THE $p$-ADIC RIEMANN HYPOTHESIS FOR EXPONENTIAL SUMS

CHUNLEI LIU AND CHUANZE NIU

Abstract. The $L$-function of exponential sums associated to the generic polynomial of degree $d$ in $n$ variables over a finite field of characteristic $p$ is studied. A polygon called the Frobenius polygon of the generic polynomial of degree $d$ in $n$ variables over a finite field of characteristic $p$ is defined. A $p$-adic Riemann hypothesis is formulated. It asserts that the Newton polygon of the $L$-function coincides with the Frobenius polygon when $p$ is large enough. This $p$-adic Riemann hypothesis is proved when $n = 2$ and $p \equiv -1 \pmod{d}$. In general, it is proved that the Newton polygon of the $L$-function lies above the Frobenius polygon with coincident endpoints when $p$ is large enough.

Key words: Newton polygon, exponential sum, finite field

MSC2000: 11L07, 14F30

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field of characteristic $p$ with $q$ elements. Let $n$ and $d$ be fixed positive integers such that $p \nmid d$. Let

$$f(x) = \sum_{u_1 + u_2 + \cdots + u_n \leq d} a_u x_1^{u_1} \cdots x_n^{u_n}$$

be a polynomial of degree $d$ over $\mathbb{F}_q$. Associated to $f$ are the exponential sums

$$S_f(k) = \sum_{x \in (\mathbb{F}_q^*)^n} \text{Tr}_{\mathbb{F}_q^k/\mathbb{F}_p}(f(x)) \zeta_p^{\text{Tr}_{\mathbb{F}_q^k/\mathbb{F}_p}(f(x))}, \quad k = 1, 2, \cdots,$$

where $\zeta_p$ is a primitive $p$-root of unity. These exponential sums are encoded into the $L$-function

$$L_f(s) = \exp \left( \sum_{k=1}^{\infty} S_f(k) \frac{s^k}{k} \right).$$

It is known that $L_f(s)$ is a rational function in $s$. The archimedean absolute values of its reciprocal zeros and poles are of the form $q^{\frac{j}{2}}$ with $j = 1, 2, \cdots, 2n$. However, when the leading form of $f$ is smooth, Deligne [1974] proved that $L_f(s)(-1)^{n-1}$ is a polynomial of degree $(d - 1)^n$ whose reciprocal zeros are of archimedean absolute value $q^{\frac{j}{2}}$.

The second author is supported by Shandong Prov. NSF No. ZR2019BA011 and by NNSFC No. 11401285.
Note that

\[ S_f(k) = \sum_{x \in \mathbb{F}_{q^k}} (1 + (\zeta_p - 1))^{\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_p}(f(x))} \in \mathbb{Z}[[\zeta_p - 1]], \ k = 1, 2, \cdots. \]

It follows that

\[ L_f(s) = \exp \left( \sum_{k=1}^{\infty} S_f(k) \frac{s^k}{k} \right) \in \mathbb{Q}_p[[s]]. \]

So it is interesting to know the \( p \)-adic absolute values of the reciprocal zeros and poles of \( L_f(s)^{(-1)^{n-1}} \). These \( p \)-adic absolute values are more subtle and mysterious, and are often encoded into a concave polygon on the coordinate plane. Usually, we called this polygon the \( q \)-adic Newton polygon of \( L_f(s)^{(-1)^{n-1}} \), and denote it as \( \text{NP}(f) \). When \( L_f(s)^{(-1)^{n-1}} \) is a polynomial, \( \text{NP}(f) \) is a concave polygon with initial point \((0, 0)\) whose slopes, counting multiplicities, are the \( q \)-adic order of the reciprocal zeros of \( L_f(s)^{(-1)^{n-1}} \). The polygon \( \text{NP}(f) \), though subtle and mysterious, is believed to be controlled by simple geometric invariants. In this circumstances, Hodge numbers show up.

**Definition 1.1.** The Hodge numbers \( h_0, h_1, \cdots, h_{nd} \) are defined by the formula

\[ h_j = \sum_{\substack{u_1, \cdots, u_n = 1 \\ \sum_{i=1}^{n} u_i = j}}^{d-1} 1, \ j = 0, 1, \cdots, nd. \]

The Hodge numbers are symmetric in the sense that

\[ h_{nd-j} = h_j, \ j = 0, 1, \cdots, nd. \]

They are of admissible length in the sense that

\[ \sum_{j=0}^{nd} h_j = (d - 1)^n. \]

Hodge numbers serve as multiplicities of Hodge slopes which are defined as follows.

**Definition 1.2.** The Hodge slopes are the numbers

\[ \frac{j}{d}, \ j = 0, 1, \cdots, nd. \]

Counting multiplicities, the Hodge slopes are of admissible height in the sense that

\[ \sum_{j=0}^{nd} \frac{j}{d} \cdot h_j = \frac{n}{2} \cdot (d - 1)^n. \]

Hodge slopes and Hodge numbers are used to define the Hodge polygon.
Definition 1.3. The Hodge polygon $\text{HP}(n, d)$ is the polygon whose vertices are the points

$$
\left( \sum_{j=0}^{i} h_j, \frac{1}{d} \sum_{j=0}^{i} jh_j \right), \ i = 0, 1, \cdots, nd.
$$

It is easy to see that the Hodge polygon $\text{HP}(n, d)$ is a concave polygon with initial point $(0, 0)$, end point $((d - 1)^{n}, \frac{n}{2} \cdot (d - 1)^{n})$, and slopes $\frac{j}{d}$ ($j = 0, 1, \cdots, nd$). The multiplicity of slope $\frac{j}{d}$ in $\text{HP}(n, d)$ is $h_j$. Moreover, $\text{HP}(n, d)$ is symmetric in the sense that the multiplicity of slope $\lambda$ is equal to the multiplicity of slope $n - \lambda$.

Adolphson and Sperber [1987; 1989] proved the following.

Theorem 1.4 (Hodge bound). If the leading form of $f$ is smooth, then

$$
\text{NP}(f) \geq \text{HP}(n, d)
$$

with coincide endpoints.

In general, it is very difficult to determine $\text{NP}(f)$. However, it is challenging to describe $\text{NP}(f)$ in terms of geometric invariants when $f$ is the generic polynomial of degree $d$ in $n$ variables. This leads to the following definition.

Definition 1.5. If $f$ is the generic polynomial of degree $d$ in $n$ variables, then by Grothendieck’s specialization lemma, the polygon $\text{NP}(f)$ is independent of $f$, and is denoted as $\text{NP}(n, d; q)$.

Combined with a result of [Gelfand et al. 1994], Adolphson-Sperber’s Hodge bound can be restated as follows.

Theorem 1.6 (Hodge bound). If $p$ is sufficiently large, then

$$
\text{NP}(n, d; q) \geq \text{HP}(n, d)
$$

with coincide endpoints.

When $p \equiv 1(\text{mod } d)$, Stickelberger’s theorem (combined with Grothendieck’s specialization lemma) gives the following.

Theorem 1.7 (Stickelberger). If $p \equiv 1(\text{mod } d)$ is sufficiently large, then

$$
\text{NP}(n, d; q) = \text{HP}(n, d).
$$

Wan [2004] put forward the following asymptotic $p$-adic Riemann hypothesis.

Conjecture 1.8 (Wan’s asymptotic $p$-adic Riemann Hypothesis). The following identity holds:

$$
\lim_{p \to \infty} \text{NP}(n, d; q) = \text{HP}(n, d).
$$

As an effort to describe $\text{NP}(n, d; q)$ in terms of geometric invariants, we introduce Frobenius numbers.
Definition 1.9. The Frobenius numbers are the numbers

\[ h_{j,0} = \sum_{i=0}^{j} h_i - \sum_{i=0}^{j-1} h_i, \quad j = 0, 1, \ldots, nd, \]

and

\[ h_{j,1} = \sum_{i=0}^{j-1} h_i - \sum_{i=0}^{j-1} h_i, \quad j = 0, 1, \ldots, nd. \]

It is obvious that the Frobenius numbers give rise to the following Frobenius decomposition of Hodge numbers.

\[ h_j = h_{j,0} + h_{j,1}. \quad (1.5) \]

That Frobenius decomposition is trivial when \( j \equiv j \pmod{d} \) is fixed under multiplication by \( p \), since

\[ h_{j,1} = 0 \text{ if } pj \equiv j \pmod{d}. \quad (1.6) \]

We shall prove the following two propositions.

Proposition 1.10 (cross symmetry). If \( pj \not\equiv j \pmod{d} \), then

\[ h_{nd-j,1-\epsilon} = h_{j,\epsilon}. \]

Proposition 1.11 (nonnegativity). The numbers \( h_{j,\epsilon} \)'s are nonnegative.

The Frobenius numbers \( h_{j,\epsilon} \)'s serve as multiplicities of the Frobenius slopes which are defined as follows.

Definition 1.12. The Frobenius slopes are the numbers

\[ \frac{1}{p-1} \left( \left\lceil \frac{(p-1)j}{d} \right\rceil - \epsilon \right), \quad (j, \epsilon) \in \{0, 1, \ldots, nd\} \times \{0, 1\}. \]

We shall prove the following admissibility for the Frobenius slopes.

