Slope Estimates for Generalized Artin-Schreier Curves

Gary McGuire and Emrah Sercan Yılmaz
School of Mathematics and Statistics
University College Dublin
Ireland

Abstract

We provide first slope estimates of the Newton polygon of generalized Artin-Schreier curves, which are proved using the action of Frobenius and Verschiebung on cohomology. We provide a number of applications such as an improved Hasse-Weil bound for this class of curves.

Keywords

Generalized Artin-Schreier, Supersingular, Newton Polygon.

1 Introduction

Let $q = p^u$ where $p$ is any prime and $u \geq 1$ is an integer, and let $Q = p^s$ where $s \geq 1$ is an integer. Let $X$ be a projective smooth absolutely irreducible curve of genus $g$ defined over $\mathbb{F}_Q$. Consider the $L$-polynomial of the curve $X$ over $\mathbb{F}_Q$, defined by

$$L_X(T) = \exp \left( \sum_{i=1}^{\infty} \left( \# X(\mathbb{F}_{Q^i}) - Q^i - 1 \right) \frac{T^i}{i} \right).$$

where $\# X(\mathbb{F}_{Q^i})$ denotes the number of $\mathbb{F}_{Q^i}$-rational points of $X$. It is well known that $L_X(T)$ is a polynomial of degree $2g$ with integer coefficients, so we write it as

$$L_X(T) = \sum_{i=0}^{2g} c_i T^i, \quad c_i \in \mathbb{Z}. \quad (1)$$

The Hasse-Weil bound places restrictions on the coefficients of $L_X(T)$ and on the values of $\# X(\mathbb{F}_{Q^i})$. When we restrict ourselves to certain types of curve, such as supersingular curves, or curves with Hasse-Witt invariant 0, even more restrictions are placed on $L_X(T)$ and $\# X(\mathbb{F}_{Q^i})$. This article is about generalized Artin-Schreier curves and these restrictions. Our main result is a bound on the first slope, see Theorem 1 below.

1 Corresponding Author, email gary.mcguire@ucd.ie, Research supported by Science Foundation Ireland Grant 13/IA/1914
2 Research supported by Science Foundation Ireland Grant 13/IA/1914
Consider the sequence of points
\[ \left\{ \left( i, \frac{\text{ord}_p(c_i)}{s} \right) : 0 \leq i \leq 2g, \right\} \]
in \( \mathbb{Q}^2 \). If \( c_i = 0 \) for some \( 1 \leq i \leq 2g \), we define \( \text{ord}_p(c_i) = \infty \). The normalized \( p \)-adic Newton polygon of \( L_X(T) \) is defined to be lower convex hull of this set of points. It is usually called the Newton polygon of \( X/\mathbb{F}_q \), and denoted by \( NP(X/\mathbb{F}_q) \). It is well known that \( c_0 = 1 \) and \( c_{2g} = q^g \), so \((0,0)\) and \((2g,g)\) are respectively the initial and the terminal points of the Newton polygon.

We call a curve \( X \) a generalized Artin-Schreier curve over \( \mathbb{F}_q \) if \( X \) can be defined by an equation of the form
\[ X : y^q - y = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 \] (2)
where \( a_i \in \mathbb{F}_q, a_d \neq 0, (d, p) = 1, q = p^u \) and \( u \) is a positive integer. We note that there is not necessarily any relationship between \( u \) and \( s \), where \( Q = p^s \). The genus of (2) is \((q - 1)(d - 1)/2\).

In the case \( q = p \) (i.e. \( u = 1 \)) the curve (2) is known as an Artin-Schreier curve. In terms of function fields, an Artin-Schreier curve is a \( p \)-cyclic covering of the projective line over \( \mathbb{F}_q \) ramified only at infinity. While there are many papers in the literature about Artin-Schreier curves, there are fewer about generalized Artin-Schreier curves, especially in our context.

Let \( X/\mathbb{F}_q \) be a generalized Artin-Schreier curve given by (2). Define the support of \( X \) by
\[ \text{supp}(X) := \{ i \in \mathbb{N} | a_i \neq 0 \} \]
Let \( s_p(i) \) be the sum of all digits in the base \( p \) expansion of \( i \in \mathbb{N} \).

Let \( NP_1(X/\mathbb{F}_q) \) denote the first slope of \( NP(X/\mathbb{F}_q) \), This is usually referred to as the first slope of \( X/\mathbb{F}_q \). The first and main result in this paper is the following.

**Theorem 1.** Let \( X : y^q - y = f(x) \in \mathbb{F}_q[x] \) has degree \( d \), and let \( \sigma = \max\{s_p(l) | l \in \text{supp}(X)\} \). Then
\[ NP_1(X/\mathbb{F}_q) \geq \frac{1}{\sigma}. \]

This theorem follows a line of results that one may call \( p \)-adic bounds, where the proofs rely on Stickelberger’s theorem, see for example Moreno and Moreno [9] and later Blache [3]. Our methods are completely different, and are similar to those of Scholten-Zhu in the papers [11], [12] and [13].

This paper is laid out as follows. Section 2 gives important applications of Theorem 1. In Section 3 we give some background for the proof of Theorem 1. Sections 4 and 5 develop this for generalized Artin-Schreier curves, and mostly follow the development of Scholten-Zhu (no new ideas are needed in generalising from \( p \) to \( q \), however we include the proof for completeness). In Section 6 we present new results for characteristic \( p \) on \( r \)-tiling sequences. Finally, Section 7 presents the proof of Theorem 1 and Section 8 presents the proof of Theorem 3.
2 Applications

In this section we will give some applications of Theorem 1 where $X$ is a generalized Artin-Schreier curve of the form (2).

2.1 First Slope

Theorem 1 allows us to give a lower bound for the first slope of Newton polygon of the generalized Artin-Schreier curves (2) depending on $d$ and $p$, but not on $u$. The following corollary states this bound.

**Corollary 1.** Let $X : y^p = f(x)$ where $f(x) \in \mathbb{F}_p[x]$ has degree $d$, and let $\tau = (p - 1)[\log_p(d)]$. Then

$$NP_1(X/\mathbb{F}_p) \geq \frac{1}{\tau}.$$  \(3\)

**Proof.** We trivially have $\max\{s_p(l) \mid l \in \text{supp}(X)\} \leq \lceil \log_p(d) \rceil(p - 1)$. The statement now follows by Theorem 1. \(\Box\)

This improves exponentially (compare $d/2$ with $\log(d + 1)$) on the bound in [5] where it is shown that $NP_1(X/\mathbb{F}_p) \geq \frac{1}{g}$ for the curve $y^2 - y = f(x)$ in characteristic 2, where $f(x)$ has degree $d = 2g + 1$.

As remarked in [13], the $1/g$ bound follows from properties of Newton polygons of abelian varieties.

The bound (3) is tight in the sense that for each $p$ and $d$ there is a curve $X$ with first slope equal to $1/\tau$: our proofs in the remainder of the paper show that the curves in Theorem 1 give equality in (3).

2.2 Divisibility

We next relate the first slope to divisibility. The $p$-divisibility of the coefficients in the L-polynomial (1) is of interest for a few reasons. For example, Manin showed that the $p$-rank of the Jacobian of a curve (also known as the Hasse-Witt invariant) is equal to the degree of the L-polynomial with coefficients reduced modulo $p$. Thus, a curve has $p$-rank 0 precisely when all coefficients except the constant term are divisible by $p$. Mazur [7] has drawn attention to the important problem of finding the $p$-adic valuations of the Frobenius eigenvalues, which is closely related to the $p$-divisibility of the coefficients.

Another reason for studying the $p$-divisibility is to prove supersingularity. The following is immediate from the definition of supersingularity.

**Lemma 2.** A curve $X$ over $\mathbb{F}_p$ (where $Q = p^s$) with the L-polynomial (1) is supersingular if and only if

$$\frac{\text{ord}_p(c_i)}{s} \geq \frac{i}{2} \text{ for all } i = 1, \ldots, 2g.$$
We will present a (partial) generalization of this for generalized Artin-Schreier curves in Corollary 2, but first we need a simple proposition.

