb{F}_p)^\times$, $\sigma_a(\zeta_p) = \zeta_p^a$. Since $\mathrm{Tr}_k$ is $\mathbb{F}_p$-linear,

$$\sigma_a(S_k(x^d)) = \sum_{x \in \mathbb{F}_p^k} \zeta_p^{a\mathrm{Tr}_k(x^d)} = \sum_{x \in \mathbb{F}_p^k} \zeta_p^{\mathrm{Tr}_k(ax^d)}.$$

From this, we see that $\sigma_a(S_k(x^d)) = S_k(x^d)$ if $a \in H := \left(\mathbb{F}_{p^k}^\times\right)^d \cap \mathbb{F}_p^\times$. Clearly,

$$H = \left\{ a \in \mathbb{F}_p^\times \,\middle|\, a^{\left(p-1, \frac{p^k-1}{(d,p^k-1)}\right)} = 1 \right\} \subset (\mathbb{F}_p)^\times.$$

Then its order

$$|H| = \left(p-1, \frac{p^k-1}{(d, p^k-1)}\right).$$

Now $S_k(x^d) \in \mathbb{Q}(\zeta_p)^H$, and hence

$$\deg S_k(x^d) \left| [\mathbb{Q}(\zeta_p)^H : \mathbb{Q}] = \frac{p-1}{|H|} = \frac{p-1}{\left(p-1, \frac{p^k-1}{(d,p^k-1)}\right)}. \right.$$

For the second case, where $d \left| \frac{p^k-1}{p-1} \right.$, we have

$$\frac{p-1}{\left(p-1, \frac{p^k-1}{(d,p^k-1)}\right)} = \frac{p-1}{\left(p-1, \frac{p^k-1}{d}\right)} = \frac{p-1}{\left(p-1, (p-1)\frac{p^k-1}{d(p-1)}\right)} = 1,$$

and hence $\deg S_k(x^d) = 1$.

It is a little more involved in the first case when $d|(p-1)$. Again, we have

$$\frac{p-1}{\left(p-1,\frac{p^k-1}{(d,p^k-1)}\right)}=\frac{p-1}{\left(p-1,\frac{p^k-1}{d}\right)}=\frac{p-1}{\left(p-1,\frac{p-1}{d}\frac{p^k-1}{p-1}\right)}=\frac{d}{\left(d,\frac{p^k-1}{p-1}\right)}=\frac{d}{(d,k+(p-1)*)}=\frac{d}{(d,k)},$$

and thus, $\deg S_k(x^d)\Big|\frac{d}{(d,k)}$. To show that the degree is equal to $\frac{d}{(d,k)}$, we consider the following polynomial

$$m(T)=\prod_{a\in\mathbb{F}_p^\times/H}\big(T-S_k(ax^d)\big)\in\mathbb{Z}[\zeta_p]^{\mathbb{F}_p^\times}[T]=\mathbb{Z}[T],$$

which is monic of degree $D:=\frac{d}{(d,k)}$ with $S_k(x^d)$ as a root. We need to show that $m(T)$ is irreducible over $\mathbb{Q}$. Write

$$m(T)=T^D-b_1T^{D-1}+b_2T^{D-2}+\cdots+(-1)^db_D,$$

where $b_i$ is the $i$-th elementary symmetric polynomial of the roots $\{S_k(ax^d)|a\in\mathbb{F}_p^\times/H\}$. By Lemma 4.11 (listed after the proof), we obtain

$$v_p(b_D)=D\frac{k}{d}=\frac{d}{(d,k)}\frac{k}{d}=\frac{k}{(d,k)}$$

and

$$v_p(b_i)\geq i\frac{k}{d}=\frac{i}{\frac{d}{(d,k)}}\frac{k}{(d,k)}=\frac{i}{D}\frac{k}{(d,k)},$$

where $(D,v_p(b_D))=\left(\frac{d}{(d,k)},\frac{k}{(d,k)}\right)=1$. Hence, $m(T)$ is generalized $p$-Eisenstein, which implies that $m(T)$ is irreducible of degree $D$. ∎

The proof suggests the importance of computing the $p$-adic valuation $v_p(S_k(f))$, or equivalently the $p$-adic absolute value $|S_k(f)|_p$. We used the following lemma in the proof.

**Lemma 4.11** *If $d|(p-1)$, then $v_p(S_k(ax^d))=\frac{k}{d}$ for all $a\in\mathbb{F}_{p^k}^\times$.*

The proof of this lemma will be presented later. It implies that the $p$-adic stability conjecture holds for $S_k(x^d)$ if $d|(p-1)$. It does not seem to be obvious if the $p$-adic stability also holds if $(d,p-1)<d$.

**Kummer Sum and Gauss Sum** Next, we briefly discuss **Kummer sum** (the case $d=3$ and $k=1$), defined as the cubic exponential sum

$$S_1(x^3)=S_1(x^3\otimes\mathbb{F}_p)=\sum_{x\in\mathbb{F}_p}\exp\left(\frac{2\pi ix^3}{p}\right)\in\mathbb{Q}(\zeta_p)^+\subset\mathbb{R}.$$

If $p\equiv 2 \mod 3$, then $S_1(x^3)=S_1(x^{(3,p-1)})=S_1(x)=0$. Assume $p\equiv 1 \mod 3$ now. Then

$$S_1(x^3)=-(G(\chi_3)+\overline{G(\chi_3)})\in\mathbb{R}$$

is a real number, where $G(\chi_3)$ is the standard **cubic Gauss sum** associated to a cubic character $\chi_3$, and $|G(\chi_3)|=\sqrt{p}$. This implies $\big|S_1(x^3)\big|\leq 2\sqrt{p}$, and hence

$$\frac{S_1(x^3\otimes\mathbb{F}_p)}{2\sqrt{p}}\in[-1,1].$$

The precise value of the real number $S_1(x^3 \otimes \mathbb{F}_p)$ is quite mysterious as $p$ varies. Based on a few numerical calculations, Kummer in 1846 made the following conjecture:

**Conjecture 4.12** (Kummer[8]) As the prime $p$ varies in the congruence class $p \equiv 1 \mod 3$, the cubic sum $S_1(x^3 \otimes \mathbb{F}_p)$ is "more often positive than negative".

However, Heath-Brown and Patterson[9] proved that the sum is actually uniformly distributed in the interval $[-1, 1]$. Yet in some sense, Kummer's conjecture is still believed to be true as the following finer conjecture suggests.

**Conjecture 4.13** (Patterson[10]) As the real number $t$ goes to infinity, we have

$$\sum_{p \le t} \frac{S_1(x^3 \otimes \mathbb{F}_p)}{2\sqrt{p}} \sim \frac{(2\pi)^{2/3}}{5\Gamma(2/3)} \frac{t^{5/6}}{\log t},$$

where $\Gamma$ denotes the Gamma-function.

### 4.5 Explicit Galois Theory of the Cyclotomic Field $\mathbb{Q}(\zeta_p)$

In this subsection, we explain how the monomial exponential sum $S_k(x^d)$ can be used to explicitly construct all subfields of the $p$-th cyclotomic field $\mathbb{Q}_p(\zeta_p)$. This provides an excellent example of explicit Galois theory.

Recall that $\mathbb{Q}(\zeta_p)$ is the splitting field of the $p$-th cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = \prod_{j=1}^{p-1} \left(x - \zeta_p^j\right).$$

The extension $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ is a Galois extension, and its Galois group is defined as

$$G := \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)\,|\mathbb{Q}\right) = \{\text{All } \mathbb{Q}\text{-isomorphisms}\, \sigma : \mathbb{Q}(\zeta_p) \to \mathbb{Q}(\zeta_p)\}.$$

Apply any $\sigma \in G$ to the equation $\Phi_p(\zeta_p) = 0$, we obtain that $\sigma(\zeta_p) \in \{\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}\}$. Hence, for any $1 \le j \le p-1$, we have

$$\mathbb{Q}(\zeta_p) \xrightarrow{\ \sim\ } \mathbb{Q}[x]/(\Phi_p(x)) \xrightarrow{\ \sim\ } \mathbb{Q}(\zeta_p^j) = \mathbb{Q}(\zeta_p)$$

$$\zeta_p \longleftarrow x \longmapsto \zeta_p^j, \qquad \sigma_j$$

and $\sigma_{j_1}\sigma_{j_2} = \sigma_{j_1 j_2}$. Hence, the Galois group

$$G = \{\sigma_j | 1 \le j \le p-1\} \cong (\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{F}_p)^\times.$$

By Galois theory, there exists a 1-1 correspondence between the subfields of $\mathbb{Q}(\zeta_p)$ and the subgroups of $(\mathbb{F}_p)^\times$, i.e.,

$$\begin{array}{ccc}
\mathbb{Q}(\zeta_p) & \text{---------} & 1 \\
| & & | \\
\mathbb{Q}(\zeta_p)^H = K & \text{---------} & H = \mathrm{Gal}\,(\mathbb{Q}(\zeta_p)\,|K\,) \\
| & & | \\
\mathbb{Q} & \text{---------} & (\mathbb{F}_p)^\times
\end{array}$$

By the structure of cyclic groups, the subgroups of $(\mathbb{F}_p)^\times$ are $H_d = \{x^d | x \in (\mathbb{F}_p)^\times\}$, one for each $d|(p-1)$. Here $|H_d| = \frac{p-1}{d}$. The number of subgroups of $(\mathbb{F}_p)^\times$ is equal to the number of subfields of $\mathbb{Q}(\zeta_p)$, which is the number of divisors of $p-1$, denoted by $\tau(p-1)$.

$$\begin{array}{ccc}
\mathbb{Q}(\zeta_p) & \text{---------} & 1 \\
{\scriptstyle \frac{p-1}{d}}\big| & & \big|{\scriptstyle \frac{p-1}{d}} \\
\mathbb{Q}(\zeta_p)^{H_d} = K_d & \text{---------} & H_d = \mathrm{Gal}\,(\mathbb{Q}(\zeta_p)\,|K_d\,) \\
{\scriptstyle d}\big| & & \big|{\scriptstyle d} \\
\mathbb{Q} & \text{---------} & (\mathbb{F}_p)^\times
\end{array}$$

Now our question is that given a divisor $d|(p-1)$, construct $K_d$ explicitly.

When $d = 1$, $K_1 = \mathbb{Q} = \mathbb{Q}(\zeta_p)^{H_1} = \mathbb{Q}(\zeta_p)^G$.

When $d = p-1$, $K_{p-1} = \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p)^{\{1\}}$.

When $d = \frac{p-1}{2}$, $H_{\frac{p-1}{2}} = \{\alpha^{\frac{p-1}{2}} | \alpha \in (\mathbb{F}_p)^\times\} = \{\pm 1\}$. Here $-1$ represents the complex conjugation. Hence

$$K_{\frac{p-1}{2}} = \mathbb{Q}(\zeta_p)^{\{\sigma_{\pm 1}\}} = \mathbb{Q}(\eta_p),$$

where $\eta_p = \zeta_p + \zeta_p^{-1}$. This is the maximal real subfield of $\mathbb{Q}(\zeta_p)$ and is often denoted by $\mathbb{Q}(\zeta_p)^+$. In fact, $\zeta_p$ is a root of the quadratic irreducible polynomial

$$x^2 - \eta_p x + 1 \in \mathbb{R}[x].$$

Hence, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\eta_p)] = 2$, which impies that $K_{\frac{p-1}{2}} = \mathbb{Q}(\eta_p)$ indeed.

When $d = 2$, consider the group $H_2 = \{a^2 : a \in (\mathbb{F}_p)^\times\}$. For all $a \in (\mathbb{F}_p)^\times$, apply $\sigma_{a^2}$ to the Gauss sum

$$\sigma_{a^2}(S_1(x^2)) = \sigma_{a^2}\left(\sum_{x\in\mathbb{F}_p} \zeta_p^{x^2}\right) = \sum_{x\in\mathbb{F}_p} \zeta_p^{a^2x^2} = \sum_{y\in\mathbb{F}_p} \zeta_p^{y^2} = S_1(x^2).$$

Hence, $S_1(x^2) \in K_2$. Since $[K_2, \mathbb{Q}] = 2$ and Gauss's formula shows that $S_1(x^2) = \sqrt{(-1)^{\frac{p-1}{2}}p}$ is quadratic over $\mathbb{Q}$. Hence $K_2 = \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}}p})$.

In general, we may ask what $K_d$ is for any $d|(p-1)$? Similarly, we calculate for any $a \in (\mathbb{F}_p)^\times$,

$$\sigma_{a^d}(S_1(x^d)) = \sigma_{a^d}\left(\sum_{x\in\mathbb{F}_p} \zeta_p^{x^d}\right) = \sum_{x\in\mathbb{F}_p} \zeta_p^{a^d x^d} = \sum_{y\in\mathbb{F}_p} \zeta_p^{y^d} = S_1(x^d).$$

Hence, $\mathbb{Q}(S_1(x^d)) \subset K_d$. We claim that

**Theorem 4.14** $K_d = \mathbb{Q}(S_1(x^d))$.

This theorem follows from

**Lemma 4.15** (Gauss) $\deg S_1(x^d) = d$.

*Proof* We give a $p$-adic proof here, which can be extended to more general situation later. Clearly, $S_1(x^d)$ is a root of the following degree $d$ polynomial

$$m(T) = \prod_{a\in(\mathbb{F}_p)^\times/H_d} \left(T - S_1(ax^d)\right) \in \mathbb{Q}(\zeta_p)^G[T] = \mathbb{Q}[T].$$

It is enough to prove that $m(T)$ is irreducible over $\mathbb{Q}$. This can be obtained from the following lemma. ∎

**Lemma 4.16** (see [1]) *Write*

$$m(T) = T^d + m_1 T^{d-1} + \cdots + m_d \in \mathbb{Q}[T],$$

*then $m(T) \in \mathbb{Z}[T]$, and $m(T)$ is $p$-Eisenstein.*

We will prove a more general version of this later. We can raise the following problems.

Problem 1: By the famous Kronecker-Weber theorem, every finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field $\mathbb{Q}(\zeta_m)$. Here the Galois group $G := \mathrm{Gal}\,(\mathbb{Q}(\zeta_m)\,|\mathbb{Q}\,) = (\mathbb{Z}/m\mathbb{Z})^\times$. By Galois theory,

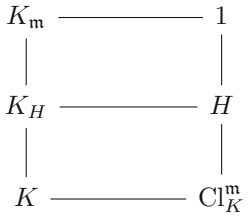
$$\begin{array}{ccc}
\mathbb{Q}(\zeta_m) & \text{———————} & 1 \\
\big| & & \big| \\
\mathbb{Q}(\zeta_m)^H = K & \text{———} & H = \mathrm{Gal}\,(\mathbb{Q}(\zeta_m)\,|K\,) \\
\big| & & \big| \\
\mathbb{Q} & \text{———————} & (\mathbb{Z}/m\mathbb{Z})^\times
\end{array}$$

The problem is to find an explicit element $\alpha_H \in \mathbb{Q}(\zeta_m)$, such that $K = \mathbb{Q}(\alpha_H)$. This should be doable.

Problem 2: By class field theory, for a number field $K$, every finite abelian extension of $K$ is contained in some Ray class field $K_\mathfrak{m}$, where $\mathfrak{m}$ is a modulus, and

$$\mathrm{Gal}\,(K_\mathfrak{m}\,|K\,) = \mathrm{Cl}_K^\mathfrak{m}.$$

The problem is that given a modulus $\mathfrak{m}$, how to construct explicitly $K_\mathfrak{m}$ and all intermediate subfields $K \subset K_H \subset K_\mathfrak{m}$ for all subgroups $H < \mathrm{Cl}_K^\mathfrak{m}$.




This is a major open problem in algebraic number theory. It might be doable for imaginary quadratic fields $K$ using the theory of complex multiplications for elliptic curves.

## 5 Kloosterman Sums

In this section, we study the degrees of Kloosterman sums as algebraic integers.