Proposition 1.13 (admissible height). Counting multiplicities, the Frobenius slopes are of admissible height in the sense that

\[ \sum_{j=0}^{nd} \sum_{\epsilon=0,1} \frac{1}{p-1} \left( \left\lceil \frac{(p-1)j}{d} \right\rceil - \epsilon \right) \cdot h_{j,\epsilon} = \frac{n}{2} \cdot (d-1)^n. \]

Frobenius slopes and Frobenius numbers are used to define the Frobenius polygon.

Definition 1.14. The Frobenius polygon \( FP(n, d; p) \) is the polygon whose vertices are the points

\[ \left( \sum_{2j-\epsilon \leq 2i - \epsilon} h_{j,\epsilon}, \frac{1}{p-1} \sum_{2j-\epsilon \leq 2i - \epsilon} \left( \left\lceil \frac{(p-1)j}{d} \right\rceil - \epsilon \right) \cdot h_{j,\epsilon} \right) \]

for every \( (i, \epsilon) \in \{0, 1, \ldots, nd\} \times \{0, 1\} \).
It is easy to see that the Frobenius polygon \( FP(n; d; p) \) is a concave polygon with initial point \( (0, 0) \), end point \( ((d - 1)n, \frac{1}{2} \cdot (d - 1)n) \), and slopes \( \frac{1}{p-1} \left( \left\lfloor \frac{(p-1)^j}{d} \right\rfloor - \epsilon \right) \) \( (j = 0, 1, \ldots, nd; \ \epsilon = 0, 1) \). The multiplicity of slope \( \frac{1}{p-1} \left( \left\lfloor \frac{(p-1)^j}{d} \right\rfloor - \epsilon \right) \) in \( FP(n; d; p) \) is \( h_{j, \epsilon} \). Moreover, \( FP(n; d; p) \) is symmetric in the sense that the multiplicity of slope \( \lambda \) is equal to the multiplicity of slope \( n - \lambda \).

The Frobenius polygon is trivial at infinity in the following sense.

\[
\lim_{p \to \infty} FP(n; d; p) = HP(n, d).
\]

And, by Equation 1.6, the Frobenius polygon is trivial at the principal class in the following sense.

\[
FP(n, d; p) = HP(n, d) \text{ if } p \equiv 1(\text{mod } d).
\]

In the general, the Frobenius polygon is a majorization of the Hodge polygon in the following sense.

**Proposition 1.15** (majorization). The Hodge polygon is majorized by the Frobenius polygon in the sense that

\[
FP(n, d; p) \geq HP(n, d).
\]

One of the main result of this paper is the following improvement of Adolphson-Sperber’s Hodge bound.

**Theorem 1.16** (Frobenius bound). If the leading form of \( f \) is smooth, then

\[
NP(f) \geq FP(n, d; p).
\]

Combined with a result of [Gelfand et al. 1994], the above Frobenius bound can be restated as follows.

**Theorem 1.17** (Frobenius bound). If \( p \) is sufficiently large, then

\[
NP(n, d; q) \geq FP(n, d; p).
\]

We put forward the following \( p \)-adic Riemann hypothesis.

**Conjecture 1.18** (\( p \)-adic Riemann Hypothesis). If \( p \) is sufficiently large, then

\[
NP(n, d; q) = FP(n, d; p).
\]

By Equation 1.7, the above \( p \)-adic Riemann hypothesis implies Wan’s asymptotic \( p \)-adic Riemann hypothesis.

When \( p \equiv 1(\text{mod } d) \), the above \( p \)-adic Riemann hypothesis is true by Stickelberger’s theorem and Equation 1.8. When \( n = 1 \), the above \( p \)-adic Riemann hypothesis is proved by Zhu [2003; 2004]. We shall prove the above \( p \)-adic Riemann hypothesis when \( n = 2 \) and \( p \equiv -1(\text{mod } d) \).

**Theorem 1.19.** If \( n = 2 \) and \( p \equiv -1(\text{mod } d) \) is sufficiently large, then

\[
NP(n, d; q) = FP(n, d; p).
\]
From above theorem one can deduce Wan’s asymptotic $p$-adic Riemann hypothesis in the case that $n = 2$ and $p \equiv -1 \pmod{d}$.

**Corollary 1.20.** If $n = 2$, then

$$\lim_{p \rightarrow \infty} \frac{\text{NP}(n, d; q)}{p} = \frac{\text{HP}(n, d)}{p}.$$ 

Applying the $T$-adic theory developed by Liu and Wan [2009], one can prove the $T$-adic version of Corollary 1.20.

2. Hodge numbers

In this section we study Hodge numbers.

**Lemma 2.1** (monotonicity). The first half Hodge numbers are increasing in the sense that

$$h_1 \leq h_2 \leq \cdots \leq h_{\frac{nd}{2}}.$$ 

**Proof.** To indicate the dependence of $h_j$ on $n$, we write $h_j$ as $h_j^{(n)}$. Then

$$\sum_{j=0}^{nd} (h_j^{(n)} - h_{j-1}^{(n)}) t^j = \frac{(t^{\frac{j}{n}} - t)^n}{(1 - t^{\frac{j}{n}})^{n-1}} = \sum_{j=0}^{nd} (h_{j-1}^{(n-1)} - h_{j-d}^{(n-1)}) t^{\frac{j}{n}}.$$ 

It follows that

$$h_j^{(n)} - h_{j-1}^{(n)} = h_{j-1}^{(n-1)} - h_{j-d}^{(n-1)}.$$ 

By induction and by Lemma 1.2,

$$h_j^{(n)} - h_{j-1}^{(n)} = h_{j-1}^{(n-1)} - h_{j-d}^{(n-1)} \geq 0 \text{ if } j \leq \frac{(n-1)d}{2} + 1,$n-1} - h_{j-d}^{(n-1)} \geq 0 \text{ if } \frac{(n-1)d}{2} + 1 < j \leq \frac{nd}{2}. \square$$

**Lemma 2.2** (stability). If $d \nmid i$, then

$$\sum_{j=0}^{nd} h_j^{(n)} = \frac{(d-1)^n - (-1)^n}{d}.$$ 

**Proof.** We have

$$\sum_{u_1 + u_2 + \cdots + u_{n-1} \equiv 1 \pmod{d}} 1 = (d-1)^{n-1} - \sum_{u_1 + u_2 + \cdots + u_{n-1} \equiv 1 \pmod{d}} 1.$$ 

By induction,

$$\sum_{u_1 + u_2 + \cdots + u_{n-1} \equiv 1 \pmod{d}} 1 = \frac{(d-1)^n - (-1)^n}{d}.$$
The lemma now follows from the identity
\[
\sum_{j=0}^{nd} h_j = \sum_{u_1, u_2, \ldots, u_n = 1}^{d-1} 1.
\]

Lemma 2.3 (monotonicity). If \(0 \leq i \leq k \leq nd\), and \(i, k \not\equiv 0 \pmod{d}\), then
\[
\sum_{j \equiv i \pmod{d}} h_j \leq \sum_{j \equiv k \pmod{d}} h_j.
\]

**Proof.** We may assume that \(n \geq 2\). By the monotonicity of the first half Hodge numbers, we may assume that \(k > \left\lfloor \frac{nd}{2} \right\rfloor\). By Lemma 2.2 and Equation 1.2,
\[
\sum_{j \equiv i \pmod{d}} h_j = \frac{(d - 1)^n - (-1)^n}{d} - \sum_{j \equiv nd - i - d \pmod{d}} h_j.
\]

So it suffices to show that
\[
\sum_{j \equiv nd - i - d \pmod{d}} h_j \geq \sum_{j \equiv nd - k - d \pmod{d}} h_j.
\]

Let \(i_0 \equiv i \pmod{d}\) be the integer such that
\[
\left\lfloor \frac{nd}{2} \right\rfloor - d < nd - i_0 - d \leq \left\lfloor \frac{nd}{2} \right\rfloor.
\]

It suffices to show that
\[
\sum_{j \equiv nd - i_0 - d \pmod{d}} h_j \geq \sum_{j \equiv nd - k - d \pmod{d}} h_j,
\]

which follows from the monotonicity of the first half Hodge numbers, as
\[
d - k - d \leq \left\lfloor \frac{nd}{2} \right\rfloor - d < nd - i_0 - d \leq \left\lfloor \frac{nd}{2} \right\rfloor.
\]

The lemma is proved. \(\Box\)

3. Frobenius numbers

In this section we prove Propositions 1.10 and 1.11.

**Proof of Proposition 1.10.** It suffices to show that
\[
h_{nd - j, 1} = h_{j, 0}.
\]
Note that
\[ h_{nd-j,1} = \sum_{i=0}^{nd-j-1} h_{nd-i} - \sum_{i=0}^{nd-j-1} h_{nd-i}. \]

A change of variables yields
\[ h_{nd-j,1} = \sum_{i=j+1}^{nd} h_i - \sum_{i=j+1}^{nd} h_i. \]

By Lemma 2.2
\[ h_{nd-j,1} = -\sum_{i=0}^{j} h_i + \sum_{i=0}^{j} h_i = h_{j,0}. \]

Proposition 1.10 is proved. □

Proof of Proposition 1.11. By Equation 1.6 we may assume that
\[(p-1)j \not\equiv 0 \pmod{d}.\]

By Proposition 1.10 it suffices to show that
\[ h_{j,1} \geq 0. \]

Let \( j_0 \leq j - 1 \) be the largest integer such that \( pj_0 \equiv j \pmod{d} \). Then, by Lemma 2.3
\[ h_{j,0} = \sum_{i=0}^{j} h_i - \sum_{i=0}^{j-1} h_i, \]
\[ = \sum_{i=0}^{j} h_i - \sum_{i=0}^{j_0} h_i \geq 0. \]

Proposition 1.11 is proved. □

4. The Frobenius Polygon

In this section we prove the following proposition.