**Proposition 1.** Let $X : y^p - y = f(x)$ be a generalized Artin-Schreier curve, where $f(x) \in \mathbb{F}_Q[x]$ has degree $d$. Suppose that $NP_1(X/\mathbb{F}_Q) = 1/\sigma$ where $\sigma \geq 2$. Then:

1. If $X$ has L-polynomial (1), then $p^{\lceil si/\sigma \rceil}$ divides $c_i$ for $1 \leq i \leq 2g$.

2. $p^{\lceil sn/\sigma \rceil}$ divides $\left| \#X(\mathbb{F}_Q^n) - (Q^n + 1) \right|$ for all integers $n \geq 1$.

**Proof.**

Let $X$ have L-polynomial (1). Since $NP_1(X/\mathbb{F}_Q) = 1/\sigma$, it follows from convexity of the Newton polygon that $p^{\lceil si/\sigma \rceil}$ divides $c_i$ where $1 \leq n \leq 2g$.

Let $S_n = \left| \#X(\mathbb{F}_Q^n) - (Q^n + 1) \right|$. Since we have $S_1 = c_1$ is divisible by $p^{\lceil s/\sigma \rceil}$, and since we have the well-known relation

$$c_1 + 2c_2t + \cdots + 2gc_{2g}t^{2g-1} = (c_0 + c_1t + \cdots + c_{2g}t^{2g}) \sum_{n=1}^{\infty} S_n t^{r-1},$$

we get the result by induction.

It follows from Proposition 1 part 1 and the result of Manin mentioned above that a generalized Artin-Schreier curve $X$ defined by (2) has $p$-rank 0. This is well known and can be proved by other methods (such as using the Deuring-Shafarevich formula).

Here is the generalization of Lemma 2.

**Corollary 2.** A generalized Artin-Schreier curve $X$ defined by (2) over $\mathbb{F}_Q$ (where $Q = p^s$) with the L-polynomial (1) and $NP_1(X/\mathbb{F}_Q) = 1/\sigma$ has

$$\frac{\text{ord}_p(c_i)}{s} \geq \frac{i}{\sigma} \text{ for all } i = 1, \ldots, 2g.$$

**Proof.** This follows from Proposition 1 part 1.

Next we state a simple corollary about the divisibility of the trace of Frobenius.

**Corollary 3.** Let $X : y^p - y = f(x)$ where $f(x) \in \mathbb{F}_Q[x]$ has degree $d$ and let $\tau = (p-1)[\log_p d]$. Then $p^{\lceil sn/\tau \rceil}$ divides $\left| \#X(\mathbb{F}_Q^n) - (Q^n + 1) \right|$ for all $n \geq 1$.

**Proof.** It is an easy consequence of Corollary 1 and Proposition 1.
2.3 Improved Hasse-Weil Bound

An improved Hasse-Weil bound is presented in [5] in characteristic 2, for $Q = 2^n$, $n$ odd. We present a stronger improvement here, for any prime power $Q$, which is strictly better for genus $> 3$.

**Corollary 4.** Let $X : y^{p^n} - y = f(x)$ where $f(x) \in \mathbb{F}_Q[x]$ has degree $d$. Let $\tau = \lceil \log_p d \rceil (p - 1)$. Then

$$|\# X(\mathbb{F}_Q^n) - (Q^n + 1)| \leq p^{\lceil \frac{sn}{\tau} \rceil} \left\lfloor \frac{g \sqrt{Q^n}}{p^{\lceil \frac{sn}{\tau} \rceil}} \right\rfloor$$

where $g$ is the genus of $X$.

**Proof.** This corollary is a consequence of Corollary 3. The right hand side is the smallest integer which is divisible by $p^{\lceil \frac{sn}{\tau} \rceil}$ and smaller than the usual Hasse-Weil bound.

Note that Corollary 3 may be more useful than Corollary 4 when considering families of curves, because using the divisibility property we can greatly reduce the number of possible values of $|\# X(\mathbb{F}_Q^n) - (Q^n + 1)|$ as $X$ ranges over the family. This can be useful when studying cyclic codes, see [8] for example.

We give a few numerical examples to illustrate our results.

**Example 1:** Let $Q = 2$, $n = 7$ and $d = 15$, then Hasse-Weil bound gives $|\# X(\mathbb{F}_2^7) - (2^7 + 1)| \leq 154$ and the bound in Corollary 4 gives $|\# X(\mathbb{F}_2^7) - (2^7 + 1)| \leq 152$.

The divisibility property in [5] implies that 2 divides $|\# X(\mathbb{F}_2^7) - (2^7 + 1)|$, however the divisibility property in Corollary 4 tells us that 4 divides $|\# X(\mathbb{F}_2^7) - (2^7 + 1)|$.

**Example 2:** Let $Q = 2$, $n = 101$ and $d = 83$, then Hasse-Weil bound gives $|\# X(\mathbb{F}_{2^{101}}) - (2^{101} + 1)| \leq 130565559286778326$, the bound in [5] gives $|\# X(\mathbb{F}_{2^{101}}) - (2^{101} + 1)| \leq 130565559286778320$ (an improvement of 6), and the bound in Corollary 4 gives $|\# X(\mathbb{F}_{2^{101}}) - (2^{101} + 1)| \leq 130565559286759424$ (an improvement of 18,902).

The divisibility property in [5] gives $2^3 \mid |\# X(\mathbb{F}_{2^{101}}) - (2^{101} + 1)|$ and the divisibility property in Corollary 4 gives $2^{15} \mid |\# X(\mathbb{F}_{2^{101}}) - (2^{101} + 1)|$.

**Example 3:** Let $Q = 3$, $n = 51$ and $d = 104$, then Hasse-Weil bound gives $|\# X(\mathbb{F}_{3^{51}}) - (3^{51} + 1)| \leq 302314665567277$ and the bound in Corollary 4 gives $|\# X(\mathbb{F}_{3^{51}}) - (3^{51} + 1)| \leq 302314665566691$.

The divisibility property in Corollary 4 gives $3^{11} \mid |\# X(\mathbb{F}_{3^{51}}) - (3^{51} + 1)|$.

2.4 Family of Supersingular Curves

A curve is said to be supersingular if its Newton polygon is a straight line segment of slope 1/2 (equivalently if $NP_{1}(X/\mathbb{F}_Q) = 1/2$). In van der Geer-van der Vlugt [6] and Scholten-Zhu [12] it is shown that
all curves of the form
\[ y^2 - y = \sum_{i=0}^{k} a_{2^i+1} x^{2^i+1} \]
are supersingular over the finite fields having characteristic 2. In van der Geer-van der Vlugt [6], Blache [2] and Bouw et al [4], it is shown that for any prime \( p \) all curves of the form
\[ y^p - y = \sum_{i=0}^{k} a_{p^i+1} x^{p^i+1} \]
are supersingular over finite fields having characteristic \( p \). In this paper we will generalize these results and prove the following theorem:

**Theorem 3.** All curves of the form
\[ y^q - y = \sum_{i,j=0}^{k} a_{p^i+p^j} x^{p^i+p^j} \]
are supersingular, where \( a_{p^i+p^j} \in \mathbb{F}_q \).

Since \( s_p(p^i + p^j) \leq 2 \) for all \( i, j \geq 0 \), Theorem 3 follows from Theorem 1.

### 2.5 Family of Non-Supersingular Curves

In the opposite direction, Sholten and Zhu showed in [13] that there is no hyperelliptic supersingular curve of genus \( 2^k - 1 \) in characteristic 2 where \( k \geq 2 \) (previously shown by Oort for genus 3). Blache proved a similar result for all primes \( p > 2 \) in [3] and showed that there is no supersingular Artin-Schreier curve of genus \( (p-1)(d-1)/2 \) in characteristic \( p \) where \( n(p-1) > 2 \) and \( d = i(p^m - 1) \), \( 1 \leq i \leq p-1 \). We will generalize this result, and prove the following using the same techniques as we use to prove Theorem 1.