### 5.1 Kloosterman Sums over $\mathbb{F}_p$

Let $n \in \mathbb{N}$ and $\lambda \in \mathbb{F}_p^\times$. Define the toric exponential sum

$$Kl_{n,1}(\lambda) = \sum_{x_1,x_2,\cdots,x_n \in \mathbb{F}_p^\times} \zeta_p^{\left(x_1+x_2+\cdots+x_n+\frac{\lambda}{x_1x_2\cdots x_n}\right)} \in \mathbb{Z}[\zeta_p].$$

This sum is called the $n$-dimensional **Kloosterman sum** over the prime field $\mathbb{F}_p$. For its complex absolute value, we have the following well known estimate.

**Theorem 5.1** (Deligne[11], 1980) *As a complex number,* $|KL_{n,1}(\lambda)| \le (n+1)\sqrt{p^n}$.

Any elementary proof for $n \ge 2$ will be valuable. The precise value of $KL_{n,1}(\lambda)$ is again very mysterious. As $\lambda$ varies in $\mathbb{F}_p$ (and $p$ grows), the $(p-1)$ normalized Kloosterman sums $Kl_{n,1}(\lambda)p^{-n/2}$ are equidistributed with respect to some Sato-Tate measure. This is the function field Sato-Tate conjecture for Kloosterman sum, proved by Deligne and Katz, see Katz[12]. For fixed integer $\lambda \ne 0$ (say, $\lambda = 1$), as $p$ varies, how the normalized Kloosterman sum $Kl_{n,1}(\lambda)p^{-n/2}$ varies is completely open.

As a $p$-adic number,

$$\begin{aligned} Kl_{n,1}(\lambda) &= \sum_{x_1,x_2,\cdots,x_n \in \mathbb{F}_p^\times} (1+\zeta_p-1)^{\left(x_1+x_2+\cdots+x_n+\frac{\lambda}{x_1x_2\cdots x_n}\right)} \\ &\equiv \sum_{x_1,x_2,\cdots,x_n \in \mathbb{F}_p^\times} 1 \mod (\zeta_p-1) \\ &\equiv (p-1)^n \mod (\zeta_p-1) \\ &\equiv (-1)^n \mod (\zeta_p-1). \end{aligned}$$

This implies that $v_p(Kl_{n,1}(\lambda)) = 0$ and $|Kl_{n,1}(\lambda)|_p = 1$.

For the degree of the Kloosterman sum, we have

**Theorem 5.2** (see [14]) *As an algebraic number,* $\deg Kl_{n,1}(\lambda) = \frac{p-1}{(n+1,p-1)}$.

### 5.2 Kloosterman Sums over $\mathbb{F}_q$

Let $k, n \in \mathbb{N}$ and $\lambda \in \mathbb{F}_p^\times$. Similarly, one defines

$$Kl_{n,k}(\lambda) = \sum_{x_1,x_2,\cdots,x_n \in \mathbb{F}_{p^k}^\times} \zeta_p^{\mathrm{Tr}_k\left(x_1+x_2+\cdots+x_n+\frac{\lambda}{x_1x_2\cdots x_n}\right)} \in \mathbb{Z}[\zeta_p].$$

This is the **Kloosterman sum** over $\mathbb{F}_{p^k}$. As a $p$-adic number, taking $\mod(\zeta_p - 1)$, we again have

$$Kl_{n,k}(\lambda) \equiv (-1)^n \mod(\zeta_p - 1),$$

and hence $|Kl_{n,k}(\lambda)|_p = 1$. Deligne's theorem again gives

**Theorem 5.3** (Deligne[11]) *As a complex number,* $|Kl_{n,k}(\lambda)| \le (n+1)\sqrt{p^{kn}}$.

For the algebraic degree, we have

**Theorem 5.4** (see [14]) *As an algebraic integer,* $\deg Kl_{n,k}(\lambda) = \frac{p-1}{(n+1,p-1)}$ *for all* $k \not\equiv 0 \mod p$.

The case $k \equiv 0 \mod p$ has been open. In a forthcoming work, we shall apply finer $p$-adic method to prove the following result.

**Theorem 5.5** *If* $p > n+2$ *and* $\lambda \in \mathbb{F}_p^\times$, *then* $\deg Kl_{n,k}(\lambda) = \frac{p-1}{(n+1,p-1)}$.

This result implies that the periodicity conjecture holds for $\deg Kl_{n,k}(\lambda)$ if $p > n+2$. This is a non-abelian example! Now we shall prove the easier Theorem 5.4.

*Proof* [Proof of Theorem 5.4] For $a \in (\mathbb{F}_p)^\times$, $\sigma_a(\zeta_p) = \zeta_p^a$. Then

$$\sigma_a(Kl_{n,k}(\lambda)) = \sum_{x_1,x_2,\cdots,x_n \in \mathbb{F}_p^\times} \zeta_p^{\mathrm{Tr}_k\left(ax_1+ax_2+\cdots+ax_n+\frac{a^{n+1}\lambda}{ax_1ax_2\cdots ax_n}\right)} = Kl_{n,k}(a^{n+1}\lambda).$$

If $a^{n+1} = 1$, then $\sigma_a(Kl_{n,k}(\lambda)) = Kl_{n,k}(\lambda)$.

Let

$$H = \left\{a \in \mathbb{F}_p^\times \,|\, a^{n+1} = 1\right\} = \left\{a \in \mathbb{F}_p^\times | a^{(p-1,n+1)} = 1\right\}.$$

Then its order $|H| = (p-1, n+1)$. Now $Kl_{n,k}(\lambda) \in \mathbb{Q}(\zeta_p)^H$, and hence by Galois theory

$$\deg Kl_{n,k}(\lambda) \,\Big|\, [\mathbb{Q}(\zeta_p)^H : \mathbb{Q}] = \frac{p-1}{|H|} = \frac{p-1}{(n+1,p-1)}.$$

As noted before, $|\deg Kl_{n,k}(\lambda)|_p = 1$, and hence the minimal polynomial will NOT be $p$-Eisenstein or generalized $p$-Eisenstein. However, we have Lemma 5.6 (listed after the proof) which is needed now. Inspired by the lemma, write

$$m(T) = \prod_{a \in \mathbb{F}_p^\times/H} \left(T - \sigma((p^k-1)Kl_{n,k}(\lambda) + (-1)^n)\right) \in \mathbb{Z}[\zeta_p]^{\mathbb{F}_p^\times}[T] = \mathbb{Z}[T],$$

which is monic of degree $D := \frac{p-1}{(n+1,p-1)}$. Write

$$m(T) = T^D - b_1T^{D-1} + b_2T^{D-2} + \cdots + (-1)^D b_D$$

and use Lemma 5.6, we obtain

$$v_p(b_D) = \frac{p-1}{(n+1,p-1)}\frac{n+1}{p-1} = \frac{n+1}{(n+1,p-1)}$$

and

$$v_p(b_i) \geq i\frac{n+1}{p-1} = \frac{i}{D}v_p(b_D) = \frac{i(n+1,p-1)}{p-1}\frac{n+1}{(n+1,p-1)},$$

where $(D, v_p(b_D)) = \left(\frac{n+1}{(n+1,p-1)}, \frac{p-1}{(n+1,p-1)}\right) = 1$. Hence, $m(T)$ is generalized $p$-Eisenstein, which implies that $m(T)$ is irreducible of degree $D$. Thus

$$\deg Kl_{n,k}(\lambda) = \deg((p^k-1)Kl_{n,k}(\lambda) + (-1)^n) = D.$$

The proof is finished. ∎

We used the following lemma in the proof.

**Lemma 5.6** *If $k \not\equiv 0 \mod p$, then*

$$v_p((p^k-1)Kl_{n,k}(\lambda) + (-1)^n) = \frac{n+1}{p-1}.$$

The proof of this lemma will be presented later.

**Remark 5.7** It would be interesting to determine $v_p((p^k-1)Kl_{n,k}(\lambda) + (-1)^n)$ when $k$ is divisible by $p$.

**Application: Construction of subfields of $\mathbb{Q}(\zeta_p)$ via Kloosterman sums**

Let $d|(p-1)$ and $K_d$ be the unique subfield of $\mathbb{Q}(\zeta_p)$ such that $[K_d : \mathbb{Q}] = d$. Previously, by Gauss, we showed that $K_d = \mathbb{Q}(S_1(x^d))$. Now we have

**Corollary 5.8** *Let $d|(p-1)$. Take $n = \frac{p-1}{d} - 1$, then $K_d = \mathbb{Q}(Kl_{n,1}(\lambda))$ for any $\lambda \in \mathbb{F}_p^\times$.*

*Proof* Use the result of degree in the previous section, we see that

$$\deg Kl_{n,1}(\lambda) = \frac{p-1}{(p-1,n+1)} = \frac{p-1}{(p-1,(p-1)/d)} = d.$$

The proof is finished. ∎

## 6 $p$-adic Estimates of Exponential Sums

In this section, we explain how to use the classical Stickelberger theorem to estimate $p$-adic valuation of various exponential sums.

### 6.1 Stickelberger Theorem

Let $\mathbb{Z}_p$ be the ring of $p$-adic integers in $\mathbb{Q}_p$, which is the $p$-adic completion of $\mathbb{Z}$ under $|\cdot|_p$. It can also be written as

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p | \, |\alpha|_p \leq 1\},$$

which is the closed unit disk in $\mathbb{Q}_p$. The maximal ideal $p\mathbb{Z}_p$ is the open unit disk and the residue field $\mathbb{Z}_p/p\mathbb{Z}_p$ is $\mathbb{F}_p$. Conversely,

$$\mathbb{Z}_p = W(\mathbb{F}_p) = \text{lifting of } \mathbb{F}_p \text{ to characteristic } 0,$$

where $W$ means the Witt vectors.

Now for each $k \in \mathbb{N}$, we want to lift $\mathbb{F}_{p^k}$ as well, i.e., $\mathbb{Z}_{p^k} = W(\mathbb{F}_{p^k})$, the Witt ring of $\mathbb{F}_{p^k}$.

The ring $\mathbb{Z}_{p^k}$ is the ring of integers in the unique unramified extension $\mathbb{Q}_{p^k}$ of $\mathbb{Q}_p$ of degree $k$ and can be written as

$$\mathbb{Z}_{p^k} = \{\alpha \in \mathbb{Q}_{p^k} | \, |\alpha|_p \leq 1\},$$

which is the closed unit disk in $\mathbb{Q}_{p^k}$. The maximal ideal $p\mathbb{Z}_{p^k}$ is the open unit disk and the residue field $\mathbb{Z}_{p^k}/p\mathbb{Z}_{p^k}$ is $\mathbb{F}_{p^k}$.

The "mod $p$" reduction $\pi : \mathbb{Z}_{p^k} \to \mathbb{F}_{p^k}$ is a surjective ring homomorphism. And there is a unique injective GROUP (not ring) homomorphism

$$\omega : \mathbb{F}_{p^k}^\times \to \mathbb{Z}_{p^k}^\times \hookrightarrow \mathbb{C}_p^\times$$

such that

$$\pi \circ \omega : \mathbb{F}_{p^k}^\times \to \mathbb{F}_{p^k}^\times$$

is an identity map and $\omega(\alpha\beta) = \omega(\alpha)\omega(\beta)$, $\omega(\alpha) \equiv \alpha \mod p$.

Moreover, if $\mathbb{F}_{p^k}^\times = \langle g \rangle$, then $\omega(g)$ is a primitive $(p^k - 1)$-th root of 1 in $\mathbb{C}_p$. Hence, the map $\omega$ is

$$\omega : \mathbb{F}_{p^k}^\times \xrightarrow{\sim} \boldsymbol{\mu}_{p^k-1} \subset \mathbb{C}_p^\times,$$

where $\boldsymbol{\mu}_{p^k-1} = \{\alpha \in \mathbb{C}_p^\times | \alpha^{p^k-1} = 1\}$. This is called the **Teichmller lifting** of $\mathbb{F}_{p^k}^\times$.

**Proposition 6.1** *Any multiplicative character $\chi : \mathbb{F}_{p^k}^\times \to \mathbb{C}_p^\times$ can be uniquely written as $\chi = \omega^{-j}$, where $0 \leq j < p^k - 1$. The case $j = 0$ corresponds to the trivial character.*

Fix a primitive $p$-th root $\zeta_p$ of 1 in $\mathbb{C}_p$. The **$p$-adic Gauss sum** attached to the multiplicative character $\omega^{-j} : \mathbb{F}_{p^k}^\times \to \mathbb{C}_p^\times$ is defined as

$$G_k(j) = -\sum_{x \in \mathbb{F}_{p^k}^\times} \omega(x)^{-j} \cdot \zeta_p^{\mathrm{Tr}_k(x)},$$

where $0 \leq j \leq p^k - 2$. Using the Teichmller lifting, we can write this as

$$G_k(j) = -\sum_{x \in \boldsymbol{\mu}_{p^k-1}} x^{-j} \cdot \zeta_p^{\mathrm{Tr}_k(x)},$$

where $\mathrm{Tr}_k : \mathbb{Z}_{p^k} \to \mathbb{Z}_p$ is the trace map. Clearly, $G_k(0) = 1$. Note that

$$G_k(pj) = -\sum_{x \in \boldsymbol{\mu}_{p^k-1}} x^{-pj} \cdot \zeta_p^{\mathrm{Tr}_k(x)} = -\sum_{x \in \boldsymbol{\mu}_{p^k-1}} (x^p)^{-j} \cdot \zeta_p^{\mathrm{Tr}_k(x^p)} = G_k(j).$$

**Example 6.2** As a complex number, $|G_k(j)| = \sqrt{p^k}$, for $1 \leq j \leq p^k - 2$.

After these preparations, we now state the Stickelberger theorem:

**Theorem 6.3** (Stickelberger[13], 1890) *For $0 \leq j \leq p^k - 2$, write*

$$j = i_0 + i_1 p + i_2 p^2 + \cdots + i_{k-1} p^{k-1}$$

*and*

$$\sigma_p(j) = i_0 + i_1 + \cdots + i_{k-1} = \textit{sum of } p\textit{-digits of } j.$$

*Then*

$$v_p(G_k(j)) = \frac{1}{p-1}\sigma_p(j).$$

Now we provide a useful example.

**Example 6.4** If $d|(p-1)$, the for all $1 \le i \le d-1$, we have

$$\frac{p^k-1}{d}i = \frac{i(p-1)}{d}\frac{p^k-1}{p-1} = \frac{i(p-1)}{d} + \frac{i(p-1)}{d}p + \cdots + \frac{i(p-1)}{d}p^{k-1}.$$

Hence $\sigma_p\left(\frac{p^k-1}{d}i\right) = ki\frac{p-1}{d}$. By Stickelberger theorem, we obtain

$$v_p\left(G_k\left(\frac{p^k-1}{d}i\right)\right) = \frac{ki}{d}.$$

An exact $p$-adic formula for $G_k(j)$ in terms of $p$-adic $\Gamma$-function was given by Gross-Koblitz in 1979, see [15].

### 6.2 $p$-adic Valuation of Monomial Sum $S_k(x^d)$

The monomial sum $S_k(x^d)$ can be expressed in terms of Gauss sums. In this subsection, we shall prove

**Theorem 6.5** *Let $d|(p^k-1)$, then $v_p(S_k(x^d)) \ge \frac{k}{d}$. The equality holds if and only if $p \equiv 1 \bmod d$.*

*Proof* Let $\chi := \omega^{-\frac{p^k-1}{d}} : \mathbb{F}_{p^k}^\times \to \mathbb{C}_p^\times$, $\chi(0) = 1$, the primitive character of degree $d$. Then

$$\begin{aligned} S_k(x^d) &= 1 + \sum_{x \in \boldsymbol{\mu}_{p^k-1}} \zeta_p^{\mathrm{Tr}_k(x^d)} \\ &= 1 + \sum_{y \in \mathbb{F}_{p^k}^\times} \left(\sum_{i=1}^{d} \chi^i(y)\right) \zeta_p^{\mathrm{Tr}_k(y)}. \end{aligned}$$

Here we are using the relation

$$\sum_{i=1}^{d} \chi^i(y) = \begin{cases} d, & \text{if } y \in \left(\mathbb{F}_{p^k}^\times\right)^d, \\ 0, & \text{if } y \notin \left(\mathbb{F}_{p^k}^\times\right)^d. \end{cases}$$

Then

$$\begin{aligned} S_k(x^d) &= \sum_{i=1}^{d-1} \sum_{y \in \mathbb{F}_{p^k}^\times} \chi^i(y)\zeta_p^{\mathrm{Tr}_k(y)} + \left(\sum_{y \in \mathbb{F}_{p^k}^\times} \zeta_p^{\mathrm{Tr}_k(y)} + 1\right) \\ &= -\sum_{i=1}^{d-1} G_k\left(\frac{p^k-1}{d}i\right). \end{aligned}$$

By the example from the previous section, if $p \equiv 1 \mod d$, then

$$v_p\left(G_k\left(\frac{p^k-1}{d}i\right)\right) = \frac{ki}{d},$$

and hence $v_p(S_k(x^d)) = \frac{k}{d}$.