Proposition 4.1. Let \( k = \sum_{2j-\ell \leq 2i-\ell} h_{j,\ell} \) be the horizontal coordinate of a vertex of \( \text{FP}(n, d; p) \). Then
\[ \text{FP}(n, d; p)(k) = \sum_{2j-\ell \leq 2i-\ell} \frac{h_{j,\ell}}{p-1}(\lfloor \frac{pj-i}{d} \rfloor - \lfloor \frac{j-i}{d} \rfloor). \]
Proof. It is easy to see that
\[
\sum_{j=0}^{i} \left( \frac{(p-1)j}{d} + \frac{j-i}{d} - \frac{pj-i}{d} \right) h_j
\]
\[= \sum_{j=0}^{i-1} \left( \frac{(p-1)j}{d} + \frac{j-i}{d} - \frac{pj-i}{d} \right) h_j
\]
\[= \sum_{j=0}^{i-1} \left( \frac{(p-1)j}{d} + \frac{j-(i-1)}{d} - \frac{pj-(i-1)}{d} \right) h_j + h_{i,1}.
\]
It follows that
\[
\sum_{j=0}^{i} h_{j,1} = \sum_{j=0}^{i} \left( \frac{(p-1)j}{d} + \frac{j-i}{d} - \frac{pj-i}{d} \right) h_j.
\]
Hence
\[
\text{FP}(n, d; p)(k) = \frac{1}{p-1} \left( \sum_{2j-\epsilon \leq 2i} h_{j,\epsilon} \left( \frac{(p-1)j}{d} \right) - \sum_{j=0}^{i} h_{j,1} \right)
\]
\[= \sum_{2j-\epsilon \leq 2i} h_{j,\epsilon} \left( \frac{pj-i}{d} - \frac{j-i}{d} \right).
\]
The proposition is proved. \( \square \)

**Corollary 4.2.** Let \( k = \sum_{2j-\epsilon \leq 2i} h_{j,\epsilon} \) be the horizontal coordinate of a vertex of \( \text{FP}(n, d; p) \). Then
\[
\text{FP}(n, d; p)(k) - \text{HP}(n, d)(k)
\]
\[= \sum_{l=0}^{d-1} \frac{l}{(p-1)d} \left( \sum_{2j-\epsilon \leq 2i} h_{j,\epsilon} \left( \frac{j-i-1}{d} \right) \right) - \sum_{pj \equiv i+l+1 \pmod{d}} h_{j,\epsilon}.
\]
Proof. By Corollary 4.1,
\[
\text{FP}(n, d; p)(k)
\]
\[= \sum_{2j-\epsilon \leq 2i} \frac{j}{d} \cdot h_{j,\epsilon} + \sum_{2j-\epsilon \leq 2i} \frac{h_{j,\epsilon}}{p-1} \left( \frac{j-i-1}{d} \right)
\]
\[= \text{HP}(n, d)(k) + \sum_{l=0}^{d-1} \frac{l}{(p-1)d} \left( \sum_{j \equiv i+l+1 \pmod{d}} h_{j,\epsilon} \right) - \sum_{pj \equiv i+l+1 \pmod{d}} h_{j,\epsilon}.
\]
The corollary now follows. \( \square \)
5. Majorization over the Hodge polygon

In this section we prove Propositions 1.13 and 1.15.

Proof of Proposition 1.13 Proposition 1.13 follows from Corollary 4.2, Equation 1.4, and Lemma 2.2.

Proof of Proposition 1.15 By Equation 1.8 we may assume that \( p \not\equiv 1(\text{mod } d) \).

Firstly, we assume that 
\[
k = \sum_{j=0}^{i} h_j.\]

Then by Corollary 4.2,
\[
\text{FP}(n, d; p)(k) - \text{HP}(n, d)(k) = \sum_{l=0}^{d-1} \sum_{\substack{j=0 \atop j \equiv i+l+1(\text{mod } d)}}^{i} h_j - \sum_{\substack{j=0 \atop p j \equiv i+l+1(\text{mod } d)}}^{i} h_j.\]

Set
\[
b_l = \sum_{\substack{j=0 \atop j \equiv i+l+1(\text{mod } d)}}^{i} h_j \text{ and } c_l = \sum_{\substack{j=0 \atop p j \equiv i+l+1(\text{mod } d)}}^{i} h_j.\]

Then
\[
\{c_l\}_{l=0, \ l \not\equiv i-1(\text{mod } d)}^{d-1} \text{ is a permutation of } \{b_l\}_{l=0, \ l \not\equiv i-1(\text{mod } d)}^{d-1}.\]

Note that
\[
b_l = \sum_{\substack{j=0 \atop j \equiv i+l+1-\text{d}(\text{mod } d)}}^{i+l+1-d} h_j.\]

So by Lemma 2.3
\[
\{b_l\}_{l=0, \ l \not\equiv i-1(\text{mod } d)}^{d-1} \text{ is an increasing sequence. It follows that } \text{FP}(n, d; p)(k) - \text{HP}(n, d)(k) \geq 0.\]

Finally, we assume that
\[
k = \sum_{j=0}^{i-1} h_j + h_{i,1}, \ h_{i,1} \neq 0.\]
Then by Corollary 4.2
\[
FP(n, d; p)(k) - HP(n, d)(k) = \sum_{l=0}^{d-2} \frac{l}{(p-1)d} \left( \sum_{j=0}^{l-1} h_j - \sum_{j=0}^{l-1} h_j \right).
\]

Hence
\[
FP(n, d; p)(k) - HP(n, d)(k) \geq 0
\]
similarly. Proposition 1.15 is proved. □

6. Elementary Estimation

Let \( A \) and \( B \) be subsets of \( \{1, \ldots, d-1\} \)\(^n\) of cardinality \( k \), and \( \tau \) a bijection from \( A \) to \( B \). In this section we give a lower bound for the sum
\[
\sum_{u \in A} \left\lceil p \deg u - \deg \tau(u) \right\rceil, \quad \deg u = \frac{u_1 + u_2 + \cdots + u_n}{d}.
\]

We begin with the following definition.

**Definition 6.1.** The degree of \( A \) is defined to be
\[
\deg A = \sum_{u \in A} \deg u.
\]

It is easy to see that
\[
(6.9) \quad \deg A \geq HP(n, d)(k).
\]
And, it is easy to prove the following lemma.

**Lemma 6.2.** If \( p \) is large enough, and
\[
\deg A > HP(n, d)(k),
\]
then
\[
\sum_{u \in A} \left\lceil p \deg u - \deg \tau(u) \right\rceil > (p - 1)FP(n, d; p)(k).
\]

We now prove the following lemma.

**Lemma 6.3.** If \( \deg A = \deg B = HP(n, d)(k) \), then
\[
\sum_{u \in A} \left\lceil p \deg u - \deg \tau(u) \right\rceil \geq (p - 1)FP(n, d; p)(k).
\]

**Proof.** Firstly we assume that
\[
\sum_{j=0}^{i-1} h_j + h_{i,1} < k \leq \sum_{j=0}^{i} h_j.
\]
Then
\[
\sum_{u \in A} \lceil \deg(pu - \tau(u)) \rceil 
\geq \sum_{u \in A} \left( \lfloor \deg(pu) + \frac{d - 1 - i}{d} \rfloor - \lfloor \deg \tau(u) + \frac{d - 1 - i}{d} \rfloor \right) 
\geq \sum_{u \in A} \left( \lfloor \deg(pu) - \frac{i}{d} \rfloor - \lfloor \deg u - \frac{i}{d} \rfloor \right) 
\geq \sum_{2j - \epsilon \leq 2i - 1} h_{j, \epsilon} \left( \lfloor \frac{pj - i}{d} \rfloor - \lfloor \frac{j - i}{d} \rfloor \right) 
+ (k - \sum_{j=0}^{i-1} h_j - h_{i,1}) \left( \frac{(p - 1)i}{d} \right) 
\]

So by Proposition 4.1,
\[
\sum_{u \in A} \lceil \deg(pu - \tau(u)) \rceil \geq (p - 1)FP(n, d; p)(k).
\]

Secondly we assume that
\[
\sum_{j=0}^{i-1} h_j < k \leq \sum_{j=0}^{i-1} h_j + h_{i,1}.
\]