**Theorem 4.** Let \( d = i(p^n - 1) \) with \( n \geq 1 \) and \( 1 \leq i \leq p-1 \) and \( n(p-1) > 2 \). Then
\[ y^{p^n} - y = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 \]
is not supersingular for any \( u \geq 1 \).

Putting \( u = 1 \) recovers the result of Blache. The curves in Theorem 4 have genus \( (p^n - 1)(d-1)/2 \), assuming \( (p, d) = 1 \).

### 2.6 Other Connections

We remark that generalized Artin-Schreier curves have come up (see [1]) in the completely different problem of studying irreducible polynomials over finite fields with certain coefficients fixed. A key part of the proof in [1] is to calculate the L-polynomials of three specific generalized Artin-Schreier curves.
3 Sharp Slope Estimate for Arbitrary Curves

This section states a little background for the slope estimates of curves over finite fields. Note that Theorem 5 and Lemma 6 hold valid when the base field is perfect of characteristic $p$.

Let $W$ be the Witt vectors over $\mathbb{F}_Q$, and $\sigma$ the absolute Frobenius automorphism of $W$. Throughout this paper we assume that $X/\mathbb{F}_Q$ is a curve of genus $g$ with a rational point. Suppose there is a smooth proper lifting $X/W$ of $X$ to $W$, together with a lifted rational point $P$. The Frobenius endomorphism $F$ (resp., Verschiebung endomorphism $V$) are $\sigma$ (resp., $\sigma^{-1}$) linear maps on the first crystalline cohomology $H^1_{\text{cr}}(X/W)$ of $X$ with $VF = FV = p$. It is know that $H^1_{\text{cr}}(X/W)$ is canonically isomorphic to the first de Rham cohomology $H^1_{\text{dR}}(X/W)$ of $X$, one gets induced $F$ and $V$ actions on $H^1_{\text{dR}}(X/W)$. Let $L$ be the image of $H^0(X, \Omega^1_{X/W})$ in $H^1_{\text{dR}}(X/W)$.

**Theorem 5.** Let $\lambda$ be a rational number with $0 \leq \lambda \leq 1/2$. Then $\text{NP}_1(X/\mathbb{F}_Q) \geq \lambda$ if and only if $p^n | V^{n+g-1}L$ for all integer $n \geq 1$.

Let $\hat{X}/W$ be formal completion of $X/W$ at rational point $P$. If $x$ is a local parameter of $P$, Then every element of $H^1_{\text{dR}}(\hat{X}/W)$ can be represented as $h(x) \frac{dx}{x}$ for some $h(x) \in xW[[x]]$, and $F$ and $V$ acts as follows:

$$F \left( h(x) \frac{dx}{x} \right) = ph^\sigma(x^p) \frac{dx}{x} \quad V \left( h(x) \frac{dx}{x} \right) = ph^{\sigma^{-1}}(x^{1/p}) \frac{dx}{x}$$

where $x^{m/p} = 0$ if $p \nmid m$.

Denote the restriction map $H^1_{\text{dR}}(\hat{X}/W) \rightarrow H^1_{\text{dR}}(X/W)$ by $\text{res}$.

**Lemma 6.** The $F$ and $V$ action on $H^1_{\text{dR}}(X/W)$ and $H^1_{\text{dR}}(\hat{X}/W)$ commutes with the restriction map $\text{res} : H^1_{\text{dR}}(X/W) \rightarrow H^1_{\text{dR}}(\hat{X}/W)$.

Furthermore,

$$\text{res}^{-1}(H^1_{\text{dR}}(\hat{X}/W)) = F(H^1_{\text{dR}}(X/W)).$$

4 Slope Estimate of Generalized Artin-Schreier Curves

Assume that $X$ is a curve over $\mathbb{F}_Q$ defined by an affine equation $y^q - y = \tilde{f}(x)$ where $q = p^u$ and $\tilde{f}(x) = \tilde{a}_dx^d + \tilde{a}_{d-1}x^{d-1} + \ldots + \tilde{a}_1x$ and $p \nmid d$ and $\tilde{a}_d \neq 0$. Take a lifting $X/W$ defined by $y^q - y = f(x)$ where $f(x) = a_dx^d + a_{d-1}x^{d-1} + \ldots + a_1x \in W[x]$ with $a_l \equiv \tilde{a}_l \mod p$ for all $l$. So $X/W$ has a rational point at the origin with a local parameter $x$. 
For any integer \( N > 0 \) and \( 0 \leq i \leq q - 2 \) let \( C_r(i, N) \) be the \( x^r \) coefficient of the power expansion of the function \( y^i(qy^{q-1} - 1)^{pN-1} \) at the origin \( P \):

\[
y^i(qy^{q-1} - 1)^{pN-1} = \sum_{r=0}^{\infty} C_r(i, N)x^r.
\]

**Lemma 7.** The curve \( X/W \) has genus \((q - 1)(d - 1)/2 \) and for \( q - 2 \geq i \geq 0 \), \( j \geq 1 \) and \( di + qj \leq (q - 1)(d - 1) - 2 + q \) the differential forms

\[
\omega_{ij} := x^j y^i(qy^{q-1} - 1)^{-1} \frac{dx}{x}
\]

form a basis for \( N \).

**Proof.** The proof of Lemma 3.1 in [11] stated for primes \( p \) but is also valid for prime powers \( q \). \( \Box \)

**Lemma 8.** For \( m \) be a positive integer. If \( p \nmid m \) then \( x^m(qy^{q-1} - 1)^{-1} \frac{dx}{x} \equiv 0 \mod q \) in \( H^1_{dR}(\hat{X}/W) \).

**Proof.** If \( p \nmid m \), then

\[
x^m(qy^{q-1} - 1)^{-1} \frac{dx}{x} \equiv -x^m \frac{dx}{x} \equiv -d \left( \frac{x^m}{m} \right) \mod q
\]

which is cohomologically zero in \( H^1_{dR}(\hat{X}/W) \). \( \Box \)

**Lemma 9.** For all nonnegative integer \( a \) and \( r \) we have

\[
C_r(i, N + a) \equiv C_r(i, N) \mod p^{N+1}.
\]

**Proof.** We have \( \binom{p^N}{l} \equiv 0 \mod p^{N+1-l} \) if \( N + 1 \geq l \geq 1 \). Thus

\[
(1 - qy^{q-1})^{pN} = \sum_{l=0}^{pN} \binom{pN}{l} (-qy^{q-1})^l \equiv 1 \mod p^{N+1}.
\]

Therefore we have

\[
y^i(qy^{q-1} - 1)^{pN+a-1} = y^i(qy^{q-1} - 1)^{pN-1}(1 - qy^{q-1})^{pN}(p^a-1) \equiv y^i(qy^{q-1} - 1)^{pN-1} \mod p^{N+1}.
\]

\( \Box \)

**Theorem 10.** Let \( \lambda \) be a rational number with \( 0 \leq \lambda \leq 1/2 \). Suppose there exists an integer \( n_0 \) such that

(i) for all \( i, j \) within the range \( 0 \leq i \leq q - 2 \), \( j \geq 1 \) and \( di + pj \leq (q - 1)(d - 1) - 2 + q \) and for all \( m \geq 1 \), \( 1 \leq n < n_0 \), we have

\[
\text{ord}_p(C_{m^{n+g-1-j}}(i, n + g - 2)) \geq \lfloor n \lambda \rfloor;
\]

(ii) for all \( m \geq 2 \) we have

\[
\text{ord}_p(C_{m^{n_0+g-1-j}}(i, n + g - 2)) \geq \lfloor n_0 \lambda \rfloor.
\]
Then

\[
\begin{cases}
{p^{[n \lambda]} \mid V^{n+g-1}(\omega_{ij})} & \text{if } n < n_0 \\
{p^{[n_0 \lambda]-1} \mid V^{n_0+g-1}(\omega_{ij})} & \text{if } n = n_0.
\end{cases}
\]

Furthermore, we have

\[V^{n_0+g-1}(\omega_{ij}) \equiv C_{p^{n_0+g-1-j}}^{\sigma^{-(n_0+g-1)}}(i, n_0 + g - 2)(\omega_{0,1}) \mod [n_0 \lambda].\]

Proof. We will prove by induction. Suppose \(n \geq 1\) and

\[p^{[n-1 \lambda]} \mid V^{n+g-2}(\omega_{ij}).\] (4)

Note this is trivially true if \(n = 1\).