Assume now $d|(p^k-1)$ but $d \nmid (p-1)$. Clearly, $k \geq 2$, and we want to show $v_p(S_k(x^d)) > \frac{k}{d}$. Write

$$\frac{p^k-1}{d}i = j_0 + j_1 p + j_2 p^2 + \cdots + j_{k-1}p^{k-1},$$

where $0 \leq j_k \leq p-1$. Then we obtain

$$\begin{aligned}
&\frac{p^k-1}{d}i = j_0 + j_1 p + j_2 p^2 + \cdots + j_{k-1}p^{k-1},\\
&\frac{p^k-1}{d}\langle pi\rangle_d = j_{k-1} + j_0 p + j_1 p^2 + \cdots + j_{k-2}p^{k-1},\\
&\quad\vdots\\
&\frac{p^k-1}{d}\left\langle p^{k-1}i\right\rangle_d = j_1 + j_2 p + j_3 p^2 + \cdots + j_0 p^{k-1},
\end{aligned}$$

where $\langle pi\rangle_d$ is the smallest positive residue of $pi \mod d$. Summing both sides, we obtain

$$\frac{p^k-1}{d}(i + \langle pi\rangle_d + \cdots + \left\langle p^{k-1}i\right\rangle_d) = (j_0 + j_1 + \cdots + j_{k-1})(1 + p + \cdots + p^{k-1}),$$

and note that

$$1 \leq i, \langle pi\rangle_d, \cdots, \left\langle p^{k-1}i\right\rangle_d \leq d-1,$$

we get

$$j_0 + \cdots + j_{k-1} = \frac{p-1}{d}(i + \langle pi\rangle_d + \cdots + \left\langle p^{k-1}i\right\rangle_d) \geq \frac{p-1}{d}(\underbrace{1 + \cdots + 1}_{k \text{ times}}) = \frac{k(p-1)}{d},$$

with the equality holding if and only if $i = 1$ and $p \equiv 1 \mod d$. Thus, if $p \not\equiv 1 \mod d$, then

$$v_p\left(G_k\left(\frac{p^k-1}{d}i\right)\right) = \frac{1}{p-1}(j_0 + j_1 + \cdots + j_{k-1}) > \frac{1}{p-1}\frac{k(p-1)}{d} = \frac{k}{d}.$$

The proof is now completed. ∎

**Remark 6.6** If $p-1$ is not divisible by $d$, it is an open problem in general to determine this sequence $v_p(S_k(x^d))$ in $k$. This is the main reason that we are not able to determine the degree sequence for $S_k(x^d)$ for general $d$.

### 6.3 $p$-adic Valuation of Kloosterman Sums

In this subsection, we shall prove

**Theorem 6.7** *Let $\lambda \in \mathbb{F}_p^\times$, then*

$$v_p\left((p^k-1)Kl_{n,k}(\lambda) + (-1)^n + (-1)^n(G_k(1))^{n+1}k\omega(\lambda)\right) \geq \frac{2(n+1)}{p-1}.$$

*Proof* Calculate

$$\begin{aligned}\sum_{j=0}^{p^k-2}\omega^j(\lambda)G_k(j)^{n+1} &= (-1)^{n+1}\sum_{j=0}^{p^k-2}\omega^j(\lambda)\left(\sum_{a\in\mathbb{F}_{p^k}^\times}\omega^{-j}(a)\zeta_p^{\mathrm{Tr}_k(a)}\right)^{n+1}\\ &= (-1)^{n+1}\sum_{a_1,\cdots,a_{n+1}\in\mathbb{F}_{p^k}^\times}\zeta_p^{\mathrm{Tr}_k(a_1+\cdots+a_{n+1})}\cdot\sum_{j=0}^{p^k-2}\omega^j\left(\frac{\lambda}{a_1\cdots a_{n+1}}\right)\\ &= (-1)^{n+1}(p^k-1)\sum_{a_1\cdots a_{n+1}=\lambda,a_1,\cdots,a_{n+1}\in\mathbb{F}_{p^k}^\times}\zeta_p^{\mathrm{Tr}_k(a_1+\cdots+a_{n+1})}\\ &= (-1)^{n+1}(p^k-1)Kl_{n,k}(\lambda).\end{aligned}$$

Hence,

$$\begin{aligned}&(p^k-1)Kl_{n,k}(\lambda)\\ =&(-1)^{n+1}\left(\sum_{j=0}^{p^k-2}\omega^j(\lambda)G_k(j)^{n+1}\right)\\ =&(-1)^{n+1}\Big(G_k(0)^{n+1}+\Big(\omega(\lambda)G_k(1)^{n+1}+\omega(\lambda^p)G_k(p)^{n+1}+\cdots+\omega(\lambda^{p^{k-1}})G_k(p^{k-1})^{n+1}\Big)\\ &\qquad+\sum_{\sigma_p(j)\geq 2}\omega^j(\lambda)G_k(j)^{n+1}\Big)\\ =&(-1)^{n+1}\left(1+k\omega(\lambda)(G_k(1))^{n+1}+\sum_{\sigma_p(j)\geq 2}\omega^j(\lambda)G_k(j)^{n+1}\right).\end{aligned}$$

Here we used the assumption that $\lambda\in\mathbb{F}_p^\times$, which implies that $\omega(\lambda)=\omega(\lambda^p)=\cdots=\omega(\lambda^{p^{k-1}})$. Furthermore, $G_k(1)=G_k(p)=\cdots=G_k(p^{k-1})$. Now for $\sigma_p(j)\geq 2$, we have

$$v_p(G_k(j))\geq\frac{2}{p-1}.$$

Hence we obtain

$$v_p\left((p^k-1)Kl_{n,k}(\lambda)+(-1)^n+(-1)^n(G_k(1))^{n+1}k\omega(\lambda)\right)\geq\frac{2(n+1)}{p-1},$$

as desired. ∎

As a corollary, we deduce

**Corollary 6.8** *If $k\neq 0 \mod p$ and $\lambda\in\mathbb{F}_p^\times$, then*

$$v_p\left((p^k-1)Kl_{n,k}(\lambda)+(-1)^n\right)=\frac{n+1}{p-1}.$$

### 6.4 General $p$-adic Estimates

Using the elementary method as above, one can prove the following result of Sperber which was orginally proved using Dwork's $p$-adic theory.

**Theorem 6.9** (Sperber[16]) *Let $f(x_1, x_2, \cdots, x_n) \in \mathbb{F}_{p^k}[x_1, x_2, \cdots, x_n]$ and $d = \deg(f)$. Then*

$$v_p(S_k(f)) \geq \frac{n}{d}k$$

*for all $k \in \mathbb{N}$.*

In the one variable case, we also have the following more precise result.

**Theorem 6.10** *Let $f(x) = x^d + a_1x^{d-1} + \cdots + a_d \in \mathbb{F}_{p^k}[x]$ be a polynomial in one variable. Then $v_p(S_k(f)) \geq k/d$ with equality holding if and only if $p \equiv 1 \mod d$.*

Again, if $p \not\equiv 1 \mod d$, the exact value of $v_p(S_k(f))$ is unknown and can be complicated. Results on $p$-adic estimates of exponential sums can be used to derive $p$-adic estimates for the number of rational points on equations over finite fields.

**Theorem 6.11** (Ax[17]) *Let $f(x_1, x_2, \cdots, x_n) \in \mathbb{F}_{p^k}[x_1, x_2, \cdots, x_n]$ and $d = \deg(f) > 0$. Let*

$$N_k(f) = \#\{(x_1, x_2, \cdots, x_n) \in \mathbb{F}_{p^k}^n | f(x_1, x_2, \cdots, x_n) = 0\}.$$

*Then $v_p(N_k(f)) \geq k\lceil \frac{n-d}{d} \rceil$.*

For a system of $m$ polynomials, we have

**Theorem 6.12** (Katz[18]) *Let $f_1(x_1, x_2, \cdots, x_n), \cdots, f_m(x_1, x_2, \cdots, x_n) \in \mathbb{F}_{p^k}[x_1, x_2, \cdots, x_n]$, with $\max_{1\leq i\leq m} \deg(f_i) > 0$. Let*

$$N_k(F) = \#\{(x_1, x_2, \cdots, x_n) \in \mathbb{F}_{p^k}^n | f_1(x_1, x_2, \cdots, x_n) = \cdots = f_m(x_1, x_2, \cdots, x_n) = 0\}.$$

*Then*

$$v_p(N_k(F)) \geq k\left(\left\lceil \frac{n - \sum_{i=1}^m \deg(f_i)}{\max_{1\leq i\leq m} \deg(f_i)} \right\rceil\right).$$

Katz's original proof was based on Dwork's $p$-adic theory. It can also be proved using just the Stickelberger theorem as above, see [19]. Alternatively, Hou[20] showed that Katz's theorem can be reduced to Ax's theorem in a quick elementary way.

More generally, we have

**Theorem 6.13** (Adolphson and Sperber[21]) *Write*

$$f(x_1, x_2, \cdots, x_n) = \sum_{j=1}^{J} a_j x_1^{v_{j1}} x_2^{v_{j2}} \cdots x_n^{v_{jn}} \in \mathbb{F}_{p^k}[x_1, x_2, \cdots, x_n].$$

*Let $\Delta$ be the convex polytope in $\mathbb{R}^n$ of the origin 0 and the lattice points $(v_{j1}, v_{j2}, \cdots, v_{jn}) \in \mathbb{R}^n$, where $1 \leq j \leq J$. Let*

$$\mu(f) = \min\{\mu > 0 | \mu\Delta(f) \cap \mathbb{N}^n \neq \emptyset\}.$$

*Then*

$$v_p(S_k(f)) \geq \mu(f)k.$$

This result was originally proved using Dwork's theory. It can again be proved using just the Stickelberger theorem as above. Here is an example:

**Example 6.14** Let $f(x_1, x_2, \cdots, x_n) \in \mathbb{F}_p[x_1, x_2, \cdots, x_n]$ and $d = \deg(f)$. Then

$$\Delta(f) \subset \Delta(x_1^d + x_2^d + \cdots + x_n^d).$$

It follows that $\mu(f) \geq \mu(\Delta) = \frac{n}{d}$. This gives Sperber's theorem. See Figure 1 for this. It is easy to check that the above Adolphson-Sperber theorem also implies the Ax-Katz theorem.

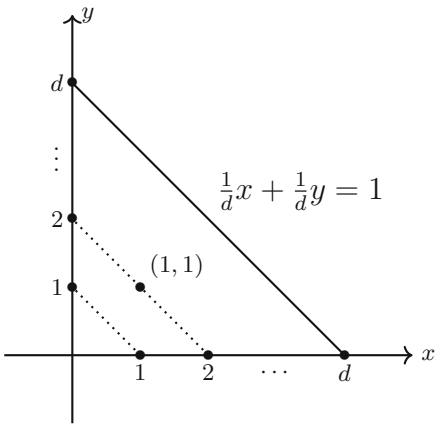



**Figure 1** For Example 6.14

**Remark 6.15** There are further improvements using finer and more complicated quantities such as $p$-weights and the degree matrix, see Moreno and Moreno[23], Blache[24], Chen and Cao[25], and Cao and Sun[26]. The idea is to use $p$-reduction to reduce the degree of $f(x)$ as follow. Write $d = d_0 + d_1 p + \cdots + d_s p^s$, where $0 \leq d_i < p$. Let $\{e_1, e_2, \cdots, e_k\}$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^k}$, then any $x \in \mathbb{F}_{p^k}$ can be written uniquely as

$$x = x_1 e_1 + x_2 e_2 + \cdots + x_k e_k$$

and

$$\begin{aligned} x^d = &(x_1 e_1 + x_2 e_2 + \cdots + x_k e_k)^{d_0} (x_1 e_1^p + x_2 e_2^p + \cdots + x_k e_k^p)^{d_1} \\ &\cdots (x_1 e_1^{p^s} + x_2 e_2^{p^s} + \cdots + x_k e_k^{p^s})^{d_s} \in \mathbb{F}_{p^k}[x_1, x_2, \cdots, x_k]. \end{aligned}$$

The degree has now dropped to $d_0 + d_1 + \cdots + d_s \leq d$. This can lead to improvements in the some cases when $p < d$.

## 7 Distinctness and Rationality of Exponential Sums

In this section, we carry on further discussion on the degree of exponential sums from two perspectives: The distinctness and rationality of exponential sums.

### 7.1 Distinctness of Kloosterman Sums

Recall that for $\lambda \in \mathbb{F}_{p^k}^\times$, the $n$-dimensional Kloostman sum over $\mathbb{F}_{p^k}$ is defined as

$$Kl_{n,k}(\lambda) = \sum_{x_1,x_2,\cdots,x_n \in \mathbb{F}_{p^k}^\times} \zeta_p^{\mathrm{Tr}_k\left(x_1+x_2+\cdots+x_n+\frac{\lambda}{x_1x_2\cdots x_n}\right)}.$$

Now our first question is:

QUESTION: As the nonzero parameter $\lambda$ varies in the prime field $\mathbb{F}_p$, when the $(p-1)$ Kloosterman sums $\{Kl_{n,k}(\lambda)|\lambda \in \mathbb{F}_p^\times\}$ are distinct?

This question is closely related to the degree of Kloosterman sums, i.e.,

$$\deg Kl_{n,k}(\lambda) = \text{number of distinct elements in } \{Kl_{n,k}(a^{n+1}\lambda)|a \in \mathbb{F}_p^\times\}.$$

The congruence formula for $Kl_{n,k}(\lambda)$ gives

**Theorem 7.1** *Assume $(k,p)=1$. Then the $(p-1)$ Kloosterman sums $\{Kl_{n,k}(\lambda)|\lambda \in \mathbb{F}_p^\times\}$ are distinct. In particular,*

$$\deg Kl_{n,k}(\lambda) = \#\{a^{n+1}|a \in \mathbb{F}_p^\times\} = \frac{p-1}{(n+1,p-1)}.$$

*Proof* By the congruence formula for Kloosterman sum,

$$(p^k-1)Kl_{n,k}(\lambda) = (-1)^{n+1}(1+k\omega(\lambda)G_k(1)^{n+1}) + O\left(p^{\frac{2(n+1)}{p-1}}\right).$$

Now if $(k,p)=1$, then $v_p(k\omega(\lambda)G_k(1)^{n+1}) = \frac{n+1}{p-1}$, and the coefficient $k\omega(\lambda)$ are distinct in $\mathbb{F}_p^\times$ as $\lambda$ varies in $\mathbb{F}_p^\times$. ∎

In the special case, $k=2^m, p>2, n=1$, the first part of this theorem was re-proved by Borissor-Boissov[22] in 2020. The first part of the special case $(k,p)=1$ and $n=1$, of the above theorem, was raised as an open problem in the same paper.

In the above, we only considered the case that the parameter $\lambda$ varies in the prime field $\mathbb{F}_p^\times$. Our second question is to consider when the parameter $\lambda$ varies in the extension field $\mathbb{F}_{p^k}^\times$. Namely,

QUESTION$^+$: When the $(p^k-1)$ Kloosterman sums $\{Kl_{n,k}(\lambda)|\lambda \in \mathbb{F}_{p^k}^\times\}$ are distinct?