Then the number of elements \( u \in A \) such that
\[
\lceil \deg(pu - \tau(u)) \rceil = \lfloor \deg(pu) + \frac{d - 1 - i}{d} \rfloor - \lfloor \deg \tau(u) + \frac{d - 1 - i}{d} \rfloor + 1
\]
is no less than
\[
\sum_{\{\deg(pu) + \frac{d - 1 - i}{d} \} > \{\deg \tau(u) + \frac{d - 1 - i}{d} \}} 1 
\geq \sum_{u \in A, \deg u < \frac{i}{d}} \sum_{\{\deg(pu)\} = \frac{i}{d}} 1 - \sum_{\{\deg u\} = \frac{i}{d}} 1 - (k - \sum_{j=0}^{i-1} h_j) 
\geq \sum_{j=0}^{i-1} h_j + h_{i,1} - k.
\]
It follows that
\[
\sum_{u \in A} \lceil \deg(pu - \tau(u)) \rceil \\
\geq \sum_{u \in A} \left( \lceil \deg(pu) \rceil - \left\lceil \frac{i}{d} \right\rceil - \lceil \deg \tau(u) \rceil - \frac{i}{d} \right) + \sum_{j=0}^{i-1} h_j + h_{i,1} - k \\
\geq \sum_{2j - \epsilon \leq 2i - 1} h_{j,\epsilon} \left( \left\lfloor \frac{pj - i}{d} \right\rfloor - \left\lfloor \frac{j - i}{d} \right\rfloor \right) \\
- \left( \sum_{j=0}^{i-1} h_j + h_{i,1} - k \right) \left( \left\lfloor \frac{(p-1)i}{d} \right\rfloor \right) + \sum_{j=0}^{i-1} h_j + h_{i,1} - k \\
\geq \sum_{2j - \epsilon \leq 2i - 1} h_{j,\epsilon} \left( \left\lfloor \frac{pj - i}{d} \right\rfloor - \left\lfloor \frac{j - i}{d} \right\rfloor \right) - \left( \sum_{j=0}^{i-1} h_j + h_{i,1} - k \right) \left( \left\lfloor \frac{(p-1)i}{d} \right\rfloor \right) - 1
\]

So by Proposition 4.1
\[
\sum_{u \in A} \lceil \deg(pu - \tau(u)) \rceil \geq (p-1)FP(n, d; p)(k).
\]

The lemma is proved.

When \(k\) is the horizontal coordinate of a vertex of the Frobenius polygon, we can prove more.

**Definition 6.4.** Let \(A\) and \(B\) be subsets of \(\{1, 2, \ldots, d-1\}^n\). Let \(\frac{i}{d}\) be the maximal degree of elements of \(A\) and \(B\). An injection \(\tau\) from \(A\) to \(B\) is called a Sun Bin correspondence if
\[
\{ \deg \tau(u) + \frac{d-1-i}{d} \} \geq \{ p \deg u + \frac{d-1-i}{d} \}, \forall u \in A.
\]
The set of Sun Bin correspondences from \(A\) to \(B\) is denoted by \(S(A, B)\).

**Lemma 6.5.** Suppose that
\[
\deg A = \deg B = HP(n, d)(k),
\]
and
\[
k = \sum_{2j - \epsilon \leq 2i - \epsilon} h_{j,\epsilon}.
\]
Then
\[
\sum_{u \in A} [p \deg u - \deg \tau(u)] = (p-1)FP(n, d; p)(k)
\]
if and only if \(\tau\) is a Sun Bin correspondence.
Proof. In fact, \( \tau \) is a Sun Bin correspondence if and only if
\[
\sum_{u \in A} \left\lceil \deg (pu - \tau(u)) \right\rceil = \sum_{u \in A} \left( \left\lceil \deg (pu) + \frac{d-1-i}{d} \right\rceil - \left\lceil \deg (u) + \frac{d-1-i}{d} \right\rceil \right) = \sum_{2j-\epsilon \leq 2i-\eta} h_{j,\epsilon} \left( \left\lceil \frac{pj + d-1-i}{d} \right\rceil - \left\lceil \frac{j + d-1-i}{d} \right\rceil \right).
\]
So by Proposition 4.1, \( \tau \) is a Sun Bin correspondence if and only if
\[
\sum_{u \in A} \left\lceil \deg (pu - \tau(u)) \right\rceil = (p-1)FP(n,d,p,k).
\]
The lemma is proved. \( \square \)

7. The \( p \)-adic Theory of Exponential Sums

In this section we review the \( p \)-adic theory of exponential sums developed by Dwork [1962; 1964], and Adolphson and Sperber [1987; 1989].

Let \( \mathbb{Z}_p \) be the ring of \( p \)-adic integers, and \( \mathbb{Q}_p \) the field of \( p \)-adic numbers. Let \( \mu_{q-1} \) be the group of \( (q-1) \)-th roots of unity, \( \mathbb{Z}_q = \mathbb{Z}_p[\mu_{q-1}] \), and \( \mathbb{Q}_q = \mathbb{Q}_p(\mu_{q-1}) \). If necessary, elements of \( \mathbb{F}_q \) as numbers in \( \mathbb{Q}_q \) via the Teichmüller lifting.

Let
\[
E(x) = \exp \left( \sum_{i=0}^{\infty} \frac{x^{p^i}}{p^i} \right)
\]
be the Artin-Hasse exponential. Let \( \pi \) be the number such that
\[
E(\pi) = \zeta_p.
\]
It is easy to see that
\[
\text{ord}_p(\pi) = \text{ord}_p(\zeta_p - 1) = \frac{1}{p-1}.
\]
Write
\[
E_f(x) = \prod_{\deg u \leq 1} E(\pi a_u x^u).
\]
The function \( E_f \) lies in \( \mathbb{Z}_q[\pi^{\frac{1}{d}}] \)-module
\[
L = \left\{ \sum_{u \in N^n} b_u \pi^{\deg u} x^u \mid b_u \in \mathbb{Z}_q[\pi^{\frac{1}{d}}] \right\}.
\]
The function \( E_f \) acts on \( L \) by multiplication. Let \( \phi_p \) be the operator on \( L \) defined by the formula
\[
\phi \left( \sum_{u \in N^n} b_u \pi^{\deg u} x^u \right) = \sum_{u \in N^n} b_{pu} \pi^{\deg u} x^u.
\]
Let
\[ B = \left\{ \sum_{u \in \mathbb{N}^n} b_u \pi^{\deg u} x^u \in L \mid \lim_{\deg u \to +\infty} \ord_p(b_u) = +\infty \right\}. \]

It is easy to see that \( B \) is closed under the composition \( \phi \circ E_f \). So we regard \( \phi \circ E_f \) as an operator on \( B \). Let \( \partial \) be the map
\[ \partial : \oplus_{k=1}^n \pi^{\frac{1}{d}} x_k B \to B \]
defined by the formula
\[ \partial(g_1, g_2, \ldots, g_n) = \sum_{k=1}^n (x_k \frac{\partial}{\partial x_k} + f_k)g_k, \]
where \( f_k \)'s are defined by the formula
\[ d \log \hat{E}_f(x) = \sum_{k=1}^n f_k \frac{dx_k}{x_k}, \hat{E}_f(x) = \prod_{j=0}^{+\infty} E_{f'}^j(x^{p^j}). \]

It is easy to see that the operator \( \phi \circ E_f \) lives on the quotient
\[ H_0 = B/\text{Im} \partial. \]
So we now regard \( \phi \circ E_f \) as an operator on \( H_0 \).

The following lemma is due to Adolphson and Sperber [1987; 1989].

Lemma 7.1. If the leading form of \( f \) is smooth, then \( H_0 \) is a free \( \mathbb{Z}_q[\pi^{\frac{1}{d}}] \)-module of finite rank, and
\[ \pi^{\deg u} x^u, \ u \in \{1, \ldots, d-1\}^n \]
represents a basis of \( H_0 \). Moreover,
\[ \pi^{\deg w} x^w \equiv \sum_{\substack{u_1, \ldots, u_n = 1 \\ \deg u \leq \deg w}} \alpha_{u,w} \pi^{\deg u} x^u \pmod{\text{Im} \partial}, \ w \in \mathbb{N}^n. \]

Let \( \sigma \) be the Frobenius element of \( \text{Gal}(\mathbb{Q}_q/\mathbb{Q}_p) \). The element \( \sigma \) acts on \( H_0 \) naturally. Let \( \phi = \sigma^{-1} \circ \phi_p \circ E_f \).

The following theorem is due to Adolphson and Sperber [1987; 1989].

Theorem 7.2. If the leading form of \( f \) is smooth, then
\[ L_f(s)^{(-1)^{n-1}} = \det_{\mathbb{Z}_p[\pi^{\frac{1}{d}}]}(1 - \phi^a s). \]

8. Scalar extension

In this section we prove the following theorems.