Write \(h(x) = (qy^g - 1)^{-1} \in W[[x]].\) By ([10], Lemma 2.2), we have

\[h(x)^{n+g-2} = h^{n^{n+g-2}}(x^{n+g-2}) + ph_1^{n^{n+g-3}}(x^{n+g-3}) + \ldots + p^{n+g-2}h_{n+g-2}(x)\]

for some power series \(h_1(x), h_2(x), \ldots, h_{n+g-2}(x) \in W[[x]].\) Thus the power series expansion of \(\omega_{ij}\) is

\[
\text{res}(\omega_{ij}) = \text{res} \left( x^j y^i (qy^g - 1)^{-1} \frac{dx}{x} \right)
\]

\[= \text{res} \left( x^j y^i (qy^g - 1)^{n+g-2} - h(x)^{n+g-2} \frac{dx}{x} \right)
\]

\[= \sum_{r=0}^{\infty} C_r(i, n + g - 2)x^{r+j}h^{n+g-2}(x^{n+g-2}) \frac{dx}{x}
\]

\[+ p \sum_{r=0}^{\infty} C_r(i, n + g - 2)x^{r+j}h_1^{n+g-3}(x^{n+g-3}) \frac{dx}{x}
\]

\[+ \ldots
\]

\[+ p^{n+g-2} \sum_{r=0}^{\infty} C_r(i, n + g - 2)x^{r+j}h_{n+g-2}(x) \frac{dx}{x}.
\]

Apply \(V^{n+g-2}\) to the first differential form above. Since \(V\) action commutes with the restriction map (by Lemma [6]), we have

\[
\text{res}(V^{n+g-2}\omega_{ij}) = \sum_{m=1}^{\infty} C_{m^{n+g-2-j}}^{\sigma^{-(n+g-2)}}(i, n + g - 2)x^m h(x) \frac{dx}{x}
\]

\[+ p \sum_{m=1}^{\infty} C_{m^{n+g-3-j}}^{\sigma^{-(n+g-2)}}(i, n + g - 2)V \left( x^m h_1(x) \frac{dx}{x} \right)
\]

\[+ p^2 \sum_{m=1}^{\infty} C_{m^{n+g-4-j}}^{\sigma^{-(n+g-2)}}(i, n + g - 2)V \left( x^m h_2(x) \frac{dx}{x} \right)
\]

\[+ \ldots
\]

\[+ p^{[n \lambda]-1} \sum_{m=1}^{\infty} C_{m^{n+g-1-j}}^{\sigma^{-(n+g-2)}}(i, n + g - 2)V^{[n \lambda]-1} \left( x^m h_{[n \lambda]-1}(x) \frac{dx}{x} \right)
\]

\[+ p^{[n \lambda]} \beta
\]
for some \( \beta \in H^1_{dR}(\hat{X}/W) \).

By the hypothesis, \( p^{[n\lambda]-1} \) divides \( C_{mp^{n+g-2-j}}(i, n + g - 3) \). For all \( m \geq 1 \), by Lemma \( 9 \)

\[ p^{[n\lambda]-1} \mid C_{mp^{n+g-2-j}}(i, n + g - 2). \]

(6)

For \( m \) coprime to \( p \) it follows from Lemma \( 8 \) that \( p \) divides \( x^m h(x) \frac{dx}{x} \). Thus

\[ p^{[n\lambda]} \mid C_{mp^{n+g-2-j}}(i, n + g - 2)x^m h(x) \frac{dx}{x}. \]

Otherwise, except possibly when \( n = n_0 \) and \( m = p \), we have

\[ p^{[n\lambda]} \mid C_{(mp^n)p^{n-1-j}}(i, n + g - 2)x^m h(x) \frac{dx}{x}. \]

Therefore,

\[ \sum_{m=1}^{\infty} C_{mp^{n+g-2-j}}(i, n + g - 2)x^m h(x) \frac{dx}{x} \]

(7)

\[ \equiv \sum_{m'=1}^{\infty} C_{mp^{n+g-2-j}}(i, n + g - 2)x^{m'} h(x) \frac{dx}{x} \]

\[ \equiv \begin{cases} 0 \mod p^{[n\lambda]} & \text{if } n < n_0 \\ C_{mp_0^{n+g-2-j}}(i, n + g - 2)x^p h(x) \frac{dx}{x} \mod p^{[n\lambda]} & \text{if } n = n_0. \end{cases} \]

For all integers \( l \geq 1 \), by the hypothesis of the theorem, we obtain

\[ \text{ord}_p(C_{mp^l} - i - g - l - 3) \geq \lceil (n - 1 - l) \lambda \rceil \geq \lceil n\lambda \rceil - l. \]

So by Lemma \( 9 \) we have \( \text{ord}_p(C_{mp^l} - i - g - 2) \geq \lceil n\lambda \rceil - l \). So \( p^{[n\lambda]} \) divides every sum of \( (5) \) except possibly one on the first line. Combining this information with \( (4), (6) \) and \( (7) \) yields for all \( n < n_0 \)

\[ \text{res} \left( \frac{V^{n+g-2} \omega_{ij}}{p^{[n\lambda]-1}} \right) \in pH^1_{dR}(\hat{X}/W). \]

Hence for such \( n \) Lemma \( 6 \) implies

\[ \frac{V^{n+g-2} \omega_{ij}}{p^{[n\lambda]-1}} \in F(H^1_{dR}(X/W)) \]

so

\[ \frac{V^{n+g-1} \omega_{ij}}{p^{[n\lambda]-1}} \in VF(H^1_{dR}(X/W)) = pH^1_{dR}(X/W) \]

which proves the induction hypothesis.

If \( n = n_0 \) then the above implies that

\[ \text{res} \left( \frac{V^{n_0+g-2} \omega_{ij}}{p^{[n_0\lambda]-1}} \right) - \frac{1}{p^{[n_0\lambda]-1}} C_{p^{n_0+g-1-j}}(i, n + g - 2)x^p h(x) \frac{dx}{x} \]
lies in $pH^1_{dR}(\bar{X}/W)$. Lemma 6 implies

$$\frac{V^{n_0+g-2} \omega_{ij}}{p^{\lceil n_0 \lambda \rceil - 1}} C^\sigma_{p^{n_0+g-1-j}}(i, n + g - 2)x^p \omega_{ij}$$

lies in $F(H^1_{dR}(X/W))$. Hence

$$\frac{V^{n_0+g-1} \omega_{ij}}{p^{\lceil n_0 \lambda \rceil - 1}} C^\sigma_{p^{n_0+g-1-j}}(i, n + g - 2)x^p V(\omega_{ij})$$

lies in $VF(H^1_{dR}(X/W)) = p(H^1_{dR}(X/W))$. \hfill \Box

The next Lemma will be referred to as the Key Lemma.

**Lemma 11.** Let $\lambda$ be a rational number with $0 \leq \lambda \leq \frac{1}{2}$.

(i) if for all $i, j$ within range and for all $m \geq 1$, $n \geq 1$ we have

$$\text{ord}_p \left( C_{mp^{n_0+g-1-j}}(i, n + g - 2) \right) \geq \lceil n \lambda \rceil$$

then

$$NP_1(X/FQ) \geq \lambda.$$  

(ii) Let $i, j$ be within range.

(a) Let $n_0 \geq 1$. Suppose that and for all $m \geq 1$, $1 \leq n < n_0$ we have

$$\text{ord}_p \left( C_{mp^{n_0+g-1-j}}(i, n + g - 2) \right) \geq \lceil n \lambda \rceil;$$

(b) suppose that for all $m \geq 2$ we have

$$\text{ord}_p \left( C_{mp^{n_0+g-1-j}}(i, n + g - 2) \right) \geq \lceil n_0 \lambda \rceil;$$

(c) suppose

$$\text{ord}_p \left( C_{p^{n_0+g-1-j}}(i, n + g - 2) \right) < \lceil n_0 \lambda \rceil;$$

then

$$NP_1(X/FQ) < \lambda.$$  

**Proof.** (i) The hypothesis in Theorem 10 are satisfied for all positive integers $n_0$ and for all possible $i, j$. Thus the statement follows from Theorem 5.