As we shall see, this problem is significantly harder! Note that

$$Kl_{n,k}(\lambda) = \sum_{x_1,x_2,\cdots,x_n \in \mathbb{F}_{p^k}^\times} \zeta_p^{\mathrm{Tr}_k\left(x_1^p+x_2^p+\cdots+x_n^p+\frac{\lambda^p}{x_1^px_2^p\cdots x_n^p}\right)} = Kl_{n,k}(\lambda^p),$$

which can be regarded as the Frobenius $\mathrm{Frob}_p$ acting on $Kl_{n,k}(\lambda)$. So the best one we can hope is that if

$$Kl_{n,k}(\lambda_1) = Kl_{n,k}(\lambda_2),$$

then $\lambda_1, \lambda_2$ are Frobenius conjugate over $\mathbb{F}_p$, i.e., $\lambda_1 = \lambda_2^{p^i}$ for some $i$. However, there are examples where $Kl_{n,k}(\lambda_1) = Kl_{n,k}(\lambda_2)$ but $\lambda_1, \lambda_2$ are not Frobenius conjugate. Some more conditions are needed.

**Conjecture 7.2** (see [14, 27]) If $p \geq k(n+1)$, $Kl_{n,k}(\lambda_1) = Kl_{n,k}(\lambda_2)$, where $\lambda_1, \lambda_2 \in \mathbb{F}_{p^k}^{\times}$, then $\lambda_1, \lambda_2$ are Frobenius conjugate.

This conjecture is equivalent to saying, for $p \geq k(n+1)$,

$$\#\{Kl_{n,k}(\lambda) | \lambda \in \mathbb{F}_{p^k}^{\times}\} = I_k(p) - 1,$$

where $I_k(p) = \#\{$ monic irreducible polynomials of degree dividing $k$ in $\mathbb{F}_p[x]\}$.

Now assume that the Ref conjecture holds, that is, $Kl_{n,k}(\lambda_1) = Kl_{n,k}(\lambda_2)$ implies $\lambda_1, \lambda_2$ are conjugate over $\mathbb{F}_p$ (where $\lambda_1, \lambda_2 \in \mathbb{F}_{p^k}^{\times}$). Then for $\lambda \in \mathbb{F}_{p^k}^{\times}$,

$$\begin{aligned}\deg Kl_{n,k}(\lambda) &= \#\{Kl_{n,k}(a^{n+1}\lambda) | a \in \mathbb{F}_p^{\times}\} \\ &= \frac{p-1}{\#\left\{a \in \mathbb{F}_p^{\times} | a^{n+1} \in \{1, \lambda^{p-1}, \lambda^{p^2-1}, \cdots\}\right\}} \\ &= \frac{p-1}{(p-1, n+1) \cdot \#\left\{\{1, \lambda^{p-1}, \lambda^{p^2-1}, \cdots\} \cap (\mathbb{F}_p^{\times})^{(n+1, p-1)}\right\}}.\end{aligned}$$

This shows that even if we assume that the Ref conjecture holds, the degree formula for $\deg Kl_{n,k}(\lambda)$ can still be somewhat complicated when $k > 1$. The Ref conjecture is known to be true in some cases.

**Theorem 7.3** (Fisher[27]) *If $p > (2(n+1)^{2k}+1)^2$ and $Kl_{n,k}(\lambda_1) = Kl_{n,k}(\lambda_2)$ for $\lambda_1, \lambda_2 \in \mathbb{F}_{p^k}^{\times}$, then $\lambda_1, \lambda_2$ are Frobenius conjugate.*

This result shows that the Ref conjecture is true if $p$ is large compared to $n$ and $k$. The proof uses $\ell$-adic cohomology for prime $\ell \neq p$.

**Theorem 7.4** (see [14]) *Assume $p \geq (k-1)(n+1)+2$ and $p \nmid N_1(n)N_2(n)\cdots N_k(n)$, where*

$$\sum_{h=1}^{\infty} \frac{N_h(n)}{(h!)^{n+1}} z^h = \log \sum_{j=0}^{\infty} \frac{z^j}{(j!)^{n+1}}.$$

*If $Kl_{n,k}(\lambda_1) = Kl_{n,k}(\lambda_2)$ for $\lambda_1, \lambda_2 \in \mathbb{F}_{p^k}^{\times}$, then $\lambda_1, \lambda_2$ are Frobenius conjugate.*

Dwork showed that $N_h(n) \neq 0$ for all $h, n$ and gave an asymptotic formula for $N_h(n)$. Thus, the above theorem shows that the Ref conjecture is true if $p$ does not divide certain non-zero integer. The proof uses $p$-adic method and Stickelberger theorem. Note that the above two theorems are proved using non-archimedian methods. It would be interesting to give a direct archimedian proof which might shed more light. Another elementary problem is

PROBLEM: Prove that $N_h(n) \in \mathbb{Z}$ for all $h, n \in \mathbb{Z}$. Explicitly, we have

$$N_h(n) = \sum_{s=1}^{k} \frac{(-1)^{s-1}}{s} \sum_{h_1+h_2+\cdots+h_s=h} \binom{h}{h_1, h_2, \cdots, h_s}^{n+1}.$$

For example, we have

$$\begin{aligned} N_1(n) &= 1, \\ N_2(n) &= 1 - 2^n, \\ N_3(n) &= 1 - 3^{n+1} + 2 \cdot 6^n, \\ &\vdots \end{aligned}$$

As a corollary, we obtain

**Corollary 7.5** *The Ref conjecture is true for $k = 1$ and all $p$.*

This is slightly stronger than the original Ref conjecture, which assumes $p \geq (n+1)$ if $k = 1$. The Ref conjecture is also true if $n = 1$, $k \leq 4$. It should be possible to extend the range of $k$ with computer calculations.

**General case**

We shall in general consider for $f(x_1, x_2, \cdots, x_n) \in \mathbb{F}_p[x_1, x_2, \cdots, x_n]$, and

$$\deg S_k(f) = \text{number of distinct Galois conjugates in } \{S_k(af) | a \in \mathbb{F}_p^\times\}.$$

Now the questions are:

QUESTION 1: $\#\{\text{distinct } S_k(af) | a \in \mathbb{F}_p^\times\} = ?$;

QUESTION 2: $\#\{\text{distinct } S_k(af) | a \in \mathbb{F}_{p^k}^\times\} = ?$.

It should be possible to prove many results in this direction using either $p$-adic method or $\ell$-adic method. The above explained the classical examples of Kloosterman sums.

As another example arising from applications, let us consider the Weil spectrum. For $1 \leq d \leq p^k - 1$, the **Weil spectrum** is the set

$$W_{p^k,d} = \{S_k(x^d + ax) | a \in \mathbb{F}_{p^k}^\times\}.$$

One interesting problem is to give a good lower bound for the size of the set $W_{p^k,d}$.

**Theorem 7.6** *Let $(d, p^k - 1) = 1$, $d \not\equiv p^i \mod (p^k - 1)$, then $\left|W_{p^k,d}\right| \geq 3$.*

Furthermore, one has the following two conjectures by Helleseth in 1971, see the survey by Katz and Langevin[28].

**Conjecture 7.7** Let $(d, p^k - 1) = 1$, $d \not\equiv p^i \mod (p^k - 1)$ and $k = 2^m$, then $\left|W_{p^k,d}\right| \geq 4$.

This conjecture is proved if $p = 2, 3$, but still open for $p \geq 5$.

**Conjecture 7.8** Let $(d, p^k - 1) = 1$, $d \equiv 1 \mod (p - 1)$ and $p^k > 2$, then there exists $a \in \mathbb{F}_{p^k}^\times$ such that $S_k(x^d + ax) = 0$.

Note that if $d \equiv 1 \mod p - 1$, then for all $b \in \mathbb{F}_p^\times$,

$$\sigma_b(S_k(x^d + ax)) = S_k(bx((bx)^{d-1} + a)) = S_k(x^d + ax),$$

which implies that $S_k(x^d + ax) \in \mathbb{Z}$.

### 7.2 Rationality of Exponential Sums

Recall that for a polynomial $f(x_1, x_2, \cdots, x_n) \in \mathbb{F}_{p^k}[x_1, x_2, \cdots, x_n]$, we defined the exponential sum

$$S_k(f) = \sum_{x_1, x_2, \cdots, x_n \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(f(x_1, x_2, \cdots, x_n))} \in \mathbb{Z}[\zeta_p].$$

In this chapter, we shall discuss the following question.

QUESTION: When the exponential sum $S_k(f)$ is a rational integer in $\mathbb{Z}$? In other words, when $\deg S_k(f) = 1$?

**Definition 7.9** Let $n_k(f)$ be the number of $\mathbb{F}_{p^k}$-rational points on the *Artin-Schreier hypersurface* defined by

$$y^p - y = f(x_1, x_2, \cdots, x_n).$$

A simple property is

**Theorem 7.10** *$S_k(f) \in \mathbb{Z}$ if and only if $S_k(f) = \frac{n_k(f)-p^{kn}}{p-1}$.*

*Proof* Since $n_k(f) \in \mathbb{Z}$, the "$\Leftarrow$" direction is immediate. For the "$\Rightarrow$" direction, note that we always have

$$n_k(f) = \sum_{a\in\mathbb{F}_p} S_k(af).$$

If now, $S_k(f) \in \mathbb{Z}$, we deduce

$$n_k(f) = p^{kn} + \sum_{a\in\mathbb{F}_p^\times} S_k(af) = p^{kn} + (p-1)S_k(f).$$

The proof is complete. ∎

As a corollary, we deduce

**Corollary 7.11** *If $n_k(f) \not\equiv 1 \mod (p-1)$, then $S_k(f) \notin \mathbb{Z}$.*

For $0 \le i \le p-1$, we define

$$n_k(f,i) = \#\{(x_1, x_2, \cdots, x_n) \in \mathbb{F}_{p^k}^n | \mathrm{Tr}_k(f(x_1, x_2, \cdots, x_n)) = i\}.$$

Then $n_k(f,0) = \frac{1}{p} n_k(f)$. Another characterization for $S_k(f) \in \mathbb{Z}$ is the following

**Theorem 7.12** *$S_k(f) \in \mathbb{Z}$ if and only if $n_k(f,1) = n_k(f,2) = \cdots = n_k(f,p-1)$, which is equivalent to $n_k(f,i) = \frac{1}{p(p-1)}(p^{kn+1} - n_k(f))$ for all $i \in \mathbb{F}_p^\times$.*

*Proof* Assume $S_k(f) = m \in \mathbb{Z}$. Then we can rewrite $S_k(f)$ as

$$S_k(f) = \sum_{i=0}^{p-1} \zeta_p^i \cdot n_k(f,i).$$

Then we have two relations over $\mathbb{Q}$:

$$\begin{cases} \sum_{i=1}^{p-1} \zeta_p^i \cdot n_k(f,i) + n_k(f,0) - m = 0, \\ \sum_{i=1}^{p-1} \zeta_p^i + 1 = 0. \end{cases}$$

Since $\deg(\zeta_p) = p-1$, the first relation must be a constant multiple of the second relation, hence

$$n_k(f,1) = \cdots = n_k(f,p-1) = n_k(f,0) - m.$$

We also have

$$n_k(f,0) + n_k(f,1) + \cdots + n_k(f,p-1) = p^{kn}.$$

Recall that $n_k(f,0)=\frac{1}{p}n_k(f)$, we obtain for $i\in\mathbb{F}_p^{times}$,

$$\frac{1}{p}n_k(f)+(p-1)n_k(f,i)=p^{kn}.$$

This shows that

$$n_k(f,i)=\frac{1}{p(p-1)}(p^{kn+1}-n_k(f))$$

for $i\in\mathbb{F}_p^{\times}$. Conversely, if $n_k(f,1)=n_k(f,2)=\cdots=n_k(f,p-1)$, then

$$S_k(f)=\sum_{i=0}^{p-1}\zeta_p^i\cdot n_k(f,i)=n_k(f,0)-n_k(f,1)\in\mathbb{Z}.$$

Recall that our basic question of this section is

QUESTION: Classify the polynomials $f(x_1,x_2,\cdots,x_n)\in\mathbb{F}_{p^k}[x_1,x_2,\cdots,x_n]$ such that $S_k(f)\in\mathbb{Z}$.

This is very interesting even in the case of $n=1$. We now consider this one variable case. Let $f(x)\in\mathbb{F}_{p^k}[x]$. Note that $\alpha^{p^k}=\alpha$ for all $\alpha\in\mathbb{F}_{p^k}$, we can assume $d=\deg(f)<p^k$. Using the reduction $\mathrm{Tr}_k(a\alpha^p)=\mathrm{Tr}_k(a^{1/p}\alpha)$, we can further assume that $f(x)$ has no terms of the form $x^{pi}$. Recall

$$n_k(f,i)=\#\{x\in\mathbb{F}_{p^k}|\mathrm{Tr}_k(f(x))=i\},\quad i\in\mathbb{F}_p.$$

By the previous theorem, our question in the one variable case is equivalent to

QUESTION: Classify polynomials $f(x)\in\mathbb{F}_{p^k}[x]$, such that $n_k(f,1)=n_k(f,2)=\cdots=n_k(f,p-1)$.

We first give some examples.

**Example 7.13** If $f(x)$ is a **permutation polynomial** (PP) over $\mathbb{F}_{p^k}$, then $S_k(f)=S_k(x)=0$, and hence $n_k(f,i)=\frac{p^k}{p}=p^{k-1}$, for all $i\in\mathbb{F}_p$.

But there are other examples if $k>1$.

**Example 7.14** Let $f(x)=x^d$ where $d\Big|\frac{p^k-1}{p-1}$, $d>1$ and $k\geq 2$. Then $f(x)$ is NOT PP over $\mathbb{F}_{p^k}$ as $(d,p^k-1)>1$. But we know that $S_k(f)\in\mathbb{Z}$. This implies that

$$n_k(f,1)=n_k(f,2)=\cdots=n_k(f,p-1)=\frac{1}{p(p-1)}(p^{k+1}-n_k(f)),\quad S_k(f)=\frac{n_k(f)-p^k}{p-1},$$

where

$$n_k(f)=\#\{(x,y)\in\mathbb{F}_{p^k}^2|y^p-y=x^d\}.$$

However, if $k=1$, there are no other examples. In fact, let $f(x)\in\mathbb{F}_p[x]$ with degree $1\leq d=\deg(f)\leq p-1$, then

$$n_1(f,i)=\#\{x\in\mathbb{F}_p|\mathrm{Tr}_1(f(x))=i\}=\#\{x\in\mathbb{F}_p|f(x)=i\}\leq p-1.$$

Note that $n_1(f,0)+\cdots+n_1(f,p-1)=p$. As $2(p-1)>p$ and

$$n_1(f,1)=n_1(f,2)=\cdots=n_1(f,p-1)=c,$$

we must have $c \in \{0, 1\}$. If $c = 0$, then $n_1(f, 0) = p$ and then $f(x) \equiv 0$ on $\mathbb{F}_p$. This is a contradiction. Hence, $c = 1$. This implies that $n_1(f, 0) = 1$ as well. Hence, $f(x)$ is PP over $\mathbb{F}_p$. To sum up, we have shown:

**Theorem 7.15** *For $f \in \mathbb{F}_p[x]$, $1 \le d = \deg(f) \le p - 1$, we have $S_1(f) \in \mathbb{Z}$ if and only if $f(x)$ is PP over $\mathbb{F}_p$.*

The classification of permutation polynomials over $\mathbb{F}_{p^k}$ is itself an interesting topic, and has been studied extensively. This has various applications.

**Definition 7.16** A polynomial $f(x) \in \mathbb{F}_{p^k}[x]$ is called **exceptional** over $\mathbb{F}_{p^k}$, if the polynomial $\frac{f(x)-f(y)}{x-y}$ has no absolutely irreducible factors defined over $\mathbb{F}_{p^k}$, other than $x - y$. In other words, every irreducible factor of $f(x) - f(y)$ in $\mathbb{F}_{p^k}[x, y]$ other than $x - y$ will further factor in $\overline{\mathbb{F}_p}[x, y]$.

**Example 7.17** $f(x) = x^d$ is PP over $\mathbb{F}_{p^k}$ if and only if $(d, p^k - 1) = 1$, which is equivalent to that $x^d$ is exceptional over $\mathbb{F}_{p^k}$.

**Definition 7.18** The **Dickson polynomial** is defined as

$$D_d(x, b) = \left(\frac{x + \sqrt{x^2 - 4b}}{2}\right)^d + \left(\frac{x - \sqrt{x^2 - 4b}}{2}\right)^d,$$

where $b \neq 0$.