Theorem 8.1. If the leading form of \( f \) is smooth, then
\[ \text{Tr}_{\mathbb{Z}_p[\pi^{\frac{1}{d}}]}(\phi^k) = 0 \text{ if } k \not\equiv 0 \pmod{a}. \]
Proof. We extend $\phi^k$ to $H_0 \otimes_{\mathbb{Z}_p[\frac{1}{\pi^2}]} \mathbb{Z}_q[\frac{1}{\pi} \pi^2]$ by scalar. Then
\[
\text{Tr}_{\mathbb{Z}_p[\frac{1}{\pi^2}]}(\phi^k) = \text{Tr}_{\mathbb{Z}_q[\frac{1}{\pi}]}(\phi^k | H_0 \otimes_{\mathbb{Z}_p[\frac{1}{\pi^2}]} \mathbb{Z}_q[\frac{1}{\pi} \pi^2]).
\]
Identifying $\phi^k$ as an operator on $H_0 \otimes_{\mathbb{Z}_p[\frac{1}{\pi^2}]} \mathbb{Z}_q[\frac{1}{\pi} \pi^2]$ via the canonical isomorphism
\[
H_0 \otimes_{\mathbb{Z}_p[\frac{1}{\pi^2}]} \mathbb{Z}_q[\frac{1}{\pi} \pi^2] \to H_0^{\mathbb{Z}(a)},
\]
we arrive at
\[
\text{Tr}_{\mathbb{Z}_p[\frac{1}{\pi^2}]}(\phi^k) = \text{Tr}_{\mathbb{Z}_q[\frac{1}{\pi}]}(\phi^k | H_0^{\mathbb{Z}(a)}).
\]
So it suffices to show that
\[
\text{Tr}_{\mathbb{Z}_q[\frac{1}{\pi}]}(\phi^k | H_0^{\mathbb{Z}(a)}) = 0 \text{ if } k \not\equiv 0(\mod a).
\]
For each $(w, j) \in \{1, \cdots, d-1\}^n \times \mathbb{Z}(a)$, let $\varepsilon_{w, j} \in H_0^{\mathbb{Z}(a)}$ be the vector whose $i$-component is represented by $\delta_{ij} \pi^{\deg w_x w}$. Then
\[
\varepsilon_{w, j}, (w, j) \in \{1, \cdots, d-1\}^n \times \mathbb{Z}(a)
\]
is a basis of $H_0^{\mathbb{Z}(a)}$. It is easy to see that
\[
\phi^k = \sigma^{-k} \circ \phi^k_p \circ \prod_{j=0}^{k-1} E_{f_j}^{\sigma_j}.
\]
Note that $\phi^k_p \circ \prod_{j=0}^{k-1} E_{f_j}^{\sigma_j}$ is $\mathbb{Z}_q[\frac{1}{\pi} \pi^2]$-linear on $H_0$. So, if $M$ is the matrix of $\phi^k_p \circ \prod_{j=0}^{k-1} E_{f_j}^{\sigma_j}$ on $H_0$ corresponding to the basis represented by $\pi^{\deg w_x w}, w \in \{1, \cdots, d-1\}^n,$
then
\[
\begin{pmatrix}
M & 0 & \cdots & 0 \\
0 & M^\sigma & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & M^{\sigma^{a-1}}
\end{pmatrix}
\]
is the matrix of $\phi^k_p \circ \prod_{j=0}^{k-1} E_{f_j}^{\sigma_j}$ on $H_0^{\mathbb{Z}(a)}$ corresponding to the basis
\[
\varepsilon_{w, j}, (w, j) \in \{1, \cdots, d-1\}^n \times \mathbb{Z}(a)
\]
Also note that
\[
\sigma^{-k}(\varepsilon_{w, j}) = \varepsilon_{w, j+k}.
\]
It follows that
\[
\text{Tr}_{\mathbb{Z}_q[\frac{1}{\pi}]}(\phi^k | H_0^{\mathbb{Z}(a)}) = 0 \text{ if } k \not\equiv 0(\mod a).
\]
The theorem is proved. \qed

**Theorem 8.2.** If the leading form of $f$ is smooth, then
\[
L_f(s^n)(-1)^{n-1} = \det_{\mathbb{Z}_p[\frac{1}{\pi^2}]}(1 - \phi s).
\]
Proof. Note that
\[ \det_{Z_p[\frac{\pi}{d}]}(1 - \phi^a s^a) = \text{Norm}_{Z_q[\frac{\pi}{d}]/Z_p[\frac{\pi}{d}]} \det_{Z_q[\frac{\pi}{d}]}(1 - \phi^a s^a). \]
Applying Theorem 7.2, we arrive at
\[ \det_{Z_p[\frac{\pi}{d}]}(1 - \phi^a s^a) = \text{Norm}_{Z_q[\frac{\pi}{d}]/Z_p[\frac{\pi}{d}]} L_f(s^a)(-1)^{n-1}. \]
By Equation 1.1,
\[ L_f(s^a)(-1)^{n-1} \in \mathbb{Q}_p(\zeta_p)[[s^a]]. \]
It follows that
\[ \det_{Z_p[\frac{\pi}{d}]}(1 - \phi^a s^a) = L_f(s^a)^{a(-1)^{n-1}}. \]
By Theorem 8.1
\[ \det_{Z_p[\frac{\pi}{d}]}(1 - \phi s)^a = \det_{Z_p[\frac{\pi}{d}]}(1 - \phi^a s^a). \]
It follows that
\[ L_f(s^a)^{a(-1)^{n-1}} = \det_{Z_p[\frac{\pi}{d}]}(1 - \phi s)^a. \]
Comparing the constant term, we arrive at
\[ L_f(s^a)(-1)^{n-1} = \det_{Z_p[\frac{\pi}{d}]}(1 - \phi s). \]
The theorem is proved. \(\square\)

**Theorem 8.3.** If the leading form of \(f\) is smooth, then
\[ L_f(s^a)(-1)^{n-1} = \det(1 - \begin{pmatrix} 0 & \cdots & 0 & M \\ M^a & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & M^{a-1} & 0 \end{pmatrix} s), \]
where \(M\) is the matrix of \(\phi_p \circ E_f\) on \(H_0\) corresponding to the basis represented by
\[ \pi^{\deg w_a w}, w \in \{1, \cdots, d-1\}^n. \]

**Proof.** By Theorem 8.2
\[ L_f(s^a)(-1)^{n-1} = \det_{Z_p[\frac{\pi}{d}]}(1 - \phi s). \]
Hence
\[ L_f(s^a)(-1)^{n-1} = \det_{Z_q[\frac{\pi}{d}]}(1 - \phi s | H_0^{\mathbb{Z}/(a)}). \]
In the proof of Theorem 8.1 we see that
\[ \begin{pmatrix} 0 & \cdots & 0 & M \\ M^a & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & M^{a-1} & 0 \end{pmatrix} \]
is the matrix of \(\phi\) on \(H_0^{\mathbb{Z}/(a)}\) corresponding to the basis
\[ \varepsilon_{w,j}, (w, j) \in \{1, \cdots, d-1\}^n \times \mathbb{Z}/(a). \]
The theorem now follows. □

9. Lower Bound Estimation

In this section we prove Theorem 1.16.

Proof of Theorem 1.16. Let
\[
(\pi^{\deg u - \deg w} c_{u,w})_{u,w \in \{1,2,\ldots,d-1\}^n}
\]
be the matrix of \(\phi_p \circ E_f\) on \(H_0\) corresponding to the basis represented by
\[
\pi^{\deg w} x^w, w \in \{1,2,\ldots,d-1\}^n.
\]
By Theorem 6.3 it suffices to show that, if \(S \subseteq \{1,2,\ldots,d-1\}^n \times \mathbb{Z}/(a)\) is of cardinality \(ak\), then
\[
\text{ord}_\pi \left( \det(\delta_{i,l+1} c_{u,w}^{\sigma_i})_{(u,i),(w,l) \in S} \right) \geq \text{FP}(n,d;p)(k).
\]
Write
\[
S = \bigcup_{i \in \mathbb{Z}/(a)} A_i \times \{i\}.
\]
Suppose that \(|A_{i_0}| \neq |A_{i_0+1}|\) for some \(i_0\). Without loss of generality, we assume that \(|A_{i_0}| > |A_{i_0+1}|\). Then the columns of the matrix
\[
(\delta_{i,l+1} c_{u,w}^{\sigma_i})_{(u,i),(w,l) \in S}
\]
indexed by \(A_{i_0} \times \{i_0\}\) are linearly dependent as their coefficients are all zero except those in the rows indexed by \(A_{i_0+1} \times \{i_0 + 1\}\). It follows that
\[
\det(\delta_{i,l+1} c_{u,w}^{\sigma_i})_{(u,i),(w,l) \in S} = 0.
\]
So we may assume that \(|A_i| = k\) for all \(i \in \mathbb{Z}/(a)\). Then
\[
\det(\delta_{i,l+1} c_{u,w}^{\sigma_i})_{(u,i),(w,l) \in S} = \pm \prod_{l \in \mathbb{Z}/(a)} \det(\sigma_i)_{u \in A_{i+1}, w \in A_i}.
\]
One can show that
\[
\text{ord}_\pi(c_{u,w}) \geq \lfloor \deg(pu - w) \rfloor.
\]
Therefore it suffices to show that
\[
\sum_{l \in \mathbb{Z}/(a)} \sum_{u \in A_{l+1}} \lfloor \deg(pu - \tau_l(u)) \rfloor \geq a(p - 1)\text{FP}(n,d;p)(k)
\]
for any \(a\)-tuple \((A_l)_{l \in \mathbb{Z}/(a)}\) of subsets of \(\{1,2,\ldots,d-1\}^n\) of cardinality \(k\), where \(\tau_l\) is a bijection from \(A_{l+1}\) to \(A_l\).