(ii) If $NP_1(X/FQ) \geq \lambda$ then $p^{\lceil n_0 \lambda \rceil} | V^{n_0+g-1}(\omega_{ij})$ for all $i, j$ in the range of Theorem 7 by Theorem 5. This implies that for the particular $i, j$ satisfying the hypothesis of Theorem 10 we have

$$\text{ord} \left( C_{p^{n_0+g-1-j}}(i, n + g - 2) \right) < \lceil n_0 \lambda \rceil.$$

This proves the Lemma. \hfill \Box

We remark that if there is an decreasing sequence $\lambda_i$ whose limit is $\lambda$, and all members $\lambda_i$ satisfy the Key Lemma Part 2, and if $\lambda$ satisfies the Key Lemma Part 1, then $NP_1(X/FQ) = \lambda$. We will use this in the proof of Theorem 4.

11
5 \ p\text{-}adic Behavior Coefficients of Power Series

Lemma 12. Let $a > 0$ and let $y \in W[[z]]$ be a power series that satisfies $y^a - y = z$ and $y(0) = 0$. Then

$$y^a = \sum_{k_1=0}^{\infty} D_{k_1}(a)z^{k_1}$$

where $D_{k_1}(a) = 0$ if $k_1 \not\equiv 0 \mod q - 1$; otherwise,

$$D_{k_1}(a) = (-1)^a \frac{k_1 - a}{q - 1} a \left(\frac{k_1 + k_1 - a - 1}{k_1}\right)! \frac{k_1}{q - 1}.$$ 

Proof. The proof of Lemma 4.1 in [11] stated for primes $p$ but is also valid for prime powers $q$. \hfill \square

Lemma 13. Let $a > 0$ and $k_1 \equiv a \mod q - 1$, write $a = i + l(q - 1)$ with integers $l$ and $1 \leq i \leq q - 1$, then

$$\begin{cases} 
\text{ord}_p(D_{k_1}(a)) = \frac{s_p(k_1) - s_p(i - 1) - 1}{p - 1} & \text{if } l = 0 \\
\text{ord}_p(D_{k_1}(a)) \geq \frac{s_p(k_1) - s_p(i - 1) - 1}{p - 1} - (l - 1)u & \text{if } l \geq 1.
\end{cases}$$

Proof. $k_1 \equiv a \mod q - 1$. Using the identity $(p - 1)\text{ord}_p(k!) = k - s_p(k)$ for all positive integers $k$ we have

$$\text{ord}_p(D_{k_1}(a)) = \text{ord}_p(a) + \frac{1}{p - 1}\left(s_p(k_1) + s_p\left(\frac{k_1 - a}{q - 1}\right) - 1 - s_p\left(1 + a + \frac{k_1 - a}{q - 1}\right)\right).$$

If $l = 0$, then (note that $a = i$)

$$s_p\left(a - 1 + \frac{k_1 - a}{q - 1}\right) = s_p(a - 1) + s_p\left(\frac{k_1 - a}{q - 1}\right).$$

If $l = 1$, then

$$s_p\left(a - 1 + \frac{k_1 - a}{q - 1}\right) \leq s_p(a - 1) + s_p\left(\frac{k_1 - a}{q - 1}\right)$$

$$= (p - 1)\text{ord}_p(a) + (1 + s_p(i - 1) - 1 + s_p\left(\frac{k_1 - a}{q - 1}\right))$$

$$= (p - 1)\text{ord}_p(a) + s_p(i - 1) + s_p\left(\frac{k_1 - a}{q - 1}\right).$$

If $l > 1$, then

$$s_p\left(a - 1 + \frac{k_1 - a}{q - 1}\right) = s_p\left(i - 1 + l(q - 1) + \frac{k_1 - a}{q - 1}\right)$$

$$\leq s_p(i - 1) + s_p(l(q - 1)) + s_p\left(\frac{k_1 - a}{q - 1}\right)$$

$$\leq s_p(i - 1) + (l - 1)(p - 1)u + s_p\left(\frac{k_1 - a}{q - 1}\right).$$

\hfill \square
Fix two integers \( N > 0 \) and \( 0 \leq i \leq q - 1 \). Let \( y \in W[[z]] \) be a power series that satisfies \( y^q - y = z \) and \( y(0) = 0 \). Define coefficients \( E_{k_1}(i, N) \) by

\[
y^i(qy^{q-1} - 1)^{pN-1} = \sum_{k_1=0}^{\infty} E_{k_1}(i, N)z^{k_1}.
\]

Let \( z = f(x) = a_1x + a_2x^2 + \cdots + a_dx^d \). For ease of formulation, set \( 0^0 := 1 \). Then

\[
\sum_{m=0}^{\infty} E_m(i, N)f(x)^m = \sum_{m=0}^{\infty} E_m(i, N)\left(a_1x + a_2x^2 + \cdots + a_dx^d\right)^m
\]

\[
= \sum_{m=0}^{\infty} E_m(i, N) \sum_{m_1, m_2, \cdots, m_d \geq 0 \atop m_1 + m_2 + \cdots + m_d = m} \left(m_1, m_2, \cdots, m_d\right) \prod_{l=1}^{d} \left(a_l x^l\right)^{m_l}.
\]

In order to find the coefficient of \( x^r \) of \( \sum_{m=0}^{\infty} E_m(i, N)f(x)^m \), we have to find all \( m_i \)'s such that

\[
\sum_{l=0}^{d} lm_i = r.
\]

Write

\[
m_i = k_i - k_{i+1} \text{ for } i = 1, 2, \cdots, d - 1 \text{ and } m_d = k_d.
\]

Since \( m_i \geq 0 \) for each \( i = 1, 2, \cdots, d \), there is a one-to-one correspondence between

\[
(m_1, m_2, \cdots, m_d) \text{ such that } m_1 + m_2 + \cdots + m_d = m
\]

and

\[
(k_1, k_2, \cdots, k_d) \text{ such that } k_1 \geq k_2 \geq \cdots \geq k_d \geq 0 \text{ and } k_1 + k_2 + \cdots + k_d = r.
\]

Moreover, we have

\[
m = \sum_{i=0}^{d} m_i = \sum_{j=0}^{d} (k_j - k_{j+1}) = k_1
\]

and

\[
\left(m_1, m_2, \cdots, m_d\right) = \left(k_1 - k_2, k_2 - k_3, \cdots, k_{d-1} - k_d, k_d\right) = \prod_{l=1}^{d-1} \left(\frac{k_l}{k_{l+1}}\right).
\]

For integers \( r \geq 0 \) let \( K_r \) denote the set of transposes \( k = ^t(k_1, k_2, \ldots, k_d) \) of \( d \)-tuple integers with \( k_1 \geq k_2 \geq \cdots \geq k_d \geq 0 \) and \( \sum_{i=1}^{d} k_l = r \). Moreover define \( k_{d+1} = 0 \).

Hence the \( x^r \) of \( \sum_{m=0}^{\infty} E_m(i, N)f(x)^m \) is

\[
\sum_{k \in K_r} E_{k_1}(i, N) \prod_{l=1}^{d} \left(\frac{k_l}{k_{l+1}}\right) a_i^{k_2 - k_{l+1}}.
\]
Since
\[ \sum_{m=0}^{\infty} C_r(i, N)x^r = \sum_{m=0}^{\infty} E_m(i, N)f(x)^m, \]
we have
\[ C_r(i, N) = \sum_{k \in K_r} E_{k_1}(i, N) \prod_{l=1}^{d} \left( \frac{k_l}{k_{l+1}} \right) a_l^{k_l-k_{l+1}}. \]

We define
\[ s_p(k) = s_p(k_1 - k_2) + s_p(k_2 - k_3) + \ldots + s_p(k_d - k_d) + s_p(d). \]
where \( k = t(k_1, k_2, \ldots, k_d) \in K_r \) for some \( r > 0 \).