If $b = 0$, then $D_d(x, 0) = x^d$. If $b \neq 0$, then

$$D_d(x, b) = \sum_{j=0}^{\lfloor d/2 \rfloor} \frac{d}{d-j} \binom{d-j}{j} (-b)^j x^{n-2j}.$$

Dickson polynomials over finite fields have been studied extensively, see the monograph by Lidl, et al.[29]. In particular, we have

**Proposition 7.19** *For $b \in \mathbb{F}_{p^k}^{\times}$, $D_d(x, b)$ is PP over $\mathbb{F}_{p^k}$, if and only if $(d, p^{2k} - 1) = 1$, if and only if $D_d(x, b)$ is exceptional over $\mathbb{F}_{p^k}$.*

In the general case, we have

**Theorem 7.20** *Let $1 \le d = \deg(f) < p^k$, $f \in \mathbb{F}_{p^k}[x]$.*

1) *If $p^k > d^4$, and $f(x)$ is PP over $\mathbb{F}_{p^k}$, then $f(x)$ is exceptional over $\mathbb{F}_{p^k}$. (This part is a consequence of the Weil bound.)*

2) *(Cohen[30]) If $f(x)$ is exceptional over $\mathbb{F}_{p^k}$, then $f(x)$ is PP over $\mathbb{F}_{p^k}$.*

3) (see [31]) *If $f(x)$ is not PP over $\mathbb{F}_{p^k}$, then*

$$\#\{f(\mathbb{F}_{p^k})\} \le p^k - \left\lfloor \frac{p^k - 1}{d} \right\rfloor.$$

**Remark 7.21** This value set bound in 3) was originally conjectured by Mullen, based on computer calculation. It can be used to give a very simple proof of 2). Note $f(x)$ is PP over

$\mathbb{F}_{p^k}$, if and only if $\#\{f(\mathbb{F}_{p^k})\} = p^k$. A simple proof of the value set bound in 3) was given by Turnwald[32], see also Tao[33] for an elegant presentation of the proof.

As a corollary, we obtain

**Corollary 7.22** *Let $f \in \mathbb{F}_{p^k}[x]$ and assume $p^k > d^4$. Then $f(x)$ is PP over $\mathbb{F}_{p^k}$, if and only if $f(x)$ is exceptional over $\mathbb{F}_{p^k}$.*

The next conjecture aims to classify all possible degrees of exceptional polynomials.

**Conjecture 7.23** (Carlitz-Wan, see [34]) Let $f(x) \in \mathbb{F}_{p^k}[x]$, $d = \deg(f) \geq 1$.

1) (Carlitz, 1966, see [35]) If $p$ is odd, $d$ is even, then $f(x)$ is NOT exceptional over $\mathbb{F}_{p^k}$.

2) (Wan[31], 1991) If $(d, p^k - 1) > 1$, then $f(x)$ is NOT exceptional over $\mathbb{F}_{p^k}$.

It is clear that the first part is a special case of the second part.

**Corollary 7.24** *There is an exceptional polynomial of degree $d$ over $\mathbb{F}_{p^k}$, if and only if $(d, p^k - 1) = 1$.*

**Remark 7.25** This conjecture is easy to prove if $p \nmid d$, the tame case. The condition $(d, p^k - 1) > 1$ can be viewed geometrically as the projective plane curve defined by

$$\frac{f(x) - f(y)}{x - y} = 0$$

has a nonsingular $\mathbb{F}_{p^k}$-rational point at $\infty$. The irreducible component over $\mathbb{F}_{p^k}$ containing this nonsingular $\mathbb{F}_{p^k}$-rational point will be absolutely irreducible. Thus $f(x)$ is NOT exceptional over $\mathbb{F}_{p^k}$.

**Theorem 7.26** (see [36]) *The Carlitz conjecture is true.*

Their proof uses sophisticated group theory, including the classification of finite simple groups. Their result is more general, which proves Wan's conjecture as well if $p \geq 5$. The general case was later settled by Lenstra.

**Theorem 7.27** (see [34]) *The Carlitz-Wan conjecture is true.*

The proof is much simpler, uses only local field and a little elementary group theory. Qifan Zhang recently further simplified Lenstra's proof, used only local fields without group theory.

### 7.3 General Degree Results

#### 7.3.1 Results over $\mathbb{F}_p$

For a polynomial $f(x) \in \mathbb{F}_p[x]$, $1 \leq d = \deg(f) \leq p - 1$, we first consider the exponential sum over the prime field $\mathbb{F}_p$ defined by

$$S_1(f) = \sum_{x \in \mathbb{F}_p} \zeta_p^{f(x)} \in \mathbb{Z}[\zeta_p].$$

Recall that we also defined

$$n(f, 0) = \#\{x \in \mathbb{F}_p | f(x) = 0\}$$

and

$$n(f,i)=\#\{x\in\mathbb{F}_p|f(x)=i\},\quad \forall i\in\mathbb{F}_p.$$

Here we prove the following general result on the degree of $S_1(f)$.

**Theorem 7.28** *We have*

$$\frac{p-1}{(p-1,n(f,0)-1)}\Big|\deg S_1(f)\Big|(p-1).$$

*The vertical line symbol "|" is the symbol of division as usual.*

*Proof* For $m\in\mathbb{N}$, define

$$N_m(f)=\#\{(x_1,x_2,\cdots,x_m)\in\mathbb{F}_p^m|f(x_1)+f(x_2)+\cdots+f(x_m)=0\}.$$

Write

$$F(T)=\prod_{a\in\mathbb{F}_p^\times}(T-S_1(af))=T^{p-1}+F_1T^{p-2}+\cdots+F_{p-1}\in\mathbb{Z}[T],$$

which is a monic polynomial in $T$ of degree $p-1$. Define

$$H=\{a\in\mathbb{F}_p^\times|\sigma_a(S_1(f))=S_1(f)\}=\text{ Stablizer of }S_1(f).$$

Then

$$F(T)=\prod_{a\in\mathbb{F}_p^\times/H}(T-S_1(af))^{|H|}=M(T)^{|H|},$$

where

$$M(T)=\prod_{a\in\mathbb{F}_p^\times/H}(T-S_1(af))\in\mathbb{Q}[T],$$

which is invariant under Galois action. By Galois theory, the polynomial $M(T)$ is the minimal polynomial of $S_1(f)$. Thus, $\deg S_1(f)=\deg M(T)=\frac{p-1}{|H|}$. The problem is that we do not know the stabilizer $H$ in general.

We consider the $m$-th power moment sum

$$\begin{aligned}P_m&=\sum_{a\in\mathbb{F}_p^\times}S_1(af)^m\\&=\sum_{a\in\mathbb{F}_p^\times}\left(\sum_{x_1\in\mathbb{F}_p}\zeta_p^{af(x_1)}\right)\cdots\left(\sum_{x_m\in\mathbb{F}_p}\zeta_p^{af(x_m)}\right)\\&=\sum_{x_1,x_2,\cdots,x_m\in\mathbb{F}_p}\left(\sum_{a\in\mathbb{F}_p}\zeta_p^{a(f(x_1)+f(x_2)+\cdots+f(x_m))}-1\right)\\&=pN_m(f)-p^m.\end{aligned}$$

Now $F(x)=x^{p-1}+F_1x^{p-2}+\cdots+F_{p-1}=M(x)^{|H|}$. Taking derivative yields

$$(p-1)x^{p-2}+(p-2)F_1x^{p-3}+\cdots+F_{p-2}=|H|\cdot M(x)^{|H|-1}\cdot M'(x).$$

Both sides are polynomials over $\mathbb{Z}$, hence

$$(p-1,(p-2)F_1,(p-3)F_2,\cdots,F_{p-2}) \equiv 0 \mod |H|.$$

Equivalently,

$$(p-1,F_1,2F_2,\cdots,(p-2)F_{p-2}) \equiv 0 \mod |H|.$$

By Newton's formula,

$$\begin{cases} 0 = P_1 + F_1, \\ 0 = P_2 + P_1F_1 + 2F_2, \\ \vdots \\ 0 = P_{p-1} + P_{p-2}F_1 + \cdots + P_1F_{p-2} + (p-1)F_{p-1}. \end{cases}$$

We have shown $jF_j \equiv 0 \mod |H|$, for all $1 \le j \le p-1$. By the above Newton's formula, one recursively finds

$$\begin{cases} P_1 \equiv 0 \mod |H|, \\ \vdots \\ P_{p-1} \equiv 0 \mod |H|. \end{cases}$$

Hence

$$0 \equiv P_m = pN_m(f) - p^m \equiv N_m(f) - 1 \mod |H|.$$

Noting that $|H| \,|(p-1)$, thus

$$|H| \,|(p-1, N_1(f)-1, \cdots, N_m(f)-1).$$

We conclude that

$$\deg S_1(f) = \frac{p-1}{|H|} = \frac{p-1}{(p-1,N_1(f)-1,\cdots,N_m(f)-1)} \cdot \frac{(p-1,N_1(f)-1,\cdots,N_m(f)-1)}{|H|}.$$

The last factor is an integer. Thus, we have proved

$$\frac{p-1}{(p-1,N_1(f)-1,\cdots,N_m(f)-1)} \Big| \deg S_1(f) \Big| p-1.$$

Note that

$$N_1(f) = \#\{x \in \mathbb{F}_p | f(x) = 0\} = n(f,0),$$

we obtain the desired result.

We now give some examples and corollaries.

**Corollary 7.29** *If* $(n(f,0)-1, p-1) = 1$, *then* $\deg S_1(f) = p-1$.

**Corollary 7.30** *If* $n(f,0) \in \{0, 2, p-1\}$, *then* $\deg S_1(f) = p-1$.

If $n(f,0) \neq 1$, then $(n(f,0)-1, p-1) \le \frac{p-1}{2}$, which implies that $\deg(S_1(f)) \ge 2$. This is consistent with the fact that $f(x)$ is not PP over $\mathbb{F}_p$ if $n(f,0) \neq 1$.

**Example 7.31** If $f(x) = x^d + bx^{d-1} = x^{d-1}(x+b)$, where $b \neq 0$. Then $n(f,0) = 2$, and hence $\deg S_1(f) = p-1$.

**Example 7.32** If $f(x)$ is odd, i.e., $f(-x) = -f(x)$, then

$$\overline{S_1(f)} = \sum_{x\in\mathbb{F}_p} \zeta_p^{-f(x)} = \sum_{x\in\mathbb{F}_p} \zeta_p^{f(-x)} = S_1(f) \in \mathbb{Q}(\zeta_p)^+.$$

From this example, we obtain

**Corollary 7.33** *If $f(x)$ is odd, then*

$$\frac{p-1}{(p-1, n(f,0)-1)} \Big| \deg S_1(f) \Big| \frac{p-1}{2}.$$

**Example 7.34** Let $f(x) = x^d - b^2x^{d-2} = x^{d-2}(x^2-b^2)$, where $2 \nmid d$ and $b \in \mathbb{F}_p^\times$. Then $n(f,0) = 3$, and thus $\deg(S_1(f)) = \frac{p-1}{2}$.

Note that $f(x)$ is odd, if and only if $f$ can be written as $f(x) = xg(x^2)$. More generally, let $e|(p-1)$, and $f(x) = xg(x^e)$, consider

$$H_e = \{a \in \mathbb{F}_p^\times | a^e = 1\}, \quad |H_e| = e.$$

For all $a \in H_e$, we have

$$\sigma_a(S_1(f)) = S_1(af) = S_1(axg((ax)^e)) = S_1(f).$$

Thus, $S_1(f) \in \mathbb{Q}(\zeta_p)^{H_e}$. Hence,

$$\deg S_1(f) | [\mathbb{Q}(\zeta_p)^{H_e} : \mathbb{Q}] = \frac{p-1}{|H_e|} = \frac{p-1}{e}.$$

To sum up, we have

**Corollary 7.35** *If $f(x) = xg(x^e)$ for some $e|(p-1)$, then*

$$\frac{p-1}{(p-1, n(f,0)-1)} \Big| \deg S_1(f) \Big| \frac{p-1}{e}.$$

*Moreover, if in addition $(p-1, n(f,0)-1) = e$, then $\deg S_1(f) = \frac{p-1}{e}$.*

**Example 7.36** Let $f(x) = x(x^e - b^e)$, where $e|(p-1)$ and $b \neq 0$. Then $n(f,0) = e+1$, and hence $(p-1, n(f,0)-1) = e$ and $\deg S_1(f) = \frac{p-1}{e}$.

**Remark**. For Dickson polynomial $D_d(x,b)$, $b \in \mathbb{F}_p^\times$, what is $\deg S_1(D_d(x,b))$? This remains open in general. For $b = 0$, $D_d(x,0) = x^d$, and Gauss showed that $\deg S_1(x^d) = (d, p-1)$.

### 7.3.2 Results over $\mathbb{F}_q$

For a polynomial $f(x) \in \mathbb{F}_{p^k}[x]$, $1 \leq d = \deg(f) \leq p^k - 1$, we defined the exponential sum over $\mathbb{F}_{p^k}$ by

$$S_k(f) = \sum_{x\in\mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(f(x))} \in \mathbb{Z}[\zeta_p].$$

The same proof as the prime field case gives

**Theorem 7.37** *We have*

$$\frac{p-1}{(p-1, n_k(f)-1)}\Big|\deg S_k(f)\Big|(p-1).$$

This result is less useful when $k>1$, as it is harder to compute $n_k(f)$ for $k>1$. In the case $k=1$,

$$\begin{aligned} n_1(f) &= \#\{(x,y)\in\mathbb{F}_p^2 | y^p - y = f(x)\} \\ &= p\cdot\#\{x\in\mathbb{F}_p | f(x)=0\} \\ &= pn(f,0) \\ &\equiv n(f,0) \mod (p-1). \end{aligned}$$

This recovers the general result in the prime field case.

**Corollary 7.38** *If* $(p-1, n_k(f)-1)=1$, *then* $\deg S_k(f)=p-1$.

**Corollary 7.39** *If* $f(x)=xg(x^e)$, $e|(p-1)$, *then* $\deg S_k(f)|\frac{p-1}{e}$. *If further* $(p-1, n_k(f)-1)=e$, *then* $\deg S_k(f)=\frac{p-1}{e}$.

As mentioned above, for $k>1$, it is harder to compute $n_k(f)$ and so harder to give useful examples to compute $\deg S_k(f)$.

Now we have finished the discussion on the results related to the degree. In next section, we shift to $p$-adic estimates for $L$-functions of exponential sums.

## 8 $L$-Functions of Exponential Sums

In this section, we give a brief exposition for $L$-functions of exponential sums, focusing on their $p$-adic properties.

### 8.1 $L$-Functions of Toric Exponential Sums

Let $\mathbb{F}_q$ be the finite field of $q=p^r$ elements, $f(x_1,x_2,\cdots,x_n)\in\mathbb{F}_q[x_1^{\pm1},x_2^{\pm1},\cdots,x_n^{\pm1}]$ be a Laurent polynomial. Note now that the base field is $\mathbb{F}_q$, not necessarily the prime field $\mathbb{F}_p$. So, we are in a slightly more general situation. We define the sequence of **toric exponential sums** $S_k(f)$ by

$$S_k(f)=\sum_{x_1,x_2,\cdots,x_n\in\mathbb{F}_{q^k}^\times}\zeta_p^{\mathrm{Tr}_k(f(x_1,x_2,\cdots,x_n))},\quad k\in\mathbb{N},$$

where $\mathrm{Tr}_k$ denotes the absolute trace map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_p$. The ***L*-function** of $f$ over $\mathbb{F}_q$ is defined as the following exponential generating function

$$L(f,T)=\exp\left(\sum_{k=1}^{\infty}\frac{T^k}{k}S_k(f)\right)\in\mathbb{Z}[\zeta_p][\![T]\!].$$

The reason that the power series $L(f,T)$ has integral coefficients is because it has an infinite Euler product. In the case when $f(x_1,x_2,\cdots,x_n)=x_1+x_2+\cdots+x_n+\frac{\lambda}{x_1x_2\cdots x_n}$, then $S_k(f)$ reduces to the Kloosterman sum over $\mathbb{F}_{q^k}$.