The theorem now follows from Lemmas 6.2 and 6.3 □
10. A Non-vanishing Theorem

Let \( k \leq \binom{d+n-2}{n} \) be the horizontal coordinate of a vertex of \( \text{FP}(n,d;p) \). We call \( k \) a coordinate of Hodge type if \( k = \sum_{j=0}^{i} h_j \) for some \( i \). Otherwise we call it a coordinate of pure Frobenius type.

Let \( V_k \) be the set of \( a \)-tuples of subsets of \( \{1,2,\ldots,d-1\} \) of cardinality \( k \) and of degree \( \text{HP}(n,d)(k) \). Let \( \lambda_i \)’s be \( p \)-adic integers such that \( \lambda_0, \lambda_1, \cdots, \lambda_{p-1} \) are \( p \)-adic units.

**Definition 10.1.** We define

\[
H(y) = \sum_{(A_j)_{j \in \mathbb{Z}/(a)}} \prod_{j=0}^{a-1} \sum_{\tau \in S(A_{j+1}, A_j)} \prod_{u \in A_{j+1}} \prod_{(i_w) \in \Delta(p\tau - \tau(u))} \lambda_{i_w} y_{i_w}^{i_w p^j},
\]

where \( S(A_{j+1}, A_j) \) is the set of Sun Bin correspondence from \( A_{j+1} \) to \( A_j \), and \( \Delta(u) \) is the set of vectors \( (i_w)_{\deg w \leq 1} \) with entries in \( \mathbb{N} \) such that

\[
\sum_{\deg w \leq 1} i_w w = u \quad \text{and} \quad \sum_{\deg w \leq 1} i_w = \lceil \deg u \rceil.
\]

In this section we prove the following non-vanishing theorem.

**Theorem 10.2.** If \( p \equiv -1 \pmod{d} \) is sufficiently large and \( n = 2 \), then \( H \) is nonzero modulo \( (p, y_w^q - y_w \mid \deg w \leq 1) \).

**Proof.** Note that, for any \( a \)-tuple \( \{\tau_j \in S(A_{j+1}, A_j)\}_{j \in \mathbb{Z}/(a)} \), and any system

\[
\{(i_w,u) \in \Delta(p\tau - \tau_j(u))\}_{u \in A_{j+1}} \quad j \in \mathbb{Z}/(a),
\]

we have

\[
\sum_{u \in A_{j+1}} \sum_{\deg w \leq 1} i_{w,u} \leq d \sum_{u \in A_{j+1}} \sum_{\deg w \leq 1} i_{w,u} (1 - \deg w)
\]

\[
\leq d \sum_{u \in A_{j+1}} (\lceil \deg(p \tau - \tau_j(u)) \rceil - \deg(p \tau - \tau_j(u))
\]

\[
\leq d^{n+1}.
\]

So, as a polynomial in the variables \( \{y_w \mid \deg w < 1\} \), the degree of

\[
\prod_{j=0}^{a-1} \sum_{\tau \in S(A_{j+1}, A_j)} \prod_{u \in A_{j+1}} \prod_{(i_w) \in \Delta(p\tau - \tau(u))} \lambda_{i_w} y_{i_w}^{i_w p^j}
\]

is bounded by \( d^{n+1}(1 + p + \cdots + p^{n-1}) \). It follows that, as a polynomial in the variables \( \{y_w \mid \deg w < 1\} \), the minimal form of

\[
\prod_{j=0}^{a-1} \sum_{\tau \in S(A_{j+1}, A_j)} \prod_{u \in A_{j+1}} \prod_{(i_w) \in \Delta(p\tau - \tau(u))} \lambda_{i_w} y_{i_w}^{i_w p^j}
\]
is
\[
\prod_{j=0}^{a-1} \sum_{\tau \in S_0(A_{j+1}, A_j)} \sum_{u \in A_{j+1}} \prod_{i_w \in \Delta_0(pu - \tau(u))} \lambda_{i_w} y_w^{i_w p^j},
\]
where \(S_0(A_{j+1}, A_j)\) is the set of correspondences \(\tau\) in \(S(A_{j+1}, A_j)\) such that
\[
\sum_{u \in A_{j+1}} \left\lfloor \deg(pu - \tau(u)) \right\rfloor
\]
is minimal, and \(\Delta_0(u)\) is the set of vectors \((i_w)_{\deg w \leq 1}\) in \(\Delta(u)\) such that
\[
\sum_{\deg w \leq 1} i_w = \left\lfloor \deg u \right\rfloor.
\]
Therefore, as a polynomial in the variables \(\{y_w \mid \deg w < 1\}\), the minimal form of \(H\) is
\[
H_0(y) = \sum_{(A_j) \in V_k} \prod_{j=0}^{a-1} \sum_{\tau \in S_0(A_{j+1}, A_j)} \sum_{u \in A_{j+1}} \prod_{i_w \in \Delta_0(pu - \tau(u))} \lambda_{i_w} y_w^{i_w p^j},
\]
where \(V_k\) is the set of \((A_j)_{j \in \mathbb{Z}/(a)} \in V_k\) such that
\[
\sum_{j \in \mathbb{Z}/(a)} p^j \sum_{u \in A_{j+1}} \left\lfloor \deg(pu - \tau(u)) \right\rfloor
\]
is minimal.

Thus the theorem follows from Lemmas 10.3 and 11.1. \(\square\)

**Lemma 10.3.** Let \(p \equiv -1 \pmod{d}\) be sufficiently large and \(n = 2\). If \(k\) is of Hodge type, then \(H_0(y)\), which is defined in the proof of Theorem 10.2, is nonzero modulo \((p, y^q - y^w \mid \deg w \leq 1)\).

**Proof.** As \(k\) is a coordinate of Hodge type, there is a unique subset \(A\) of \(\{1, 2, \cdots, d - 1\}\) of cardinality \(k\) and of degree \(\text{HP}(n, d)(k)\). So it suffices to show that
\[
\sum_{\tau \in S_0(A, A)} \sum_{i_w \in \Delta_0(pu - \tau(u))} \lambda_{i_w} y_w^{i_w w} \prod_{u \in A} \prod_{i_w \in \Delta_0(pu - \tau(u))} \lambda_{i_w} y_w^{i_w w}
\]
is nonzero modulo \(p\).

Let \(\Delta_1(u)\) be the set of vectors \((i_w)_{\deg w \leq 1}\) in \(\Delta_0(u)\) such that
\[
i_w = 0 \text{ if } \deg w = 1 \text{ and } w_1 w_2 (w_1 - \left\lfloor \frac{d + 1}{2} \right\rfloor)(w_1 - \left\lfloor \frac{d}{2} \right\rfloor) \neq 0.
\]
Then it suffices to show that
\[
\sum_{\tau \in S_0(A, A)} \sum_{i_w \in \Delta_1(pu - \tau(u))} \lambda_{i_w} y_w^{i_w w} \prod_{u \in A} \prod_{i_w \in \Delta_1(pu - \tau(u))} \lambda_{i_w} y_w^{i_w w}
\]
is nonzero modulo \(p\).

Let \(\Delta_2(u)\) be the set of vectors \((i_w)_{\deg w \leq 1}\) in \(\Delta_1(u)\) such that
\[
i_w = \begin{cases} 0 & \text{if } \left\{ \frac{w_1}{d}, \frac{w_1}{d} \right\} < 1, \\ 1 & \text{if } \left\{ \frac{w_1}{d}, \frac{w_1}{d} \right\} \geq 1. \end{cases}
\]
Let $S_1(A, A)$ be the set of correspondences in $S_1(A, A)$ such that
$$\Delta_2(\nu - \tau(u)) \neq \emptyset, \ \forall u \in A.$$ If $S_1(A, A) \neq \emptyset$, then as a polynomial in $y((\frac{pu}{d}, \frac{n}{d}))$, the minimal form of
$$\sum_{\tau \in S_0(A, A)} \prod_{w \in A} \sum_{(i_w) \in \Delta_1(\nu - \tau(u))} \prod_{w \in A} \lambda_{i_w} y_{i_w}^w$$
is
$$H_1(y) = \sum_{\tau \in S_1(A, A)} \prod_{w \in A} \sum_{(i_w) \in \Delta_3(\nu - \tau(u))} \prod_{w \in A} \lambda_{i_w} y_{i_w}^w.$$ Therefore the lemma follows from the following one. \qed

**Lemma 10.4.** If $p \equiv -1 (\text{mod } d)$ is sufficiently large and $n = 2$, then $H_1(y)$, which is defined in the proof of Lemma 10.3, is nonzero modulo $p$.

**Proof.** Let $\Delta_3(u)$ be the set of vectors $(i_w)_{\deg w \leq 1}$ in $\Delta_2(u)$ such that
$$i_{(d, 0)} = \left\lceil \frac{u_1}{d} \right\rceil$$and $i_{(0, d)} = \left\lceil \frac{u_2}{d} \right\rceil$. Let $S_2(A, A)$ be the set of correspondences $\tau$ in $S_1(A, A)$ such that
$$\tau(u)_1 \leq d - u_1 \text{ and } \tau(u)_2 \leq d - u_2, \ \forall u \in A.$$If $S_2(A, A) \neq \emptyset$, then as a polynomial in the variables $y_{(d, 0)}$ and $y_{(0, d)}$, the leading form of $H_1$ is
$$H_2(y) = \sum_{\tau \in S_2(A, A)} \prod_{w \in A} \sum_{(i_w) \in \Delta_3(\nu - \tau(u))} \prod_{w \in A} \lambda_{i_w} y_{i_w}^w.$$Therefore the lemma follows from the following one. \qed

**Lemma 10.5.** If $p \equiv -1 (\text{mod } d)$ is sufficiently large and $n = 2$, then $H_2(y)$, which is defined in the proof of Lemma 10.4, is nonzero modulo $p$.