**Lemma 14.** Let \( k = t(k_1, k_2, \ldots, k_d) \in K_r \). If \( k_1 \not\equiv 0 \mod q-1 \) then \( E_{k_1}(i, N) = 0 \). If \( k_1 \equiv \mod q-1 \) then (define \( s(-1) := -1 \))
\[ \text{ord}_p(E_{k_1}(i, N)) = \frac{s_p(k_1) - s_p(i - 1) - 1}{p - 1}, \]
\[ \text{ord}_p\left( E_{k_1}(i, N) \prod_{l=1}^{d-1} \left( \frac{k_l}{k_{l+1}} \right) \right) = \frac{s_p(k) - s_p(i - 1) - 1}{p - 1}. \]

**Proof.** Take the identity
\[ y^j(qy^{q-1} - 1)^{p^N-1} = \sum_{l=0}^{p^{N-1}} (-1)^{p^n-1-l} \binom{p^N-1}{l} y^{j+l(q-1)}. \]
Substituting the power series expansion of \( y^{j+l(q-1)} \) above, we get
\[ E_{k_1}(i, N) = \sum_{l=0}^{p^N-1} (-1)^{p^n-1-l} \binom{p^N-1}{l} D_{k_1}(i + l(q-1))p^{ul}. \]

If \( k_1 \not\equiv 0 \mod q-1 \), then \( D_{k_1}(i + l(q-1)) = 0 \) by Lemma 13 hence \( E_{k_1}(i, N) = 0 \).
If \( k_1 = i = 0 \), then \( E_{k_1}(i, N) = (-1)^{p^{N-1}} \), hence \( \text{ord}_p(E_{k_1}(i, N)) = 0 \).
If \( i = 0 \) and \( k_1 > 0 \) and \( k_1 \equiv \mod q-1 \), by Lemma 13 the term of minimal valuation occurs at \( l = 1 \), we have
\[ \text{ord}_p(E_{k_1}(i, N)) = u + \text{ord}_p(D_{k_1}(p-1)) = u + \frac{s_p(k_1) - u(p-1)}{p-1} = \frac{s_p(k_1)}{p-1}. \]
If \( i > 0 \) and \( k_1 \equiv \mod q-1 \), by Lemma 13 the term of minimal valuation occurs at \( l = 0 \), we have
\[ \text{ord}_p(E_{k_1}(i, N)) = u + \text{ord}_p(D_{k_1}(i)) = \frac{s_p(k_1) - s_p(i - 1) - 1}{p-1}. \]
Moreover,
\[ \text{ord}_p\left( \prod_{l=1}^{d-1} \left( \frac{k_l}{k_{l+1}} \right) \right) = \sum_{l=1}^{d-1} \text{ord}_p\left( \left( \frac{k_l}{k_{l+1}} \right) \right) = \sum_{l=1}^{d-1} \frac{s_p(k_l) - s_p(k_{l+1}) + s_p(k_l - k_{l+1})}{p-1} = \frac{s_p(k) - s_p(k_1)}{p-1}. \]
6   p-adic Boxes and r-tiling Sequences

Let $k = \mathcal{t}(k_1, k_2, ..., k_d) \in \mathbb{K}_r$. We define integers $k_{l,v}$ as follows: For $l = d$ we let $k_d = \sum_{v \geq 0}k_{d,v}p^v$ be the $p$-ary expansion of $k_d$. For $1 \leq l \leq d$ we define $k_{l,v}$ inductively by

$$k_{l,v} := k_{l+1,v} + p^v - \text{coefficient in the } p\text{-ary expansion of } (k_l - k_{l+1}),$$

for all $v \geq 0$. We call the representation $\mathcal{t}(k_1, k_2, ..., k_d)$ the $p$-adic box of $k$, denoted by $\boxed{k}$ for short:

$$\boxed{k} = \begin{bmatrix} \cdots & k_{1,2} & k_{1,1} & k_{1,0} \\ \cdots & k_{2,2} & k_{2,1} & k_{2,0} \\ & \vdots & & \\ \cdots & k_{d,2} & k_{d,1} & k_{d,0} \end{bmatrix}.$$

Let $S$ be a finite set of positive integers. For any positive integers $r$, an $r$-tiling sequence (of length $v$) is a sequence of integer 3-tuples $\{[a_i, b_i, l_i]\}_{i=1}^v$ such that

1) $l_i \in S, 0 \leq b_i \leq b_{i+1}, 1 \leq a_i \leq p - 1$;
2) $l_i > l_{i+1}$ if $b_i = b_{i+1}$;
3) $\sum_{i=1}^va_i l_i p^{b_i} = r$.

If no such sequence exists we set $\tilde{s}_p(r, S) := \infty$; otherwise, define $\tilde{s}_p(r, S)$ the length of the shortest $r$-tiling sequence to be $\sum a_i$. Let $\tilde{K}(r, S)$ denote set of all shortest $r$-tiling sequences.

**Lemma 15.** For any positive integer $r$ and a finite set $S$ of positive integers,

1. if $k \in \mathbb{K}_r$ with $k_l = k_{l+1}$ for all $l \notin S$, then $s_p(k) \geq \tilde{s}_p(r, S)$.
2. there is a bijection between the set $\tilde{K}(r, S)$ and the set 

$$\{k \in \mathbb{K}_r | s_p(k) = \tilde{s}_p(r, S) \text{ and } k_l = k_{l+1} \text{ for all } l \notin S\}.$$

**Proof.** We shall define the maps first. An $r$-tiling sequence $\{[a_i, b_i, l_i]\}_{i=1}^{\tilde{s}_p(r, S)} \in \tilde{K}(r, S)$ is sent to the element $k \in \mathbb{K}$ whose $p$-adic box $\boxed{k}$ has $k_{l,v} = \sum_{i \in U} a_i$ where $U = \{ j | v = b_j \text{ and } l \leq l_j \}$. Given $k \in \mathbb{K}$ with $k_l = k_{l+1}$ for all $l \notin S$, one defines $\{[a_i, b_i, l_i]\}_{i=1}^{s_p(k)}$ as follows: Given $b$ let $l$ be largest value such that $k_{l,b} = a$ is nonzero. Then we get a 3-tuple $[a, b, l]$. Subtract $a$ from each component $k_{l',b}$ with $1 \leq l' \leq l$, then apply the same procedure if there is a nonzero element. Note that: $l$ is in $S$ by definition, since it only change when $l \in S$; and $a \in \{1, ..., p - 1\}$ since $a$ is $p^{l'-1}$-th coefficient in the "base $p$" expansion of $(k_l - k_{l+1})$.

These the maps are well-defined and one-to-one. Since the sets are finite, the maps are bijective. \qed

15
7 Proof of Theorem 1

Recall

\[ C_r(i, N) = \sum_{k \in K_r} E_{k_l}(i, N) \prod_{l=1}^{d-1} \left( \frac{k_l}{k_{l+1}} \right)^{d-1} a_{k_{l+1}}^{k_{l+1}}. \]

Note that \( \prod_{l=1}^{d-1} a_{k_{l+1}}^{k_{l+1}} = 0 \) if \( k_l > k_{l+1} \) for some \( l \not\in s(X) \) and if \( k_l = k_{l+1} \) for all \( l \not\in s(X) \) then \( s_p(k) \geq \tilde{s}_p(r, s(X)) \) where \( k \in K_r \) by Lemma 15 Part 1. Therefore, for \( r \) in \( \{ mp^{n+g-1} - j | m, n \geq 1, j \text{ within range} \} \), we have

\[ \text{ord}_p(C_r(i, N)) \geq \frac{\tilde{s}_p(r, s(X)) - s_p(i - 1) - 1}{p - 1}. \]