**Theorem 8.1** (Dwork[4], Bombieri[5]) *$L(f,T)$ is rational in $T$.*

The total degree (the sum) of numerator and denominator for the rational function $L(f,T)$ can be effectively bounded, see Bombieri[37], Adolphson and Sperber[38], and Katz[39]. Such explicit degree bounds are important in algorithms for computing zeta functions and $L$-functions over finite fields, see Lauder and Wan[40], Harvey[41] and the survey[42]. But no exact total degree formula is possible in general. We shall consider a nice case studied by Adolphson and Sperber[43], where one can push much further.

Write $f(x_1,x_2,\cdots,x_n)=\sum_{j=1}^{J}a_j\boldsymbol{x}^{\boldsymbol{v}_j}$, where $a_j\in\mathbb{F}_q^\times$. Here $\boldsymbol{v}_j=(v_{j1},v_{j2},\cdots,v_{jn})\in\mathbb{Z}^n$ and $\boldsymbol{x}^{\boldsymbol{v}_j}=x_1^{v_{j1}}x_2^{v_{j2}}\cdots x_n^{v_{jn}}$. Define

$$\Delta(f):=\text{convex closure of }\{0,\boldsymbol{v}_j(1\le j\le J)\}$$

in $\mathbb{R}^n$. Without loss of generality, we assume that $\Delta=\Delta(f)$ is $n$-dimensional in $\mathbb{R}^n$. If $\delta$ is a closed face of $\Delta$, we define

$$f^\delta=\sum_{\boldsymbol{v}_j\in\delta}a_j\boldsymbol{x}^{\boldsymbol{v}_j}.$$

**Definition 8.2** The polynomial $f$ is called **non-degenerate** if for every closed face $\delta$ of arbitrary dimension, not containing 0, the system

$$\frac{\partial f^\delta}{\partial x_1}=\frac{\partial f^\delta}{\partial x_2}=\cdots=\frac{\partial f^\delta}{\partial x_n}=0$$

has no common solutions in $(\overline{\mathbb{F}_q}^\times)^n$.

**Theorem 8.3** (Adolphson and Sperber[43]) *Let $f$ be non-degenerate. Then $L(f,T)^{(-1)^{n-1}}$ is a polynomial of degree $n!\,\mathrm{Vol}(\Delta)$.*

Write

$$L(f,T)^{(-1)^{n-1}}=\prod_{i=1}^{n!\,\mathrm{Vol}(\Delta)}(1-\alpha_iT)\in\mathbb{C}[T].$$

Then

$$S_k(f)=(-1)^n\left(\alpha_1^k+\alpha_2^k+\cdots+\alpha_{n!\,\mathrm{Vol}(\Delta)}^k\right),\quad\forall k\in\mathbb{N}.$$

By Deligne, $|\alpha_i|=\sqrt{q}^{u_i}$, where $u_i\in\{0,1,\cdots,n\}$. Let $w_i=\#\{1\le j\le n!\,\mathrm{Vol}(\Delta)|\,|\alpha_j|=\sqrt{q}^i\}$, where $0\le i\le n$. Then

$$w_0+w_1+\cdots+w_n=n!\,\mathrm{Vol}(\Delta).$$

The weight sequence $\{w_0,w_1,\cdots,w_n\}$ is completely determined by Denef and Loeser[44] using a complicated combinatorial formula derived from intersection cohomology. This result has been extended to twisted character sum case in [45].

For us, we write

$$L(f,T)^{(-1)^{n-1}}=\prod_{i=1}^{n!\,\mathrm{Vol}(\Delta)}(1-\alpha_iT)\in\mathbb{C}_p[T].$$

We would like to determine the $q$-slope sequence

$$\{v_q(\alpha_1),v_q(\alpha_2),\cdots,v_q(\alpha_{n!\,\mathrm{Vol}(\Delta)})\}.$$

This is rather complicated in general, even in the one variable case. We shall explain a tool which is useful in many interesting cases.

**Remark** For toric exponential sums, $S_k(f) \equiv (q^k-1)^n \mod (\zeta_p - 1)$. Thus, $v_q(S_k(f)) = 0$ and $v_q(\alpha_1) = 0$. We want to find $v_q(\alpha_i)$, for all $1 \le i \le n!\,\mathrm{Vol}(\Delta)$.

### 8.2 Lower Bound for Newton Polygon

Let $C(\Delta) = \cup_{c\ge 0} c\Delta$, i.e., the cone in $\mathbb{R}^n$ generated by $\Delta$. See Figure 2 for this.

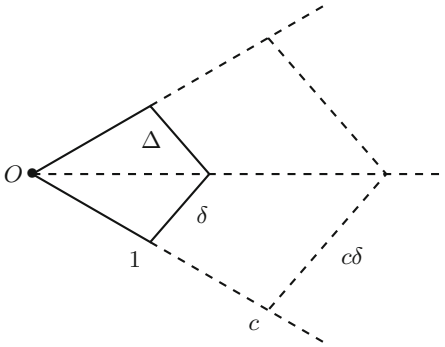



**Figure 2** Cone $C(\Delta)$

**Definition 8.4** For $u \in \mathbb{R}^n$, define a weight function

$$w(u) = \begin{cases} \infty, & \text{if } u \notin C(\Delta), \\ \inf\{c \ge 0 | u \in c\Delta\}, & \text{if } u \in C(\Delta). \end{cases}$$

If $u \in C(\Delta)$, then there exists a codimension-one face $\delta \in \Delta$, $O \notin \delta$, such that $\frac{u}{w(u)} \in \delta$. Let the equation of $\delta$ be $\sum_{i=1}^n e_i x_i = 1$, where $e_i \in \mathbb{Q}$. Then

$$\sum_{i=1}^n e_i \frac{u_i}{w(u)} = 1, \quad u = (u_1, u_2, \cdots, u_n).$$

Hence,

$$w(u) = \sum_{i=1}^n e_i u_i.$$

Let $D(\delta)$ be the least common denominator of $e_i$, for $1 \le i \le n$. Then

$$w(u) \in \frac{1}{D(\delta)} \mathbb{Z}_{\ge 0}, \quad \forall u \in C(\delta) \cap \mathbb{Z}^n.$$

**Definition 8.5** $D = D(\Delta) = \mathrm{lcm}_\delta\, D(\delta)$, where $\delta$ runs through all codimension-one faces of $\Delta$, not containing 0.

**Proposition 8.6** *We have* $w(\mathbb{Z}^n) \subset \frac{1}{D}\mathbb{Z}_{\ge 0} \cup \{\infty\}$. *See Figure* 3 *for this.*

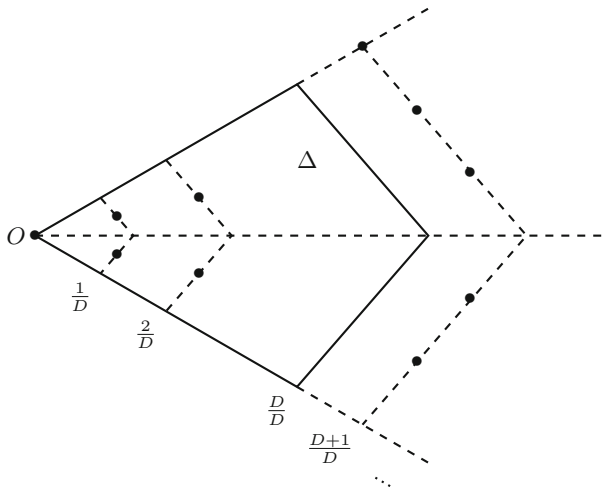



**Figure 3** Lattice points in $C(\Delta)$

**Definition 8.7** Let $S_\Delta = \mathbb{F}_q\left[x^{C(\Delta)\cap\mathbb{Z}^n}\right]$. This is a finitely generated graded $\mathbb{F}_q$-algebra. Let $\deg(x^u) := w(u)$. Then

$$(S_\Delta)_k = \bigoplus_{u\in C(\Delta)\cap\mathbb{Z}^n,\quad w(u)=k/D} \mathbb{F}_q[x^u],$$

which is the homogeneous graded degree $k$ (or weight $k/D$) part of $S_\Delta$. Clearly,

$$S_\Delta = \bigoplus_{k=0}^{\infty}(S_\Delta)_k.$$

**Definition 8.8** For $k \in \mathbb{Z}_{\geq 0}$, define

$$W_\Delta(k) = \#\{u \in C(\Delta)\cap\mathbb{Z}^n | w(u) = k/D\} = \dim_{\mathbb{F}_q}(S_\Delta)_k.$$

As an $n$-dimensional graded algebra, the Poincare series of $S_\Delta$ is of the following form

$$\sum_{k=0}^{\infty}\dim_{\mathbb{F}_q}(S_\Delta)_k T^k = \sum_{k=0}^{\infty} W_\Delta(k)T^k = \frac{\sum_{k=0}^{nD} H_\Delta(k)T^k}{(1-T)^n}.$$

Thus,

$$H_\Delta(k) = \sum_{i=0}^{n}(-1)^i\binom{n}{i}W_\Delta(k-iD).$$

If $f$ is non-degenerate, then $\{x_1\frac{\partial f}{\partial x_1}, x_2\frac{\partial f}{\partial x_2}, \cdots, x_n\frac{\partial f}{\partial x_n}\}$ form a regular sequence of the ring $S_\Delta$, i.e., the multiplication map

$$x_i\frac{\partial f}{\partial x_i} : S_\Delta\Big/\left(x_1\frac{\partial f}{\partial x_1}, x_2\frac{\partial f}{\partial x_2}, \cdots, x_{i-1}\frac{\partial f}{\partial x_{i-1}}\right) \to S_\Delta\Big/\left(x_1\frac{\partial f}{\partial x_1}, x_2\frac{\partial f}{\partial x_2}, \cdots, x_{i-1}\frac{\partial f}{\partial x_{i-1}}\right)$$

is injective for all $1 \leq i \leq n$. This means that the associated Koszul complex

$$K_\bullet(f) : 0 \to S_\Delta^{\binom{n}{0}} \to S_\Delta^{\binom{n}{1}} \to \cdots \to S_\Delta^{\binom{n}{n}} \to 0$$

is acyclic. Furthermore,

$$\dim_{\mathbb{F}_q} H^0(K_\bullet(f)) = \dim_{\mathbb{F}_q} S_\Delta \Big/ \left( x_1 \frac{\partial f}{\partial x_1}, x_2 \frac{\partial f}{\partial x_2}, \cdots, x_n \frac{\partial f}{\partial x_n} \right) = n! \operatorname{Vol}(\Delta).$$

This non-degenerate condition ensures a similar property on the lifted $p$-adic Dwork homology and thus $L(f,T)^{(-1)^{n-1}}$ is a polynomial of degree $n! \operatorname{Vol}(\Delta)$. Furthermore,

$$H_\Delta(k) = \dim_{\mathbb{F}_q} \left( S_\Delta \Big/ \left( x_1 \frac{\partial f}{\partial x_1}, x_2 \frac{\partial f}{\partial x_2}, \cdots, x_n \frac{\partial f}{\partial x_n} \right) \right)_k,$$

the dimension of the graded degree $k$ part of $S_\Delta / \left( x_1 \frac{\partial f}{\partial x_1}, x_2 \frac{\partial f}{\partial x_2}, \cdots, x_n \frac{\partial f}{\partial x_n} \right)$. In particular, $H_\Delta(k) \geq 0$, and

$$\sum_{k=0}^{nD} H_\Delta(k) = \dim_{\mathbb{F}_q} S_\Delta \Big/ \left( x_1 \frac{\partial f}{\partial x_1}, x_2 \frac{\partial f}{\partial x_2}, \cdots, x_n \frac{\partial f}{\partial x_n} \right) = n! \operatorname{Vol}(\Delta).$$

**Definition 8.9** The **Hodge polygon** $\mathrm{HP}(\Delta)$ of $\Delta$ is the lower convex polygon in $\mathbb{R}^2$ with vertices (see Figure 4)

$$\left( \sum_{k=0}^{m} H_\Delta(k), \sum_{k=0}^{m} \frac{k}{D} H_\Delta(k) \right), \quad m = 0, 1, \cdots, nD.$$

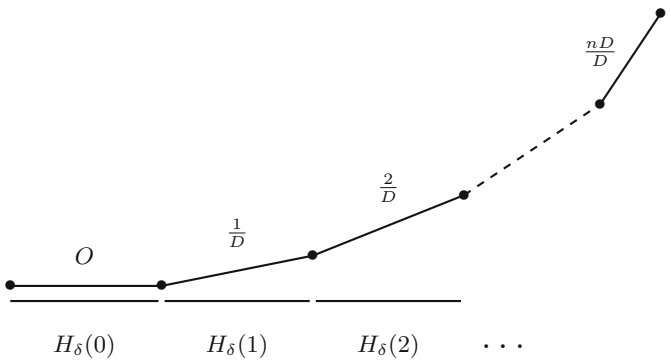



**Figure 4** The Hodge polygon

**Definition 8.10** Let $f$ be non-degenerate over $\mathbb{F}_q$. Write

$$L(f,T)^{(-1)^{n-1}} = 1 + A_1 T + \cdots + A_{n! \operatorname{Vol}(\Delta)} T^{n! \operatorname{Vol}(\Delta)}.$$

The $q$-adic **Newton polygon** of $L(f,T)^{(-1)^{n-1}}$, denoted by $\mathrm{NP}(f)$, is the lower convex closure in $\mathbb{R}^2$ of the following points

$$(k, v_q(A_k)), \quad k = 0, 1, \cdots, n! \operatorname{Vol}(\Delta).$$

The slope sequence $\{v_q(\alpha_1), v_q(\alpha_2), \cdots, v_q(\alpha_{n!\,\mathrm{Vol}(\Delta)})\}$ is determined by $\mathrm{NP}(f)$. For any rational number $s$,

$$\#\{1 \le i \le n!\,\mathrm{Vol}(\Delta) | v_q(\alpha_i) = s\} = \text{ the horizontal length of the slope } s \text{ side in } \mathrm{NP}(f).$$

Then, we have

**Theorem 8.11** (Adolphson and Sperber[43]) *Let $f$ be non-degenerate over $\mathbb{F}_q$. Then we have $\mathrm{NP}(f) \ge \mathrm{HP}(\Delta)$ with endpoints coincide. That is, the Newton polygon lies above the Hodge polygon (see Figure 5 for this).*

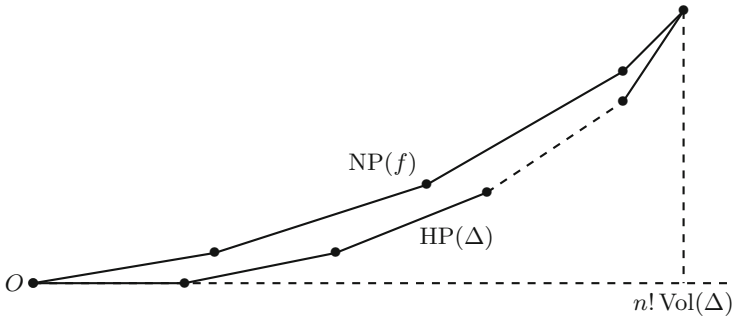



**Figure 5** Figure for Adolphson-Sperber theorem

**Definition 8.12** The polynomial $f$ is called **ordinary** if $\mathrm{NP}(f) = \mathrm{HP}(\Delta)$.

In the ordinary case, the slope sequence is given explicitly by

$$\underbrace{0, \cdots, 0}_{H_\Delta(0)}, \underbrace{\frac{1}{D}, \cdots, \frac{1}{D}}_{H_\Delta(1)}, \cdots, \underbrace{\frac{nD}{D}, \cdots, \frac{nD}{D}}_{H_\Delta(nD)}.$$

It is therefore of interest to determine when $f$ is ordinary.

**Conjecture 8.13** (Adolphson and Sperber[43]) If $p \equiv 1 \mod D$, then $\mathrm{NP}(f) = \mathrm{HP}(\Delta)$ generically, i.e., for all $f(x)$ in a Zariski open dense subset of parameter space for $f \in \overline{\mathbb{F}_p}[x_1^{\pm 1}, x_2^{\pm 2}, \cdots, x_n^{\pm 1}]$ with $\Delta(f) = \Delta$.

**Theorem 8.14** (see [46, 47]) *The AS conjecture is true for $n \le 3$ but can be false for all $n \ge 4$.*

These papers introduced several decomposition theorems which are useful to determine when $f$ is ordinary. We explain one of them in next two sections.

To conclude this section, we mention one open problem.