**Proof.** Firstly, we order the variables $\{y_w \mid \deg w < 1\}$ such that $y_w > y_v$ if one of the following items holds:

1. $\deg w > \deg v$;
2. $\deg w = \deg v$ but $|w_1 - w_2| < |v_1 - v_2|$;
3. $\deg w = \deg v$, $|w_1 - w_2| = |v_1 - v_2|$, but $w_1 < v_1$.

Secondly, we order the monomials in the variables $\{y_w \mid \deg w < 1\}$ in accordance with the ordering of these variables. Thirdly, let $\Delta_4(\nu - \tau(u))$ be the subset of $\Delta_3(\nu - \tau(u))$ such that as a polynomial in the variables $\{y_w \mid \deg w < 1\}$, the leading form of
$$\sum_{(i_w) \in \Delta_3(\nu - \tau(u))} \prod_{w \in A} \lambda_{i_w} y_{i_w}^w$$is
$$\sum_{(i_w) \in \Delta_3(\nu - \tau(u))} \prod_{w \in A} \lambda_{i_w} y_{i_w}^w.$$
It is easy to see that $\Delta_4(pu - \tau(u))$ consists of one element. Finally, let $S_3(A, A)$ be the subset of $S_2(A, A)$ such that, as a polynomial in the variables $\{y_w\}_{\deg w < 1}$, the leading form of $H_2$ is

$$
\sum_{\tau \in S_3(A, A)} \prod_{u \in A} \sum_{(i_w) \in \Delta_4(pu - \tau(u))} \prod_{\deg w \leq 1} \lambda_{i_w} y_w^{i_w}.
$$

The lemma then follows from the following one. \qed

**Lemma 10.6.** Let $S_3(A, A)$ be as defined in the proof of Lemma 10.5. If $p \equiv -1(\text{mod } d)$ is sufficiently large and $n = 2$, then $|S_3(A, A)| = 1$.

**Proof.** Firstly, $\tau \in S_0(A, A)$ if and only if

$$
\sum_{\deg(\tau(u)) = 1 - \deg u} 1 = |A| - \sum_{u \in A} \left[\{\deg(pu - \tau(u))\}\right]
$$

is maximal, if and only if

$$
\deg(\tau(u)) = 1 - \deg u \text{ if } \frac{1}{2} \leq 1 - \deg u \leq \frac{i}{d},
$$

and

$$
\#\{\deg u = \frac{j}{d} | \deg(\tau(u)) = 1 - \deg u\} = d - j - 1 \text{ if } j \geq \max\{d - i, \frac{d}{2}\}.
$$

Secondly, let $\tau \in S_2(A, A)$ and $\deg(\tau(u)) = 1 - \deg u$. Then

$$
([\frac{d+1}{2}], [\frac{d}{2}]) \equiv -u - \tau(u)(\text{mod } d),
$$

So

$$
\tau(u)_1 \equiv [\frac{d}{2}] - u_1(\text{mod } d),
$$

and

$$
\tau(u)_2 \equiv [\frac{d+1}{2}] - u_2(\text{mod } d).
$$

Hence

$$
\tau(u) = ([\frac{d}{2}], [\frac{d+1}{2}]) - u,
$$

and

$$
d - i \leq u_1 + u_2, \quad u_1 < [\frac{d}{2}], \quad u_2 < [\frac{d+1}{2}].
$$

Finally, it is easy to see that $\tau \in S_3(A, A)$ if and only if

$$
\tau(u) = \begin{cases} ([\frac{d}{2}], [\frac{d+1}{2}]) - u, & d - i \leq u_1 + u_2, \quad u_1 < [\frac{d}{2}], \quad u_2 < [\frac{d+1}{2}], \\ u, & u_1 = [\frac{d-1}{2}], \quad u_2 < [\frac{d+1}{2}], \\ (u_2, u_1), & \text{otherwise}. \end{cases}
$$

The lemma is proved. \qed
11. Pure Frobenius coordinates

In this section we prove the following lemma.

**Lemma 11.1.** Let \( p \equiv -1 \pmod{d} \) be sufficiently large and \( n = 2 \). If \( k \) is of pure Frobenius type, then \( H_0(y) \), which is defined in the proof of Theorem 10.2, is nonzero modulo \( (p,y^d_w-y_w \mid \deg w \leq 1) \).

**Proof.** Let \( \Delta_1(u) \) be as defined in the proof of Lemma 10.3. It suffices to show that
\[
\sum_{(A_j) \in V_k, j=0}^{a-1} \prod_{u \in A_{j+1}} \prod_{(i_w) \in \Delta_1(\tau) \mid \deg w \leq 1} \lambda_{i_w} y_i^{w^p}
\]
is nonzero modulo \( (p, y^d_w - y_w \mid \deg w \leq 1) \).

As \( k \) is a coordinate of pure Frobenius type, we may assume that
\[
k = \sum_{j=0}^{i-1} h_j + h_{i,1}, \quad h_{i,1} \neq 0.
\]
Hence
\[
i > \frac{d}{2} \quad \text{and} \quad h_{i,1} = h_{d-i}.
\]
Let \( \tau \in S_0(A_{j+1}, A_j) \). Then
\[
\deg(\tau(u)) = 1 - \deg u \quad \text{if} \quad \deg u = \frac{i}{d}, \quad 1 - \frac{i}{d}.
\]
Let
\[
A = \{ \deg u < i \mid u_1 + u_2 \neq d - i \}.
\]
Let \( S_0(A, A) \) be the set of correspondences \( \tau \) in \( S(A, A) \) such that
\[
\sum_{u \in A} [\{(\deg(\tau(u))\}] \quad \text{is minimal, and let} \quad S_0(A_{j+1} \setminus A, A_j \setminus A) \quad \text{be the set of correspondences} \quad \tau \quad \text{in} \quad S(A_{j+1} \setminus A, A_j \setminus A) \quad \text{such that}
\]
\[
\deg(\tau(u)) = 1 - \deg u, \quad u \in A_{j+1} \setminus A.
\]
Then
\[
\sum_{\tau \in S_0(A_{j+1}, A_j) \mid \deg u \leq 1} \prod_{u \in A_{j+1}} \prod_{(i_w) \in \Delta_1(\tau) \mid \deg w \leq 1} \lambda_{i_w} y_i^{w^p} = g_j^{p^j} \sum_{\tau \in S_0(A, A) \mid \deg u \leq 1} \prod_{u \in A} \prod_{(i_w) \in \Delta_1(\tau) \mid \deg w \leq 1} \lambda_{i_w} y_i^{w^p},
\]
where
\[
g_j = \sum_{\tau \in S_0(A_{j+1} \setminus A, A_j \setminus A) \mid \deg u \leq 1} \prod_{u \in A_{j+1} \setminus A} \prod_{(i_w) \in \Delta_1(\tau) \mid \deg w \leq 1} \lambda_{i_w} y_i^{w^p}.
\]
Thus
\[
\sum_{(A_j) \in V_{k,0}} \prod_{j=0}^{a-1} \sum_{\tau \in S_0(A_j+1, A_j, A)} \sum_{l \in A_{j+1}} \sum_{(i_w) \in \Delta_1 (pu - \tau(u))} \prod_{w \leq 1} \lambda_{i_w} y_i^{w^{pu_j}}.
\]

We can prove that
\[
\sum_{\tau \in S_0(A, A) \in A} \sum_{(i_w) \in \Delta_1 (pu - \tau(u))} \prod_{w \leq 1} \lambda_{i_w} y_i^{w^{pu}}
\]
is nonzero modulo \(p\) as we prove Lemma 10.3. Therefore the lemma follows from the following one.

**Lemma 11.2.** Let \(p \equiv -1 (\text{mod} \ d)\) be sufficiently large and \(n = 2\). If \(k\) is of pure Frobenius type, then

\[
\sum_{(A_j) \in V_{k,0}} \prod_{j=0}^{a-1} g_j^{pu_j}
\]
is nonzero modulo \((p, y_q^w - y^w \mid \deg w \leq 1)\), where \(g_j\) is as defined in the proof of Lemma 11.1.

**Proof.** As the degree of \(y_i^{[\left(\frac{d+1}{2}\right), \left(\frac{d}{2}\right)]}\) in \(g_j\) is at least 1, it suffices to show that

\[
\sum_{(A_j) \in V_{k,0}} \prod_{j=0}^{a-1} g_j^{pu_j}
\]
is nonzero modulo \((p, y_q^w - y^w \mid \deg w \leq 1)\).