Moreover, for \( r = mp^{n+g-1} - j \) consider any \( r \)-tiling sequence given by \( mp^{n+g-1} - j = \sum_{i=0}^v a_i l_i p^{b_i} \), then we have

\[ \sigma \tilde{s}_p(r, s(X)) = \sum_{i=0}^v \sigma a_i \geq \sum_{i=0}^v s_p(a_i l_i) = \sum_{i=0}^v s_p(a_i l_i p^{b_i}) \geq s_p(\sum_{i=0}^v a_i l_i p^{b_i}) = s_p(r). \]

Let \( p \) be an odd prime and \( d > 2 \) be a positive integer. Note that the case \( d = 2 \) is easy, so we can restrict it as \( d > 2 \). We have \( 0 \leq i \leq p - 2 \) and \( 1 \leq j < d(p - 1) - 1 \). Therefore,

\[ \tilde{s}_p(r, X) \geq \frac{1}{\sigma} [(p - 1) (n + g - 1 - \sigma) + 1] \]

and hence

\[ C_r(i, N) \geq \frac{\tilde{s}_p(r, X) - s_p(i)}{p - 1} \geq \frac{1}{\sigma} \left( (p - 1) (n + g - 1 - \sigma) + 1 \right) - (p - 2) \]

\[ = \frac{n}{\sigma} + \frac{g + 2 - p - \sigma}{p - 1} \geq \frac{n}{\sigma}. \]

Let \( q = p^u \) be a prime power with \( p \) prime, \( u \geq 2 \) integer and \( d \) positive integer. We have \( 0 \leq i \leq p^u - 2 \) and \( 1 \leq j < d(q - 1) - 1 \). Therefore,

\[ \tilde{s}_p(r, X) \geq \frac{1}{\sigma} (p - 1) (n + g - 1 - \sigma) \]

and hence

\[ C_r(i, N) \geq \frac{\tilde{s}_p(r, X) - s_p(i - 1) - 1}{p - 1} \geq \frac{1}{\sigma} (p - 1) (n + g - 1 - \sigma) - u(p - 1) \]

\[ = \frac{n}{\sigma} + \frac{g - 1 - \sigma - u}{p - 1} \geq \frac{n}{\sigma}. \]
except for \((q, d) \neq (4, 3)\). This easy case is also fine when we specially optimize the upper bounds of \(s_p(i)\) and \(s_p(j)\). We omit the details.

\[\begin{align*}
8 & \text{ Proof of Theorem 4} \\
\end{align*}\]

In this section, we will prove Lemma 16 and Lemma 17 and then prove Theorem 4. Let \(d = j(p^h - 1)\) with \(h \geq 1\) and \(1 \leq j \leq p - 1\).

**Lemma 16.** Let \(k \in K_r\) with \(r \geq 1\).

1. We have \(s_p(k) \geq \left\lfloor \frac{s_p(r)}{h(p-1)} \right\rfloor\).
2. If \(s_p(k) = \left\lfloor \frac{s_p(r)}{h(p-1)} \right\rfloor\) then
   \[\begin{align*}
   & (a) \text{ the } p\text{-adic boxes } k \text{ consists of only 0 or 1; or 2 when } \frac{p^2-1}{2} \leq d < p^2 - 1. \\
   & (b) \text{ for every } v \geq 0, s_p(\sum_{l=1}^{d} k_{1,v}) = k_{1,v}h(p-1). \\
   & (c) \text{ For any } r = j(p^h - 1) \text{ with } 1 \leq j \leq p - 1 \text{ and } h \geq 1, \text{ the } p\text{-adic boxes } k \text{ consists of only 0 or 1.}
   \end{align*}\]

**Proof.** Let \(k\) be a nonnegative integer and note that \(d \geq p - 1\). Then we have

\[
\begin{align*}
|\log_p(kd + 1)| &\leq |\log_p(kd + d)| \\
&= |\log_p(k(d + 1))| \\
&= |\log_p k + \log_p(d + 1)| \\
&\leq |(k - 1) + \log_p(d + 1)| \\
&= (k - 1) + |\log_p(d + 1)| \\
&\leq (k - 1)|\log_p(d + 1)| + |\log_p(d + 1)| \\
&\leq k|\log_p(d + 1)|.
\end{align*}
\]

Therefore, for any nonnegative integer \(k\) and any degree \(d\) greater than \(p - 2\) the inequality

\[|\log_p(kd + 1)| \leq k|\log_p(d + 1)|\]

holds and it is obvious that equality holds for \(k = 0\) or \(k = 1\).

Now assume the equality holds, the above system tells us \(|\log_p(d + 1)|\) must equal to 1. The equation \(|\log_p(d + 1)| = 1\) holds if and only if \(p - 1 \leq d < p^2 - 1\). Moreover, if \(p - 1 \leq d < p^2 - 1\) and \(|\log_p(kd + 1)| = k\), we have

\[
p - 1 \leq d < p^2 - 1 \implies kp - (k - 1) \leq kd + 1 < kp^2 - (k - 1) \\
\implies p^k < kp^2 - (k + 1).
\]
The last inequality holds only for \( k \leq 2 \). Now assume \( k = 2 \). Then
\[
p \leq d + 1 < p^2 \leq 2d + 1 < p^3
\]
\[
\implies \frac{p^2 - 1}{2} \leq d < p^2 - 1.
\]
Since \( r = \sum_{v \geq 0} \sum_{l=1}^{d} k_{l,v}p^v \), we have
\[
s_p(r) = s_p \left( \sum_{v \geq 0} \sum_{l=1}^{d} k_{l,v}p^v \right)
\]
\[
= \sum_{v \geq 0} s_p \left( \sum_{l=1}^{d} k_{l,v}p^v \right)
\]
\[
\leq \sum_{v \geq 0} s_p \left( \sum_{l=1}^{d} k_{l,v} \right)
\]
\[
\leq \sum_{v \geq 0} (p - 1) \left\lfloor \log_p \left( \sum_{l=1}^{d} k_{l,v} + 1 \right) \right\rfloor
\]
\[
\leq (p - 1) \sum_{v \geq 0} \left\lfloor \log_p(k_{1,v}d + 1) \right\rfloor
\]
\[
\leq (p - 1) \left( \sum_{v \geq 0} k_{1,v} \left\lfloor \log_p(d + 1) \right\rfloor \right)
\]
\[
= \left\lfloor \log_p(d + 1) \right\rfloor (p - 1) \sum_{v \geq 0} k_{1,v}
\]
\[
= h(p - 1)s_p(k).
\]
Thus we have \( s_p(k) \geq \left\lfloor \frac{s_p(r)}{h(p - 1)} \right\rfloor \). This proves the first assertion.

Suppose above equality holds then \( k_{1,v} = 0 \) or 2 when \( \frac{p^2 - 1}{2} \leq d < p^2 - 1 \). Since \( k_{l,v} \geq k_{l+1,v} \), the first observation in the second assertion is proved.

By the arguments we used from equation (8) to equation (9), we have
\[
s_p \left( \sum_{l=1}^{d} k_{l,v} \right) = k_{1,v}(p - 1)\left\lfloor \log_p(d + 1) \right\rfloor = k_{1,v}h(p - 1).\]
This proves the second observation in the second assertion.

Let \( d \leq (p - 1)^2 \). Then \( 2d \leq 2(p - 1)^2 \) but the only value \( a \leq 2d \) such that \( s_p(a) = 2(p - 1) \) can be \( p^2 - 1 \). Since \( p^2 - 1 < j(p^2 - 1) \) for all \( j \) such that \( j \in \left[ \frac{p^2 - 1}{2}, p - 1 \right] \), trivially, for any \( j(p^h - 1) \) with \( 1 \leq j \leq p - 1 \) and \( h \geq 1 \) the p-adic boxes \( K \) consists of only 0 or 1. This proves the third observation in the second assertion.