**Conjecture 8.15** Let $f(x) \in \mathbb{F}_q[x_1, x_2, \cdots, x_n]$ be non-degenerate. Then, the Newton polygon $\mathrm{NP}(\lambda f(x))$ is independent of the non-zero parameter $\lambda \in \overline{\mathbb{F}_q}^\times$.

This is open, even in the case $n = 1$ and $p \nmid d$, where

$$f(x) = x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{F}_q[x].$$

It is indeed true for the monomial $f(x) = x^d$.

### 8.3 Diagonal Laurent Polynomials

**Definition 8.16** Let $f(x_1, x_2, \cdots, x_n) = \sum_{j=1}^{n} a_j \boldsymbol{x}^{\boldsymbol{v}_j}$, where $a_j \in \mathbb{F}_q^{\times}$. Here $\boldsymbol{v}_j = (v_{j1}, v_{j2}, \cdots, v_{jn}) \in \mathbb{Z}^n$ and $\boldsymbol{x}^{\boldsymbol{v}_j} = x_1^{v_{j1}} x_2^{v_{j2}} \cdots x_n^{v_{jn}}$. Note that the number of non-zero terms is equal to the number of variables. If the square matrix

$$M(f) = (\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n)$$

is nonsingular, i.e., $\det(M(f)) \neq 0$, where $\boldsymbol{v}_j = \begin{pmatrix} v_{1j} \\ \vdots \\ v_{nj} \end{pmatrix} \in \mathbb{Z}^n$, then, $f$ is called a **diagnoal Laurent polynomial**.

**Proposition 8.17** *A diagonal $f$ is non-degenerate over $\mathbb{F}_q$, if and only if $p \nmid \det(M(f))$.*

Write

$$M(f) \sim \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & d_n \end{pmatrix}, \quad d_1 | d_2 | \cdots | d_n,$$

where $\{d_1, d_2, \cdots, d_n\}$ are the invariant factors of the finite abelian group $\mathbb{Z}^n / M(f)\mathbb{Z}^n$.

**Proposition 8.18** (see [46]) *Let $d_n$ be the largest invariant factor of a diagonal Laurent polynomial $f$ over $\mathbb{F}_q$. If $p \equiv 1 \mod d_n$, then* $\mathrm{NP}(f) = \mathrm{HP}(\Delta)$.

**Example 8.19** The polynomial $f(x) = x_1^{d_1} + x_2^{d_2} + \cdots + x_n^{d_n}$, where $d_i > 0$, is diagonal. It is non-degenerate, if and only if $p \nmid d_1 d_2 \cdots d_n$. It is ordinary, if and only if $p \equiv 1 \mod [d_1, d_2, \cdots, d_n]$, where $[d_1, d_2, \cdots, d_n]$ is the largest invariant factor.

**Example 8.20** Let $f(x) = x^d$, $p \equiv 1 \mod d$. Then the slope sequence is

$$\left\{ \frac{0}{d}, \frac{1}{d}, \cdots, \frac{d-1}{d} \right\}$$

and $n! \operatorname{Vol}(\Delta) = d$.

### 8.4 Facial Decomposition Theorem

Returning to the general non-degenerate Laurent polynomial case. Recall that $\Delta = \Delta(f)$ is $n$-dimensional in $\mathbb{R}^n$. Let $\{\delta_1, \delta_2, \cdots, \delta_h\}$ be all the closed codimension-one faces of $\Delta$, not containing the origin $O$. Then the restriction

$$f^{\delta_i} = \sum_{\boldsymbol{v}_j \in \delta_i} a_j \boldsymbol{x}^{\boldsymbol{v}_j}$$

is also non-degenerate with respect to $\Delta(f_i) = \Delta_i$. The decomposition

$$\Delta = \bigcup_{i=1}^{h} \Delta_i$$

is called the **facial decomposition** of $\Delta$. See Figure 6 for this.

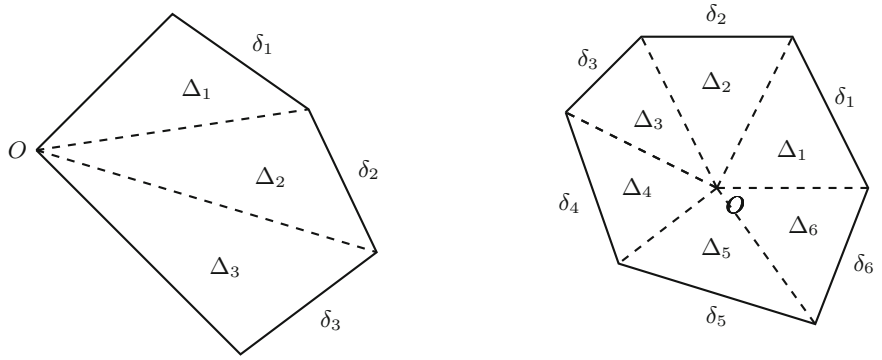



**Figure 6** Facial decomposition

**Theorem 8.21** (see [46]) *Let $f$ be non-degenerate over $\mathbb{F}_q$. Then $\mathrm{NP}(f) = \mathrm{HP}(\Delta)$ if and only if $\mathrm{NP}(f_i) = \mathrm{HP}(\Delta_i)$ for all $1 \leq i \leq h$.*

**Example 8.22** Let $f(x) = x_1^d + x_2^d + \cdots + x_n^d + g_{<d}(x_1, x_2, \cdots, x_n) \in \mathbb{F}_q[x_1, x_2, \cdots, x_n]$. Then $\Delta(f)$ has a unique codimensional-1 face $\delta$ not containing the origin. One checks that

$$f^\delta = x_1^d + x_2^d + \cdots + x_n^d.$$

By the facial decomposition theorem, $f$ is ordinary, if and only if $f^\delta$ is ordinary, if and only if $x^d$ is ordinary, if and only if $p \equiv 1 \mod d$.

**Example 8.23** Let $f(x) = x^d + a_1 x^{d-1} + \cdots + a_0$. If $p \equiv 1 \mod d$, then it is ordinary. The slope sequence

$$\left\{\frac{0}{d}, \frac{1}{d}, \cdots, \frac{d-1}{d}\right\}$$

is the same as the case $f(x) = x^d$.

**Example 8.24** Let

$$f(x_1, x_2, \cdots, x_n) = x_1 + x_2 + \cdots + x_n + \frac{\lambda}{x_1 x_2 \cdots x_n} = \sum_{j=1}^{n+1} a_j \boldsymbol{x}^{\boldsymbol{v}_j}, \quad \lambda \neq 0,$$

where

$$(\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_{n+1}) = \begin{pmatrix} 1 & 0 & \cdots & 0 & -1 \\ 0 & 1 & \cdots & 0 & -1 \\ 0 & 0 & \ddots & 0 & -1 \\ 0 & 0 & \cdots & 1 & -1 \end{pmatrix}_{n \times (n+1)}$$

and $n!\,\mathrm{Vol}(\Delta) = n + 1$. For each $1 \leq i \leq n+1$, let $\delta_i$ be the codimensional-one face with vertices $\{v_1, v_2, \cdots, v_{n+1}\} - \{v_i\}$. Then $\det \delta_i = \pm 1$. Then $f^{\delta_i}$ is ordinary for all $p$, and hence $f$ is ordinary for all $p$, i.e., the slope sequence of $L(f,T)^{(-1)^{n-1}}$ is $\{0, 1, \cdots, n\}$, see Figure 7.

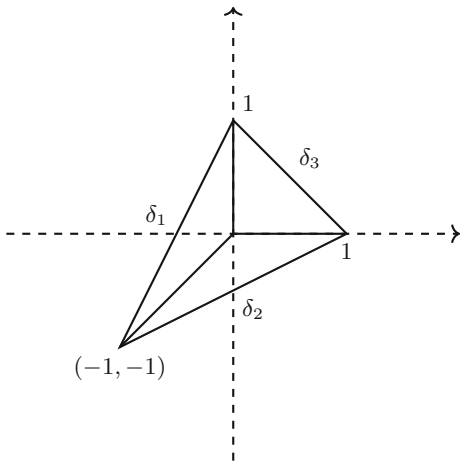



**Figure 7** Facial decomposition and Kloosterman sums

This result was first proved by Sperber[48] for $p > n$.

**Example 8.25** (Xu and Zhu[49]) In their work on Bessel $F$-crystals for reductive groups, one class of generalized Kloosterman sums is the toric exponential sums associated to the Laurent polynomial,

$$f(x_1, x_2 \cdots, x_{2n+1}) = x_1 + \cdots + x_{2n} - x_{2n+1}^d + \frac{a x_{2n+1}^d}{x_1 x_2 \cdots x_{2n}},$$

where $a \in \mathbb{F}_q^\times$, $p \equiv 1 \mod d$. Applying the facial decomposition, they deduce that the slope sequence for $L(f, T)$ is

$$\left\{0, \frac{1}{d}, \frac{2}{d}, \cdots, 2n + \frac{d-1}{d}\right\}.$$

**Example 8.26** (Chen and Lin[50]) For $a_1, a_2, \cdots, a_4 \in \mathbb{F}_q^\times$, let

$$S_k(a) = \sum_{\frac{1}{x_1 x_2} + \frac{1}{x_3 x_4} = 1, \quad x_i \in \mathbb{F}_{q^k}^\times} \zeta_p^{\mathrm{Tr}_k(a_1 x_1 + a_2 x_2 + \cdots + a_4 x_4)}.$$

This sum arises from many applications in analytic number theory, including Zhang's work on the twin prime conjecture. Let $L(T) = \exp\left(\sum_{k=1}^\infty \frac{T^k}{k} S_k(a)\right)$. Then

$$L(T) = (1 - T)(1 - qT) \prod_{i=1}^{6} (1 - \alpha_i T),$$

where $|\alpha_i| = \sqrt{q}^3$ for $1 \le i \le 6$, and the slope sequence for the $\alpha_i$'s is $\{0, 1, 1, 2, 2, 3\}$.

Several additional interesting examples can be found in Sperber[51, 52], Wan[47], Hong[53, 54], Yang[55], Zhu[56, 57], Blache[58, 59], Le[60], Zhang and Feng[61], Chen[62] and Fu and Wan[63].

## 9 Exponential Sums of Higher $p$-Power Orders

Previously, we considered exponential sums associated to the additive character of order $p$. In this last section, we consider exponential sums associated to characters of all higher $p$-power orders.

For simplicity of illustration, we restrict to one variable exponential sums, namely, the polynomial $f(x)$ has one variable:

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{F}_q[x], \quad a_d \neq 0,\ p \nmid d.$$

Let $\zeta_p$ be a primitive $p$-th root of 1. Let

$$S_k(f) = \sum_{x \in \mathbb{F}_{q^k}} \zeta_p^{\mathrm{Tr}_k(f(x))} \in \mathbb{Z}[\zeta_p], \quad k \in \mathbb{N}.$$

The $L$-function is

$$L(f,T) = \exp\left(\sum_{k=1}^{\infty} \frac{T^k}{k} S_k(f)\right) = \prod_{i=1}^{d-1}(1 - \alpha_i T^k).$$

As a complex number, by Weil's celebrated theorem, $|\alpha_i| = \sqrt{q}$ for $1 \leq i \leq d-1$. As a $p$-adic number, the slope sequence

$$\{v_q(\alpha_1), v_q(\alpha_2), \cdots, v_q(\alpha_{d-1})\}$$

is unknown in general. If $p \equiv 1 \mod d$, then

$$\{v_q(\alpha_1), v_q(\alpha_2), \cdots, v_q(\alpha_{d-1})\} = \left\{\frac{1}{d}, \frac{2}{d}, \cdots, \frac{d-1}{d}\right\}.$$

Now, for each $m \in \mathbb{N}$, let $\zeta_{p^m}$ be a primitive $p^m$-th root of 1. Let

$$f^{\omega}(x) = \sum_{i=0}^{d} \omega(a_i) x^i \in \mathbb{Z}_q[x],$$

where $\omega$ denotes the Teichmüller character. Define the **$p^m$-th order exponential sums** by

$$S_{k,m}(f) = \sum_{x \in \mathbb{F}_{q^k}} \zeta_{p^m}^{\mathrm{Tr}_k(f^{\omega}(\omega(x)))} \in \mathbb{Z}[\zeta_{p^m}].$$

The number $S_{k,m}(f)$ now has two integer parameters $k$ and $m$. The integer $k$ denotes the extension degree, and the integer $m$ determines the order of the character.

For each fixed $m$, we define the **$m$-th $L$-function** by

$$L_m(f,T) = \exp\left(\sum_{k=1}^{\infty} \frac{T^k}{k} S_{k,m}(f)\right).$$

In the case $m = 1$, this $L$-function $L_1(f,T)$ reduces to the previous $L$-function $L(f,T)$. For general $m \geq 1$, the $L$-function $L_m(f,T)$ is a polynomial of degree $p^{m-1}(d-1)$. Write

$$L_m(f,T) = \prod_{i=1}^{p^{m-1}d-1} (1 - \alpha_i(m) T^k), \quad m \in \mathbb{N}.$$

Again, as complex numbers, Weil's celebrated theorem shows that $|\alpha_i(m)| = \sqrt{q}$, for $1 \le i \le p^{m-1}d - 1$. As $p$-adic numbers, what is the $q$-slope sequence for $L_m(f,T)$? i.e.,

$$\left\{v_q(\alpha_1(m)), \cdots, v_q(\alpha_{p^{m-1}d-1}(m)\right\} =?$$

As mentioned above, this is already unknown for $m = 1$, if $p \not\equiv 1 \mod d$.

We raise a question here:

QUESTION: Any stable behaviour for the $m$-th slope sequence

$$\left\{v_q(\alpha_1(m)), v_q(\alpha_2(m)), \cdots, v_q(\alpha_{p^{m-1}d-1}(m)\right\}$$

as $m \to \infty$?

**Theorem 9.1** (Liu and Wan[64]) *If $p \equiv 1 \mod d$, then for all $m \ge 1$, the $m$-th slope sequence is given explicitly by*

$$\left\{v_q(\alpha_1(m)), v_q(\alpha_2(m)), \cdots, v_q(\alpha_{p^{m-1}d-1}(m)\right\} = \left\{\frac{1}{dp^{m-1}}, \frac{2}{dp^{m-1}}, \cdots, \frac{dp^{m-1}-1}{dp^{m-1}}\right\}.$$

*The truncation of an arithmetic progression.*

The idea is to introduce the sequence of the universal $t$-adic exponential sums

$$S_k(f,t) = \sum_{x \in \mathbb{F}_{q^k}} (1+t)^{\mathrm{Tr}_k(f^\omega(\omega(x)))} \in \mathbb{Z}_p[\![t]\!], \quad |t|_p < 1,$$

and its $t$-adic $L$-function

$$L(f,t,T) = \exp\left(\sum_{k=1}^{\infty} \frac{T^k}{k} S_k(f,t)\right) \in \mathbb{Z}_p[\![T]\!][\![t]\!].$$

Note

$$S_{k,m}(f) = S_k(f, \zeta_{p^m} - 1), \quad L_m(f,T) = L(f, \zeta_{p^m} - 1, T).$$

Thus, it is enough to study the $t$-adic $L$-function.

**Proposition 9.2** *$L_m(f,T)$ is ordinary for one $m$, if and only if $L(f,t,T)$ is ordinary, if and only if $L_m(f,T)$ is ordinary for all $1 \le m < \infty$. If $p \equiv 1 \mod d$, then $L_1(f,T)$ is ordinary, which implies that $L_m(f,T)$ is ordinary for all $m$.*

What if $p \not\equiv 1 \mod d$? We have a slightly weaker but similar stability result.