Let \(\Delta_2(u)\) be as defined in the proof of Lemma 11.1. Let
\[
g_{j,1} = \sum_{\tau \in S_0(A_{j+1} \setminus A, A_j \setminus A)} \prod_{w \in A_{j+1} \setminus A} \sum_{(i_w) \in \Delta_2 (pu - \tau(u))} \prod_{w = (d,0), (0,d)} \lambda_{i_w} y_i^{w}.
\]

It suffices to show that

\[
\sum_{(A_j) \in V_{k,0}} \prod_{j=0}^{a-1} g_{j,1}^{pu_j}
\]
is nonzero modulo \((p, y_q^{d/2} - y^w \mid \deg w \leq 1)\).

Let \(\tau \in S_0(A_{j+1} \setminus A, A_j \setminus A), \deg u = 1 - \frac{d}{2}\), and
\[
(i_w)_{\deg w \leq 1} \in \Delta_2 (pu - \tau(u)).
\]

Then
\[
([d + 1, 1), 2] - u - \tau(u) (\text{mod} \ d).
\]

So
\[
\tau(u)_{1} \equiv \left[\frac{d}{2}\right] - u_1 (\text{mod} \ d),
\]
\[ \tau(u)_2 = \left\lfloor \frac{d+1}{2} \right\rfloor - u_2 \pmod{d}. \]

It follows that
\[ \tau(u) = \left( \left\lfloor \frac{d}{2} \right\rfloor, \left\lfloor \frac{d+1}{2} \right\rfloor \right) - u. \]

Hence
\[ \{ u \in A_j \mid u_1 + u_2 = i \} = \tilde{A}, \]

where
\[ \tilde{A} = \{ u_1 + u_2 = i \mid 0 < u_1 < \frac{d}{2}, 0 < u_2 < \frac{d+1}{2} \} \]

Thus
\[ \sum_{(A_j) \in V_{k,0}} \prod_{j=0}^{a-1} g_{j,1}^{p_j} = \prod_{j=0}^{a-1} g_{j,2}^{p_j}, \]

where
\[ g_{j,2} = \sum_{\tau \in S_1(\tilde{A}, \tilde{A})} \prod_{u, w} \sum_{(i_w) \in \Delta_2(p u - \tau(u))} \prod_{w,(d,0), (0,d)} \lambda_{i_w} y_{i_w}^{i_u}, \]

with \( S_1(\tilde{A}, \tilde{A}) \) being the set of correspondences in \( S_0(\tilde{A}, \tilde{A}) \) such that
\[ \tau(u) = \left( \left\lfloor \frac{d}{2} \right\rfloor, \left\lfloor \frac{d+1}{2} \right\rfloor \right) - u. \]

Note that
\[ |S_1(\tilde{A}, \tilde{A})| = 1, \]

and
\[ |\Delta_2(p u - \tau(u))| = 1 \text{ when } u \in \tilde{A}, \tau \in S_1(\tilde{A}, \tilde{A}). \]

The lemma now follows. \( \square \)

12. The Exact Bound Estimation

In this section we prove Theorems 1.19

Proof of Theorems 1.19 Let \( f \) be the generic polynomial of degree \( d \) in \( n \) variables. By a result of [Gelfand et al. 1994], we may assume that the leading form of \( f \) is smooth. Let
\[ (\pi^{\deg u \deg w} c_{u,w})_{u,w \in \{1,2,\ldots,d-1\}^n} \]
be the matrix of \( \phi_p \circ E_f \) on \( H_0 \) corresponding to the basis represented by
\[ \pi^{\deg w} x^w, w \in \{1,2,\ldots,d-1\}^n. \]

Let \( k \leq \binom{d+n-2}{n} \) be a horizontal coordinate of vertices of \( \text{FP}(n,d;p) \). By the symmetry of the Frobenius polygon and the functional equation of \( L_f(s)^{(-1)^{n-1}} \), it suffices to show that
\[ \text{NP}(f)(k) = \text{FP}(n,d;p)(k). \]

By Theorem 8.3 it suffices to show that
\[ q^{-\text{FP}(n,d;p)(k)} \sum_S \det(\delta_{j+1} c_{u,w}^{p_j})(u,j),(w,l) \in S \]
is a \( p \)-adic unit, where \( S \) runs over subsets of \( \{1, 2, \cdots, d-1\}^n \times \mathbb{Z}/(a) \) of cardinality \( ak \). As in the proof of Theorem 1.16 we may assume that \( S = \bigcup_{j \in \mathbb{Z}/(a)} A_j \times \{j\} \) with \(|A_j| = k\). Then

\[
\det(\delta_{j,l+1}c_{u,w}^{j})_{(u,j),(w,l) \in S} = \pm \prod_{j \in \mathbb{Z}/(a)} \det(c_{u,w}^{j})_{u \in A_{j+1}, w \in A_j}.
\]

So it suffices to show that

\[
q^{-\text{FP}(n,d;p)(k)} \sum_{(A_0, A_1, \cdots, A_{a-1})} \prod_{j=0}^{a-1} \det(c_{u,w}^{j})_{u \in A_{j+1}, w \in A_j}
\]

is a \( p \)-adic unit, where \((A_0, A_1, \cdots, A_{a-1})\) runs over \( a \)-tuples of subsets of \( \{1, 2, \cdots, d-1\}^n \) of cardinality \( k \).

One can show that

\[
\text{ord}_\pi(c_{u,w}) \geq \lceil \text{deg}(pu - w) \rceil.
\]

So, by Lemma 6.2, we may assume that each \( A_j \) is of degree \( \text{HP}(n,d)(k) \).

Then one can show that

\[
c_{u,w} \equiv \gamma_{pu - w} \pmod{\pi^{\lceil \text{deg}(pu - w) \rceil + 1}}, \forall u \in A_{j+1}, w \in A_j,
\]

where the numbers \( \gamma_u \)'s are defined by the formula

\[
E_f(x) = \sum_{u \in \mathbb{N}^n} \gamma_u x^u.
\]

Therefore it suffices to show that

\[
q^{-\text{FP}(n,d;p)(k)} \sum_{(A_0, A_1, \cdots, A_{a-1})} \prod_{j=0}^{a-1} \sum_{\tau \in S(A_{j+1}, A_j)} \prod_{u \in A_{j+1}} \prod_{w \in A_j} \lambda_{i,w} a_{i,w}^{i,w \tau(u)}
\]

is a \( p \)-adic unit.

One can show that

\[
\gamma_u \equiv \pi^{\lceil \text{deg } u \rceil} \sum_{(i,w) \in \Delta(u) \deg w \leq 1} \prod_{w \leq 1} \lambda_{i,w} a_{i,w}^{i,w \tau(u)(\mod \pi^{\lceil \text{deg } u \rceil + 1})},
\]

where \( \Delta(u) \) is defined in Definition 10.1 and the numbers \( \lambda_i \)'s are defined by the formula

\[
E(x) = \sum_{j=0}^{+\infty} \lambda_j x^j.
\]

So, by Lemma 6.5, it suffices to show that

\[
\sum_{(A_0, A_1, \cdots, A_{a-1})} \prod_{j=0}^{a-1} \sum_{\tau \in S(A_{j+1}, A_j)} \prod_{u \in A_{j+1}} \prod_{w \in A_j} \lambda_{i,w} a_{i,w}^{i,w \tau(u)}
\]

is a \( p \)-adic unit. Theorem 1.19 now follows from Theorem 10.2.
THE $p$-ADIC RIEMANN HYPOTHESIS FOR EXPONENTIAL SUMS

REFERENCES

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

[Adolphson and Sperber 1989] A. Adolphson and S. Sperber, Exponential sums and Newton polyhedra: cohomology and estimates, Ann. Math. 130 (1989), 367-406.

[Deligne 1974] P. Deligne, La conjecture de Weil I, Publ. Math. I.H.E.S. 43 (1974), 273-307.

[Dwork 1962] B. Dwork, On the zeta function of a hypersurface, Publ. Math. I.H.E.S. 12 (1962), 5-68.

[Dwork 1964] B. Dwork, On the zeta function of a hypersurface II, Ann. Math. 80 (1964), 227-299.

[Gelfand et al. 1994] I.M. Gelfand, M.M. Kapranov and A.V. Zelevinsky, Discriminants, Resultants and Multidimensional Determinants, Birkhäuser Boston, Inc., Boston, MA, 1994.

[Liu and Wan 2009] C. Liu and D. Wan, $T$-adic exponential sums over finite fields, Algebra and Number Theory., Vol 3, 5(2009), 489-509.

[Wan 2004] D. Wan, Variation of $p$-adic Newton polygons for $L$-functions of exponential sums, Asian J. Math., Vol 8, 3(2004), 427-474.

[Zhu 2003] J. H. Zhu, $p$-adic variation of $L$-functions of one variable exponential sums, I. Amer. J. Math., 125 (2003), 669-690.

[Zhu 2004] J. H. Zhu, Asymptotic variation of $L$ functions of one-variable exponential sums, J. Reine Angew. Math., 572 (2004), 219–233. 1529–1550.

Chunlei Liu, School of Mathematical Sciences, Shanghai Jiao Tong University, Shanghai 200240, email: clli@situ.edu.cn

Chuanze Niu, School of Mathematical Sciences, Liaocheng University, Liaocheng 252059, email: niuchuanze@lcu.edu.cn