Lemma 17. Let notation be as above. \( C_j(a_{j(p^h - 1)}) \equiv p^h(a_{j(p^h - 1)}) \frac{p^h - 1}{p^h - 1} \mod p^{h+1}. \)
Proof. Let \( r_{j,b} = j(p^h - 1) \) where \( 0 \leq j \leq p - 1 \) and \( b \geq 1 \). Let \( k \in K_{r_{j,b}} \) then we have \( s_p(k) \geq \left\lceil \frac{s_p(j(p^h - 1))}{h(p-1)} \right\rceil = \left\lceil \frac{h(p-1)}{h(p-1)} \right\rceil = b \). Now suppose \( s_p(k) = b \). Let \( \gamma_k(k) \) be the sum of entries in the \( t \)-th none-zero column (from left). Recall that \( K \) has \( d \) rows. By Lemma \[16\] we know that \( K \) consists of only 0 or 1. Therefore we have \( \gamma_k(k) \leq d \). For \( d = i(p^h - 1) \) we have \( s_p(\gamma_k(k)) = h(p - 1) \) for all such \( t \). This only can happen when all the entries of the \( t \)-th column is 1. Hence we have all 0 columns or all 1 columns. Since \( j(p^h - 1) = [j(p^h - 1)](p^h(b-1) + p^h(b-2) \ldots + 1) \). The only possibility is that \( \gamma_k(k) = j(p^h - 1) \) for all such \( t \). It is clear that \( k = i(k_1, \ldots, k_d) \in K_{r_{j,b}} \) is defined by \( k_1 = \ldots = k_j(p^h - 1) = \frac{r_{j,b}}{j(p^h - 1)} \). Thus we have

\[
C_{r_{j,b}}(i, N) \equiv p^h(a_{j(p^h - 1)}) \frac{r_{j,b}}{j(p^h - 1)} \mod p^{h+1}.
\]

Proof of Theorem \[4\] From Lemma \[16\] it follows that

\[
\ord_p \left( C_{mp^n+g-1-j}(i, N) \right) \geq \frac{s_p(k) - s_p(i - 1) - 1}{p - 1} \geq \frac{s_p(k) - u(p - 1)}{p - 1}
\]

\[
\geq \left\lceil \frac{s_p(mp^n+g-1-j)}{h(p-1)} \right\rceil - s_p(i - 1) - 1
\]

\[
\geq \left\lceil \frac{(p - 1)(n + g - h) - u(p - 1)}{h(p-1)} \right\rceil - \left\lceil \frac{n + g - h - uh(p - 1)}{h(p-1)} \right\rceil
\]

\[
\geq \left\lceil \frac{n}{h(p - 1)} \right\rceil
\]

for all \( m, n \geq 1 \). By Lemma \[11\] a we have \( NP_1(X) \geq \frac{1}{n(p-1)} \).

From now on assume \( NP_1(X) > \frac{1}{n(p-1)} \). For any integer \( n > 1 \) define

\[
\lambda_n := \frac{n + g - 2 - uh(p - 1)}{h(p-1)(n - 1)}.
\]

We now apply the observation made in the remark after the Key Lemma (Lemma \[11\]). Consider \( \lambda_n \) as a function in \( n \), it is clear that \( \lambda_n \) is monotonically decreasing and converges to \( \frac{1}{h(p-1)} \) as \( n \) approaches \( \infty \). Choose \( n_0 \) such that \( \lambda_{n_0} \leq NP_1(X) \) and such that \( n_0 + g - 1 \) is a multiple of \( h(p - 1) \) and \( \frac{g-1-uh(p-1)}{h(p-1)(n_0-1)} \leq 1 \). For all \( 1 \leq n < n_0 \) we have \( \lambda_{n_0} \leq \lambda_{n+1} = \frac{n+g-1-uh(p-1)}{n(h(p-1))} \); that is,

\[
\left\lceil n\lambda_{n_0} \right\rceil \leq \left\lceil \frac{n + g - 1 - uh(p - 1)}{h(p-1)} \right\rceil
\]
Therefore, for all \( m \geq 1 \) and \( 1 \leq n < n_0 \) one has

\[
\text{ord}_p(C_{mp^n + g-1-j}(i, N)) \geq \left\lfloor \frac{n + g - 1 - uh(p-1)}{h(p-1)} \right\rfloor \geq [n\lambda_{n_0}] .
\]

On the other hand,

\[
[n_0\lambda_0] = \left\lfloor \frac{n_0 \cdot (n_0 + g - 2 - uh(p-1))}{h(p-1)(n_0 - 1)} \right\rfloor = \left\lfloor \frac{(n_0 - 1) + g - 1 - uh(p-1)}{h(p-1)} \left( 1 + \frac{1}{n_0 - 1} \right) \right\rfloor = \left\lfloor \frac{n_0 + g - 1 - uh(p-1)}{h(p-1)} + \frac{g - 1 - uh(p-1)}{h(p-1)(n_0 - 1)} \right\rfloor = \frac{n_0 + g - 1}{h(p-1)} - u + \left\lfloor \frac{g - 1 - uh(p-1)}{h(p-1)(n_0 - 1)} \right\rfloor = \frac{n_0 + g - 1}{h(p-1)} - u + 1 .
\]

Hence for all \( m \geq 2 \) one has

\[
\text{ord}_p(C_{mp^n + g-1-j}(i, N)) \geq \left\lfloor \frac{n_0 + g}{h(p-1)} - u \right\rfloor = \frac{n_0 + g - 1}{h(p-1)} - u + 1 = [n_0\lambda_{n_0}] .
\]

Thus the hypotheses of Lemma 11.b are satisfied (for \( j = 1 \) and \( \lambda = \lambda_{n_0} \) too) so we

\[
\text{ord}_p(C_j(p^{n_0 + g-1-1})(i, N) \geq [n_0\lambda_{n_0}] .
\]

for \( 1 \leq j \leq p - 1 \). We also have

\[
\text{ord}_p(C_j(p^{n_0 + g-1-1})(i, N) \equiv p^{[n_0\lambda_{n_0}] - 1}a_j(p^{n_0 + g-1-1}/(p^h-1)) \mod p^{[n_0\lambda_{n_0}]}. 
\]

Hence \( a_j(p^{n-1}) = 0 \mod p \). Thus \( c_j(p^{n-1}) = 0 \).

References

[1] O. Ahmadi, F. Gologlu, R. Granger, G. McGuire, E. S. Yilmaz, Fibre Products of Supersingular Curves and the Enumeration of Irreducible Polynomials with Prescribed Coefficients, Finite Fields and Their Applications, vol 42 (2016) 128–164.

[2] R. Blache, Valuation of exponential sums and the generic first slope for Artin-Schreier curves. Journal of Number Theory, 132:23362352, 2012.

[3] R. Blache, Valuations of exponential sums and Artin-Schreier curves, arXiv:1502.00969

[4] I. Bouw, W. Ho, B. Malmskog, R. Scheidler, P. Srinivasan, and C. Vincent, Zeta functions of a class of Artin-Schreier curves with many automorphisms, 2014.

[5] R. Cramer, C. Xing, An improvement to the Hasse-Weil bound and applications to character sums, cryptography and coding, Advances in Mathematics, Vol 309, March 2017, Pages 238-253
[6] G. van der Geer, M. van der Vlugt, Reed-Muller Codes and supersingular curves I, Compositio Mathematica, 84, No. 3 (1992) 333-367.

[7] B. Mazur, Frobenius and the Hodge filtration, Bulletin of the AMS, vol 78, No 5, Sept. 1972, 653–667.

[8] G. McGuire, An alternative proof of a result on the weight divisibility of a cyclic code using supersingular curves, Finite Fields Appl. 18 (2012) no.2, 434-436

[9] O. Moreno and C. J. Moreno, An elementary proof of a partial improvement to the Ax-Katz Theorem; Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), 257–268, Lecture Notes in Comput. Sci., 673, Springer, Berlin, 1993.

[10] N. Nygaard, On supersingular abelian varieties. Algebraic geometry (Ann Arbor, Mich., 1981), 83-101.

[11] J. Scholten, H. J. Zhu, Slope Estimates of Artin-Schreier Curves, Compositio Mathematica 137: 275–292, 2003.

[12] J. Scholten, H. J. Zhu, Families of supersingular curves in characteristic 2, Math. Research Letters 9, no 5-6, (2002) 639–650.

[13] J. Scholten, H. J. Zhu: Hyperelliptic curves in characteristic 2. Inter. Math. Research Notices. 17 (2002), 905917.