**Theorem 9.3** (see [65]) *The $m$-th slope sequence for $L_m(f,T)$ can be recovered from the $m_0$-th slope sequence for all $m \ge m_0$, where*

$$q = p^r, \quad m_0 = \left\lceil 1 + \log_p \frac{(d-1)^2 r}{8d} \right\rceil.$$

*(Note that $m_0 = 2$ if $p \ge \frac{dr}{8}$). More precisely, let $\{s_1, s_2, \cdots, s_{dp^{m_0-1}-1}\}$ be the slope sequence for $L_{m_0}(f,T)$. Then for all $m \ge m_0$, the slope sequence for $L_m(f,T)$ is given by*

$$\bigcup_{i_0=0}^{p^{m-m_0}} \left\{\frac{i}{p^{m-m_0}}, \frac{i+s_1}{p^{m-m_0}}, \cdots, \frac{i+s_{dp^{m_0-1}-1}}{p^{m-m_0}}\right\} - \{0\}.$$

*This is a truncation of $dp^{n_0-1}$ arithmetic progressions!*

The idea is that for $p \not\equiv 1 \mod d$, the $t$-adic $L$-function is not ordinary, but it is partially ordinary in the sense that the Newton polygon and its lower bound (the Hodge polygon) agree at all vertices in an arithmetic progression. Then we can get a tight upper bound. Then we get finite number of arithmetic progressions.

**Remark 9.4** In the special cases $f(x) = x^d + ax^{d-1}$ or $f(x) = x^d + ax$, where $p \equiv -1 \mod d$, more precise improvements were obtained by Ouyang and Zhang[66], Ouyang and Yang[67, 68].

**Remark 9.5** This striking slope stability has been generalized to various cases when the polynomial $f^\omega(x)$ is replaced by

1) Any polynomial $g(x) \in \mathbb{Z}_q[x]$, see Li[69].

2) A much larger class of convergent power series $g(x) \in \mathbb{Z}_q[[x]]$, see Kosters and Zhu[70].

3) Generalization to higher rank and higher dimensional case, see Ren, et al.[71] and Ren[72].

4) Generalization to higher genus curves ramified at several points, see forthcoming works of Joe Kramer-Miller and James Upton.

**Remark 9.6** These ideas also inspired the works in another direction.

- Wan, et al.[73]. On slopes of $p$-adic modular forms.
- Liu, et al.[74]. On the spectral halo conjecture for eigenvalues near the boundary.

This last paper further inspired the works of

- L. Ye's Harvard Ph.D thesis[75]. On eigenvarieties for definite unitary groups.
- Johansson and Newton[76]. On Hilbert modular eigenvarieties.
- Ren and Zhao[77]. On spectral halo for Hilbert modular forms.

## 10 Concluding Remarks

Recall that we defined the exponential sum

$$S_k(f) = \sum_{x_1,x_2,\cdots,x_n \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(f(x_1,x_2,\cdots,x_n))} \in \mathbb{Z}[\zeta_p]$$

for polynomial $f(x_1, x_2, \cdots, x_n)$ in $\mathbb{F}_p[x_1, x_2, \cdots, x_n]$.

The main questions are

QUESTION 1: $\sum_{k=1}^{\infty} |S_k(f)|\, T^k \in \mathbb{R}(T)$?

As indicated earlier, the answer is probably no although we do not have an explicit counter-example. But something slightly weaker is true: $\sum_{k=1}^{\infty} |S_k(f)|^2 T^k \in \mathbb{R}(T)$.

QUESTION 2: $\sum_{k=1}^{\infty} |S_k(f)|_p T^k \in \mathbb{Q}(T)$?
It is not clear if this would be true. But we can make a slightly weaker conjecture: $\sum_{k=1}^{\infty} |S_k(f)|_p T^k$ is a meromorphic function in $T \in \mathbb{C}$, and $\sum_{k=1}^{\infty} v_p(S_k(f))T^k$ is a $p$-adic meromorphic function in $T \in \mathbb{C}_p$.

QUESTION 3: $\sum_{k=1}^{\infty} \deg(S_k(f))T^k \in \mathbb{Q}(T)$?

In a forthcomming joint work, we prove that the third question has a positive answer. Namely,

**Theorem 10.1** *The sequence* $\deg S_k(f)$ *is periodic for* $k >> 0$. *In particular,*

$$\sum_{k=1}^{\infty} \deg(S_k(f))T^k \in \mathbb{Q}(T).$$

As a corollary,

**Corollary 10.2** $S_k(x^d)$ *is periodic,* $\forall k >> 0$. $Kl_{n,k}(\lambda)$ *is periodic,* $\forall k >> 0$.

But explicitly, what are these two virtual periodic sequences? Are they effectively computable? We have given a number of partial results in this course. It would be very interesting to know the complete answer, even for these two most classical examples!

## References


[1] Wan D Q, Some arithmetic properties of the minimal polynomials of Gauss sums, *Proc. Amer. Math. Soc.*, 1987, **100**(2): 225–228.

[2] Koblitz N, *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*, 2nd Edition, Springer-Verlag, New York, 1984.

[3] Deng Y, Luo L, Pan Y, et al., On Some Computational Problems in Local Fields, *J. Syst. Sci. Complex.* , 2021, https://doi.org/10.1007/s11424-021-0074-8.

[4] Dwork B, On the rationality of the zeta function of an algebraic variety, *Amer. J. Math.*, 1960, **82**: 631–648.

[5] Bombieri E, On exponential sums in finite fields, *Amer. J. Math.*, 1966, **88**: 71–105.

[6] Berndt B C and Evans R J, The determination of Gauss sums, *Bull. Amer. Math. Soc.* (*N.S.*), 1981, **5**(2): 107–129.

[7] Myerson G, Period polynomials and Gauss sums for finite fields, *Acta Arith.*, 1981, **39**(3): 251–264.

[8] Kummer E, De residuis cubicis disquisitiones nonnullae analyticae, *J. reine angew. Math.*, 1846, **32**: 341–359.

[9] Heath-Brown D R and Patterson S J, The distribution of Kummer sums at prime arguments, *J. Reine Angew. Math.*, 1979, **310**: 111–130.

[10] Patterson S J, On the distribution of Kummer sums, *J. Reine Angew. Math.*, 1978, **303**(304): 126–143.

[11] Deligne P, La conjecture de Weil II, *Pub. Math. I.H.E.S.*, 1980, **52**: 137–252.

[12] Katz N M, *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*, Princeton University Press, Princeton, NJ, 1988.
[13] Stickelberger L, Ueber eine Verallgemeinerung der Kreistheilung, *Math. Ann.*, 1890, **37**: 312–367.
[14] Wan D Q, Minimal polynomials and distinctness of Kloosterman sums, Special issue dedicated to Leonard Carlitz, 1995, **1**: 189–203.
[15] Gross B H and Koblitz N, Gauss sums and the $p$-adic $\Gamma$-function, *Ann. of Math.* (2), 1979, **109**(3): 569–581.
[16] Sperber S, On the $p$-adic theory of exponential sums, *Amer. J. Math.*, 1986, **108**(2): 255–296.
[17] Ax J, Zeroes of polynomials over finite fields, *Amer. J. Math.*, 1964, **86**: 255–261.
[18] Katz N M, On a theorem of Ax, *Amer. J. Math.*, 1971, **93**: 485–499.
[19] Wan D Q, An elementary proof of a theorem of Katz, *Amer. J. Math.*, 1989, **111**(1): 1–8.
[20] Hou X D, A note on the proof of a theorem of Katz, *Finite Fields Appl.*, 2005, **11**(2): 316–319.
[21] Adolphson A and Sperber S, $p$-adic estimates for exponential sums and the theorem of Chevalley-Warning, *Ann. Sci. École Norm. Sup.* (4), 1987, **20**(4): 545–556.
[22] Borissov Y and Borissov L, A note on the distinctness of some Kloosterman sums, *Cryptography and Communications*, 2020, **12**: 1051–1056.
[23] Moreno O and Moreno C J, Improvements of the Chevalley-Warning and the Ax-Katz theorems, *Amer. J. Math.*, 1995, **117**(1): 241–244.
[24] Blache R, Valuation of exponential sums and the generic first slope for Artin-Schreier curves, *J. Number Theory*, 2012, **132**(10): 2336–2352.
[25] Chen J M and Cao W, Degree matrices and divisibility of exponential sums over finite fields, *Arch. Math.* (*Basel*), 2010, **94**(5): 435–441.
[26] Cao W and Sun Q, Improvements upon the Chevalley-Warning-Ax-Katz-type estimates, *J. Number Theory*, 2007, **122**(1): 135–141.
[27] Fisher B, Distinctness of Kloosterman sums, *p-adic methods in number theory and algebraic geometry*, Volume 133 of *Contemp. Math.*, Amer. Math. Soc., Providence, RI, 1992, 81–102.
[28] Katz D J and Langevin P, New open problems related to old conjectures by Helleseth, *Cryptogr. Commun.*, 2016, **8**(2): 175–189.
[29] Lidl R, Mullen G L, and Turnwald G, *Dickson polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*, Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993.
[30] Cohen S D, The distribution of polynomials over finite fields, *Acta Arith.*, 1970, **17**: 255–271.
[31] Wan D Q, A generalization of the Carlitz conjecture, *Finite fields, coding theory, and advances in communications and computing* (*Las Vegas, NV*, 1991), volume 141 of *Lecture Notes in Pure and Appl. Math.*, Dekker, New York, 1993, 209–216.
[32] Turnwald G, A new criterion for permutation polynomials, *Finite Fields Appl.*, 1995, **1**(1): 64–82.
[33] Tao T, Algebraic combinatorial geometry: The polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory, *EMS Surv. Math. Sci.*, 2014, **1**(1): 1–46.
[34] Cohen S D and Fried M D, Lenstra's proof of the Carlitz-Wan conjecture on exceptional polynomials: An elementary version, *Finite Fields Appl.*, 1995, **1**(3): 372–375.
[35] Lidl R and Mullen G L, When does a polynomial over a finite field permute the elements of the field II, *Amer. Math Monthly*, 1993, **100**(1): 71–74.
[36] Fried M D, Guralnick R, and Saxl J, Schur covers and Carlitz's conjecture, *Israel J. Math.*, 1993, **82**(1–3): 157–225.

[37] Bombieri E, On exponential sums in finite fields II, *Invent. Math.*, 1978, **47**(1): 29–39.

[38] Adolphson A and Sperber S, Newton polyhedra and the degree of the $L$-function associated to an exponential sum, *Invent. Math.*, 1987, **88**(3): 555–569.

[39] Katz N M, Sums of Betti numbers in arbitrary characteristic, Dedicated to Professor Chao Ko on the occasion of his 90th birthday, 2001, **7**: 29–44.

[40] Lauder A G B and Wan D Q, Counting points on varieties over finite fields of small characteristic, *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, *Math. Sci. Res. Inst. Publ.*, Cambridge University Press, Cambridge, 2008, **44**: 579–612.

[41] Harvey D, Computing zeta functions of arithmetic schemes, *Proc. Lond. Math. Soc.* (3), 2015, **111**(6): 1379–1401.

[42] Wan D Q, Algorithmic theory of zeta functions over finite fields, *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, *Math. Sci. Res. Inst. Publ.*, Cambridge University Press, Cambridge, 2008, **44**: 551–578.

[43] Adolphson A and Sperber S, Exponential sums and Newton polyhedra: Cohomology and estimates, *Ann. of Math.* (2), 1989, **130**(2): 367–406.

[44] Denef J and Loeser F, Weights of exponential sums, intersection cohomology, and Newton polyhedra, *Invent. Math.*, 1991, **106**(2): 275–294.

[45] Fu L, Weights of twisted exponential sums, *Math. Z.*, 2009, **262**(2): 449–472.

[46] Wan D Q, Newton polygons of zeta functions and $L$ functions, *Ann. of Math.* (2), 1993, **137**(2): 249–293.

[47] Wan D Q, Variation of $p$-adic Newton polygons for $L$-functions of exponential sums, *Asian J. Math.*, 2004, **8**(3): 427–471.

[48] Sperber S, $p$-adic hypergeometric functions and their cohomology, *Duke Math. J.*, 1977, **44**(3): 535–589.

[49] Xu D X and Zhu X W, Bessel $f$-isocrystals for reductive groups, 2019.

[50] Chen C and Lin X, L-functions of certain exponential sums over finite fields, 2020.

[51] Sperber S, Congruence properties of the hyper-Kloosterman sum, *Compositio Math.*, 1980, **40**(1): 3–33.

[52] Sperber S, Newton polygons for general hyper-Kloosterman sums, *Asterisque — Societe Mathematique de France*, 1984, (119–120): 267–330.

[53] Hong S F, Newton polygons of $L$ functions associated with exponential sums of polynomials of degree four over finite fields, Dedicated to Professor Chao Ko on the occasion of his 90th birthday, 2001, **7**: 205–237.

[54] Hong S F, Newton polygons for $L$-functions of exponential sums of polynomials of degree six over finite fields, *J. Number Theory*, 2002, **97**(2): 368–396.

[55] Yang R, Newton polygons of $L$-functions of polynomials of the form $x^d + \lambda x$, *Finite Fields Appl.*, 2003, **9**(1): 59–88.

[56] Zhu H J, $p$-adic variation of $L$ functions of one variable exponential sums. I, *Amer. J. Math.*, 2003, **125**(3): 669–690.

[57] Zhu H J, Generic $A$-family of exponential sums, *J. Number Theory*, 2014, **143**: 82–101.

[58] Blache R, Newton polygons for character sums and Poincaré series, *Int. J. Number Theory*, 2011, **7**(6): 1519–1542.

[59] Bellovin R, Garthwaite S A, Ozman E, et al., Newton polygons for a variant of the Kloosterman family, *Women in Numbers 2: Research Directions in Number Theory*, volume 606 of *Contemp.*

*Math.*, Amer. Math. Soc., Providence, RI, 2013, 47–63.

[60] Le P, Regular decomposition of ordinarity in generic exponential sums, *J. Number Theory*, 2013, **133**(8): 2648–2683.

[61] Zhang J and Feng W D, On $L$-functions of certain exponential sums, *Finite Fields Appl.*, 2014, **26**: 7–31.

[62] Chen C, Hasse polynomials of $L$-functions of certain exponential sums, *Finite Fields Appl.*, 2020, **68**: 101736, 19.

[63] Fu L and Wan D Q, On Katz's $(a, b)$-exponential sums, *Quarterly J. Math*, 2020, **00**: 1–21. doi:10.1093/qmath/haaa045

[64] Liu C L and Wan D Q, $T$-adic exponential sums over finite fields, *Algebra Number Theory*, 2009, **3**(5): 489–509.

[65] Davis C, Wan D Q, and Xiao L, Newton slopes for Artin-Schreier-Witt towers, *Math. Ann.*, 2016, **364**(3–4): 1451–1468.

[66] Ouyang Y and Zhang S X, Newton polygons of $L$-functions of polynomials $x^d + ax^{d-1}$ with $p \equiv -1$ mod $d$, *Finite Fields Appl.*, 2016, **37**: 285–294.

[67] Ouyang Y and Yang J B, Newton polygons of $L$ functions of polynomials $x^d + ax$, *J. Number Theory*, 2016, **160**: 478–491.

[68] Ouyang Y and Yang J B, On a conjecture of Wan about limiting Newton polygons, *Finite Fields Appl.*, 2016, **41**: 64–71.

[69] Li X, The stable property of Newton slopes for general Witt towers, *J. Number Theory*, 2018, **185**: 144–159.

[70] Kosters M and Zhu H J, On slopes of $L$-functions of $Z_p$-covers over the projective line, *J. Number Theory*, 2018, **187**: 430–452.

[71] Ren R F, Wan D Q, Xiao L, et al., Slopes for higher rank Artin-Schreier-Witt towers, *Trans. Amer. Math. Soc.*, 2018, **370**(9): 6411–6432.

[72] Ren R F, Generic Newton polygon for exponential sums in $n$ variables with parallelotope base, *Amer. J. Math.*, 2020, **142**(5): 1595–1639.

[73] Wan D Q, Xiao L, and Zhang J, Slopes of eigencurves over boundary disks, *Math. Ann.*, 2017, **369**(1–2): 487–537.

[74] Liu R C, Wan D Q, and Xiao L, The eigencurve over the boundary of weight space, *Duke Math. J.*, 2017, **166**(9): 1739–1787.

[75] Ye L L, *Slopes in Eigenvarieties for Definite Unitary Groups*, PhD thesis, Harvard University, Cambridge, 2019.

[76] Johansson C and Newton J, Parallel weight 2 points on Hilbert modular eigenvarieties and the parity conjecture, *Forum Math. Sigma*, 2019, **7**: e27, 36.

[77] Ren R F and Zhao B, Spectral halo for Hilbert modular forms, 2020, arXiv: 2005.14267.